



Guide de l'utilisateur

AWS IAM Identity Center



AWS IAM Identity Center: Guide de l'utilisateur

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

Qu'est-ce que IAM Identity Center ?	1
Pourquoi utiliser IAM Identity Center ?	1
Renommer le centre d'identité IAM	3
Les anciens espaces de noms restent les mêmes	3
Prise en main	4
Conditions préalables et considérations relatives à l'IAM Identity Center	6
Choisir un Région AWS	7
Utilisation d'IAM Identity Center pour les applications uniquement	14
Rôles IAM créés par IAM Identity Center	15
IAM Identity Center et AWS Organizations	16
Instances du centre d'identité IAM	17
Compte AWS types qui peuvent activer IAM Identity Center	17
Instances organisationnelles d'IAM Identity Center	20
Instances de compte d'IAM Identity Center	21
Supprimer votre instance IAM Identity Center	26
Activer IAM Identity Center	28
Pour activer une instance d'IAM Identity Center	29
Confirmez vos sources d'identité	32
Mettre à jour les pare-feux et les passerelles	34
Considérations relatives à l'autorisation de répertoire des domaines et des points de terminaison d'URL	36
Tutoriels d'identification des sources	38
Active Directory	39
CyberArk	42
Conditions préalables	43
Considérations relatives au SCIM	43
Étape 1 : activer le provisionnement dans IAM Identity Center	44
Étape 2 : configurer le provisionnement dans CyberArk	45
(Facultatif) Étape 3 : Configuration des attributs utilisateur CyberArk pour le contrôle d'accès (ABAC) dans IAM Identity Center	46
(Facultatif) Transmission d'attributs pour le contrôle d'accès	46
Google Workspace	47
Considérations	48
Étape 1 Google Workspace : Configuration de l'application SAML	49

Étape 2 : IAM Identity Center et Google Workspace : Modification de la source d'identité IAM Identity Center et configuration en Google Workspace tant que fournisseur d'identité SAML	50
Étape 3 Google Workspace : Activez les applications	52
Étape 4 : IAM Identity Center : configurer le provisionnement automatique d'IAM Identity Center	52
Étape 5 Google Workspace : Configuration du provisionnement automatique	53
Transmission d'attributs pour le contrôle d'accès - Facultatif	55
Attribuez l'accès à Comptes AWS	55
Étapes suivantes	58
Résolution des problèmes	59
JumpCloud	60
Conditions préalables	61
Considérations relatives au SCIM	61
Étape 1 : activer le provisionnement dans IAM Identity Center	62
Étape 2 : configurer le provisionnement dans JumpCloud	63
(Facultatif) Étape 3 : Configuration des attributs utilisateur JumpCloud pour le contrôle d'accès dans IAM Identity Center	64
(Facultatif) Transmission d'attributs pour le contrôle d'accès	64
Microsoft Entra ID	65
Conditions préalables	66
Considérations	66
Étape 1 : préparer votre client Microsoft	68
Étape 2 : Préparez votre AWS compte	70
Étape 3 : configurer et tester votre connexion SAML	73
Étape 4 : configurer et tester votre synchronisation SCIM	77
Étape 5 : Configuration de l'ABAC - Facultatif	81
Attribuez l'accès à Comptes AWS	83
Microsoft Entra ID configuration pour l'accès à des régions supplémentaires	85
Résolution des problèmes	86
Okta	88
Considérations	90
Étape 1 Okta : Obtenir les métadonnées SAML de votre compte Okta	91
Étape 2 : IAM Identity Center : configurer Okta en tant que source d'identité pour IAM Identity Center	91
Étape 3 : IAM Identity Center et Okta Okta provisionnement des utilisateurs	93

Étape 4 Okta : Synchroniser les utilisateurs depuis Okta IAM Identity Center	95
Transmission d'attributs pour le contrôle d'accès - Facultatif	96
Attribuez l'accès à Comptes AWS	97
Oktaconfiguration pour l'accès à des régions supplémentaires	99
Étapes suivantes	100
Résolution des problèmes	101
OneLogin	103
Conditions préalables	104
Étape 1 : activer le provisionnement dans IAM Identity Center	105
Étape 2 : configurer le provisionnement dans OneLogin	106
(Facultatif) Étape 3 : Configuration des attributs utilisateur OneLogin pour le contrôle d'accès dans IAM Identity Center	107
(Facultatif) Transmission d'attributs pour le contrôle d'accès	108
Résolution des problèmes	108
Ping Identity	109
PingFederate	110
PingOne	118
Répertoire d'Identity Center	124
Didacticiels vidéo	131
Configuration de votre main-d'œuvre	132
Utilisateurs, groupes et provisionnement	132
Unicité du nom d'utilisateur et de l'adresse e-mail	132
Groupes	133
Provisionnement d'utilisateurs et de groupes	133
Déprovisionnement des utilisateurs et des groupes	133
Gérez votre source d'identité	134
Considérations relatives à la modification de votre source d'identité	135
Modifier la source de votre identité	141
Attributs d'utilisateur et de groupe dans IAM Identity Center	143
Fournisseurs d'identité externes	144
Microsoft ADannuaire	163
Gérer les utilisateurs dans le répertoire Identity Center	185
Provisionnement lorsque les utilisateurs se trouvent dans IAM Identity Center	186
Modification de la source de votre identité	186
Ajout d'utilisateurs	186
Ajouter des groupes	190

Ajouter des utilisateurs à des groupes	191
Supprimer des groupes	192
Suppression d'utilisateurs	193
Supprimer des utilisateurs des groupes	195
Modifier les propriétés de l'utilisateur	195
Accès à la main-d'œuvre	197
Comprendre les sessions d'authentification	197
Types de sessions d'authentification	198
Moyens de mettre fin aux sessions utilisateur	199
Qu'advient-il de l'accès utilisateur lorsque vous mettez fin à une session ?	200
Déconnexion unique	204
Bonnes pratiques pour la gestion des sessions	204
Configuration de la durée de session	205
Sessions interactives pour les utilisateurs	205
Sessions d'arrière-plan pour les utilisateurs	206
Sessions prolongées pour Kiro	208
Mettre fin aux sessions actives pour les utilisateurs du personnel	209
Considérations relatives aux sources d'identité, à la AWS CLI et AWS SDKs	210
Désactiver l'accès utilisateur	214
Refuser l'accès aux utilisateurs	216
Gestion de l'accès des utilisateurs dans le répertoire Identity Center	217
Gestion des mots de passe	217
MFA	218
Configuration des mots de passe utilisateur	218
Authentification multifacteur	222
Accès aux applications	237
AWS applications gérées	238
Contrôle de l'accès aux applications	238
Partage d'informations d'identité	239
Limiter l'utilisation des applications AWS gérées	240
Applications que vous pouvez utiliser avec IAM Identity Center	241
Configuration d'IAM Identity Center pour tester les applications AWS gérées	247
Afficher et modifier les détails de l'application	253
Désactivation d'une application AWS gérée	254
Activation de sessions de console à identité améliorée	255
Applications gérées par le client	258

Applications SAML 2.0 et OAuth 2.0	259
Configuration de l'application SAML 2.0	264
Propagation d'identité de confiance	268
Avantages d'une propagation d'identité fiable	268
Permettre une propagation d'identité fiable	269
Comment fonctionne la propagation fiable des identités	269
Prérequis et considérations	271
Cas d'utilisation	273
Services d'autorisation	300
Configuration de votre propre application OAuth 2.0	310
Configuration d'applications gérées par le client	311
Spécifier les applications fiables	315
Émetteur de jetons de confiance	317
Rotation des certificats	332
Considérations relatives à la rotation d'un certificat	333
Rotation d'un certificat IAM Identity Center	333
Indicateurs du statut d'expiration des certificats	336
Comprendre les propriétés de l'application	336
URL de démarrage de l'application	336
État du relais	337
Durée de la session	338
Attribuer l'accès des utilisateurs aux applications	339
Supprimer l'accès des utilisateurs aux applications	340
Attributs de carte	340
Compte AWS accès	342
Compte AWS types	342
Attribution d'un accès Compte AWS	345
Expérience de l'utilisateur final	345
Renforcer et limiter l'accès	346
Délégation et renforcement de l'accès	347
Limiter l'accès à la banque d'identités depuis les comptes des membres	347
Administration déléguée	348
Bonnes pratiques	349
Conditions préalables	354
Enregistrez un compte membre	354
Annuler l'enregistrement d'un compte membre	356

Afficher les comptes d'administrateurs délégués	357
Accès surélevé temporaire	357
Accès par authentification unique à Comptes AWS	358
Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS	359
Supprimer l'accès des utilisateurs et des groupes à un Compte AWS	362
Révoquer une session d'ensemble d'autorisations active	363
Délégué qui peut attribuer l'accès à l'authentification unique	365
Ensembles d'autorisations	366
Créez un ensemble d'autorisations qui applique les autorisations du moindre privilège	367
Autorisations prédéfinies	369
Autorisations personnalisées	370
Création, gestion et suppression des jeux d'autorisations	373
Configurer les propriétés des ensembles d'autorisations	387
Référencement d'ensembles d'autorisations	395
Recommandations pour éviter les interruptions d'accès	397
Exemple de politique de confiance personnalisée	398
Contrôle d'accès basé sur les attributs	399
Avantages	400
Liste de contrôle : Configuration d'ABAC à AWS l'aide d'IAM Identity Center	401
Attributs pour le contrôle d'accès	403
Rôles liés à un service	411
AWS portail d'accès	413
Commencer à utiliser le portail AWS d'accès	413
Configuration du portail AWS d'accès	414
Ce que vous pouvez configurer	414
Activation du portail AWS d'accès	414
Personnalisation de l'URL du portail AWS d'accès	415
Confirmez que les utilisateurs peuvent se connecter au portail AWS d'accès	416
Utiliser le portail AWS d'accès	418
Comment utiliser le portail AWS d'accès	418
Connexion au portail d' AWS accès	419
Réinitialisation de votre mot de passe utilisateur	421
AWS CLI et AWS accès au SDK	423
Création de liens de raccourci	429
Enregistrement de votre appareil à la MFA	431
Fin de votre session active	434

Utilisation d'IAM Identity Center sur plusieurs Régions AWS	436
Avantages du support multirégional	436
Prérequis et considérations	436
Choix d'une région supplémentaire	437
Répliquer le centre d'identité IAM dans une région supplémentaire	438
Étape 1 : Création d'une réplique de clé	438
Étape 2 : ajouter la région	439
Étape 3 : Mettre à jour la configuration de l'IdP externe	440
Étape 4 : Confirmer les listes d'autorisation du pare-feu et de la passerelle	441
Étape 5 : Fournissez des informations à vos utilisateurs	441
Changements de région au-delà de l'ajout de la première région	441
Quelles données sont répliquées ?	441
Accès à la main-d'œuvre par le biais d'une région supplémentaire	443
Sessions utilisateur sur plusieurs Régions AWS	443
AWS accéder aux points de terminaison du portail dans le système principal et dans le système supplémentaire Régions AWS	443
Points de terminaison ACS dans le primaire et dans le module supplémentaire Régions AWS	445
Utilisation d'applications AWS gérées sans plusieurs ACS URLs	447
Basculement vers une région supplémentaire pour y accéder Compte AWS	447
Compte AWS résilience des accès sans plusieurs ACS URLs	448
Déploiement et gestion d'applications sur plusieurs Régions AWS	449
Déploiement et gestion d'applications AWS gérées sur plusieurs Régions AWS	449
Déploiement et gestion des applications gérées par les clients dans plusieurs AWS régions	451
Supprimer une région du centre d'identité IAM	452
Étape 1 : Mettre à jour la configuration de l'IdP externe	452
Étape 2 : supprimer la région	452
Étape 3 : supprimer la clé de réplique	453
Service APIs pris en charge en supplément Régions AWS	454
CloudTrail événements dans les régions principales et supplémentaires	454
Cas d'utilisation d'IAM Identity Center dans la région principale et dans les régions supplémentaires	455
Conception de la résilience et comportement régional	458
Conçu pour la disponibilité	459
Configurez un accès d'urgence au AWS Management Console	459

Résumé de la configuration des accès d'urgence	461
Comment concevoir vos rôles opérationnels critiques	461
Comment planifier votre modèle d'accès	462
Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence	463
Comment créer votre configuration d'accès d'urgence	464
Tâches de préparation aux urgences	465
Processus de basculement d'urgence	466
Retour aux activités normales	466
Configuration unique d'une application de fédération IAM directe dans Okta	467
Configuration unique d'une application de fédération IAM directe avec ADFS	470
Sécurité	477
Gestion des identités et des accès pour IAM Identity Center	478
Authentification	478
Contrôle d'accès	478
Présentation de la gestion des accès	479
Exemples de politiques basées sur l'identité	483
Exemple de politique basée sur les ressources	492
AWS politiques gérées	494
Utilisation des rôles liés à un service	517
Autorisation de la console et de l'API IAM Identity Center	525
Actions relatives à l'API après novembre 2023	525
Actions de l'API après octobre 2020	526
AWS STS clés de condition pour IAM Identity Center	528
UserId	529
IdentityStoreArn	530
ApplicationArn	530
CredentialId	531
InstanceArn	531
Journalisation et surveillance	531
Journalisation des appels d'API IAM Identity Center avec AWS CloudTrail	532
Enregistrement d'IAM Identity Center SCIM avec AWS CloudTrail	573
Amazon EventBridge	580
Enregistrement des erreurs de synchronisation AD configurables	580
Validation de conformité	583
Normes de conformité prises en charge	584

Résilience	586
Sécurité de l'infrastructure	586
Protection des données	587
Chiffrement en transit	587
Confidentialité des données	588
Conservation des données	588
Chiffrement au repos	588
Contexte de chiffrement IAM Identity Center	590
Contrôle de l'accès à votre clé gérée par le client à l'aide du contexte de chiffrement	591
Surveillance de vos clés de chiffrement pour IAM Identity Center	591
AWS stockage, chiffrement et suppression des attributs d'identité d'IAM Identity Center dans les applications gérées	591
Mise en œuvre de clés KMS gérées par le client	592
Déclarations de base relatives aux clés KMS et à la politique IAM	602
Déclarations de politique clés avancées de KMS	625
Balisage de ressources	634
Restrictions liées aux étiquettes	635
Gérez les tags avec la console	635
AWS CLI exemples	636
Affectation de balises	636
Affichage des balises	637
Suppression de balises	637
Appliquer des balises lors de la création d'un ensemble d'autorisations	638
Actions d'API	638
Intégration de la AWS CLI à IAM Identity Center	639
Comment intégrer la AWS CLI à IAM Identity Center	639
Considérations relatives à l'accès privé	640
Quotas	641
Quotas de candidatures	641
Compte AWS quotas	642
Quotas Active Directory	643
Quotas de banque d'identités IAM Identity Center	643
Limites de limitation de l'IAM Identity Center	644
Quotas de demandes de service OIDC	645
Quotas supplémentaires	646
Résolution des problèmes	648

Problèmes lors de la création d'une instance de compte d'IAM Identity Center	648
Vous recevez un message d'erreur lorsque vous tentez d'afficher la liste des applications cloud préconfigurées pour fonctionner avec IAM Identity Center	648
Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center	650
Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe	650
Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe	652
Les utilisateurs ne peuvent pas se connecter lorsque leur nom d'utilisateur est au format UPN	653
Je reçois le message d'erreur « Impossible d'effectuer l'opération sur le rôle protégé » lors de la modification d'un rôle IAM	653
Les utilisateurs de l'annuaire ne peuvent pas réinitialiser leur mot de passe	654
Mon utilisateur est référencé dans un ensemble d'autorisations mais ne peut pas accéder aux comptes ou applications assignés	655
Je ne parviens pas à configurer correctement mon application à partir du catalogue d'applications	655
Erreur « Une erreur inattendue s'est produite » lorsqu'un utilisateur tente de se connecter à l'aide d'un fournisseur d'identité externe	656
Erreur « Impossible d'activer les attributs du contrôle d'accès »	657
Je reçois un message « Navigateur non pris en charge » lorsque je tente d'enregistrer un appareil pour le MFA	657
Le groupe « Utilisateurs du domaine » Active Directory ne se synchronise pas correctement avec IAM Identity Center	657
Erreur d'identification MFA non valide	658
Je reçois un message « Une erreur inattendue s'est produite » lorsque je tente de m'inscrire ou de me connecter à l'aide d'une application d'authentification	658
Je reçois un message d'erreur « Ce n'est pas toi, c'est nous » lorsque j'essaie de me connecter à IAM Identity Center	658
Mes utilisateurs ne reçoivent pas d'e-mails d'IAM Identity Center	659
Erreur : vous ne pouvez pas delete/modify/remove/assign accéder aux ensembles d'autorisations fournis dans le compte de gestion	659
Erreur : jeton de session introuvable ou non valide	659
Les membres du groupe issus de domaines approuvés ne se synchronisent pas avec IAM Identity Center	660
Résoudre les problèmes liés aux clés gérées par le client dans AWS IAM Identity Center	660

Accès refusé : problème d'autorisation de déchiffrement KMS	660
AWS échecs de connexion aux applications gérées avec une clé KMS gérée par le client activée dans IAM Identity Center	661
AWS échec de l'installation d'applications gérées et de and/or l'attribution des utilisateurs lorsque la clé KMS gérée par le client est activée dans IAM Identity Center	661
Problème d'autorisations KMS : configuration de la clé gérée par le client avec AWS IAM Identity Center	662
AWS échecs de connexion au portail d'accès avec une clé KMS gérée par le client activée dans IAM Identity Center	662
Résoudre les problèmes de configuration multirégionale dans AWS IAM Identity Center	663
La région vers laquelle je souhaite répliquer mon instance IAM Identity Center n'est pas disponible dans la console IAM Identity Center	663
AWS échecs de connexion à une application gérée dans une région supplémentaire	663
Historique de la documentation	664
AWS Glossaire	675
.....	dclxxvi

Qu'est-ce que IAM Identity Center ?

AWS IAM Identity Center est la AWS solution pour connecter les utilisateurs de votre personnel à des applications AWS gérées telles que Kiro et Amazon Quick, ainsi qu'à d'autres AWS ressources. Vous pouvez connecter votre fournisseur d'identité existant et synchroniser les utilisateurs et les groupes à partir de votre annuaire, ou créer et gérer vos utilisateurs directement dans IAM Identity Center. Vous pouvez ensuite utiliser IAM Identity Center pour l'une ou l'autre des opérations suivantes, ou pour les deux :

- Accès des utilisateurs aux applications
- Accès utilisateur à Comptes AWS

Vous utilisez déjà IAM pour accéder à ? Comptes AWS

Vous n'avez pas besoin de modifier vos Compte AWS flux de travail actuels pour utiliser IAM Identity Center pour accéder aux applications AWS gérées. Si vous utilisez la [fédération avec IAM](#) pour l' Compte AWS accès, vos utilisateurs peuvent continuer à accéder Comptes AWS de la même manière qu'ils l'ont toujours fait, et vous pouvez continuer à utiliser vos flux de travail existants pour gérer cet accès.

Pourquoi utiliser IAM Identity Center ?

IAM Identity Center rationalise et simplifie l'accès des utilisateurs du personnel aux applications Comptes AWS, ou aux deux, grâce aux fonctionnalités clés suivantes.

Intégration aux applications AWS gérées

[AWS applications gérées](#) telles que Kiro et Amazon Redshift intégration à IAM Identity Center.

IAM Identity Center fournit aux applications AWS gérées une vue commune des utilisateurs et des groupes.

Propagation d'identité fiable entre les applications

Grâce à une propagation d'identité fiable, les applications AWS gérées telles qu'Amazon Quick peuvent partager en toute sécurité l'identité d'un utilisateur avec d'autres applications AWS gérées, par exemple, Amazon Redshift et autoriser l'accès aux AWS ressources en fonction de l'identité de l'utilisateur. Vous pouvez plus facilement auditer l'activité des utilisateurs car les CloudTrail événements sont enregistrés en fonction de l'utilisateur et des actions qu'il a initiées.

Il est ainsi plus facile de comprendre qui a accédé à quoi. Pour plus d'informations sur les cas d'utilisation pris en charge, y compris les conseils de end-to-end configuration, consultez [Cas d'utilisation de propagation d'identité fiables](#).

Un seul endroit pour attribuer des autorisations à plusieurs Comptes AWS

Grâce aux autorisations multi-comptes, IAM Identity Center fournit un emplacement unique où vous pouvez attribuer des autorisations à des groupes d'utilisateurs multiples. Comptes AWS Vous pouvez créer des autorisations basées sur des fonctions professionnelles courantes ou définir des autorisations personnalisées répondant à vos besoins en matière de sécurité. Vous pouvez ensuite attribuer ces autorisations aux utilisateurs du personnel afin de contrôler leur accès à des informations spécifiques Comptes AWS.

Cette fonctionnalité facultative n'est disponible que pour les [instances d'organisation](#) d'IAM Identity Center.

Un point de fédération pour simplifier l'accès des utilisateurs à AWS

En fournissant un point de fédération unique, IAM Identity Center réduit les efforts administratifs requis pour utiliser plusieurs applications AWS gérées et Comptes AWS. Avec IAM Identity Center, vous ne fédérez qu'une seule fois et vous n'avez qu'un seul certificat à gérer lorsque vous utilisez un fournisseur d'[SAML 2.0](#) identité. IAM Identity Center fournit aux applications AWS gérées une vue commune des utilisateurs et des groupes pour des cas d'utilisation fiables de propagation d'identité ou lorsque les utilisateurs partagent l'accès aux AWS ressources avec d'autres personnes.

Pour plus d'informations sur la façon de configurer les fournisseurs d'identité couramment utilisés pour qu'ils fonctionnent avec IAM Identity Center, consultez [Tutoriels sur les sources d'identité IAM Identity Center](#). Si vous n'avez pas de fournisseur d'identité existant, vous pouvez [créer et gérer des utilisateurs directement dans IAM Identity Center](#).

Deux types d'instances

IAM Identity Center prend en charge deux types d'instances : les instances d'organisation et les instances de compte. Une instance d'organisation est la meilleure pratique. Il s'agit de la seule instance qui vous permet de gérer l'accès aux applications, Comptes AWS et elle est recommandée pour toutes les utilisations en production. Une instance d'organisation est déployée dans le compte AWS Organizations de gestion et vous fournit un point unique à partir duquel vous pouvez gérer l'accès des utilisateurs AWS.

Les instances de compte sont liées à Compte AWS celles dans lesquelles elles sont activées. Utilisez les instances de compte d'IAM Identity Center uniquement pour prendre en charge les

déploiements isolés de certaines applications AWS gérées. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Accès convivial au portail Web pour vos utilisateurs

Le portail AWS d'accès est un portail Web convivial qui fournit à vos utilisateurs un accès fluide à toutes les applications qui leur sont assignées Comptes AWS, ou aux deux.

Accès multirégional aux Comptes AWS applications

Lorsque vous répliquez votre instance IAM Identity Center dans des régions supplémentaires, votre personnel peut accéder aux applications qui lui sont attribuées Comptes AWS par le biais de toutes les régions activées, et il peut déployer des applications AWS gérées dans chaque région activée.

Renommer le centre d'identité IAM

Le 26 juillet 2022, AWS Single Sign-On a été renommé en AWS IAM Identity Center.

Les anciens espaces de noms restent les mêmes

Les espaces de noms sso et identitystore API ainsi que les espaces de noms associés suivants restent inchangés à des fins de rétrocompatibilité.

- Commandes CLI
 - [aws configure sso](#)
 - [identitystore](#)
 - [sso](#)
 - [sso-admin](#)
 - [sso-oidc](#)
- [Politiques gérées](#) contenant AWSSSO des AWSIdentitySync préfixes
- [Points de terminaison de service](#) contenant sso et identitystore
- Ressources [CloudFormation](#) contenant des préfixes AWS : :SSO
- [Rôle lié à un service](#) contenant AWSServiceRoleForSSO
- Console URLs contenant sso et singlesignon
- Documentation URLs contenant singlesignon

Commencer à utiliser IAM Identity Center

Ce qui suit explique comment démarrer avec IAM Identity Center.

1. Activer IAM Identity Center

Lorsque vous [activez IAM Identity Center](#), vous avez le choix entre deux types d'instances IAM Identity Center. Ces types sont les suivants : [instances d'organisation](#) (recommandées) et [instances de compte](#). Pour en savoir plus sur les différentes fonctionnalités de ces types d'instances, consultez la section [Instances d'organisation et de compte d'IAM Identity Center](#).

Note

Une fois IAM Identity Center activé, vous pouvez vous connecter et ouvrir la [console IAM Identity Center](#) en effectuant l'une des opérations suivantes :

- Instance d'organisation : connectez-vous à AWS l'aide des informations d'identification associées aux autorisations administratives du compte de gestion.
- Instance de compte : connectez-vous à AWS l'aide d'informations d'identification dotées d'autorisations administratives dans le Compte AWS pays où IAM Identity Center est activé.

2. Connectez votre source d'identité à IAM Identity Center

Dans la console IAM Identity Center, confirmez la source d'identité que vous souhaitez utiliser. Consultez ce qui suit pour les sources d'identité :

- Fournisseur d'identité externe : si vous disposez déjà d'un fournisseur d'identité pour gérer les utilisateurs de votre personnel, vous pouvez le connecter à IAM Identity Center. Pour plus d'informations sur la configuration des fournisseurs d'identité couramment utilisés pour qu'ils fonctionnent avec IAM Identity Center, consultez [Tutoriels sur les sources d'identité IAM Identity Center](#).
- Active Directory : si vous utilisez Active Directory pour gérer les utilisateurs de votre personnel, vous pouvez le connecter à IAM Identity Center. Pour de plus amples informations, veuillez consulter [Utilisation d'Active Directory comme source d'identité](#).
- IAM Identity Center : vous pouvez également [créer et gérer des utilisateurs et des groupes directement dans IAM Identity Center](#).

 Note

À l'heure actuelle, vous devez utiliser un fournisseur d'identité externe comme source d'identité pour tirer parti d'une configuration multirégionale avec votre IAM Identity Center. Pour plus d'informations sur les avantages de cette configuration, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

3. Configurer l'accès utilisateur à Comptes AWS (instance d'organisation uniquement)

Si vous utilisez une instance d'organisation d'IAM Identity Center, vous pouvez [attribuer un accès à un utilisateur ou à un groupe Comptes AWS](#), en utilisant des [ensembles d'autorisations](#) pour accorder à vos utilisateurs l'accès aux ressources Comptes AWS et aux ressources.

4. Configurer l'accès des utilisateurs aux applications

Avec IAM Identity Center, vous pouvez autoriser les utilisateurs à accéder à deux types d'applications :

a. [AWS applications gérées](#)

- Vous pouvez utiliser IAM Identity Center avec des applications AWS gérées telles qu'Amazon Q Business et Amazon Redshift. AWS CLI Pour plus d'informations, consultez [AWS applications gérées](#) et [Intégration de la AWS CLI à IAM Identity Center](#).

b. [Applications gérées par le client](#)

- Vous pouvez intégrer l'un des types suivants d'applications gérées par le client à IAM Identity Center :
 - [Applications répertoriées dans le catalogue IAM Identity Center](#)
 - [Vos applications personnalisées](#)
- Après avoir configuré votre application, vous pouvez [attribuer à vos utilisateurs l'accès à l'application](#).

5. Fournissez à vos utilisateurs des instructions de connexion pour le portail AWS d'accès

Le portail AWS d'accès est un portail Web qui fournit à vos utilisateurs un accès fluide à toutes les applications qui leur sont assignées Comptes AWS, ou aux deux. Les nouveaux utilisateurs d'IAM Identity Center doivent activer leurs informations d'identification avant de pouvoir se connecter au portail AWS d'accès.

Pour plus d'informations sur la procédure de connexion au portail AWS d'accès, voir [Connexion au portail AWS d'accès](#) dans le guide de Connexion à AWS l'utilisateur. Pour en savoir plus sur le processus de connexion au portail AWS d'accès, voir [Connexion au portail AWS d'accès](#).

Conditions préalables et considérations relatives à l'IAM Identity Center

Vous pouvez utiliser IAM Identity Center pour accéder uniquement aux applications AWS gérées, Comptes AWS uniquement, ou les deux. Si vous utilisez la fédération IAM pour gérer l'accès à Comptes AWS, vous pouvez continuer à le faire tout en utilisant IAM Identity Center pour accéder aux applications.

Avant d'activer IAM Identity Center, tenez compte des points suivants :

- AWS Région

Vous devez d'abord activer IAM Identity Center dans une seule région [prise en charge](#) pour chaque instance d'IAM Identity Center. Si vous souhaitez utiliser IAM Identity Center pour accéder aux AWS comptes par authentification unique, la région doit être accessible à tous les utilisateurs de votre organisation. Si vous envisagez d'utiliser IAM Identity Center pour accéder aux applications, sachez que certaines applications AWS gérées, telles qu'Amazon SageMaker AI, ne peuvent fonctionner que dans les régions qu'elles prennent en charge. En outre, la plupart des applications AWS gérées nécessitent qu'IAM Identity Center soit disponible dans la même région que l'application. Cela peut être réalisé en les colocalisant dans la même région, ou en cas de prise en charge, en répliquant l'instance IAM Identity Center dans la région de déploiement souhaitée d'une AWS application gérée. Pour de plus amples informations, veuillez consulter [Considérations relatives au choix d'un Région AWS](#).

- Accès aux applications uniquement

Vous pouvez utiliser IAM Identity Center uniquement pour accéder aux applications telles que Kiro, en utilisant votre fournisseur d'identité existant. Pour de plus amples informations, veuillez consulter [Utilisation d'IAM Identity Center pour l'accès des utilisateurs aux applications uniquement](#).

 Note

L'accès aux ressources de l'application est géré indépendamment par le propriétaire de l'application.

- Quota pour les rôles IAM

IAM Identity Center crée des rôles IAM pour autoriser les utilisateurs à accéder aux ressources du compte. Pour de plus amples informations, veuillez consulter [Rôles IAM créés par IAM Identity Center](#).

- IAM Identity Center et AWS Organizations

AWS Organizations est recommandé, mais non obligatoire, pour une utilisation avec IAM Identity Center. Si vous n'avez pas créé d'organisation, vous n'êtes pas obligé de le faire. Si vous avez déjà configuré AWS Organizations et que vous comptez ajouter IAM Identity Center à votre organisation, assurez-vous que toutes les AWS Organizations fonctionnalités sont activées. Pour de plus amples informations, veuillez consulter [IAM Identity Center et AWS Organizations](#).

Les interfaces Web d'IAM Identity Center, y compris le portail d'accès et la console IAM Identity Center, sont destinées à être accessibles aux humains via les navigateurs Web compatibles. Les navigateurs compatibles incluent les trois dernières versions de Microsoft Edge, Mozilla Firefox, Google Chrome et Apple Safari. L'accès à ces points de terminaison à l'aide de chemins non basés sur un navigateur n'est pas pris en charge. Pour un accès programmatique aux services IAM Identity Center, nous vous recommandons d'utiliser la documentation APIs disponible dans les guides de référence de l'API IAM Identity Center et Identity Store.

Considérations relatives au choix d'un Région AWS

Vous pouvez activer IAM Identity Center en un seul outil, compatible Région AWS de votre choix et disponible pour les utilisateurs du monde entier. Cette disponibilité globale vous permet de configurer plus facilement l'accès des utilisateurs à plusieurs applications Comptes AWS et applications. Voici les principales considérations à prendre en compte pour choisir un Région AWS.

- Emplacement géographique de vos utilisateurs : lorsque vous sélectionnez la région la plus proche géographiquement de la majorité de vos utilisateurs finaux, ils bénéficieront d'une latence d'accès plus faible au portail AWS d'accès et aux applications AWS gérées, telles qu'Amazon SageMaker AI.

- Régions optionnelles (régions désactivées par défaut) — Une région optionnelle est une Région AWS région désactivée par défaut. Pour utiliser une région opt-in, vous devez l'activer. Pour plus d'informations, consultez [la section Gestion du centre d'identité IAM dans une région optionnelle](#).
- Réplication d'IAM Identity Center vers des régions supplémentaires : si vous prévoyez de répliquer IAM Identity Center vers d'autres régions Régions AWS, vous devez choisir une région activée par défaut. Pour de plus amples informations, veuillez consulter [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).
- Choix des régions de déploiement pour les applications AWS AWS gérées : les applications gérées ne peuvent fonctionner que Régions AWS dans les régions dans lesquelles elles sont disponibles. De nombreuses applications AWS gérées peuvent également fonctionner uniquement dans une région dans laquelle le centre d'identité IAM est activé ou répliqué (région principale ou région supplémentaire). Pour vérifier si votre instance IAM Identity Center prend en charge la réplication vers des régions supplémentaires, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#). Si la réplication n'est pas une option, pensez à activer IAM Identity Center dans la région où vous prévoyez d'utiliser des applications AWS gérées.
- Souveraineté numérique — Les réglementations en matière de souveraineté numérique ou les politiques de l'entreprise peuvent imposer l'utilisation d'un élément particulier Région AWS. Consultez le service juridique de votre entreprise.
- Source d'identité : si vous utilisez [AWS Managed Microsoft AD](#) votre répertoire autogéré dans [Active Directory \(AD\)](#) comme source d'identité, sa région d'origine doit correspondre à celle Région AWS dans laquelle vous avez activé IAM Identity Center.
- E-mails interrégionaux avec Amazon Simple Email Service : dans certaines régions, IAM Identity Center peut appeler [Amazon Simple Email Service \(Amazon SES\)](#) dans une autre région pour envoyer des e-mails. Lors de ces appels interrégionaux, le centre d'identité IAM envoie certains attributs utilisateur à l'autre région. Pour de plus amples informations, veuillez consulter [E-mails interrégionaux avec Amazon SES](#).
- AWS Control Tower— Si vous activez une instance d'organisation d'IAM Identity Center depuis AWS Control Tower, l'instance sera créée dans la même région que la zone de AWS Control Tower landing zone.

Rubriques

- [Stockage des données et opérations dans la région du centre d'identité IAM](#)
- [Commutation Régions AWS](#)
- [Désactiver et Région AWS activer IAM Identity Center](#)

Stockage des données et opérations dans la région du centre d'identité IAM

Découvrez comment IAM Identity Center gère le stockage des données et les opérations dans l'ensemble Régions AWS.

Découvrez comment IAM Identity Center stocke les données

Lorsque vous activez IAM Identity Center, toutes les données que vous configurez dans IAM Identity Center sont stockées dans la région où vous l'avez activé. Ces données incluent les configurations d'annuaires, les ensembles d'autorisations, les instances d'applications et les affectations d'utilisateurs aux Compte AWS applications. Si vous utilisez le magasin d'identités IAM Identity Center, tous les utilisateurs et groupes que vous créez dans IAM Identity Center sont également stockés dans la même région. Si vous répliquez votre instance IAM Identity Center vers des régions supplémentaires, IAM Identity Center réplique automatiquement les utilisateurs, les groupes, les ensembles d'autorisations et leurs attributions, ainsi que les autres métadonnées et configurations vers ces régions.

E-mails interrégionaux avec Amazon SES

IAM Identity Center utilise [Amazon Simple Email Service \(Amazon SES\)](#) pour envoyer des e-mails aux utilisateurs finaux lorsqu'ils tentent de se connecter avec un mot de passe à usage unique (OTP) comme deuxième facteur d'authentification. Ces e-mails sont également envoyés pour certains événements de gestion de l'identité et des informations d'identification, par exemple lorsque l'utilisateur est invité à configurer un mot de passe initial, à vérifier une adresse e-mail et à réinitialiser son mot de passe. Amazon SES est disponible dans un sous-ensemble de Régions AWS ceux pris en charge par IAM Identity Center.

IAM Identity Center appelle les points de terminaison locaux d'Amazon SES lorsqu'Amazon SES est disponible localement dans un. Région AWS Lorsqu'Amazon SES n'est pas disponible localement, IAM Identity Center appelle les points de terminaison Amazon SES d'une autre manière Région AWS, comme indiqué dans le tableau suivant.

Code de région du centre d'identité IAM	Nom de la région du centre d'identité IAM	Code de région Amazon SES	Nom de la région Amazon SES
ap-east-1	Asie-Pacifique (Hong Kong)	ap-northeast-2	Asie-Pacifique (Séoul)

Code de région du centre d'identité IAM	Nom de la région du centre d'identité IAM	Code de région Amazon SES	Nom de la région Amazon SES
ap-east-2	Asie-Pacifique (Taipei)	ap-northeast-1	Asie-Pacifique (Tokyo)
ap-south-2	Asie-Pacifique (Hyderabad)	ap-south-1	Asie-Pacifique (Mumbai)
ap-southeast-4	Asie-Pacifique (Melbourne)	ap-southeast-2	Asie-Pacifique (Sydney)
ap-southeast-5	Asie-Pacifique (Malaisie)	ap-southeast-1	Asie-Pacifique (Singapour)
ap-southeast-6	Asie-Pacifique (Nouvelle Zélande)	ap-southeast-2	Asie-Pacifique (Sydney)
ap-southeast-7	Asie-Pacifique (Thaïlande)	ap-northeast-3	Asie-Pacifique (Osaka)
ca-west-1	Canada-Ouest (Calgary)	ca-central-1	Canada (Centre)
eu-south-2	Europe (Espagne)	eu-west-3	Europe (Paris)
eu-central-2	Europe (Zurich)	eu-central-1	Europe (Francfort)
mx-central-1	Mexique (Centre)	us-east-2	USA Est (Ohio)
me-central-1	Moyen-Orient (EAU)	eu-central-1	Europe (Francfort)
us-gov-east-1	AWS GovCloud (USA Est)	us-gov-west-1	AWS GovCloud (US-Ouest)

Lors de ces appels interrégionaux, IAM Identity Center peut envoyer les attributs utilisateur suivants :

- Adresse e-mail
- Prénom

- Nom
- Compte dans AWS Organizations
- AWS URL du portail d'accès
- Nom d'utilisateur
- ID de l'annuaire
- ID de l'utilisateur

Gestion du centre d'identité IAM dans une région optionnelle (région désactivée par défaut)

La plupart Régions AWS sont activées par défaut pour les opérations dans tous les AWS services, mais vous devez activer les [régions optionnelles](#) suivantes si vous souhaitez utiliser IAM Identity Center :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Taipei)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Malaisie)
- Asie-Pacifique (Nouvelle Zélande)
- Asie-Pacifique (Thaïlande)
- Canada-Ouest (Calgary)
- Europe (Milan)
- Europe (Espagne)
- Europe (Zurich)
- Israël (Tel Aviv)
- Mexique (Centre)
- Middle East (Bahrain)
- Moyen-Orient (EAU)

Si vous déployez IAM Identity Center dans une région optionnelle, vous devez activer cette région dans tous les comptes pour lesquels vous souhaitez gérer l'accès à IAM Identity Center. Tous les comptes ont besoin de cette configuration, que vous créiez ou non des ressources dans cette région. Vous pouvez activer une région pour les comptes courants de votre organisation et vous devez répéter cette action lorsque vous ajoutez de nouveaux comptes. Pour obtenir des instructions, voir [Activer ou désactiver une région dans votre organisation](#) dans le guide de AWS Organizations l'utilisateur. Pour éviter de répéter ces étapes supplémentaires, vous pouvez choisir de déployer votre IAM Identity Center dans une [région activée par défaut](#).

 Note

Votre compte de AWS membre doit être enregistré dans la même région que la région optionnelle dans laquelle se trouve votre instance IAM Identity Center, afin que vous puissiez accéder au compte de AWS membre depuis le portail d' AWS accès.

Métadonnées stockées dans les régions optionnelles

Lorsque vous activez IAM Identity Center pour un compte de gestion dans le cadre d'un opt-in Région AWS, les métadonnées IAM Identity Center suivantes pour tous les comptes membres sont stockées dans la région.

- ID de compte
- Nom du compte
- Adresse e-mail du compte
- Amazon Resource Names (ARNs) des rôles IAM créés par IAM Identity Center dans le compte membre

Régions AWS qui sont activés par défaut

Les régions suivantes sont activées par défaut et vous pouvez activer IAM Identity Center dans ces régions.

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Oregon)
- USA Ouest (Californie du Nord)

- Europe (Paris)
- Amérique du Sud (São Paulo)
- Asie-Pacifique (Mumbai)
- Europe (Stockholm)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Tokyo)
- Europe (Irlande)
- Europe (Francfort)
- Europe (Londres)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Canada (Centre)
- Asie-Pacifique (Osaka)

Commutation Régions AWS

Nous vous recommandons d'installer IAM Identity Center dans une région que vous souhaitez garder accessible aux utilisateurs, et non dans une région que vous devrez peut-être désactiver. Pour de plus amples informations, veuillez consulter [Considérations relatives au choix d'un Région AWS](#).

Vous pouvez changer de région de centre d'identité IAM uniquement en [supprimant votre instance actuelle de centre d'identité IAM](#) et en créant une instance dans une autre région. Si vous avez déjà activé une application AWS gérée avec votre instance IAM Identity Center existante, désactivez-la avant de supprimer IAM Identity Center. Pour obtenir des instructions sur la désactivation des applications AWS gérées, consultez [Désactivation d'une application AWS gérée](#).

Note

Si vous envisagez de changer de région de centre d'identité IAM pour permettre le déploiement d'une application AWS gérée dans une autre région, pensez plutôt à répliquer votre instance de centre d'identité IAM dans cette région. Pour de plus amples informations, veuillez consulter [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

Considérations relatives à la configuration dans la nouvelle région

Vous devez recréer les utilisateurs, les groupes, les ensembles d'autorisations, les applications et les attributions dans la nouvelle instance d'IAM Identity Center. Vous pouvez utiliser le compte IAM Identity Center et l'attribution d'application [APIs](#) pour obtenir un instantané de votre configuration, puis utiliser cet instantané pour reconstruire votre configuration dans une nouvelle région. Le passage à une autre région modifie également l'URL du [portail AWS d'accès](#), qui fournit à vos utilisateurs un accès par authentification unique à leurs applications Comptes AWS et à leurs applications. Vous devrez peut-être également recréer une configuration d'IAM Identity Center via la console de gestion de votre nouvelle instance.

Désactiver et Région AWS activer IAM Identity Center

Si vous désactivez un Région AWS système dans lequel IAM Identity Center est installé, IAM Identity Center est également désactivé. Une fois le centre d'identité IAM désactivé dans une région, les utilisateurs de cette région ne pourront plus accéder aux Comptes AWS applications par authentification unique.

Pour réactiver IAM Identity Center en mode [opt-in Régions AWS](#), vous devez réactiver la région. Comme IAM Identity Center doit retraiter tous les événements suspendus, la réactivation d'IAM Identity Center peut prendre un certain temps.

Note

IAM Identity Center peut gérer l'accès uniquement à ceux Comptes AWS qui sont activés pour une utilisation dans un Région AWS. Pour gérer l'accès à tous les comptes de votre organisation, activez IAM Identity Center dans le compte de gestion Région AWS qui est automatiquement activé pour être utilisé avec IAM Identity Center.

Pour plus d'informations sur l'activation et la désactivation Régions AWS, consultez [la section Gestion Régions AWS](#) dans le manuel de référence AWS général.

Utilisation d'IAM Identity Center pour l'accès des utilisateurs aux applications uniquement

Vous pouvez utiliser IAM Identity Center pour accéder aux utilisateurs à des applications telles que Kiro Comptes AWS, ou les deux. Vous pouvez connecter votre fournisseur d'identité existant et synchroniser les utilisateurs et les groupes depuis votre annuaire, ou [créer et gérer des utilisateurs directement dans IAM Identity Center](#). Pour plus d'informations sur la façon de connecter votre

fournisseur d'identité existant à IAM Identity Center, consultez le [Tutoriels sur les sources d'identité IAM Identity Center](#).

Vous utilisez déjà IAM pour accéder à ? Comptes AWS

Vous n'avez pas besoin de modifier vos Compte AWS flux de travail actuels pour utiliser IAM Identity Center pour accéder aux applications AWS gérées. Si vous utilisez la [fédération avec IAM](#) pour l' Compte AWS accès, vos utilisateurs peuvent continuer à accéder Comptes AWS de la même manière qu'ils l'ont toujours fait, et vous pouvez continuer à utiliser vos flux de travail existants pour gérer cet accès.

Rôles IAM créés par IAM Identity Center

Lorsque vous attribuez un AWS compte à un utilisateur, IAM Identity Center crée des rôles IAM pour autoriser les utilisateurs à accéder aux ressources.

Lorsque vous attribuez un ensemble d'autorisations, IAM Identity Center crée les rôles IAM contrôlés par IAM Identity Center correspondants dans chaque compte et associe les politiques spécifiées dans le jeu d'autorisations à ces rôles. IAM Identity Center gère le rôle et permet aux utilisateurs autorisés que vous avez définis d'assumer le rôle, en utilisant le portail d' AWS accès ou. AWS CLI Lorsque vous modifiez l'ensemble d'autorisations, IAM Identity Center veille à ce que les politiques et rôles IAM correspondants soient mis à jour en conséquence. La réplication de votre instance IAM Identity Center vers des régions supplémentaires n'affecte pas les rôles IAM existants et ne crée pas de nouveaux rôles IAM.

Note

Les ensembles d'autorisations ne sont pas utilisés pour accorder des autorisations aux applications.

Si vous avez déjà configuré des rôles IAM dans votre compte Compte AWS, nous vous recommandons de vérifier si votre compte atteint le quota de rôles IAM. Le quota par défaut pour les rôles IAM par compte est de 1 000 rôles. Pour plus d'informations, consultez la section [Quotas d'objets IAM](#).

Si vous approchez du quota, pensez à demander une augmentation du quota. Sinon, vous risquez de rencontrer des problèmes avec IAM Identity Center lorsque vous attribuez des ensembles

d'autorisations à des comptes qui ont dépassé le quota de rôles IAM. Pour plus d'informations sur la procédure à suivre pour demander une augmentation de quota, voir [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur du Service Quotas.

Note

Si vous passez en revue les rôles IAM dans un compte qui utilise déjà IAM Identity Center, vous remarquerez peut-être que les noms de rôles commencent par. "AWSReservedSSO_" Il s'agit des rôles que le service IAM Identity Center a créés dans le compte, et ils proviennent de l'attribution d'un ensemble d'autorisations au compte.

IAM Identity Center et AWS Organizations

AWS Organizations est recommandé, mais non obligatoire, pour une utilisation avec IAM Identity Center. Si vous n'avez pas créé d'organisation, vous n'êtes pas obligé de le faire. Lorsque vous activez IAM Identity Center, vous devez choisir d'activer ou non le service avec AWS Organizations. Lorsque vous configurez une organisation, le Compte AWS compte de gestion de l'organisation devient le compte de gestion de l'organisation. L'utilisateur root du Compte AWS est désormais le propriétaire du compte de gestion de l'organisation. Tout compte supplémentaire Comptes AWS que vous invitez à rejoindre votre organisation est un compte de membre. Le compte de gestion crée les ressources, les unités organisationnelles et les politiques de l'organisation qui gèrent les comptes des membres. Les autorisations sont déléguées aux comptes des membres par le compte de gestion.

Note

Nous vous recommandons d'activer IAM Identity Center avec AWS Organizations, ce qui crée une instance organisationnelle d'IAM Identity Center. Une instance d'organisation est notre meilleure pratique recommandée, car elle prend en charge toutes les fonctionnalités d'IAM Identity Center et fournit des fonctionnalités de gestion centralisée. Pour de plus amples informations, veuillez consulter [Instances organisationnelles d'IAM Identity Center](#).

Si vous avez déjà configuré AWS Organizations et que vous comptez ajouter IAM Identity Center à votre organisation, assurez-vous que toutes les AWS Organizations fonctionnalités sont activées. Lorsque vous créez une organisation, toutes les fonctions sont activées par défaut. Pour de plus amples informations, consultez [Activation de toutes les fonctionnalités de l'organisation](#) dans le Guide de l'utilisateur AWS Organizations .

Pour activer une instance organisationnelle d'IAM Identity Center, vous devez vous connecter au en vous AWS Management Console connectant à votre compte de AWS Organizations gestion en tant qu'utilisateur disposant d'informations d'identification administratives ou en tant qu'utilisateur root (ce n'est pas recommandé, sauf s'il n'existe aucun autre utilisateur administratif). Pour plus d'informations, consultez la section [Création et gestion d'une AWS organisation](#) dans le guide de AWS Organizations l'utilisateur.

Lorsque vous êtes connecté avec les informations d'identification administratives d'un compte AWS Organizations membre, vous pouvez activer une instance de compte d'IAM Identity Center. Les instances de compte ont des capacités limitées et sont liées à un seul AWS compte.

Instances d'organisation et de compte d'IAM Identity Center

Une instance est un déploiement unique d'IAM Identity Center. Deux types d'instances sont disponibles pour IAM Identity Center : les instances d'organisation et les instances de compte.

- Instance d'organisation (recommandée)

Instance d'IAM Identity Center que vous activez dans le compte AWS Organizations de gestion. Les instances d'organisation prennent en charge toutes les fonctionnalités d'IAM Identity Center. Nous vous recommandons de déployer une instance d'organisation plutôt que des instances de compte afin de minimiser le nombre de points de gestion.

- Instance de compte

Instance d'IAM Identity Center liée à une instance unique Compte AWS et visible uniquement dans la AWS région Compte AWS et dans laquelle elle est activée. Utilisez une instance de compte pour des scénarios de compte unique plus simples. Vous pouvez activer une instance de compte à partir de l'une des méthodes suivantes :

- Et Compte AWS cela n'est pas géré par AWS Organizations
- Un compte de membre dans AWS Organizations

Compte AWS types qui peuvent activer IAM Identity Center

Pour activer IAM Identity Center, connectez-vous au en AWS Management Console utilisant l'une des informations d'identification suivantes, selon le type d'instance que vous souhaitez créer :

- Votre compte AWS Organizations de gestion (recommandé) : obligatoire pour créer une [instance organisationnelle](#) d'IAM Identity Center. Utilisez une instance d'organisation pour les autorisations multi-comptes et les attributions d'applications au sein de l'organisation.
- Votre compte de AWS Organizations membre : à utiliser pour créer une [instance de compte](#) d'IAM Identity Center afin de permettre l'attribution d'applications au sein de ce compte membre. Un ou plusieurs comptes dotés d'une instance de niveau membre peuvent exister dans une organisation.
- Une instance autonome Compte AWS : à utiliser pour créer une instance d'[organisation ou une instance de compte](#) d'IAM Identity Center. Le système autonome Compte AWS n'est pas géré par AWS Organizations. Vous ne pouvez associer qu'une seule instance d'IAM Identity Center à une instance autonome Compte AWS et utiliser cette instance pour les attributions d'applications au sein de cette instance autonome. Compte AWS

Utilisez le tableau suivant pour comparer les fonctionnalités fournies par le type d'instance :

Capacité	Instance dans le compte AWS Organizations de gestion (recommandé)	Instance dans un compte membre	Instance dans un environnement autonome Compte AWS
Gérer les utilisateurs			
AWS portail d'accès pour un accès par authentification unique à vos applications AWS gérées			
OAuth Applications gérées par le client 2.0 (OIDC)			

Capacité	Instance dans le compte AWS Organizations de gestion (recommandé)	Instance dans un compte membre	Instance dans un environnement autonome Compte AWS
Autorisations multi-comptes			
AWS portail d'accès pour un accès par authentification unique à votre Comptes AWS			
Applications SAML 2.0 gérées par le client			
L'administrateur délégué peut gérer l'instance			
Chiffrement au repos à l'aide d'une clé KMS gérée par le client			
Réplication d'IAM Identity Center vers d'autres régions			

Pour plus d'informations sur les applications AWS gérées et IAM Identity Center, consultez [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#).

Rubriques

- [Instances organisationnelles d'IAM Identity Center](#)
- [Instances de compte d'IAM Identity Center](#)
- [Supprimer votre instance IAM Identity Center](#)

Instances organisationnelles d'IAM Identity Center

Lorsque vous activez IAM Identity Center conjointement avec AWS Organizations, vous créez une instance organisationnelle d'IAM Identity Center. Votre instance d'organisation doit être activée dans votre compte de gestion. Vous pouvez gérer de manière centralisée l'accès des utilisateurs et des groupes avec une seule instance d'organisation. Vous ne pouvez avoir qu'une seule instance d'organisation pour chaque compte de gestion dans AWS Organizations.

Si vous avez activé IAM Identity Center avant le 15 novembre 2023, vous disposez d'une instance organisationnelle d'IAM Identity Center.

Pour activer une instance organisationnelle d'IAM Identity Center, consultez [Pour activer une instance d'IAM Identity Center](#).

Quand utiliser une instance d'organisation

Une instance d'organisation est la principale méthode d'activation d'IAM Identity Center et une instance d'organisation est généralement recommandée. Les instances d'organisation offrent les avantages suivants :

- Support pour toutes les fonctionnalités d'IAM Identity Center, y compris la gestion des autorisations pour plusieurs Comptes AWS utilisateurs de votre organisation, l'attribution d'accès aux applications gérées par les clients et la réplication multirégionale.
- Réduction du nombre de points de gestion — Une instance d'organisation possède un point de gestion unique, le compte de gestion. Nous vous recommandons d'activer une instance d'organisation plutôt qu'une instance de compte afin de réduire le nombre de points de gestion.
- Contrôle centralisé de la création des instances de compte : vous pouvez contrôler si des instances de compte peuvent être créées par les comptes des membres de votre organisation tant que vous n'avez pas déployé d'instance d'IAM Identity Center dans votre organisation dans une région optionnelle (Région AWS qui est désactivée par défaut).

Pour obtenir des instructions sur l'activation d'une instance d'organisation d'IAM Identity Center, consultez [Pour activer une instance d'IAM Identity Center](#).

Instances de compte d'IAM Identity Center

Avec une instance de compte d'IAM Identity Center, vous pouvez déployer des applications AWS gérées prises en charge et des applications gérées par le client basées sur l'OIDC. Les instances de compte prennent en charge les déploiements isolés d'applications en une seule instance Compte AWS, en tirant parti des fonctionnalités du portail d'identité et d'accès du personnel d'IAM Identity Center.

Les instances de compte sont liées à une instance unique Compte AWS et sont utilisées uniquement pour gérer l'accès des utilisateurs et des groupes pour les applications prises en charge dans le même compte et Région AWS. Vous êtes limité à une instance de compte par Compte AWS. Vous pouvez créer une instance de compte à partir de l'une des options suivantes : un compte de membre dans AWS Organizations ou un compte autonome Compte AWS qui n'est pas géré par AWS Organizations.

Pour obtenir des instructions sur l'activation d'une instance de compte d'IAM Identity Center, consultez [Pour activer une instance d'IAM Identity Center](#) et sélectionnez l'onglet Compte.

Quand utiliser une instance de compte

Dans la plupart des cas, une [instance d'organisation](#) est recommandée. Utilisez les instances de compte uniquement si l'un des scénarios suivants s'applique :

- Vous souhaitez tester temporairement une application AWS gérée prise en charge afin de déterminer si l'application répond aux besoins de votre entreprise.
- Vous n'avez pas l'intention d'adopter IAM Identity Center au sein de votre organisation, mais vous souhaitez prendre en charge une ou plusieurs applications AWS gérées.
- Vous disposez d'une instance d'organisation d'IAM Identity Center, mais vous souhaitez déployer une application AWS gérée prise en charge vers un ensemble isolé d'utilisateurs distincts des utilisateurs de votre instance d'organisation.
- Vous ne contrôlez pas l' AWS organisation dans laquelle vous opérez. Par exemple, un tiers contrôle l' AWS organisation qui gère votre Comptes AWS.

 Important

Si vous envisagez d'utiliser IAM Identity Center pour prendre en charge les applications de plusieurs comptes, utilisez une instance d'organisation. Les instances de compte ne prennent pas en charge ce cas d'utilisation.

AWS applications gérées qui prennent en charge les instances de compte

Consultez [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#) la section pour savoir quelles applications AWS gérées prennent en charge les instances de compte d'IAM Identity Center. Vérifiez la disponibilité de la création d'instances de compte avec votre application AWS gérée.

Contraintes de disponibilité pour les comptes membres

Pour déployer des instances de compte d'IAM Identity Center dans des comptes AWS Organizations membres, l'une des conditions suivantes doit être remplie :

- Il n'existe aucune instance d'IAM Identity Center dans votre organisation.
- Il existe une instance organisationnelle d'IAM Identity Center dans votre organisation et l'administrateur de l'instance autorise la création d'instances de compte d'IAM Identity Center (pour les instances d'organisation créées après le 15 novembre 2023).
- Il existe une instance organisationnelle d'IAM Identity Center dans votre organisation et l'administrateur de l'instance a activé manuellement la création d'instances de compte par les comptes membres de l'organisation (pour les instances d'organisation créées avant le 15 novembre 2023). Pour obtenir des instructions, veuillez consulter [Autoriser la création d'instances de compte dans les comptes des membres](#).

Une fois que l'une des conditions précédentes est remplie, toutes les conditions suivantes doivent être remplies :

- Votre administrateur n'a pas créé de [politique de contrôle des services](#) qui empêche les comptes membres de créer des instances de compte.
- Quoi qu'il en soit, vous ne possédez pas encore d'instance d'IAM Identity Center dans ce même compte. Région AWS

- Vous travaillez dans un Région AWS endroit où IAM Identity Center est disponible. Pour plus d'informations sur les régions, consultez [Stockage des données et opérations dans la région du centre d'identité IAM](#).

Considérations relatives aux instances de compte

Une instance de compte est conçue pour des cas d'utilisation spécialisés et propose un sous-ensemble de fonctionnalités disponibles pour une instance d'organisation. Tenez compte des points suivants avant de créer une instance de compte :

- Les instances de compte ne prennent pas en charge les ensembles d'autorisations et ne prennent donc pas en charge l'accès à Comptes AWS.
- Vous ne pouvez pas convertir ou fusionner une instance de compte en une instance d'organisation.
- Seules certaines [applications AWS gérées prennent en charge les](#) instances de compte.
- Utilisez des instances de compte pour les utilisateurs isolés qui utiliseront les applications d'un seul compte et pendant toute la durée de vie des applications utilisées.
- Les applications associées à une instance de compte doivent rester attachées à l'instance de compte jusqu'à ce que vous supprimiez l'application et ses ressources.
- Une instance de compte doit rester Compte AWS là où elle a été créée.

Autoriser la création d'instances de compte dans les comptes des membres

Si vous avez activé IAM Identity Center avant le 15 novembre 2023, vous disposez d'une [instance organisationnelle](#) d'IAM Identity Center dont la possibilité pour les comptes membres de créer des instances de compte est désactivée par défaut. Vous pouvez choisir si vos comptes membres peuvent créer des instances de compte en activant la fonctionnalité d'instance de compte dans la console IAM Identity Center.

Pour permettre la création d'instances de compte par les comptes membres de votre organisation

Important

L'activation des instances de compte d'IAM Identity Center pour les comptes des membres est une opération unique. Cela signifie que cette opération ne peut pas être annulée. Une fois activée, vous pouvez limiter la création d'instances de compte en créant une politique de

contrôle des services (SCP). Pour obtenir des instructions, consultez la section [Contrôle de la création d'instances de compte à l'aide des politiques de contrôle des services](#).

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Paramètres, puis sélectionnez l'onglet Gestion.
3. Dans la section Instances de compte d'IAM Identity Center, choisissez Activer les instances de compte d'IAM Identity Center.
4. Dans la boîte de dialogue Activer les instances de compte d'IAM Identity Center, confirmez que vous souhaitez autoriser les comptes membres de votre organisation à créer des instances de compte en choisissant Activer.

Utiliser les politiques de contrôle des services pour contrôler la création d'instances de compte

La possibilité pour les comptes membres de créer des instances de compte dépend de la date à laquelle vous avez activé IAM Identity Center :

- Avant novembre 2023 : vous devez [autoriser la création d'instances de compte dans les comptes des membres](#), une action irréversible.
- Après le 15 novembre 2023, les comptes membres peuvent créer des instances de compte par défaut.

Dans les deux cas, vous pouvez utiliser les politiques de contrôle des services (SCPs) pour :

- Empêchez tous les comptes membres de créer des instances de compte.
- N'autorisez que des comptes de membres spécifiques à créer des instances de compte.

Empêcher les instances de compte

Utilisez la procédure suivante pour générer un SCP qui empêche les comptes membres de créer des instances de compte d'IAM Identity Center.

1. Ouvrez la [console IAM Identity Center](#).
2. Sur le tableau de bord, dans la section Gestion centrale, cliquez sur le bouton Empêcher les instances de compte.

3. Dans la boîte de dialogue Attacher un SCP pour empêcher la création de nouvelles instances de compte, un SCP vous est fourni. Copiez le SCP et cliquez sur le bouton Accéder au tableau de bord du SCP. Vous serez dirigé vers la [AWS Organizations console](#) pour créer le SCP ou le joindre sous forme de déclaration à un SCP existant. SCPs sont une fonctionnalité de AWS Organizations. Pour obtenir des instructions sur la connexion d'un SCP, consultez les [politiques de contrôle de service relatives à l'attachement et au détachement](#) du guide de l'AWS Organizations utilisateur.

Limitier les instances de compte

Au lieu d'empêcher toute création d'instance de compte, cette politique interdit toute tentative de création d'une instance de compte d'IAM Identity Center pour tous, à l'exception de ceux qui sont explicitement répertoriés dans l'"<ALLOWED-ACCOUNT-ID>" espace réservé.

Exemple: politique de refus visant à limiter la création d'instances de compte

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyMemberAccountInstances",
      "Effect": "Deny",
      "Action": "sso:CreateInstance",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
        }
      }
    }
  ]
}
```

- Remplacez ["<ALLOWED-ACCOUNT-ID>"] par le ou les Compte AWS identifiants réels que vous souhaitez autoriser à créer une instance de compte d'IAM Identity Center.

- Vous pouvez répertorier plusieurs comptes IDs autorisés au format tableau : ["111122223333", "444455556666"].
- Associez cette politique au SCP de votre organisation pour renforcer le contrôle centralisé de la création d'instances de compte IAM Identity Center.

Pour obtenir des instructions sur la connexion d'un SCP, consultez les [politiques de contrôle de service relatives à l'attachement et au détachement](#) du guide de l'AWS Organizations utilisateur.

Supprimer votre instance IAM Identity Center

Lorsqu'une instance IAM Identity Center est supprimée, toutes les données de cette instance sont supprimées et ne peuvent pas être récupérées. Le tableau suivant décrit les données supprimées en fonction du type de répertoire configuré dans IAM Identity Center.

Quelles données sont supprimées	Annuaire connecté - AWS Managed Microsoft AD, AD Connector ou fournisseur d'identité externe	Boutique d'identités IAM Identity Center	
Tous les ensembles d'autorisations que vous avez configurés pour Comptes AWS			Oui
Toutes les applications que vous avez configurées dans IAM Identity Center			Oui
Toutes les attributions d'utilisateurs que vous avez configurées pour Comptes AWS et les applications			Oui

Quelles données sont supprimées	Annuaire connecté - AWS Managed Microsoft AD, AD Connector ou fournisseur d'identité externe	Boutique d'identités IAM Identity Center	
Tous les utilisateurs et groupes de l'annuaire ou du magasin	S/O		Oui

Si vous avez répliqué votre instance IAM Identity Center dans des régions supplémentaires, vous devez supprimer ces régions avant de supprimer l'instance.

Utilisez la procédure suivante pour supprimer votre instance IAM Identity Center.

Pour supprimer votre instance IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Gestion.
4. Dans la section Supprimer la configuration du centre d'identité IAM, choisissez Supprimer.
5. Dans la boîte de dialogue de configuration Supprimer IAM Identity Center, cochez chaque case pour confirmer que vous comprenez que vos données seront supprimées. Tapez votre instance IAM Identity Center dans la zone de texte, puis choisissez Confirmer.

Activer IAM Identity Center

Lorsque vous activez IAM Identity Center, vous choisissez le type d' AWS IAM Identity Center instance à activer. Une instance de service est le déploiement unique d'un service au sein de votre AWS environnement. Deux types d'instances sont disponibles pour IAM Identity Center : les instances d'organisation et les instances de compte. Les types d'instances que vous pouvez activer dépendent du type de compte auquel vous êtes connecté.

La liste suivante identifie le type d'instances IAM Identity Center que vous pouvez activer pour chaque type de Compte AWS :

- Votre compte AWS Organizations de gestion (recommandé) : obligatoire pour créer une [instance organisationnelle](#) d'IAM Identity Center. Utilisez une instance d'organisation pour les autorisations multi-comptes et les attributions d'applications au sein de l'organisation. Vous pouvez répliquer ce type d'instance vers des régions supplémentaires pour améliorer la résilience de l'accès aux comptes et la flexibilité dans le choix des régions de déploiement des AWS applications.
- Votre compte de AWS Organizations membre : à utiliser pour créer une [instance de compte](#) d'IAM Identity Center afin de permettre l'attribution d'applications au sein de ce compte membre. Un ou plusieurs comptes dotés d'une instance de niveau membre peuvent exister dans une organisation.
- Une instance autonome Compte AWS : à utiliser pour créer une instance d'[organisation ou une instance de compte](#) d'IAM Identity Center. Le système autonome Compte AWS n'est pas géré par AWS Organizations. Vous ne pouvez associer qu'une seule instance d'IAM Identity Center à une instance autonome Compte AWS et utiliser cette instance pour les attributions d'applications au sein de cette instance autonome. Compte AWS

Important

Le compte de gestion de l'organisation peut contrôler si les [comptes des membres de l'organisation peuvent créer des instances de compte d'IAM Identity Center](#) à l'aide d'une politique de contrôle des services.

Si vous utilisez un compte gratuit, la création d'une AWS organisation fait automatiquement passer votre compte à un forfait payant avec pay-as-you-go tarification. Vos crédits de niveau gratuit expirent immédiatement. Pour plus d'informations, consultez la page sur l'[offre gratuite AWS FAQs](#).

Pour une comparaison des différentes fonctionnalités fournies par les différents types d'instances, consultez [Instances d'organisation et de compte d'IAM Identity Center](#).

Avant d'activer IAM Identity Center, nous vous recommandons de consulter le [Conditions préalables et considérations relatives à l'IAM Identity Center](#).

Pour activer une instance d'IAM Identity Center

Choisissez l'onglet correspondant au type d'instance IAM Identity Center que vous souhaitez activer, qu'il s'agisse d'une instance d'organisation ou de compte :

Organization (recommended)

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
 - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
 - Utilisez-le déjà AWS avec un appareil autonome Compte AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
 - Vous utilisez déjà AWS Organizations (informations d'identification IAM) : connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Ouvrez la [console IAM Identity Center](#).
3. (Facultatif) Si vous souhaitez utiliser une clé KMS gérée par le client pour le chiffrement au repos plutôt que la clé AWS gérée par défaut, configurez la clé gérée par le client dans la section Clé pour chiffrer les données IAM Identity Center au repos. Pour plus d'informations, consultez [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#).



Important

Effectuez cette étape uniquement si vous avez configuré les autorisations nécessaires pour utiliser la clé gérée par le client KMS. Sans autorisations appropriées, cette étape peut échouer ou perturber l'administration d'IAM Identity Center et les applications AWS gérées.

4. Sous Activer IAM Identity Center, sélectionnez Activer.

5. Sur la AWS Organizations page Activer le centre d'identité IAM avec, passez en revue les informations, puis sélectionnez Activer pour terminer le processus.

 Note

AWS Organizations IAM Identity Center ne peut être activé que dans une seule AWS région. Après avoir activé IAM Identity Center, si vous devez modifier la région dans laquelle IAM Identity Center est activé, vous devez [supprimer](#) l'instance actuelle et créer une instance dans l'autre région.

Après avoir activé l'instance de votre organisation, nous vous recommandons de suivre les étapes suivantes pour terminer la configuration de votre environnement :

- Vérifiez que vous utilisez la source d'identité de votre choix. Si une source d'identité vous est déjà attribuée, vous pouvez continuer à l'utiliser. Pour de plus amples informations, veuillez consulter [Confirmation de vos sources d'identité dans IAM Identity Center](#).
- Enregistrez un compte membre en tant qu'administrateur délégué. Pour de plus amples informations, veuillez consulter [Administration déléguée](#).
- IAM Identity Center vous fournit un portail d'accès aux AWS ressources. Si vous filtrez l'accès à des AWS domaines ou à des points de terminaison d'URL spécifiques à l'aide d'une solution de filtrage de contenu Web telle que des pare-feux de nouvelle génération (NGFW) ou des passerelles Web sécurisées (SWG), consultez. [Mettez à jour les pare-feux et les passerelles pour autoriser l'accès au Portail d'accès AWS](#)

Account

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
 - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
 - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
 - Vous utilisez déjà AWS Organizations (informations d'identification IAM) : connectez-vous à l'aide des informations d'identification administratives de votre compte membre.

2. Ouvrez la [console IAM Identity Center](#).
3. Si vous utilisez un centre autonome pour la AWS première fois ou si vous en possédez un Compte AWS, sous Activer le centre d'identité IAM, sélectionnez Activer.

La AWS Organizations page Activer le centre d'identité IAM avec s'affiche. Nous recommandons cette option, mais elle n'est pas obligatoire.

Sélectionnez le lien activer une instance de compte d'IAM Identity Center.

4. Si vous êtes administrateur d'un compte AWS Organizations membre, sous Activer une instance de compte d'IAM Identity Center, sélectionnez Activer une instance de compte.
5. Sur la page Activer une instance de compte d'IAM Identity Center, passez en revue les informations et ajoutez éventuellement les balises que vous souhaitez associer à cette instance de compte. Sélectionnez ensuite Activer pour terminer le processus.

 Note

Si votre AWS compte est membre d'une organisation, votre capacité à activer une instance de compte d'IAM Identity Center peut être limitée.

- Si votre organisation a activé IAM Identity Center avant le 15 novembre 2023, la possibilité pour les comptes membres de créer des instances de compte est désactivée par défaut et doit être activée par le compte de gestion de l'organisation.
- Si votre organisation a activé IAM Identity Center après le 15 novembre 2023, la possibilité pour le compte membre de créer des instances de compte est activée par défaut. Toutefois, les politiques de contrôle des services peuvent être utilisées pour empêcher la création d'instances de compte d'IAM Identity Center au sein d'une organisation.

Pour plus d'informations, consultez [the section called “Autoriser la création d'instances de compte dans les comptes des membres”](#) et [the section called “SCPs pour la création d'une instance de compte”](#).

Confirmation de vos sources d'identité dans IAM Identity Center

Votre source d'identité dans IAM Identity Center définit l'endroit où vos utilisateurs et vos groupes sont gérés. Après avoir activé IAM Identity Center, vérifiez que vous utilisez la source d'identité de votre choix. Si une source d'identité vous est déjà attribuée, vous pouvez continuer à l'utiliser.

Si vous gérez déjà des utilisateurs et des groupes au sein d'un IdP externe Active Directory ou au sein d'un IdP externe, nous vous recommandons d'envisager de connecter cette source d'identité lorsque vous activez IAM Identity Center et que vous choisissez votre source d'identité. Cela doit être fait avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center et d'effectuer des assignations.

Si vous gérez déjà des utilisateurs et des groupes dans une source d'identité dans IAM Identity Center, le passage à une autre source d'identité risque de supprimer toutes les attributions d'utilisateurs et de groupes que vous avez configurées dans IAM Identity Center. Dans ce cas, tous les utilisateurs, y compris l'utilisateur administratif d'IAM Identity Center, perdront l'accès par authentification unique à leurs applications Comptes AWS et à leurs applications. Pour de plus amples informations, veuillez consulter [Considérations relatives à la modification de votre source d'identité](#).

Pour confirmer votre source d'identité

1. Ouvrez la [console IAM Identity Center](#).
2. Sur la page du tableau de bord, sous la section Étapes de configuration recommandées, choisissez Confirmer votre source d'identité. Vous pouvez également accéder à cette page en choisissant Paramètres et en choisissant l'onglet Source d'identité.
3. Aucune action n'est nécessaire si vous souhaitez conserver la source d'identité qui vous a été attribuée. Si vous préférez le modifier, choisissez Actions, puis Change identity source.

Vous pouvez choisir l'une des sources d'identité suivantes :

Répertoire d'Identity Center

Lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire Identity Center comme source d'identité par défaut. Si vous n'utilisez pas encore un autre fournisseur d'identité externe, vous pouvez commencer à créer vos utilisateurs et groupes, et attribuer leur niveau d'accès à vos applications Comptes AWS et à vos applications.

Pour un didacticiel sur l'utilisation de cette source d'identité, consultez [Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut](#).

Active Directory

Si vous gérez déjà des utilisateurs et des groupes dans votre AWS Managed Microsoft AD annuaire en utilisant Directory Service ou dans votre annuaire autogéré Active Directory (AD), nous vous recommandons de connecter cet annuaire lorsque vous activez IAM Identity Center. Ne créez aucun utilisateur ni groupe dans le répertoire par défaut d'Identity Center. IAM Identity Center utilise la connexion fournie par le AWS Directory Service pour synchroniser les informations relatives aux utilisateurs, aux groupes et aux membres entre votre répertoire source dans Active Directory et le magasin d'identités IAM Identity Center. Pour de plus amples informations, veuillez consulter [Microsoft AD annuaire](#).

Note

IAM Identity Center ne prend pas en charge SAMBA4 Simple AD en tant que source d'identité.

Fournisseur d'identité externe

Pour les fournisseurs d'identité externes (IdPs) tels que Okta ou Microsoft Entra ID, vous pouvez utiliser IAM Identity Center pour authentifier les identités IdPs via la norme SAML (Security Assertion Markup Language) 2.0. Le protocole SAML ne permet pas d'interroger l'IdP pour en savoir plus sur les utilisateurs et les groupes. Vous informez IAM Identity Center de l'existence de ces utilisateurs et groupes en les configurant dans IAM Identity Center. Vous pouvez effectuer le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis votre IdP vers IAM Identity Center à l'aide du protocole System for Cross-domain Identity Management (SCIM) v2.0 si votre IdP prend en charge le SCIM. Sinon, vous pouvez configurer manuellement vos utilisateurs et vos groupes en saisissant manuellement les noms d'utilisateur, les adresses e-mail et les groupes dans IAM Identity Center.

Pour obtenir des instructions détaillées sur la configuration de votre source d'identité, consultez [Tutoriels sur les sources d'identité IAM Identity Center](#).

Note

Si vous envisagez d'utiliser un fournisseur d'identité externe, notez que c'est l'IdP externe, et non le IAM Identity Center, qui gère les paramètres d'authentification multifactorielle.

(MFA). L'authentification MFA dans IAM Identity Center n'est pas prise en charge par les fournisseurs d'identité externes. Pour de plus amples informations, veuillez consulter [Inviter les utilisateurs à utiliser le MFA](#).

 Note

Si vous prévoyez de répliquer IAM Identity Center dans d'autres régions, vous devez configurer un fournisseur d'identité externe. Pour plus de détails, notamment sur les prérequis, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

Mettez à jour les pare-feux et les passerelles pour autoriser l'accès au Portail d'accès AWS

Le portail AWS d'accès fournit aux utilisateurs un accès par authentification unique à toutes vos applications cloud Comptes AWS et aux applications cloud les plus couramment utilisées, telles qu'Office 365, Concur, Salesforce et bien d'autres encore. Vous pouvez lancer rapidement plusieurs applications en cliquant simplement sur l'icône Compte AWS ou de l'application dans le portail.

 Note

AWS les applications gérées s'intègrent à IAM Identity Center et l'utilisent pour l'authentification et les services d'annuaire, mais peuvent ne pas utiliser le portail AWS d'accès pour accéder aux applications.

Si vous filtrez l'accès à des AWS domaines ou points de terminaison d'URL spécifiques à l'aide d'une solution de filtrage de contenu Web telle que des pare-feux de nouvelle génération (NGFW) ou des passerelles Web sécurisées (SWG), vous devez autoriser la liste des domaines et des points de terminaison d'URL associés au portail d'accès. AWS

La liste suivante fournit les domaines à double pile IPv4 et les points de terminaison d'URL à ajouter aux listes d'autorisation de votre solution de filtrage de contenu Web.

IPv4 liste d'autorisations

- *[Directory ID or alias].awsapps.com*

- *[Identity Center instance ID].[Region].portal.amazonaws.com*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Liste d'autorisations à double pile

- *[Identity Center instance ID].portal.[Region].app.aws*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

Liste d'autorisation combinée (IPv4 + double pile avec rétrocompatibilité)

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.com*
- *[Identity Centers instance ID].portal.[Region].app.aws*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- *oidc.[Region].amazonaws.com*
- *oidc.[Region].api.aws*
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *sso.[Region].api.aws*
- *.sso-portal.*[Region]*.amazonaws.com
- *portal.sso.[Region].api.aws*
- *[Region].prod.pr.panorama.console.api.aws/panoramamaroute*
- *[Region].signin.aws*
- *[Region].sso.signin.aws*
- *[Region].signin.aws.amazon.com*
- *signin.aws.amazon.com*
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- *cdn.us-east-1.threat-mitigation.aws.amazon.com*
- *us-east-1.threat-mitigation.aws.amazon.com*
- *amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com*

Considérations relatives à l'autorisation de répertoire des domaines et des points de terminaison d'URL

Outre les exigences relatives à la liste d'autorisation pour le portail AWS d'accès, les autres services et applications que vous utilisez peuvent nécessiter une liste d'autorisation de domaines.

- Pour accéder à Comptes AWS AWS Management Console, et à la console IAM Identity Center depuis votre portail d' AWS accès, vous devez autoriser des domaines supplémentaires sur la liste. Reportez-vous à la section [Résolution](#) des problèmes du Guide de démarrage pour AWS Management Console obtenir la liste des AWS Management Console domaines.
- Pour accéder aux applications AWS gérées depuis votre portail AWS d'accès, vous devez autoriser leurs domaines respectifs sur la liste d'autorisation. Reportez-vous à la documentation de service correspondante pour obtenir des conseils.
- Si vous utilisez un logiciel externe, tel qu'un logiciel externe IdPs (par exemple, Okta etMicrosoft Entra ID), vous devez inclure leurs domaines dans vos listes d'autorisation.

Tutoriels sur les sources d'identité IAM Identity Center

Vous pouvez connecter votre source d'identité existante dans votre compte AWS Organizations de gestion à [une instance organisationnelle d'IAM Identity Center](#). Si vous n'avez pas de fournisseur d'identité existant, vous pouvez créer et gérer des utilisateurs directement dans le répertoire par défaut de l'IAM Identity Center. Vous ne pouvez avoir qu'une seule source d'identité par organisation.

Les didacticiels de cette section expliquent comment configurer une instance organisationnelle d'IAM Identity Center avec une source d'identité couramment utilisée, créer un utilisateur administratif et si vous utilisez IAM Identity Center pour gérer l'accès aux ensembles d'autorisations Comptes AWS, les créer et les configurer. Si vous utilisez IAM Identity Center uniquement pour accéder aux applications, il n'est pas nécessaire d'utiliser des ensembles d'autorisations.

Ces didacticiels ne décrivent pas comment configurer les instances de compte d'IAM Identity Center. Vous pouvez utiliser des instances de compte pour attribuer des utilisateurs et des groupes à des applications, mais vous ne pouvez pas utiliser ce type d'instance pour gérer l'accès des utilisateurs à Comptes AWS. Pour de plus amples informations, veuillez consulter [Instances de compte d'IAM Identity Center](#).

Note

Avant de commencer l'un de ces didacticiels, activez IAM Identity Center. Pour de plus amples informations, veuillez consulter [Activer IAM Identity Center](#).

Rubriques

- [Utilisation d'Active Directory comme source d'identité](#)
- [Setting up SCIM provisioning between CyberArk and IAM Identity Center](#)
- [Configurer SAML et SCIM avec un IAM Google Workspace Identity Center](#)
- [Utilisation d'IAM Identity Center pour vous connecter à votre plateforme d'JumpCloudannuaire](#)
- [Configurer SAML et SCIM avec un IAM Microsoft Entra ID Identity Center](#)
- [Configurer SAML et SCIM avec un IAM Okta Identity Center](#)
- [Configuration du provisionnement SCIM entre OneLogin et IAM Identity Center](#)
- [Utilisation de Ping Identity produits avec IAM Identity Center](#)
- [Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut](#)

- [Didacticiels vidéo](#)

Utilisation d'Active Directory comme source d'identité

Si vous gérez les utilisateurs de votre AWS Managed Microsoft AD annuaire à l'aide d'Active Directory (AD) Directory Service ou de votre annuaire autogéré dans Active Directory (AD), vous pouvez modifier la source d'identité de votre IAM Identity Center pour qu'elle fonctionne avec ces utilisateurs. Nous vous recommandons d'envisager de connecter cette source d'identité lorsque vous activez IAM Identity Center et que vous choisissez votre source d'identité. Cette opération avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center vous permettra d'éviter la configuration supplémentaire requise si vous modifiez votre source d'identité ultérieurement.

Pour utiliser Active Directory comme source d'identité, votre configuration doit répondre aux conditions préalables suivantes :

- Si vous utilisez AWS Managed Microsoft AD, vous devez activer IAM Identity Center dans le même Région AWS endroit où votre AWS Managed Microsoft AD annuaire est configuré. IAM Identity Center stocke les données d'attribution dans la même région que le répertoire. Pour administrer IAM Identity Center, vous devrez peut-être passer à la région dans laquelle IAM Identity Center est configuré. Notez également que le portail AWS d'accès utilise la même URL d'accès que votre annuaire.
- Utilisez un Active Directory résidant dans le compte de gestion :

Un AD Connector ou un AWS Managed Microsoft AD annuaire AD Connector existant doit être configuré dans AWS Directory Service votre compte AWS Organizations de gestion. Vous ne pouvez connecter qu'un seul répertoire AD Connector ou un seul annuaire AWS Managed Microsoft AD à la fois. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisez AWS Managed Microsoft AD. Pour en savoir plus, consultez :

- [Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center](#)
- [Connectez un annuaire autogéré dans Active Directory à IAM Identity Center](#)
- Utilisez un Active Directory résidant dans le compte d'administrateur délégué :

Si vous envisagez d'activer un administrateur délégué IAM Identity Center et d'utiliser Active Directory comme source d'identité IAM Identity Center, vous pouvez utiliser un AD Connector ou un AWS Managed Microsoft AD annuaire existant configuré dans AWS Directory résidant dans le compte d'administrateur délégué.

Si vous décidez de remplacer la source d'identité IAM Identity Center d'une autre source par Active Directory, ou de la remplacer par une autre source, le répertoire doit résider dans le compte membre administrateur délégué d'IAM Identity Center (s'il en existe un) ; sinon, il doit se trouver dans le compte de gestion.

Ce didacticiel explique la configuration de base pour utiliser Active Directory comme source d'identité IAM Identity Center.

Étape 1 : Connecter Active Directory et spécifier un utilisateur

Si vous utilisez déjà Active Directory, les rubriques suivantes vous aideront à préparer la connexion de votre annuaire à IAM Identity Center.

Note

Si vous envisagez de connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory et que vous n'utilisez pas RADIUS MFA AWS Directory Service avec, activez l'authentification MFA dans IAM Identity Center.

AWS Managed Microsoft AD

1. Consultez les directives dans [Microsoft ADannuaire](#).
2. Suivez les étapes de [Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center](#).
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour de plus amples informations, veuillez consulter [Synchroniser un utilisateur administratif dans IAM Identity Center](#).

Répertoire autogéré dans Active Directory

1. Consultez les directives dans [Microsoft ADannuaire](#).
2. Suivez les étapes de [Connectez un annuaire autogéré dans Active Directory à IAM Identity Center](#).
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour de plus amples informations, veuillez consulter [Synchroniser un utilisateur administratif dans IAM Identity Center](#).

Étape 2 : Synchroniser un utilisateur administratif dans IAM Identity Center

Après avoir connecté votre annuaire à IAM Identity Center, vous pouvez spécifier un utilisateur auquel vous souhaitez accorder des autorisations administratives, puis synchroniser cet utilisateur depuis votre annuaire avec IAM Identity Center.

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Utilisateurs, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Dans l'onglet Utilisateurs, sous Utilisateur, entrez le nom d'utilisateur exact et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, procédez comme suit :
 - a. Vérifiez que l'utilisateur auquel vous souhaitez accorder des autorisations administratives est spécifié.
 - b. Cochez la case située à gauche du nom d'utilisateur.
 - c. Sélectionnez Soumettre.
7. Sur la page Gérer la synchronisation, l'utilisateur que vous avez spécifié apparaît dans la liste Utilisateurs synchronisés.
8. Dans le panneau de navigation, choisissez utilisateurs.
9. Sur la page Utilisateurs, l'utilisateur que vous avez spécifié peut mettre un certain temps à apparaître dans la liste. Cliquez sur l'icône d'actualisation pour mettre à jour la liste des utilisateurs.

À ce stade, votre utilisateur n'a pas accès au compte de gestion. Vous allez configurer l'accès administratif à ce compte en créant un ensemble d'autorisations administratives et en affectant l'utilisateur à cet ensemble d'autorisations. Pour de plus amples informations, veuillez consulter [Crée un jeu d'autorisations](#).

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations utilisateur depuis CyberArk Directory Platform IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Pour de plus amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Note

CyberArk ne prend actuellement pas en charge le service de consommation d'assertions multiples (ACS) SAML URLs dans l' AWS IAM Identity Center application. Cette fonctionnalité SAML est requise pour tirer pleinement parti de la prise en [charge multirégionale](#) dans IAM Identity Center. Si vous envisagez de répliquer IAM Identity Center vers d'autres régions, sachez que l'utilisation d'une seule URL ACS peut affecter l'expérience utilisateur dans ces régions supplémentaires. Votre région principale continuera de fonctionner normalement. Nous vous recommandons de travailler avec votre fournisseur d'IdP pour activer cette fonctionnalité. Pour plus d'informations sur l'expérience utilisateur dans des régions supplémentaires dotées d'une seule URL ACS, consultez [the section called “Utilisation d'applications AWS gérées sans plusieurs ACS URLs”](#) et [the section called “Compte AWS résilience des accès sans plusieurs ACS URLs”](#).

Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord le [Considérations relatives à l'utilisation du provisionnement automatique](#). Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- [Conditions préalables](#)
- [Considérations relatives au SCIM](#)
- [Étape 1 : activer le provisionnement dans IAM Identity Center](#)
- [Étape 2 : configurer le provisionnement dans CyberArk](#)
- [\(Facultatif\) Étape 3 : Configuration des attributs utilisateur CyberArk pour le contrôle d'accès \(ABAC\) dans IAM Identity Center](#)

- [\(Facultatif\) Transmission d'attributs pour le contrôle d'accès](#)

Conditions préalables

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- CyberArkabonnement ou essai gratuit. Pour vous inscrire à un essai gratuit, rendez-vous sur [CyberArk](#).
- Un compte compatible avec IAM Identity Center ([gratuit](#)). Pour plus d'informations, voir [Activer le centre d'identité IAM](#).
- Une connexion SAML entre votre CyberArk compte et IAM Identity Center, comme décrit dans la [CyberArkdocumentation d'IAM](#) Identity Center.
- Associez le connecteur IAM Identity Center aux rôles, utilisateurs et organisations auxquels vous souhaitez autoriser l'accès Comptes AWS.

Considérations relatives au SCIM

Voici les points à prendre en compte lors de l'utilisation CyberArk de la fédération pour IAM Identity Center :

- Seuls les rôles mappés dans la section Provisioning des applications seront synchronisés avec IAM Identity Center.
- Le script de provisionnement n'est pris en charge que dans son état par défaut. Une fois modifié, le provisionnement SCIM peut échouer.
 - Un seul attribut de numéro de téléphone peut être synchronisé et l'attribut par défaut est « téléphone professionnel ».
- Si le mappage des rôles dans l'application CyberArk IAM Identity Center est modifié, le comportement ci-dessous est attendu :
 - Si les noms de rôles sont modifiés, aucune modification n'est apportée aux noms de groupes dans IAM Identity Center.
 - Si les noms des groupes sont modifiés, de nouveaux groupes seront créés dans IAM Identity Center, les anciens groupes resteront mais n'auront aucun membre.
- Le comportement de synchronisation et de déprovisionnement des utilisateurs peut être configuré à partir de l'application CyberArk IAM Identity Center. Assurez-vous de configurer le comportement adapté à votre organisation. Voici les options qui s'offrent à vous :

- Remplacez (ou non) les utilisateurs du répertoire Identity Center par le même nom principal.
- Déprovisionnez les utilisateurs du centre d'identité IAM lorsque l'utilisateur est supprimé du CyberArk rôle.
- Déprovisionner le comportement de l'utilisateur : désactiver ou supprimer.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console [IAM Identity Center](#).
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez le point de terminaison SCIM et le jeton d'accès. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
 - a. Point de terminaison SCIM : par exemple, `https://scim.us-east-2.amazonaws.com/ /scim/v2 1111111111-2222-3333-4444-555555555555`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisirez ces valeurs pour configurer le provisionnement automatique dans votre IdP plus loin dans ce didacticiel.

5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide de l'application CyberArk IAM Identity Center. Ces étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans CyberArk

Utilisez la procédure suivante dans l'application CyberArk IAM Identity Center pour activer le provisionnement avec IAM Identity Center. Cette procédure suppose que vous avez déjà ajouté l'application CyberArk IAM Identity Center à votre console CyberArk d'administration sous Web Apps. Si vous ne l'avez pas encore fait, reportez-vous au [Conditions préalables](#), puis suivez cette procédure pour configurer le provisionnement SCIM.

Pour configurer le provisionnement dans CyberArk

1. Ouvrez l'application CyberArk IAM Identity Center que vous avez ajoutée dans le cadre de la configuration de SAML pour CyberArk (Apps > Web App). Consultez [Conditions préalables](#).
2. Choisissez l'application IAM Identity Center et accédez à la section Provisioning.
3. Cochez la case Activer le provisionnement pour cette application et choisissez Live Mode.
4. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM depuis IAM Identity Center. Collez cette valeur dans le champ URL du service SCIM. Dans l'application CyberArk IAM Identity Center, définissez le type d'autorisation comme en-tête d'autorisation.
5. Définissez le type d'en-tête sur Bearer Token.
6. À partir de la procédure précédente, vous avez copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ Bearer Token de l'application CyberArk IAM Identity Center.
7. Cliquez sur Vérifier pour tester et appliquer la configuration.
8. Dans les options de synchronisation, choisissez le comportement approprié pour lequel vous souhaitez que le provisionnement sorte fonctionneCyberArk. Vous pouvez choisir de remplacer (ou non) les utilisateurs IAM Identity Center existants par un nom principal et un comportement de déprovisionnement similaires.
9. Sous Mappage des rôles, configurez le mappage à partir CyberArk des rôles, dans le champ Nom, vers le groupe IAM Identity Center, sous le groupe de destination.
10. Cliquez sur Enregistrer en bas de page une fois que vous avez terminé.
11. Pour vérifier que les utilisateurs ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs

synchronisés depuis CyberArk apparaîtront sur la page Utilisateurs. Ces utilisateurs peuvent désormais être affectés à des comptes et peuvent se connecter au sein d'IAM Identity Center.

(Facultatif) Étape 3 : Configuration des attributs utilisateur CyberArk pour le contrôle d'accès (ABAC) dans IAM Identity Center

Il s'agit d'une procédure facultative CyberArk si vous choisissez de configurer des attributs pour IAM Identity Center afin de gérer l'accès à vos AWS ressources. Les attributs que vous définissez CyberArk sont transmis dans une assertion SAML à IAM Identity Center. Vous créez ensuite un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmis CyberArk.

Avant de commencer cette procédure, vous devez d'abord activer la [Attributs pour le contrôle d'accès](#) fonctionnalité. Pour plus d'informations sur cette étape, consultez [Activer et configurer les attributs pour le contrôle d'accès](#).

Pour configurer les attributs utilisateur CyberArk pour le contrôle d'accès dans IAM Identity Center

1. Ouvrez l'application CyberArk IAM Identity Center que vous avez installée dans le cadre de la configuration de SAML pour CyberArk (Apps > Web Apps).
2. Accédez à l'option SAML Response.
3. Sous Attributs, ajoutez les attributs appropriés au tableau en suivant la logique ci-dessous :
 - a. Le nom de l'attribut est le nom d'attribut d'origine de CyberArk.
 - b. La valeur d'attribut est le nom d'attribut envoyé dans l'assertion SAML à IAM Identity Center.
4. Choisissez Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un Attribute élément dont l'Nameattribut est défini sur `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Configurer SAML et SCIM avec un IAM Google Workspace Identity Center

Si votre organisation l'utilise, Google Workspace vous pouvez intégrer vos utilisateurs depuis Google Workspace IAM Identity Center pour leur donner accès aux AWS ressources. Vous pouvez réaliser cette intégration en remplaçant la source d'identité par défaut de votre source d'identité IAM Identity Center par. Google Workspace

Note

Google Workspacene prend actuellement pas en charge le service de consommation d'assertions multiples (ACS) SAML URLs dans l' AWS IAM Identity Center application. Cette fonctionnalité SAML est requise pour tirer pleinement parti de la prise en [charge multirégionale](#) dans IAM Identity Center. Si vous envisagez de répliquer IAM Identity Center vers d'autres régions, sachez que l'utilisation d'une seule URL ACS peut affecter l'expérience utilisateur dans ces régions supplémentaires. Votre région principale continuera de fonctionner normalement. Nous vous recommandons de travailler avec votre fournisseur d'IdP pour activer cette fonctionnalité. Pour plus d'informations sur l'expérience utilisateur dans des régions supplémentaires dotées d'une seule URL ACS, consultez [the section called "Utilisation d'applications AWS gérées sans plusieurs ACS URLs"](#) et [the section called "Compte AWS résilience des accès sans plusieurs ACS URLs"](#).

Les informations utilisateur provenant de Google Workspace sont synchronisées dans IAM Identity Center à l'aide du protocole [SCIM \(System for Cross-Domain Identity Management\) 2.0](#). Pour de plus

amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Vous configurez cette connexion en Google Workspace utilisant votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec Google Workspace les attributs nommés dans IAM Identity Center. Ce mappage correspond aux attributs utilisateur attendus entre IAM Identity Center et Google Workspace. Pour ce faire, vous devez vous configurer en Google Workspace tant que fournisseur d'identité et vous connecter à votre IAM Identity Center.

Objectif

Les étapes de ce didacticiel vous aident à établir la connexion SAML entre Google Workspace et AWS. Plus tard, vous synchroniserez les utilisateurs à Google Workspace l'aide de SCIM. Pour vérifier que tout est correctement configuré, une fois les étapes de configuration terminées, vous vous connecterez en tant qu'utilisateur Google Workspace et vérifierez l'accès aux AWS ressources. Notez que ce didacticiel est basé sur un environnement de test de petits Google Workspace répertoires. Les structures de répertoires telles que les groupes et les unités organisationnelles ne sont pas incluses dans ce didacticiel. Après avoir terminé ce didacticiel, vos utilisateurs pourront accéder au portail d'AWS accès avec vos Google Workspace informations d'identification.

Note

Pour vous inscrire à un essai gratuit ou Google Workspace rendez-vous [Google Workspaces](#) sur le Google's site Web.

Si vous n'avez pas encore activé IAM Identity Center, consultez [Activer IAM Identity Center](#).

Considérations

- Avant de configurer le provisionnement SCIM entre Google Workspace et IAM Identity Center, nous vous recommandons de procéder à un premier examen. [Considérations relatives à l'utilisation du provisionnement automatique](#)
- La synchronisation automatique depuis SCIM Google Workspace est actuellement limitée au provisionnement des utilisateurs. Le provisionnement automatique des groupes n'est pas pris en charge pour le moment. Les groupes peuvent être créés manuellement à AWS CLI l'aide de la commande Identity Store [create-group](#) ou de l'API Gestion des identités et des accès AWS (IAM).

[CreateGroup](#) Vous pouvez également utiliser [ssosync](#) pour synchroniser Google Workspace les utilisateurs et les groupes dans IAM Identity Center.

- Chaque Google Workspace utilisateur doit avoir un prénom, un nom de famille, un nom d'utilisateur et une valeur de nom d'affichage spécifiés.
- Chaque Google Workspace utilisateur ne dispose que d'une seule valeur par attribut de données, tel qu'une adresse e-mail ou un numéro de téléphone. Les utilisateurs possédant plusieurs valeurs ne parviendront pas à se synchroniser. Si certains utilisateurs ont plusieurs valeurs dans leurs attributs, supprimez les attributs dupliqués avant de tenter de configurer l'utilisateur dans IAM Identity Center. Par exemple, un seul attribut de numéro de téléphone peut être synchronisé, étant donné que l'attribut de numéro de téléphone par défaut est « téléphone professionnel », utilisez l'attribut « téléphone professionnel » pour stocker le numéro de téléphone de l'utilisateur, même si le numéro de téléphone de l'utilisateur est un téléphone fixe ou un téléphone mobile.
- Les attributs sont toujours synchronisés si l'utilisateur est désactivé dans IAM Identity Center, mais toujours actif dans Google Workspace
- Si un utilisateur existe déjà dans le répertoire Identity Center avec le même nom d'utilisateur et le même e-mail, il sera remplacé et synchronisé à l'aide de SCIM from Google Workspace
- Des considérations supplémentaires doivent être prises en compte lors de la modification de votre source d'identité. Pour de plus amples informations, veuillez consulter [the section called “Passage d'IAM Identity Center à un IdP externe”](#).

Étape 1 Google Workspace : Configuration de l'application SAML

1. Connectez-vous à votre console d'Googleadministration à l'aide d'un compte doté de privilèges de super administrateur.
2. Dans le panneau de navigation de gauche de votre console Google d'administration, sélectionnez Applications, puis Applications Web et mobiles.
3. Dans la liste déroulante Ajouter une application, sélectionnez Rechercher des applications.
4. Dans le champ de recherche, saisissez Amazon Web Services, puis sélectionnez l'application Amazon Web Services (SAML) dans la liste.
5. Sur la page Informations sur le fournisseur d'Googleidentité - Amazon Web Services, vous pouvez effectuer l'une des opérations suivantes :
 - a. Téléchargez les métadonnées de l'IdP.
 - b. Copiez l'URL SSO, l'URL de l'identifiant de l'entité et les informations du certificat.

Vous aurez besoin du fichier XML ou des informations d'URL à l'étape 2.

6. Avant de passer à l'étape suivante dans la console Google d'administration, laissez cette page ouverte et passez à la console IAM Identity Center.

Étape 2 : IAM Identity Center et Google Workspace : Modification de la source d'identité IAM Identity Center et configuration en Google Workspace tant que fournisseur d'identité SAML

1. Connectez-vous à la [console IAM Identity Center](#) à l'aide d'un rôle doté d'autorisations administratives.
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, choisissez Actions, puis Modifier la source d'identité.
 - Si vous n'avez pas activé IAM Identity Center, consultez [Activer IAM Identity Center](#) pour plus d'informations. Après avoir activé et accédé à IAM Identity Center pour la première fois, vous arriverez au tableau de bord où vous pourrez sélectionner Choisissez votre source d'identité.
4. Sur la page Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
5. La page Configurer le fournisseur d'identité externe s'ouvre. Pour compléter cette page et celle de l'Google Workspaceétape 1, vous devez effectuer les opérations suivantes :
 - Dans la section des métadonnées du fournisseur d'identité de la console IAM Identity Center, vous devez effectuer l'une des opérations suivantes :
 - i. Téléchargez les métadonnées GoogleSAML en tant que métadonnées IDP SAML dans la console IAM Identity Center.
 - ii. Copiez et collez l'URL GoogleSSO dans le champ URL de connexion de l'IdP Google, l'URL de l'émetteur dans le champ URL de l'émetteur de l'IdP et téléchargez le certificat en tant que certificat IdP. Google
6. Après avoir fourni les Google métadonnées dans la section des métadonnées du fournisseur d'identité de la console IAM Identity Center, copiez l'URL du IAM Identity Assertion Consumer Service (ACS) et l'URL de l'émetteur du IAM Identity Center. Vous devrez les fournir URLs dans la console Google d'administration à l'étape suivante.

7. Laissez la page ouverte avec la console IAM Identity Center et revenez à la console Google d'administration. Vous devriez être sur la page de détails d'Amazon Web Services - Service Provider. Sélectionnez Continuer.
8. Sur la page de détails du fournisseur de services, entrez les valeurs de l'URL ACS et de l'ID d'entité. Vous avez copié ces valeurs à l'étape précédente et elles se trouvent dans la console IAM Identity Center.
 - Collez l'URL du IAM Identity Center Assertion Consumer Service (ACS) dans le champ URL ACS
 - Collez l'URL de l'émetteur du IAM Identity Center dans le champ Entity ID.
9. Sur la page de détails du fournisseur de services, complétez les champs sous le nom ID comme suit :
 - Pour le format du nom et de l'identifiant, sélectionnez EMAIL
 - Pour Name ID, sélectionnez Informations de base > E-mail principal
10. Sélectionnez Continuer.
11. Sur la page Mappage d'attributs, sous Attributs, choisissez AJOUTER UN MAPPAGE, puis configurez les champs suivants sous Attribut de Google répertoire :
 - Pour l'attribut de l'**`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**application, sélectionnez le champ Informations de base, e-mail principal dans les Google Directoryattributs.
 - Pour l'attribut de **`https://aws.amazon.com/SAML/Attributes/Role`** l'application, sélectionnez n'importe quel Google Directoryattribut. Un attribut de Google répertoire peut être Department.
12. Choisissez Finish
13. Revenez à la console IAM Identity Center et choisissez Next. Sur la page Vérifier et confirmer, passez en revue les informations, puis saisissez ACCEPT dans l'espace prévu à cet effet. Choisissez Modifier la source d'identité.

Vous êtes maintenant prêt à activer l'application Amazon Web Services Google Workspace afin que vos utilisateurs puissent être connectés à IAM Identity Center.

Étape 3 Google Workspace : Activez les applications

1. Retournez à la console Google d'administration et à votre AWS IAM Identity Center application, qui se trouvent sous Applications et applications Web et mobiles.
2. Dans le panneau Accès utilisateur situé à côté de Accès utilisateur, cliquez sur la flèche vers le bas pour étendre l'accès utilisateur afin d'afficher le panneau d'état du service.
3. Dans le panneau d'état du service, sélectionnez Activé pour tout le monde, puis sélectionnez ENREGISTRER.

Note

Pour respecter le principe du moindre privilège, nous vous recommandons de changer le statut du service sur OFF pour tous après avoir terminé ce didacticiel. Le service AWS doit être activé uniquement pour les utilisateurs ayant besoin d'un accès. Vous pouvez utiliser Google Workspace des groupes ou des unités organisationnelles pour donner aux utilisateurs l'accès à un sous-ensemble particulier de vos utilisateurs.

Étape 4 : IAM Identity Center : configurer le provisionnement automatique d'IAM Identity Center

1. Retournez à la console IAM Identity Center.
2. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
3. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. À l'étape 5 de ce didacticiel, vous allez entrer ces valeurs pour configurer le provisionnement automatique dans Google Workspace.
 - a. Point de terminaison SCIM - Par exemple,
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`

- Double pile `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`

b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

 Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer.

4. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, à l'étape suivante, vous allez configurer le provisionnement automatique dans Google Workspace

Étape 5 Google Workspace : Configuration du provisionnement automatique

1. Retournez à la console Google d'administration et à votre AWS IAM Identity Center application, qui se trouvent sous Applications et applications Web et mobiles. Dans la section Approvisionnement automatique, choisissez Configurer le provisionnement automatique.
2. Dans la procédure précédente, vous avez copié la valeur du jeton d'accès dans la console IAM Identity Center. Collez cette valeur dans le champ du jeton d'accès et choisissez Continuer. Dans la procédure précédente, vous avez également copié la valeur du point de terminaison SCIM dans la console IAM Identity Center. Collez cette valeur dans le champ URL du point de terminaison et choisissez Continuer.
3. Vérifiez que tous les attributs obligatoires du centre d'identité IAM (ceux marqués d'un *) sont mappés aux Google Cloud Directory attributs. Si ce n'est pas le cas, cliquez sur la flèche vers le bas et mappez vers l'attribut approprié. Sélectionnez Continuer.
4. Dans la section Provisioning Scope, vous pouvez choisir un groupe avec votre Google Workspace annuaire pour fournir un accès à l'application Amazon Web Services. Ignorez cette étape et sélectionnez Continuer.
5. Dans la section Déprovisionnement, vous pouvez choisir comment répondre aux différents événements qui suppriment l'accès à un utilisateur. Pour chaque situation, vous pouvez spécifier le délai avant le début du déprovisionnement afin de :

- dans les 24 heures
- après une journée
- après sept jours
- après 30 jours

Chaque situation est assortie d'un délai pour suspendre l'accès à un compte et quand supprimer le compte.

 Tip

Prévoyez toujours plus de temps avant de supprimer le compte d'un utilisateur que pour le suspendre.

6. Choisissez Finish (Terminer). Vous êtes redirigé vers la page de l'application Amazon Web Services.
7. Dans la section Provisionnement automatique, activez le commutateur pour le faire passer d'Inactif à Actif.

 Note

Le curseur d'activation est désactivé si IAM Identity Center n'est pas activé pour les utilisateurs. Choisissez Accès utilisateur et activez l'application pour activer le curseur.

8. Dans la boîte de dialogue de confirmation, choisissez Activer.
9. Pour vérifier que les utilisateurs sont correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. La page Utilisateurs répertorie les utilisateurs de votre Google Workspace répertoire qui ont été créés par SCIM. Si les utilisateurs ne figurent pas encore dans la liste, il se peut que le provisionnement soit toujours en cours. Le provisionnement peut prendre jusqu'à 24 heures, mais dans la plupart des cas, il ne prend que quelques minutes. Assurez-vous d'actualiser la fenêtre du navigateur toutes les quelques minutes.

Sélectionnez un utilisateur et consultez ses informations. Les informations doivent correspondre à celles du Google Workspace répertoire.

Félicitations !

Vous avez correctement configuré une connexion SAML entre Google Workspace et AWS et vous avez vérifié que le provisionnement automatique fonctionne. Vous pouvez désormais attribuer ces utilisateurs à des comptes et à des applications dans IAM Identity Center. Dans le cadre de ce didacticiel, à l'étape suivante, désignons l'un des utilisateurs comme administrateur du centre d'identité IAM en lui accordant des autorisations administratives sur le compte de gestion.

Transmission d'attributs pour le contrôle d'accès - Facultatif

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name` attribut est défini sur `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Attribuez l'accès à Comptes AWS

Les étapes suivantes ne sont requises que pour accorder l'accès à Comptes AWS . Ces étapes ne sont pas obligatoires pour autoriser l'accès aux AWS applications.

 Note

Pour effectuer cette étape, vous aurez besoin d'une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Étape 1 : IAM Identity Center : accordez aux Google Workspace utilisateurs l'accès aux comptes

1. Retournez à la console IAM Identity Center. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWSpage, la structure organisationnelle affiche la racine de votre organisation avec vos comptes en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il se compose de trois étapes :
 - a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez l'utilisateur qui exécutera la fonction d'administrateur. Ensuite, sélectionnez Suivant.
 - b. Pour l'étape 2 : Sélectionnez des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous indique les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.
 - i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :
 - Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.
 - Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.Choisissez Suivant.
 - ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *AdministratorAccess* avec une durée de session fixée à une heure.

- iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée `AdministratorAccess`. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.
 - iv. Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.
 - v. Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble `AdministratorAccess` d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.
- c. Pour l'étape 3 : vérifier et envoyer, passez en revue l'utilisateur et l'ensemble d'autorisations sélectionnés, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Patientez jusqu'à ce que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations mis à jour a été appliqué. Lorsque l'utilisateur se connecte, il a la possibilité de choisir le `AdministratorAccess` rôle.

 Note

La synchronisation automatique SCIM depuis Google Workspace ne prend en charge que le provisionnement des utilisateurs. Le provisionnement automatique des groupes n'est pas pris en charge pour le moment. Vous ne pouvez pas créer de groupes pour vos Google Workspace utilisateurs à l'aide du AWS Management Console. Après avoir configuré les utilisateurs, vous pouvez créer des groupes à l'aide de la commande AWS CLI Identity Store [create-group](#) ou de l'API IAM. [CreateGroup](#)

Étape 2 Google Workspace : Confirmer l'accès Google Workspace des utilisateurs aux AWS ressources

1. Connectez-vous à Google l'aide d'un compte utilisateur de test. Pour savoir comment ajouter des utilisateurs Google Workspace, consultez [Google Workspacela documentation](#).
2. Sélectionnez l'icône du Google apps lanceur (gaufre).
3. Faites défiler la liste des applications vers le bas où se trouvent vos Google Workspace applications personnalisées. L'application Amazon Web Services s'affiche.
4. Sélectionnez l'application Amazon Web Services. Vous êtes connecté au portail AWS d'accès et vous pouvez voir l' Compte AWS icône. Développez cette icône pour voir la liste des Comptes AWS objets auxquels l'utilisateur peut accéder. Dans ce didacticiel, vous n'avez travaillé qu'avec un seul compte. Par conséquent, l'extension de l'icône ne permet d'afficher qu'un seul compte.
5. Sélectionnez le compte pour afficher les ensembles d'autorisations disponibles pour l'utilisateur. Dans ce didacticiel, vous avez créé l'ensemble AdministratorAccessd'autorisations.
6. À côté de l'ensemble d'autorisations se trouvent des liens indiquant le type d'accès disponible pour cet ensemble d'autorisations. Lorsque vous avez créé l'ensemble d'autorisations, vous avez indiqué que la console de gestion et l'accès par programmation devaient être activés. Ces deux options sont donc présentes. Sélectionnez Console de gestion pour ouvrir le AWS Management Console.
7. L'utilisateur est connecté à la console.

Étapes suivantes

Maintenant que vous avez configuré Google Workspace en tant que fournisseur d'identité et que vous avez configuré les utilisateurs dans IAM Identity Center, vous pouvez :

- Utilisez la commande AWS CLI Identity Store [create-group](#) ou l'API IAM [CreateGroup](#) pour créer des groupes pour vos utilisateurs.

Les groupes sont utiles lors de l'attribution de l'accès aux applications Comptes AWS et de leur attribution. Plutôt que d'affecter chaque utilisateur individuellement, vous accordez des autorisations à un groupe. Plus tard, lorsque vous ajoutez ou supprimez des utilisateurs d'un groupe, l'utilisateur obtient ou perd l'accès dynamique aux comptes et aux applications que vous avez affectés au groupe.

- Configurez les autorisations en fonction des fonctions du travail, voir [Création d'un ensemble d'autorisations](#).

Les ensembles d'autorisations définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Les ensembles d'autorisations sont stockés dans IAM Identity Center et peuvent être fournis à une ou plusieurs personnes. Comptes AWS Vous pouvez attribuer plus d'un jeu d'autorisations à un utilisateur.

Note

En tant qu'administrateur du centre d'identité IAM, vous devrez parfois remplacer les anciens certificats IdP par des certificats plus récents. Par exemple, il se peut que vous deviez remplacer un certificat IdP lorsque la date d'expiration du certificat approche. Le processus de remplacement d'un ancien certificat par un nouveau est appelé rotation des certificats. Assurez-vous de vérifier comment [gérer les certificats SAML](#) pour Google Workspace.

Résolution des problèmes

Pour le dépannage général des systèmes SCIM et SAML Google Workspace, consultez les sections suivantes :

- [Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe](#)
- [Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center](#)
- [Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe](#)
- Pour le Google Workspace dépannage, consultez [Google Workspacela documentation](#).

Les ressources suivantes peuvent vous aider à résoudre les problèmes lorsque vous travaillez avec AWS :

- [AWS re:Post](#)- Trouvez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- [AWS Support](#)- Bénéficiez d'un support technique

Utilisation d'IAM Identity Center pour vous connecter à votre plateforme d'JumpCloudannuaire

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations utilisateur depuis JumpCloud Directory Platform vers IAM Identity Center. Ce provisionnement utilise le protocole [SAML \(Security Assertion Markup Language\) 2.0](#). Pour de plus amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Vous configurez cette connexion à JumpCloud l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec JumpCloud les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et JumpCloud.

Ce guide est basé sur JumpCloud la version de juin 2021. Les étapes à suivre pour les nouvelles versions peuvent varier. Ce guide contient quelques remarques concernant la configuration de l'authentification des utilisateurs via SAML.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs et des groupes depuis IAM Identity Center JumpCloud à l'aide du protocole SCIM.

Note

Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord le [Considérations relatives à l'utilisation du provisionnement automatique](#). Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- [Conditions préalables](#)
- [Considérations relatives au SCIM](#)
- [Étape 1 : activer le provisionnement dans IAM Identity Center](#)
- [Étape 2 : configurer le provisionnement dans JumpCloud](#)
- [\(Facultatif\) Étape 3 : Configuration des attributs utilisateur JumpCloud pour le contrôle d'accès dans IAM Identity Center](#)
- [\(Facultatif\) Transmission d'attributs pour le contrôle d'accès](#)

Conditions préalables

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- JumpCloudabonnement ou essai gratuit. Pour vous inscrire à un essai gratuit, rendez-vous sur [JumpCloud](#).
- Un compte compatible avec IAM Identity Center ([gratuit](#)). Pour plus d'informations, voir [Activer le centre d'identité IAM](#).
- Une connexion SAML entre votre JumpCloud compte et IAM Identity Center, comme décrit dans la [JumpClouddocumentation d'IAM](#) Identity Center.
- Si vous avez répliqué IAM Identity Center vers des régions supplémentaires, vous devez mettre à jour la configuration de votre fournisseur d'identité pour permettre l'accès aux applications AWS gérées et à Comptes AWS partir de ces régions. Pour en savoir plus, consultez [the section called "Étape 3 : Mettre à jour la configuration de l'IdP externe"](#). Consultez la JumpCloud documentation pour plus de détails.
- Associez le connecteur IAM Identity Center aux groupes auxquels vous souhaitez autoriser l'accès aux AWS comptes.

Considérations relatives au SCIM

Les points suivants sont à prendre en compte lors de l'utilisation JumpCloud de la fédération pour IAM Identity Center.

- Seuls les groupes associés au connecteur AWS Single Sign-On JumpCloud seront synchronisés avec SCIM.
- Un seul attribut de numéro de téléphone peut être synchronisé et l'attribut par défaut est « téléphone professionnel ».
- Les noms et prénoms des utilisateurs de l'JumpCloudannuaire doivent être configurés pour être synchronisés avec IAM Identity Center avec SCIM.
- Les attributs sont toujours synchronisés si l'utilisateur est désactivé dans IAM Identity Center mais qu'il est toujours activé. JumpCloud
- Vous pouvez choisir d'activer la synchronisation SCIM uniquement pour les informations utilisateur en décochant la case « Activer la gestion des groupes d'utilisateurs et de l'appartenance aux groupes » dans le connecteur.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console [IAM Identity Center](#).
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez le point de terminaison SCIM et le jeton d'accès. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
 - a. Point de terminaison SCIM : par exemple, `https://scim.us-east-2.amazonaws.com/ /scim/v2 1111111111-2222-3333-4444-555555555555`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisirez ces valeurs pour configurer le provisionnement automatique dans votre IdP plus loin dans ce didacticiel.

5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide du connecteur JumpCloud IAM Identity Center. Ces étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans JumpCloud

Utilisez la procédure suivante dans le connecteur JumpCloud IAM Identity Center pour activer le provisionnement avec IAM Identity Center. Cette procédure suppose que vous avez déjà ajouté le connecteur JumpCloud IAM Identity Center à votre portail d'JumpCloudadministration et à vos groupes. Si vous ne l'avez pas encore fait, reportez-vous à cette procédure [Conditions préalables](#), puis exécutez-la pour configurer le provisionnement SCIM.

Pour configurer le provisionnement dans JumpCloud

1. Ouvrez le connecteur JumpCloud IAM Identity Center que vous avez installé dans le cadre de la configuration de SAML pour JumpCloud (Authentification utilisateur > IAM Identity Center). Consultez [Conditions préalables](#).
2. Choisissez le connecteur IAM Identity Center, puis le troisième onglet Gestion des identités.
3. Cochez la case Activer la gestion des groupes d'utilisateurs et de l'appartenance aux groupes dans cette application si vous souhaitez que les groupes soient synchronisés avec SCIM.
4. Cliquez sur Configurer.
5. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL de base du connecteur JumpCloud IAM Identity Center.
6. À partir de la procédure précédente, vous avez copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ Token Key du connecteur JumpCloud IAM Identity Center.
7. Cliquez sur Activer pour appliquer la configuration.
8. Assurez-vous d'avoir un indicateur vert à côté de l'authentification unique activée.
9. Passez au quatrième onglet Groupes d'utilisateurs et cochez les groupes que vous souhaitez approvisionner avec SCIM.
10. Cliquez sur Enregistrer en bas de page une fois que vous avez terminé.
11. Pour vérifier que les utilisateurs ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés JumpCloud apparaissent sur la page Utilisateurs. Ces utilisateurs peuvent désormais être affectés à des comptes au sein d'IAM Identity Center.

(Facultatif) Étape 3 : Configuration des attributs utilisateur JumpCloud pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative JumpCloud si vous choisissez de configurer des attributs pour IAM Identity Center afin de gérer l'accès à vos AWS ressources. Les attributs que vous définissez JumpCloud sont transmis dans une assertion SAML à IAM Identity Center. Vous créez ensuite un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmis JumpCloud.

Avant de commencer cette procédure, vous devez d'abord activer la fonctionnalité [Attributs pour le contrôle d'accès](#). Pour plus d'informations sur la procédure à suivre, voir [Activer et configurer les attributs pour le contrôle d'accès](#).

Pour configurer les attributs utilisateur JumpCloud pour le contrôle d'accès dans IAM Identity Center

1. Ouvrez le connecteur JumpCloud IAM Identity Center que vous avez installé dans le cadre de la configuration de SAML pour JumpCloud (Authentification utilisateur > IAM Identity Center).
2. Choisissez le connecteur IAM Identity Center. Choisissez ensuite le deuxième onglet IAM Identity Center.
3. Au bas de cet onglet, vous trouverez le mappage des attributs utilisateur. Choisissez Ajouter un nouvel attribut, puis procédez comme suit : vous devez effectuer ces étapes pour chaque attribut que vous allez ajouter afin de l'utiliser dans IAM Identity Center à des fins de contrôle d'accès.
 - a. Dans le champ Nom de l'attribut du fournisseur de services, saisissez `https://aws.amazon.com/SAML/Attributes/AccessControl: AttributeName`. Remplacer **AttributeName** par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl: Email` .
 - b. Dans le champ Nom de JumpCloud l'attribut, sélectionnez les attributs utilisateur de votre JumpCloud répertoire. Par exemple, Email (Work).
4. Choisissez Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Nameattribut` est défini sur. `https://`

`aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Configurer SAML et SCIM avec un IAM Microsoft Entra ID Identity Center

AWS IAM Identity Center prend en charge l'intégration avec le [langage SAML \(Security Assertion Markup Language\) 2.0](#) ainsi que le [provisionnement automatique](#) (synchronisation) des informations sur les utilisateurs et les groupes Microsoft Entra ID (anciennement connu sous le nom de Azure Active Directory ou Azure AD) dans IAM Identity Center à l'aide du protocole [System for Cross-domain Identity Management \(SCIM\) 2.0](#). Pour de plus amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Objectif

Dans ce didacticiel, vous allez configurer un laboratoire de test et configurer une connexion SAML et un provisionnement SCIM entre IAM Identity Center Microsoft Entra ID et IAM. Au cours des étapes de préparation initiales, vous allez créer un utilisateur de test (Nikki Wolf) à la fois Microsoft Entra ID dans IAM Identity Center, que vous utiliserez pour tester la connexion SAML dans les deux sens. Plus tard, dans le cadre des étapes SCIM, vous créerez un autre utilisateur de test (Richard Roe) pour vérifier que les nouveaux attributs Microsoft Entra ID sont synchronisés avec IAM Identity Center comme prévu.

Conditions préalables

Avant de commencer ce didacticiel, vous devez d'abord configurer les éléments suivants :

- Un Microsoft Entra ID locataire. Pour plus d'informations, voir [Démarrage rapide : configurer un locataire](#) dans Microsoft la documentation.
- Un compte AWS IAM Identity Center activé. Pour plus d'informations, voir [Activer le centre d'identité IAM](#) dans le guide de l'AWS IAM Identity Center utilisateur.

Considérations

Voici quelques considérations importantes Microsoft Entra ID qui peuvent affecter la manière dont vous prévoyez de mettre en œuvre le [provisionnement automatique](#) avec IAM Identity Center dans votre environnement de production à l'aide du protocole SCIM v2.

Provisionnement automatique

Avant de commencer à déployer le SCIM, nous vous recommandons de procéder à un premier examen [Considérations relatives à l'utilisation du provisionnement automatique](#).

Attributs pour le contrôle d'accès

Les attributs de contrôle d'accès sont utilisés dans les politiques d'autorisation qui déterminent qui, dans votre source d'identité, peut accéder à vos AWS ressources. Si un attribut est supprimé d'un utilisateur dans Microsoft Entra ID, cet attribut ne sera pas supprimé de l'utilisateur correspondant dans IAM Identity Center. Il s'agit d'une limitation connue dans Microsoft Entra ID. Si un attribut est remplacé par une valeur différente (non vide) pour un utilisateur, cette modification sera synchronisée avec IAM Identity Center.

Groupes imbriqués

Le service de provisionnement des Microsoft Entra ID utilisateurs ne peut ni lire ni approvisionner les utilisateurs dans des groupes imbriqués. Seuls les utilisateurs qui sont membres immédiats d'un groupe explicitement assigné peuvent être lus et approvisionnés. Microsoft Entra ID ne décompresse pas de manière récursive les appartenances aux groupes ou utilisateurs assignés indirectement (utilisateurs ou groupes membres d'un groupe directement attribué). Pour plus d'informations, consultez la section [Délimitation basée sur les assignations dans la documentation](#). Microsoft Vous pouvez également utiliser la [synchronisation AD configurable d'IAM Identity Center](#) pour intégrer Active Directory des groupes à IAM Identity Center.

Groupes dynamiques

Le service de provisionnement des Microsoft Entra ID utilisateurs peut lire et provisionner les utilisateurs dans des [groupes dynamiques](#). Vous trouverez ci-dessous un exemple illustrant la structure des utilisateurs et des groupes lors de l'utilisation de groupes dynamiques et la manière dont ils sont affichés dans IAM Identity Center. Ces utilisateurs et groupes ont été approvisionnés depuis Microsoft Entra ID IAM Identity Center via SCIM.

Par exemple, si Microsoft Entra ID la structure des groupes dynamiques est la suivante :

1. Groupe A avec les membres ua1, ua2
2. Groupe B avec membres ub1
3. Groupe C avec membres uc1
4. Groupe K avec une règle pour inclure les membres des groupes A, B, C
5. Groupe L avec une règle pour inclure les membres des groupes B et C

Une fois que les informations sur les utilisateurs et les groupes ont été Microsoft Entra ID fournies depuis IAM Identity Center via SCIM, la structure sera la suivante :

1. Groupe A avec les membres ua1, ua2
2. Groupe B avec membres ub1
3. Groupe C avec membres uc1
4. Groupe K avec les membres ua1, ua2, ub1, uc1
5. Groupe L avec membres ub1, uc1

Lorsque vous configurez le provisionnement automatique à l'aide de groupes dynamiques, tenez compte des considérations suivantes.

- Un groupe dynamique peut inclure un groupe imbriqué. Cependant, le service de Microsoft Entra ID provisionnement n'aplatit pas le groupe imbriqué. Par exemple, si vous avez la Microsoft Entra ID structure suivante pour les groupes dynamiques :
 - Le groupe A est le parent du groupe B.
 - Le groupe A compte ua1 comme membre.
 - Le groupe B a ub1 comme membre.

Le groupe dynamique qui inclut le groupe A inclura uniquement les membres directs du groupe A (c'est-à-dire ua1). Il n'inclura pas de manière récursive les membres du groupe B.

- Les groupes dynamiques ne peuvent pas contenir d'autres groupes dynamiques. Pour plus d'informations, consultez la section [Limitations relatives à la prévisualisation](#) dans la Microsoft documentation.

Étape 1 : préparer votre client Microsoft

Au cours de cette étape, vous allez découvrir comment installer et configurer votre application AWS IAM Identity Center d'entreprise et comment attribuer l'accès à un nouvel utilisateur de Microsoft Entra ID test.

Step 1.1 >

Étape 1.1 : Configuration de l'application AWS IAM Identity Center d'entreprise dans Microsoft Entra ID

Dans cette procédure, vous allez installer l'application AWS IAM Identity Center d'entreprise dans Microsoft Entra ID. Vous aurez besoin de cette application ultérieurement pour configurer votre connexion SAML avec AWS.

1. Connectez-vous au [centre d'administration Microsoft Entra](#) en tant qu'administrateur d'applications cloud au moins.
2. Accédez à Identité > Applications > Applications d'entreprise, puis sélectionnez Nouvelle application.
3. Sur la page Parcourir la galerie Microsoft Entra, entrez **AWS IAM Identity Center** dans le champ de recherche.
4. Sélectionnez AWS IAM Identity Center l'un des résultats.
5. Choisissez Créer.

Step 1.2 >

Étape 1.2 : créer un utilisateur de test dans Microsoft Entra ID

Nikki Wolf est le nom de l'utilisateur de Microsoft Entra ID test que vous allez créer dans cette procédure.

1. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Utilisateurs > Tous les utilisateurs.
2. Sélectionnez Nouvel utilisateur, puis choisissez Créer un nouvel utilisateur en haut de l'écran.
3. Dans Nom d'utilisateur principal, entrez **NikkiWolf**, puis sélectionnez le domaine et l'extension de votre choix. Par exemple, NikkiWolf@*example.org*.
4. Dans Nom d'affichage, entrez **NikkiWolf**.
5. Dans Mot de passe, entrez un mot de passe fort ou sélectionnez l'icône en forme d'œil pour afficher le mot de passe généré automatiquement, puis copiez ou notez la valeur affichée.
6. Choisissez Propriétés, dans Prénom, entrez **Nikki**. Dans Nom de famille, entrez **Wolf**.
7. Choisissez Réviser + créer, puis sélectionnez Créer.

Step 1.3

Étape 1.3 : Testez l'expérience de Nikki avant d'attribuer ses autorisations à AWS IAM Identity Center

Au cours de cette procédure, vous allez vérifier ce que Nikki peut connecter avec succès à son [portail Microsoft My Account](#).

1. Dans le même navigateur, ouvrez un nouvel onglet, accédez à la page de connexion au [portail Mon compte](#) et saisissez l'adresse e-mail complète de Nikki. Par exemple, NikkiWolf@*example.org*.
2. Lorsque vous y êtes invité, entrez le mot de passe de Nikki, puis choisissez Se connecter. S'il s'agit d'un mot de passe généré automatiquement, vous serez invité à le modifier.
3. Sur la page Action requise, choisissez Demander plus tard pour ignorer l'invite à utiliser des méthodes de sécurité supplémentaires.
4. Sur la page Mon compte, dans le volet de navigation de gauche, sélectionnez Mes applications. Notez qu'à part les compléments, aucune application n'est affichée pour le moment. Vous allez ajouter une AWS IAM Identity Center application qui apparaîtra ici lors d'une étape ultérieure.

Step 1.4

Étape 1.4 : Attribuer des autorisations à Nikki dans Microsoft Entra ID

Maintenant que vous avez vérifié que Nikki peut accéder correctement au portail Mon compte, suivez cette procédure pour attribuer son utilisateur à l'AWS IAM Identity Center application.

1. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Applications > Applications d'entreprise, puis AWS IAM Identity Center choisissez dans la liste.
2. Sur la gauche, sélectionnez Utilisateurs et groupes.
3. Choisissez Add user/group (Ajouter un utilisateur/groupe). Vous pouvez ignorer le message indiquant que les groupes ne sont pas disponibles pour l'attribution. Ce didacticiel n'utilise pas de groupes pour les devoirs.
4. Sur la page Ajouter une attribution, sous Utilisateurs, sélectionnez Aucune sélection.
5. Sélectionnez NikkiWolf, puis sélectionnez Sélectionner.
6. Sur la page Ajouter une affectation, choisissez Attribuer. NikkiWolf apparaît désormais dans la liste des utilisateurs assignés à l'AWS IAM Identity Center application.

Étape 2 : Préparez votre AWS compte

Au cours de cette étape, vous découvrirez comment configurer les autorisations IAM Identity Center d'accès (via un ensemble d'autorisations), créer manuellement un utilisateur Nikki Wolf correspondant et lui attribuer les autorisations nécessaires pour administrer les ressources dans AWS.

Step 2.1 >

Étape 2.1 : Création d'un ensemble d' RegionalAdmin autorisations dans IAM Identity Center

Cet ensemble d'autorisations sera utilisé pour accorder à Nikki les autorisations de AWS compte nécessaires pour gérer les régions depuis la page Compte du AWS Management Console. Toutes les autres autorisations permettant de consulter ou de gérer d'autres informations relatives au compte de Nikki sont refusées par défaut.

1. Ouvrez la [console IAM Identity Center](#).
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez Create permission set (Créer un jeu d'autorisations).
4. Sur la page Sélectionner le type d'ensemble d'autorisations, sélectionnez Ensemble d'autorisations personnalisé, puis cliquez sur Suivant.

5. Sélectionnez Stratégie intégrée pour l'étendre, puis créez une politique pour l'ensemble d'autorisations en suivant les étapes suivantes :
 - a. Choisissez Ajouter une nouvelle déclaration pour créer une déclaration de politique.
 - b. Sous Modifier le relevé, sélectionnez Compte dans la liste, puis cochez les cases suivantes.
 - **ListRegions**
 - **GetRegionOptStatus**
 - **DisableRegion**
 - **EnableRegion**
 - c. À côté de Ajouter une ressource, choisissez Ajouter.
 - d. Sur la page Ajouter une ressource, sous Type de ressource, sélectionnez Toutes les ressources, puis choisissez Ajouter une ressource. Vérifiez que votre politique ressemble à ce qui suit :

```
{
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "account:ListRegions",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetRegionOptStatus"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Choisissez Suivant.
7. Sur la page Spécifier les détails de l'ensemble d'autorisations, sous Nom du jeu d'autorisations **RegionalAdmin**, entrez, puis choisissez Suivant.
8. Sur la page Review and create (Vérifier et créer), choisissez Create (Créer). Vous devriez RegionalAdmin apparaître dans la liste des ensembles d'autorisations.

Step 2.2 >

Étape 2.2 : créer un NikkiWolf utilisateur correspondant dans IAM Identity Center

Étant donné que le protocole SAML ne fournit aucun mécanisme permettant d'interroger l'IdP Microsoft Entra ID () et de créer automatiquement des utilisateurs ici dans IAM Identity Center, utilisez la procédure suivante pour créer manuellement un utilisateur dans IAM Identity Center qui reflète les principaux attributs de l'utilisateur Nikki Wolfs dans Microsoft Entra ID

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Utilisateurs, choisissez Ajouter un utilisateur, puis fournissez les informations suivantes :
 - a. Pour le nom d'utilisateur et l'adresse e-mail : entrez le même **NikkiWolf@**
yourcompanydomain.extension que celui que vous avez utilisé lors de la création de votre Microsoft Entra ID utilisateur. Par exemple, NikkiWolf@***example.org***.
 - b. Confirmer l'adresse e-mail — Entrez à nouveau l'adresse e-mail de l'étape précédente
 - c. Prénom — Entrez **Nikki**
 - d. Nom de famille — Entrez **Wolf**
 - e. Nom d'affichage — Entrez **Nikki Wolf**
3. Choisissez Suivant deux fois, puis sélectionnez Ajouter un utilisateur.
4. Sélectionnez Fermer.

Step 2.3

Étape 2.3 : Attribuer Nikki aux RegionalAdmin autorisations définies dans IAM Identity Center

Vous trouvez ici les régions Compte AWS dans lesquelles Nikki administrera les régions, puis vous lui attribuez les autorisations nécessaires pour qu'elle puisse accéder correctement au portail AWS d'accès.

1. Ouvrez la [console IAM Identity Center](#).
2. Sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Cochez la case à côté du nom du compte (par exemple, ***Sandbox***) auquel vous souhaitez accorder à Nikki l'accès pour gérer les régions, puis choisissez Attribuer des utilisateurs et des groupes.

4. Sur la page Attribuer des utilisateurs et des groupes, choisissez l'onglet Utilisateurs, recherchez et cochez la case à côté de Nikki, puis choisissez Suivant.
5.
Example

<caption>On the Sélectionnez les ensembles d'autorisations page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Suivant.</caption>
6. Sur la page Révision et envoi, passez en revue vos sélections, puis choisissez Soumettre.

Étape 3 : configurer et tester votre connexion SAML

Au cours de cette étape, vous configurez votre connexion SAML à l'aide de l'application AWS IAM Identity Center d'entreprise Microsoft Entra ID ainsi que des paramètres IdP externes dans IAM Identity Center.

Step 3.1 >

Étape 3.1 : Collecter les métadonnées des fournisseurs de services requises auprès d'IAM Identity Center

Au cours de cette étape, vous lancerez l'assistant de modification de la source d'identité depuis la console IAM Identity Center et récupérerez le fichier de métadonnées et l'URL de connexion AWS spécifique que vous devrez saisir lors de la configuration de la connexion Microsoft Entra ID à l'étape suivante.

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Modifier la source d'identité.
3. Sur la page Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
4. Sur la page Configurer le fournisseur d'identité externe, sous Métadonnées du fournisseur de services, choisissez Default IPv4 ou Dual-Stack. Vous pouvez télécharger le fichier de métadonnées du fournisseur de services après avoir effectué le changement de source d'identité.
5. Dans la même section, recherchez la valeur de l'URL de connexion AWS au portail d'accès et copiez-la. Vous devrez saisir cette valeur lorsque vous y serez invité à l'étape suivante.

6. Laissez cette page ouverte et passez à l'étape suivante (**Step 3.2**) pour configurer l'application AWS IAM Identity Center d'entreprise dans Microsoft Entra ID. Plus tard, vous reviendrez sur cette page pour terminer le processus.

Step 3.2 >

Étape 3.2 : Configuration de l'application AWS IAM Identity Center d'entreprise dans Microsoft Entra ID

Cette procédure établit la moitié de la connexion SAML côté Microsoft en utilisant les valeurs du fichier de métadonnées et de l'URL de connexion que vous avez obtenues à l'étape précédente.

1. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
2. Sur la gauche, choisissez 2. Configurez l'authentification unique.
3. Sur la page Configurer l'authentification unique avec SAML, choisissez SAML. Choisissez ensuite Télécharger le fichier de métadonnées, choisissez l'icône du dossier, sélectionnez le fichier de métadonnées du fournisseur de services que vous avez téléchargé à l'étape précédente, puis choisissez Ajouter.
4. Sur la page de configuration SAML de base, vérifiez que les valeurs de l'identifiant et de l'URL de réponse (URL du service client d'assertion) pointent désormais vers des points de terminaison. AWS
 - Identifiant : il s'agit de l'URL de l'émetteur provenant d'IAM Identity Center. La même valeur s'applique, que vous utilisiez des points de IPv4 terminaison à double pile ou uniquement.
 - URL de réponse (URL d'Assertion Consumer Service) : les valeurs indiquées ici incluent à la fois les points de terminaison à double IPv4 pile et les points de terminaison à double pile provenant de toutes les régions activées de votre centre d'identité IAM. Vous pouvez utiliser l'URL ACS de la région principale comme URL par défaut afin que les utilisateurs soient redirigés vers la région principale lorsqu'ils lancent l'application Amazon Web Services Microsoft Entra ID. Pour plus d'informations sur ACS URLs, voir [Points de terminaison ACS dans le primaire et dans le module supplémentaire Régions AWS](#).
 - (Facultatif) Si vous avez répliqué IAM Identity Center dans d'autres régions, vous pouvez également créer une application de favoris Microsoft Entra ID pour le portail AWS d'accès de chaque région supplémentaire. Cela permet à vos utilisateurs d'accéder au portail AWS d'accès dans des régions supplémentaires à partir de Microsoft Entra ID. Assurez-

vous d'autoriser vos utilisateurs à accéder aux applications de favoris dans Microsoft Entra ID. Consultez [Microsoft Entra ID la documentation](#) pour plus de détails. Si vous prévoyez de répliquer IAM Identity Center dans d'autres régions ultérieurement, consultez la page [Microsoft Entra ID configuration pour l'accès à des régions supplémentaires](#) pour savoir comment activer l'accès aux régions supplémentaires après cette configuration initiale.

5. Sous URL de connexion (facultatif), collez la valeur de l'URL de connexion AWS au portail d'accès que vous avez copiée à l'étape précédente (**Step 3.1**), choisissez Enregistrer, puis X pour fermer la fenêtre.
6. Si vous êtes invité à tester l'authentification unique avec AWS IAM Identity Center, choisissez Non, je testerai plus tard. Vous effectuerez cette vérification dans une étape ultérieure.
7. Sur la page Configurer l'authentification unique avec SAML, dans la section Certificats SAML, à côté de Federation Metadata XML, choisissez Télécharger pour enregistrer le fichier de métadonnées sur votre système. Vous devrez télécharger ce fichier lorsque vous y serez invité à l'étape suivante.

Step 3.3 >

Étape 3.3 : Configuration de l'IdP Microsoft Entra ID externe dans AWS IAM Identity Center

Ici, vous allez revenir à l'assistant de modification de la source d'identité de la console IAM Identity Center pour terminer la seconde moitié de la connexion SAML. AWS

1. Revenez à la session de navigateur que vous avez laissée ouverte **Step 3.1** dans la console IAM Identity Center.
2. Sur la page Configurer le fournisseur d'identité externe, dans la section Métadonnées du fournisseur d'identité, sous Métadonnées IDP SAML, cliquez sur le bouton Choisir un fichier, sélectionnez le fichier de métadonnées du fournisseur d'identité à partir duquel vous avez téléchargé Microsoft Entra ID à l'étape précédente, puis choisissez Ouvrir.
3. Choisissez Suivant.
4. Après avoir lu la clause de non-responsabilité et être prêt à continuer, entrez **ACCEPT**.
5. Choisissez Modifier la source d'identité pour appliquer vos modifications.

Step 3.4 >

Étape 3.4 : Vérifiez que Nikki est redirigée vers le portail AWS d'accès

Dans cette procédure, vous allez tester la connexion SAML en vous connectant au portail My Account de Microsoft avec les informations d'identification de Nikki. Une fois authentifié, vous allez sélectionner l' AWS IAM Identity Center application qui redirigera Nikki vers le portail d' AWS accès.

1. Accédez à la page de connexion au [portail Mon compte](#) et saisissez l'adresse e-mail complète de Nikki. Par exemple, **NikkiWolf@example.org**.
2. Lorsque vous y êtes invité, entrez le mot de passe de Nikki, puis choisissez Se connecter.
3. Sur la page Mon compte, dans le volet de navigation de gauche, sélectionnez Mes applications.
4. Sur la page Mes applications, sélectionnez l'application nommée AWS IAM Identity Center. Cela devrait vous demander une authentification supplémentaire.
5. Sur la page de connexion de Microsoft, choisissez vos NikkiWolf informations d'identification. Si vous êtes invité une deuxième fois à vous authentifier, sélectionnez à nouveau vos NikkiWolf informations d'identification. Cela devrait vous rediriger automatiquement vers le portail AWS d'accès.

 Tip

Si vous n'êtes pas redirigé correctement, assurez-vous que la valeur de l'URL de connexion AWS au portail d'accès que vous avez saisie **Step 3.2** correspond à la valeur à partir **Step 3.1** de laquelle vous l'avez copiée.

6. Vérifiez que votre Comptes AWS écran.

 Tip

Si la page est vide et ne s' Comptes AWS affiche pas, vérifiez que Nikki a bien été affectée à l'ensemble RegionalAdmin d'autorisations (voir **Step 2.3**).

Step 3.5

Étape 3.5 : Testez le niveau d'accès de Nikki pour la gérer Compte AWS

Au cours de cette étape, vous allez vérifier le niveau d'accès de Nikki pour gérer les paramètres régionaux pour elle Compte AWS. Nikki ne doit disposer de privilèges d'administrateur suffisants que pour gérer les régions depuis la page des comptes.

1. Dans le portail AWS d'accès, cliquez sur l'onglet Comptes pour afficher la liste des comptes. Les noms de compte IDs, les comptes et les adresses e-mail associés à tous les comptes pour lesquels vous avez défini des ensembles d'autorisations apparaissent.
2. Choisissez le nom du compte (par exemple *Sandbox*) sur lequel vous avez appliqué l'ensemble d'autorisations (voir **Step 2.3**). Cela élargira la liste des ensembles d'autorisations parmi lesquels Nikki pourra choisir pour gérer son compte.
3. Ensuite, RegionalAdmin choisissez la console de gestion pour assumer le rôle que vous avez défini dans le jeu RegionalAdmin d'autorisations. Cela vous redirigera vers la page d' AWS Management Console accueil.
4. Dans le coin supérieur droit de la console, choisissez le nom de votre compte, puis sélectionnez Compte. Vous serez redirigé vers la page du compte. Notez que toutes les autres sections de cette page affichent un message indiquant que vous ne disposez pas des autorisations nécessaires pour afficher ou modifier ces paramètres.
5. Sur la page Compte, faites défiler la page jusqu'à la section AWS Régions. Cochez une case pour n'importe quelle région disponible dans le tableau. Notez que Nikki dispose des autorisations nécessaires pour activer ou désactiver la liste des régions pour son compte, comme prévu.

Bien fait !

Les étapes 1 à 3 vous ont aidé à implémenter et à tester avec succès votre connexion SAML. Maintenant, pour terminer le didacticiel, nous vous encourageons à passer à l'étape 4 pour implémenter le provisionnement automatique.

Étape 4 : configurer et tester votre synchronisation SCIM

Au cours de cette étape, vous allez configurer le [provisionnement automatique](#) (synchronisation) des informations utilisateur depuis Microsoft Entra ID IAM Identity Center à l'aide du protocole SCIM v2.0. Vous configurez cette connexion en Microsoft Entra ID utilisant votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur créé automatiquement par IAM Identity Center.

Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec Microsoft Entra ID les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et Microsoft Entra ID.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs résidant principalement dans IAM Identity Center Microsoft Entra ID à l'aide de l'application IAM Identity Center dans Microsoft Entra ID

Step 4.1 >

Étape 4.1 : créer un deuxième utilisateur de test dans Microsoft Entra ID

À des fins de test, vous allez créer un nouvel utilisateur (Richard Roe) dans Microsoft Entra ID. Plus tard, après avoir configuré la synchronisation SCIM, vous testerez que cet utilisateur et tous les attributs pertinents ont été correctement synchronisés avec IAM Identity Center.

1. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Utilisateurs > Tous les utilisateurs.
2. Sélectionnez Nouvel utilisateur, puis choisissez Créer un nouvel utilisateur en haut de l'écran.
3. Dans Nom d'utilisateur principal, entrez **RichRoe**, puis sélectionnez le domaine et l'extension de votre choix. Par exemple, RichRoe@*example.org*.
4. Dans Nom d'affichage, entrez **RichRoe**.
5. Dans Mot de passe, entrez un mot de passe fort ou sélectionnez l'icône en forme d'œil pour afficher le mot de passe généré automatiquement, puis copiez ou notez la valeur affichée.
6. Choisissez Propriétés, puis indiquez les valeurs suivantes :
 - Prénom - Entrez **Richard**
 - Nom de famille - Enter **Roe**
 - Intitulé du poste - Entrez **Marketing Lead**
 - Département - Entrez **Sales**
 - ID d'employé - Entrez **12345**
7. Choisissez Réviser + créer, puis sélectionnez Créer.

Step 4.2 >

Étape 4.2 : activer le provisionnement automatique dans IAM Identity Center

Dans cette procédure, vous allez utiliser la console IAM Identity Center pour activer le provisionnement automatique des utilisateurs et des groupes provenant d'IAM Microsoft Entra ID Identity Center.

1. Ouvrez la [console IAM Identity Center](#), puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, sous l'onglet Source d'identité, notez que la méthode de provisionnement est définie sur Manuel.
3. Localisez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes. Vous devrez les coller à l'étape suivante lorsque vous configurerez le provisionnement dans Microsoft Entra ID.
 - a. Point de terminaison SCIM - Par exemple,
 - IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Double pile : `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

 Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer.

5. Choisissez Fermer.
6. Dans l'onglet Source d'identité, notez que la méthode de provisionnement est désormais définie sur SCIM.

Step 4.3 >

Étape 4.3 : Configuration du provisionnement automatique dans Microsoft Entra ID

Maintenant que votre utilisateur de RichRoe test est en place et que vous avez activé le SCIM dans IAM Identity Center, vous pouvez procéder à la configuration des paramètres de synchronisation SCIM dans Microsoft Entra ID

1. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
2. Choisissez Provisioning, sous Manage, choisissez à nouveau Provisioning.
3. En mode de provisionnement, sélectionnez Automatique.
4. Sous Informations d'identification de l'administrateur, dans URL du locataire, collez la valeur de l'URL du point de terminaison SCIM que vous avez copiée **Step 4.2** précédemment. Dans Secret Token, collez la valeur du jeton d'accès.
5. Choisissez Test Connection (Connexion test). Vous devriez voir un message indiquant que les informations d'identification testées ont été correctement autorisées pour activer le provisionnement.
6. Choisissez Enregistrer.
7. Sous Gérer, sélectionnez Utilisateurs et groupes, puis choisissez Ajouter un utilisateur/un groupe.
8. Sur la page Ajouter une attribution, sous Utilisateurs, sélectionnez Aucune sélection.
9. Sélectionnez RichRoe, puis sélectionnez Sélectionner.
10. Sur la page Add Assignment (Ajouter une affectation), sélectionnez Assign (Affecter).
11. Choisissez Vue d'ensemble, puis sélectionnez Démarrer le provisionnement.

Step 4.4

Étape 4.4 : vérifier que la synchronisation a bien eu lieu

Dans cette section, vous allez vérifier que l'utilisateur de Richard a été correctement configuré et que tous les attributs sont affichés dans IAM Identity Center.

1. Dans la [console IAM Identity Center](#), sélectionnez Users.
2. Sur la page Utilisateurs, vous devriez voir votre nom RichRoed'utilisateur affiché. Notez que dans la colonne Created by, la valeur est définie sur SCIM.
3. Choisissez RichRoe, sous Profil, de vérifier que les attributs suivants ont été copiés depuis Microsoft Entra ID.
 - Prénom - **Richard**
 - Nom de famille - **Roe**
 - Département - **Sales**

- Titre - **Marketing Lead**
- Numéro d'employé - **12345**

Maintenant que l'utilisateur de Richard a été créé dans IAM Identity Center, vous pouvez l'attribuer à n'importe quel ensemble d'autorisations afin de contrôler le niveau d'accès dont il dispose à vos AWS ressources. Par exemple, vous pouvez attribuer RichRoe à l'ensemble d'**RegionalAdmin** autorisations que vous avez utilisé précédemment pour accorder à Nikki les autorisations nécessaires pour gérer les régions (voir **Step 2.3**), puis tester son niveau d'accès à l'aide **Step 3.5** de.

 Félicitations !

Vous avez correctement configuré une connexion SAML entre Microsoft AWS et vous avez vérifié que le provisionnement automatique fonctionne pour que tout reste synchronisé. Vous pouvez désormais appliquer ce que vous avez appris pour configurer plus facilement votre environnement de production.

Étape 5 : Configuration de l'ABAC - Facultatif

Maintenant que vous avez correctement configuré SAML et SCIM, vous pouvez éventuellement choisir de configurer le contrôle d'accès basé sur les attributs (ABAC). L'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction des attributs.

Avec Microsoft Entra ID, vous pouvez utiliser l'une des deux méthodes suivantes pour configurer ABAC afin de l'utiliser avec IAM Identity Center.

Configure user attributes in Identifiant Microsoft Entra for access control in IAM Identity Center

Configuration des attributs utilisateur Microsoft Entra ID pour le contrôle d'accès dans IAM Identity Center

Dans la procédure suivante, vous allez déterminer quels attributs Microsoft Entra ID doivent être utilisés par IAM Identity Center pour gérer l'accès à vos AWS ressources. Une fois définis, Microsoft Entra ID envoie ces attributs à IAM Identity Center via des assertions SAML. Vous devrez ensuite accéder [Crée un jeu d'autorisations](#) à IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmis Microsoft Entra ID.

Avant de commencer cette procédure, vous devez d'abord activer la [Attributs pour le contrôle d'accès](#) fonctionnalité. Pour plus d'informations sur cette étape, consultez [Activer et configurer les attributs pour le contrôle d'accès](#).

1. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
2. Choisissez Single sign-on (Authentification unique).
3. Dans la section Attributs et revendications, choisissez Modifier.
4. Sur la page Attributs et réclamations, procédez comme suit :
 - a. Choisissez Ajouter une nouvelle réclamation
 - b. Pour Nom, saisissez `AccessControl:AttributeName`. *AttributeName* Remplacez-le par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `AccessControl:Department`.
 - c. Pour Espace de noms, saisissez `https://aws.amazon.com/SAML/Attributes`.
 - d. Pour Source, choisissez Attribut.
 - e. Pour Attribut source, utilisez la liste déroulante pour sélectionner les attributs Microsoft Entra ID utilisateur. Par exemple, `user.department`.
5. Répétez l'étape précédente pour chaque attribut que vous devez envoyer à IAM Identity Center dans l'assertion SAML.
6. Choisissez Enregistrer.

Configure ABAC using IAM Identity Center

Configuration d'ABAC à l'aide d'IAM Identity Center

Avec cette méthode, vous utilisez la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Nameattribut` est défini sur `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Vous pouvez utiliser cet élément pour transmettre des attributs sous forme de balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagDepartment=billing`, utilisez l'attribut suivant :

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:Department">
<saml:AttributeValue>billing
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Attribuez l'accès à Comptes AWS

Les étapes suivantes ne sont requises que pour accorder l'accès à Comptes AWS . Ces étapes ne sont pas obligatoires pour autoriser l'accès aux AWS applications.

Note

Pour effectuer cette étape, vous aurez besoin d'une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Étape 1 : IAM Identity Center : accordez aux Microsoft Entra ID utilisateurs l'accès aux comptes

1. Retournez à la console IAM Identity Center. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWSpage, la structure organisationnelle affiche la racine de votre organisation avec vos comptes en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il se compose de trois étapes :
 - a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez l'utilisateur qui exécutera la fonction d'administrateur. Ensuite, sélectionnez Suivant.

- b. Pour l'étape 2 : Sélectionnez des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous indique les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.
 - i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :
 - Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.
 - Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.

Choisissez Suivant.

- ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *AdministratorAccess* avec une durée de session fixée à une heure.

- iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée AdministratorAccess. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.
 - iv. Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.
 - v. Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble *AdministratorAccess* d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.
- c. Pour l'étape 3 : vérifier et envoyer, passez en revue l'utilisateur et l'ensemble d'autorisations sélectionnés, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Patientez jusqu'à ce que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations

mis à jour a été appliqué. Lorsque l'utilisateur se connecte, il a la possibilité de choisir le *AdministratorAccess* rôle.

Étape 2 Microsoft Entra ID : Confirmer l'accès Microsoft Entra ID des utilisateurs aux AWS ressources

1. Retournez à la Microsoft Entra IDconsole et accédez à votre application de connexion basée sur SAML IAM Identity Center.
2. Sélectionnez Utilisateurs et groupes, puis sélectionnez Ajouter des utilisateurs ou des groupes. Vous allez ajouter à l'Microsoft Entra IDapplication l'utilisateur que vous avez créé dans ce didacticiel à l'étape 4. En ajoutant l'utilisateur, vous l'autorisez à se connecter à AWS. Recherchez l'utilisateur que vous avez créé à l'étape 4. Si vous suiviez cette étape, ce serait le cas**RichardRoe**.
 - Pour une démonstration, voir [Fédérer votre instance IAM Identity Center existante](#) avec Microsoft Entra ID

Microsoft Entra IDconfiguration pour l'accès à des régions supplémentaires d'IAM Identity Center - Facultatif

Si vous avez répliqué IAM Identity Center vers des régions supplémentaires, vous devez mettre à jour la configuration de votre fournisseur d'identité pour permettre l'accès aux applications AWS gérées et Comptes AWS via les régions supplémentaires. Les étapes ci-dessous vous guident tout au long de la procédure. Pour plus de détails sur cette rubrique, y compris les prérequis, consultez[Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

1. Récupérez l'ACS URLs pour les régions supplémentaires à partir de la console IAM Identity Center, comme indiqué dans[Points de terminaison ACS dans le primaire et dans le module supplémentaire Régions AWS](#).
2. Dans la console du [centre d'administration Microsoft Entra](#), accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center.
3. Sur la gauche, choisissez 2. Configurez l'authentification unique.
4. Sur la page de configuration SAML de base, dans la section URL de réponse (URL de service client d'assertion), choisissez Ajouter une URL de réponse pour l'URL ACS de chaque région supplémentaire. Vous pouvez conserver l'URL ACS de la région principale comme URL par

défaut afin que les utilisateurs continuent d'être redirigés vers la région principale lorsqu'ils lancent l' AWS IAM Identity Center applicationMicrosoft Entra ID.

5. Lorsque vous avez terminé d'ajouter l'ACS URLs, enregistrez l'AWS IAM Identity Centerapplication.
6. Vous pouvez créer une application de favoris Microsoft Entra ID pour le portail AWS d'accès dans chaque région supplémentaire. Cela permet à vos utilisateurs d'accéder au portail AWS d'accès dans des régions supplémentaires à partir deMicrosoft Entra ID. Assurez-vous d'autoriser vos utilisateurs à accéder aux applications de favoris dansMicrosoft Entra ID. Consultez [Microsoft Entra IDla documentation](#) pour plus de détails.
7. Vérifiez que vous pouvez vous connecter au portail AWS d'accès dans chaque région supplémentaire. Accédez au [portail AWS d'accès URLs](#) ou lancez les applications de favoris à partir deMicrosoft Entra ID.

Résolution des problèmes

Pour le dépannage général des systèmes SCIM et SAML avecMicrosoft Entra ID, consultez les sections suivantes :

- [Problèmes de synchronisation avec Microsoft Entra ID IAM Identity Center](#)
- [Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe](#)
- [Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center](#)
- [Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe](#)
- [Ressources supplémentaires](#)

Problèmes de synchronisation avec Microsoft Entra ID IAM Identity Center

Si vous rencontrez des problèmes lorsque Microsoft Entra ID les utilisateurs ne se synchronisent pas avec IAM Identity Center, cela peut être dû à un problème de syntaxe signalé par IAM Identity Center lorsqu'un nouvel utilisateur est ajouté à IAM Identity Center. Vous pouvez le confirmer en vérifiant les journaux Microsoft Entra ID d'audit pour détecter les événements ayant échoué, tels qu'un 'Export '. Le motif du statut de cet événement indiquera :

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

Vous pouvez également vérifier AWS CloudTrail l'échec de l'événement. Cela peut être fait en effectuant une recherche dans la console de l'historique des événements CloudTrail ou en utilisant le filtre suivant :

```
"eventName":"CreateUser"
```

L'erreur de l' CloudTrail événement indiquera ce qui suit :

```
"errorCode": "ValidationException",  
  "errorMessage": "Currently list attributes only allow single item"
```

En fin de compte, cette exception signifie que l'une des valeurs transmises Microsoft Entra ID contenait plus de valeurs que prévu. La solution consiste à examiner les attributs de l'utilisateur en Microsoft Entra ID veillant à ce qu'aucun ne contienne de valeurs dupliquées. Un exemple courant de valeurs dupliquées est la présence de plusieurs valeurs pour les numéros de contact tels que les numéros de téléphone portable, professionnel et de télécopie. Bien que les valeurs soient distinctes, elles sont toutes transmises à IAM Identity Center sous l'attribut parent unique PhoneNumbers.

Pour obtenir des conseils généraux de résolution des problèmes liés au SCIM, consultez la section [Résolution des problèmes](#).

Microsoft Entra IDSynchronisation du compte invité

Si vous souhaitez synchroniser vos utilisateurs Microsoft Entra ID invités avec IAM Identity Center, consultez la procédure suivante.

Microsoft Entra ID l'adresse e-mail des utilisateurs invités est différente de celle Microsoft Entra ID des utilisateurs. Cette différence pose des problèmes lors des tentatives de synchronisation des utilisateurs Microsoft Entra ID invités avec IAM Identity Center. Par exemple, consultez l'adresse e-mail suivante pour un utilisateur invité :

exampleuser_domain.com#EXT#@domain.onmicrosoft.com.

IAM Identity Center ne s'attend pas à ce que l'adresse e-mail contienne ce **#EXT#@domain** format.

1. Connectez-vous au [centre d'administration Microsoft Entra](#) et accédez à Identité > Applications > Applications d'entreprise, puis choisissez AWS IAM Identity Center

2. Accédez à l'onglet Single Sign On dans le volet de gauche.
3. Sélectionnez Modifier qui apparaît à côté de Attributs et revendications de l'utilisateur.
4. Sélectionnez un identifiant utilisateur unique (nom ID) après les demandes requises.
5. Vous allez créer deux conditions de réclamation pour vos Microsoft Entra ID utilisateurs et vos utilisateurs invités :
 - a. Pour Microsoft Entra ID les utilisateurs, créez un type d'utilisateur pour les membres dont l'attribut source est défini sur `user.userprincipalname`.
 - b. Pour les utilisateurs Microsoft Entra ID invités, créez un type d'utilisateur pour les invités externes avec l'attribut source défini sur `user.mail`.
 - c. Sélectionnez Enregistrer et réessayez de vous connecter en tant qu'utilisateur Microsoft Entra ID invité.

Ressources supplémentaires

- Pour obtenir des conseils généraux de résolution des problèmes liés au SCIM, consultez [Résolution des problèmes liés à IAM Identity Center](#).
- Pour le Microsoft Entra ID dépannage, consultez [Microsoft la documentation](#).
- Pour en savoir plus sur la fédération entre plusieurs entités Comptes AWS, consultez la section [Sécurisation Comptes AWS avec Azure Active Directory Federation](#).

Les ressources suivantes peuvent vous aider à résoudre les problèmes au fur et à mesure que vous travaillez avec AWS :

- [AWS re:Post](#)- Trouvez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- [AWS Support](#)- Bénéficiez d'un support technique

Configurer SAML et SCIM avec un IAM Okta Identity Center

Vous pouvez automatiquement fournir ou synchroniser les informations des utilisateurs et des groupes depuis Okta IAM Identity Center à l'aide du protocole [SCIM \(System for Cross-domain Identity Management\) 2.0](#). Pour de plus amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Pour configurer cette connexion Okta, vous utilisez votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur créé automatiquement par IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec Okta les attributs nommés dans IAM Identity Center. Ce mappage correspond aux attributs utilisateur attendus entre IAM Identity Center et votre Okta compte.

Okta prend en charge les fonctionnalités de provisionnement suivantes lorsqu'il est connecté à IAM Identity Center via SCIM :

- Créer des utilisateurs : les utilisateurs affectés à l'application IAM Identity Center dans Okta sont provisionnés dans IAM Identity Center.
- Mettre à jour les attributs utilisateur : les modifications d'attributs pour les utilisateurs affectés à l'application IAM Identity Center Okta sont mises à jour dans IAM Identity Center.
- Désactiver les utilisateurs : les utilisateurs qui ne sont pas affectés par l'application IAM Identity Center dans Okta sont désactivés dans IAM Identity Center.
- Push de groupe : les groupes (et leurs membres) Okta sont synchronisés avec IAM Identity Center.

Note

Pour minimiser les frais administratifs, tant Okta pour IAM Identity Center, que pour IAM Identity Center, nous vous recommandons d'attribuer et de transférer des groupes plutôt que des utilisateurs individuels.

- Importer des utilisateurs : les utilisateurs peuvent être importés depuis IAM Identity Center vers Okta.

Objectif

Dans ce didacticiel, vous allez découvrir comment configurer une connexion SAML avec Okta IAM Identity Center. Plus tard, vous synchroniserez les utilisateurs depuis Okta, à l'aide de SCIM. Dans ce scénario, vous gérez tous les utilisateurs et groupes dans Okta. Les utilisateurs se connectent via le Okta portail. Pour vérifier que tout est correctement configuré, une fois les étapes de configuration terminées, vous vous connecterez en tant qu'Okta utilisateur et vérifierez l'accès aux AWS ressources.

Les fonctionnalités suivantes sont prises en charge lors de la connexion Okta à IAM Identity Center via SAML :

- Connexion SAML initiée par l'IDP : les utilisateurs se connectent via le Okta portail et ont accès à IAM Identity Center.
- Connexion SAML initiée par le SP : les utilisateurs accèdent au portail d' AWS accès, qui les redirige pour qu'ils se connectent via le portail. Okta

Note

Vous pouvez créer un Okta compte ([essai gratuit](#)) sur lequel l'application Okta's [IAM Identity Center est installée](#). Pour les Okta produits payants, vous devrez peut-être confirmer que votre Okta licence prend en charge la gestion du cycle de vie ou des fonctionnalités similaires permettant le provisionnement sortant. Ces fonctionnalités peuvent être nécessaires pour configurer le SCIM depuis Okta IAM Identity Center.

Si vous n'avez pas encore activé IAM Identity Center, consultez [Activer IAM Identity Center](#).

Considérations

- Avant de configurer le provisionnement SCIM entre Okta et IAM Identity Center, nous vous recommandons de procéder à un premier examen. [Considérations relatives à l'utilisation du provisionnement automatique](#)
- Chaque Okta utilisateur doit avoir un prénom, un nom de famille, un nom d'utilisateur et une valeur de nom d'affichage spécifiés.
- Chaque Okta utilisateur ne dispose que d'une seule valeur par attribut de données, tel qu'une adresse e-mail ou un numéro de téléphone. Les utilisateurs possédant plusieurs valeurs ne parviendront pas à se synchroniser. Si certains utilisateurs ont plusieurs valeurs dans leurs attributs, supprimez les attributs dupliqués avant de tenter de configurer l'utilisateur dans IAM Identity Center. Par exemple, un seul attribut de numéro de téléphone peut être synchronisé, étant donné que l'attribut de numéro de téléphone par défaut est « téléphone professionnel », utilisez l'attribut « téléphone professionnel » pour stocker le numéro de téléphone de l'utilisateur, même si le numéro de téléphone de l'utilisateur est un téléphone fixe ou un téléphone mobile.
- Lors de l'utilisation Okta avec IAM Identity Center, IAM Identity Center est généralement configuré en tant qu'application dans Okta. Cela vous permet de configurer plusieurs instances d'IAM Identity Center en tant que plusieurs applications, prenant en charge l'accès à plusieurs AWS Organisations, au sein d'une seule instance d'Okta.

- Les droits et les attributs de rôle ne sont pas pris en charge et ne peuvent pas être synchronisés avec IAM Identity Center.
- L'utilisation du même Okta groupe pour les devoirs et le transfert de groupe n'est actuellement pas prise en charge. Pour maintenir des appartenances de groupe cohérentes entre IAM Identity Center Okta et IAM Identity Center, créez un groupe distinct et configurez-le pour transférer des groupes vers IAM Identity Center.
- Si vous avez répliqué IAM Identity Center vers des régions supplémentaires, vous devez mettre à jour la configuration de votre fournisseur d'identité pour permettre l'accès aux applications AWS gérées et Comptes AWS via des régions supplémentaires. Pour plus de détails, notamment sur les prérequis, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#). Les étapes spécifiques à Okta sont décrites dans [Oktaconfiguration pour l'accès à des régions supplémentaires](#)

Étape 1 Okta : Obtenir les métadonnées SAML de votre compte Okta

1. Connectez-vous au Okta admin dashboard, développez Applications, puis sélectionnez Applications.
2. Sur la page Applications, choisissez Browse App Catalog (Parcourir le catalogue d'applications).
3. Dans le champ de recherche, tapez AWS IAM Identity Center, sélectionnez l'application pour ajouter l'application IAM Identity Center.
4. Sélectionnez l'onglet Se connecter.
5. Sous Certificats de signature SAML, sélectionnez Actions, puis Afficher les métadonnées IdP. Un nouvel onglet de navigateur s'ouvre et affiche l'arborescence du document d'un fichier XML. Sélectionnez tout le code XML de `<md:EntityDescriptor>` à `</md:EntityDescriptor>` et copiez-le dans un fichier texte.
6. Enregistrez le fichier texte sous `metadata.xml`.

Laissez la console Okta admin dashboard ouverte, vous continuerez à utiliser cette console dans les étapes ultérieures.

Étape 2 : IAM Identity Center : configurer Okta en tant que source d'identité pour IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#) en tant qu'utilisateur doté de privilèges administratifs.

2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, choisissez Actions, puis Modifier la source d'identité.
4. Sous Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
5. Sous Configurer le fournisseur d'identité externe, procédez comme suit :
 - a. Sous Métadonnées du fournisseur de services, copiez les éléments suivants dans un fichier texte pour y accéder facilement :
 - URL du service ACS (IAM Identity Center Assertion Consumer Service) : vous avez le choix entre un ACS IPv4 uniquement ou un ACS à double pile. URLs De plus, si votre instance IAM Identity Center est activée dans plusieurs régions, chaque région supplémentaire possède son propre ACS à double IPv4 pile uniquement. URLs Pour plus d'informations sur ACS URLs, voir [Points de terminaison ACS dans le primaire et dans le module supplémentaire Régions AWS](#).
 - URL de l'émetteur du IAM Identity Center

Vous aurez besoin de ces valeurs plus loin dans ce didacticiel.

- b. Sous Métadonnées du fournisseur d'identité, sous Métadonnées IDP SAML, sélectionnez Choisir un fichier, puis sélectionnez le metadata .xml fichier que vous avez créé à l'étape précédente.
 - c. Choisissez Suivant.
6. Une fois que vous avez lu la clause de non-responsabilité et que vous êtes prêt à continuer, entrez ACCEPT.
7. Choisissez Modifier la source d'identité.

Laissez la AWS console ouverte, vous continuerez à l'utiliser à l'étape suivante.

8. Revenez à Okta admin dashboard l'onglet Connexion de l' AWS IAM Identity Center application et sélectionnez-le, puis sélectionnez Modifier.
9. Dans Paramètres de connexion avancés, entrez les informations suivantes :
 - Pour l'URL ACS, entrez la ou les valeurs que vous avez copiées pour l'URL IAM Identity Center Assertion Consumer Service (ACS). Vous pouvez utiliser l'URL ACS de la région principale comme URL par défaut afin que les utilisateurs soient redirigés vers la région principale lorsqu'ils lancent l'application Amazon Web ServicesOkta.

- (Facultatif) Si vous avez répliqué IAM Identity Center dans d'autres régions, vous pouvez également créer une application de favoris Okta pour le portail AWS d'accès de chaque région supplémentaire. Cela permet à vos utilisateurs d'accéder au portail AWS d'accès dans des régions supplémentaires à partir de Okta. Assurez-vous d'autoriser vos utilisateurs à accéder aux applications de favoris dans Okta. Consultez [Okta documentation](#) pour plus de détails. Si vous prévoyez de répliquer IAM Identity Center dans d'autres régions ultérieurement, consultez la page [Okta configuration pour l'accès à des régions supplémentaires](#) pour savoir comment activer l'accès aux régions supplémentaires après cette configuration initiale.
- Pour URL de l'émetteur, entrez la valeur que vous avez copiée pour l'URL de l'émetteur d'IAM Identity Center
- Pour le format du nom d'utilisateur de l'application, sélectionnez l'une des options du menu.

Assurez-vous que la valeur que vous choisissez est unique pour chaque utilisateur. Pour ce didacticiel, sélectionnez le nom d'utilisateur Okta

10. Choisissez Enregistrer.

Vous êtes maintenant prêt à approvisionner les utilisateurs depuis Okta IAM Identity Center. Laissez le champ Okta admin dashboard ouvert et revenez à la console IAM Identity Center pour passer à l'étape suivante.

Étape 3 : IAM Identity Center et Okta Okta provisionnement des utilisateurs

1. Dans la console IAM Identity Center, sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela permet le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
2. Dans la boîte de dialogue de provisionnement automatique entrant, copiez chacune des valeurs des options suivantes :
 - a. Point de terminaison SCIM : le format du point de terminaison dépend de votre configuration :
 - IPv4: `https://scim.us-east-2.amazonaws.com/ /scim/v2`
`1111111111-2222-3333-4444-5555555555`
 - Double pile : `https://scim.us-east-2.api.aws/ /scim/v2`
`1111111111-2222-3333-4444-5555555555`

- b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

 Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisirez ces valeurs pour configurer le provisionnement automatique Okta plus loin dans ce didacticiel.

3. Choisissez Fermer.
4. Retournez à l'application IAM Identity Center Okta admin dashboard et naviguez vers celle-ci.
5. Sur la page de l'application IAM Identity Center, choisissez l'onglet Provisioning, puis dans le menu de navigation de gauche, sous Paramètres, choisissez Integration.
6. Choisissez Modifier, puis cochez la case à côté de Activer l'intégration des API pour activer le provisionnement automatique.
7. Configurez Okta avec les valeurs de provisionnement SCIM AWS IAM Identity Center que vous avez copiées plus tôt dans cette étape :
 - a. Dans le champ URL de base, entrez la valeur du point de terminaison SCIM.
 - b. Dans le champ API Token, entrez la valeur du jeton d'accès.
8. Choisissez Test API Credentials pour vérifier que les informations d'identification saisies sont valides.

Le message AWS IAM Identity Center a été vérifié avec succès ! écrans.

9. Choisissez Enregistrer. Vous êtes redirigé vers la section Paramètres, où l'option Intégration est sélectionnée.
10. Sous Paramètres, choisissez Vers l'application, puis cochez la case Activer pour chacune des fonctionnalités de provisionnement vers l'application que vous souhaitez activer. Pour ce didacticiel, sélectionnez toutes les options.
11. Choisissez Enregistrer.

Vous êtes maintenant prêt à synchroniser vos utilisateurs depuis Okta IAM Identity Center.

Étape 4 Okta : Synchroniser les utilisateurs depuis Okta IAM Identity Center

Par défaut, aucun groupe ou utilisateur n'est attribué à votre application Okta IAM Identity Center. Les groupes de provisionnement provisionnent les utilisateurs membres du groupe. Procédez comme suit pour synchroniser les groupes et les utilisateurs avec AWS IAM Identity Center.

1. Sur la page de l'application Okta IAM Identity Center, choisissez l'onglet Assignments. Vous pouvez attribuer à la fois des personnes et des groupes à l'application IAM Identity Center.
 - a. Pour affecter des personnes :
 - Sur la page Attributions, choisissez Attribuer, puis Attribuer à des personnes.
 - Choisissez les Okta utilisateurs auxquels vous souhaitez avoir accès à l'application IAM Identity Center. Choisissez Attribuer, puis Enregistrer et revenir en arrière, puis cliquez sur Terminé.

Cela lance le processus de mise en service des utilisateurs dans IAM Identity Center.

- b. Pour attribuer des groupes :
 - Sur la page Attributions, choisissez Attribuer, puis Attribuer aux groupes.
 - Choisissez les Okta groupes auxquels vous souhaitez avoir accès à l'application IAM Identity Center. Choisissez Attribuer, puis Enregistrer et revenir en arrière, puis cliquez sur Terminé.

Cela lance le processus de mise en service des utilisateurs du groupe dans IAM Identity Center.

Note

Vous devrez peut-être spécifier des attributs supplémentaires pour le groupe s'ils ne figurent pas dans tous les enregistrements utilisateur. Les attributs spécifiés pour le groupe remplaceront toute valeur d'attribut individuelle.

2. Choisissez l'onglet Push Groups. Choisissez le Okta groupe que vous souhaitez synchroniser avec IAM Identity Center. Choisissez Enregistrer.

Le statut du groupe passe à Actif une fois que le groupe et ses membres ont été transférés vers IAM Identity Center.

3. Retournez à l'onglet Affectations.
4. Pour ajouter des Okta utilisateurs individuels à IAM Identity Center, procédez comme suit :
 - a. Sur la page Attributions, choisissez Attribuer, puis Attribuer à des personnes.
 - b. Choisissez les Okta utilisateurs auxquels vous souhaitez avoir accès à l'application IAM Identity Center. Choisissez Attribuer, puis Enregistrer et revenir en arrière, puis cliquez sur Terminé.

Cela lance le processus de mise en service des utilisateurs individuels dans IAM Identity Center.

 Note

Vous pouvez également attribuer des utilisateurs et des groupes à l' AWS IAM Identity Center application, depuis la page Applications duOkta admin dashboard. Pour ce faire, sélectionnez l'icône Paramètres, puis choisissez Attribuer aux utilisateurs ou Attribuer aux groupes, puis spécifiez l'utilisateur ou le groupe.

5. Retournez à la console IAM Identity Center. Dans le volet de navigation de gauche, sélectionnez Utilisateurs. Vous devriez voir la liste des utilisateurs renseignée par vos Okta utilisateurs.

 Félicitations !

Vous avez correctement configuré une connexion SAML entre Okta et AWS et vous avez vérifié que le provisionnement automatique fonctionne. Vous pouvez désormais attribuer ces utilisateurs à des comptes et à des applications dans IAM Identity Center. Dans le cadre de ce didacticiel, à l'étape suivante, désignons l'un des utilisateurs comme administrateur du IAM Identity Center en lui accordant des autorisations administratives sur le compte de gestion.

Transmission d'attributs pour le contrôle d'accès - Facultatif

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Nameattribut` est défini sur `https://`

`aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Attribuez l'accès à Comptes AWS

Les étapes suivantes ne sont requises que pour accorder l'accès à Comptes AWS . Ces étapes ne sont pas obligatoires pour autoriser l'accès aux AWS applications.

Note

Pour effectuer cette étape, vous aurez besoin d'une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Étape 1 : IAM Identity Center : accordez aux Okta utilisateurs l'accès aux comptes

1. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWSpage, la structure organisationnelle affiche la racine de votre organisation avec vos comptes en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il se compose de trois étapes :

- a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez l'utilisateur qui exécutera la fonction d'administrateur. Ensuite, sélectionnez Suivant.
- b. Pour l'étape 2 : sélectionner des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous guide à travers les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.
 - i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :
 - Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.
 - Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.

Choisissez Suivant.

- ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *AdministratorAccess* avec une durée de session fixée à une heure.

- iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée AdministratorAccess. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.

Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.

Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble *AdministratorAccess* d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.

- c. Pour l'étape 3 : Révision et envoi, passez en revue l'utilisateur et l'ensemble d'autorisations sélectionnés, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Patientez jusqu'à ce que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations mis à jour a été appliqué. Lorsque l'utilisateur se connecte, il a la possibilité de choisir le *AdministratorAccess* rôle.

Étape 2 Okta : Confirmer l'accès Okta des utilisateurs aux AWS ressources

1. Connectez-vous à l'aide d'un compte de test auOkta dashboard.
2. Sous Mes applications, sélectionnez l'AWS IAM Identity Centericône.
3. Vous devriez voir l' Compte AWS icône. Développez cette icône pour voir la liste des Comptes AWS objets auxquels l'utilisateur peut accéder. Dans ce didacticiel, vous n'avez travaillé qu'avec un seul compte. Par conséquent, l'extension de l'icône ne permet d'afficher qu'un seul compte.
4. Sélectionnez le compte pour afficher les ensembles d'autorisations disponibles pour l'utilisateur. Dans ce didacticiel, vous avez créé l'ensemble AdministratorAccessd'autorisations.
5. À côté de l'ensemble d'autorisations se trouvent des liens indiquant le type d'accès disponible pour cet ensemble d'autorisations. Lorsque vous avez créé l'ensemble d'autorisations, vous avez spécifié l'accès à la fois à l'accès programmatique AWS Management Console et à l'accès programmatique. Sélectionnez Console de gestion pour ouvrir le AWS Management Console.
6. L'utilisateur est connecté au AWS Management Console.

Vous pouvez également utiliser le portail AWS d'accès. Cela vous redirige pour vous connecter via le Okta portail avant d' AWS accéder au portail d'accès. Ce chemin suit le flux de connexion SAML initié par le SP.

Oktaconfiguration pour l'accès à des régions supplémentaires d'IAM Identity Center - Facultatif

Si vous avez répliqué IAM Identity Center vers des régions supplémentaires, vous devez mettre à jour la configuration de votre fournisseur d'identité pour permettre l'accès aux applications AWS gérées et Comptes AWS via les régions supplémentaires. Les étapes ci-dessous vous guident tout au long de la procédure. Pour plus de détails sur cette rubrique, y compris les prérequis, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

1. Récupérez l'ACS URLs pour les régions supplémentaires à partir de la console IAM Identity Center, comme indiqué dans [Points de terminaison ACS dans le primaire et dans le module supplémentaire Régions AWS](#).
2. Dans le volet de navigation du tableau de bord de l'Oktaadministrateur, sélectionnez Applications, puis à nouveau Applications dans la liste étendue.
3. Choisissez l'application AWS IAM Identity Center.
4. Choisissez l'onglet Sign On (Se connecter).
5. Sous Paramètres de connexion avancés et autre authentification unique requise URLs, choisissez Ajouter une autre URL ACS pour chaque région supplémentaire, puis collez l'URL ACS dans le champ de texte.
6. Lorsque vous avez terminé d'ajouter l'ACS URLs, enregistrez l'AWS IAM Identity Centerapplication.
7. Vous pouvez créer une application de favoris Okta pour le portail AWS d'accès dans chaque région supplémentaire. Cela permet à vos utilisateurs d'accéder au portail AWS d'accès dans des régions supplémentaires à partir deOkta. Assurez-vous d'autoriser vos utilisateurs à accéder aux applications de favoris dansOkta. Consultez [Okta documentation](#) pour plus de détails.
8. Vérifiez que vous pouvez vous connecter au portail AWS d'accès dans chaque région supplémentaire. Accédez au [portail AWS d'accès URLs](#) ou lancez les applications de favoris à partir deOkta.

Étapes suivantes

Maintenant que vous avez configuré Okta en tant que fournisseur d'identité et que vous avez configuré les utilisateurs dans IAM Identity Center, vous pouvez :

- Accorder l'accès à Comptes AWS, voir [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).
- Accordez l'accès aux applications cloud, voir [Attribuer un accès utilisateur aux applications dans la console IAM Identity Center](#).
- Configurez les autorisations en fonction des fonctions de la tâche, voir [Création d'un ensemble d'autorisations](#).

Résolution des problèmes

Pour le dépannage général des systèmes SCIM et SAML avec Okta, consultez les sections suivantes :

- [Reprovisionnement des utilisateurs et des groupes supprimés d'IAM Identity Center](#)
- [Erreur de provisionnement automatique dans Okta](#)
- [Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe](#)
- [Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center](#)
- [Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe](#)
- [Ressources supplémentaires](#)

Reprovisionnement des utilisateurs et des groupes supprimés d'IAM Identity Center

- Le message d'erreur suivant peut s'afficher dans la Okta console si vous essayez de modifier un utilisateur ou un groupe Okta qui a déjà été synchronisé puis supprimé d'IAM Identity Center :
 - Le transfert automatique du profil de l'utilisateur *Jane Doe* vers l'application AWS IAM Identity Center a échoué : erreur lors de la tentative de transfert de la mise à jour du profil pour *jane_doe@example.com* : aucun utilisateur n'a été renvoyé pour l'utilisateur *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Le groupe lié est absent dans AWS IAM Identity Center. Modifiez le groupe lié pour recommencer à envoyer des adhésions à des groupes.
- Vous pouvez également recevoir le message d'erreur suivant dans les Okta journaux des systèmes pour les utilisateurs ou les groupes IAM Identity Center synchronisés et supprimés :
 - Erreur Okta : Eventfailed application.provision.user.push_profile : aucun utilisateur renvoyé pour l'utilisateur *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Erreur Okta : application.provision.group_push.mapping.update.or.delete.failed.with.error : le groupe lié est absent dans. AWS IAM Identity Center Modifiez le groupe lié pour recommencer à envoyer des adhésions à des groupes.

 Warning

Les utilisateurs et les groupes doivent être supprimés de IAM Identity Center Okta plutôt que d'IAM Identity Center si vous avez synchronisé Okta IAM Identity Center à l'aide de SCIM.

Résolution des problèmes liés à la suppression des utilisateurs d'IAM Identity Center

Pour résoudre ce problème concernant les utilisateurs supprimés de l'IAM Identity Center, ceux-ci doivent être supprimés de Okta. Si nécessaire, ces utilisateurs devront également être recréés dans Okta. Lorsque l'utilisateur est recréé dans Okta, il est également reprovisionné dans le IAM Identity Center via SCIM. Pour plus d'informations sur la suppression d'un utilisateur, consultez [Okta documentation](#).

 Note

Si vous devez supprimer l'accès Okta d'un utilisateur à IAM Identity Center, vous devez d'abord le supprimer de son groupe Push, puis de son groupe d'affectation. Cela garantit que l'utilisateur est retiré de son appartenance au groupe associé dans IAM Identity Center. Pour plus d'informations sur la résolution des problèmes liés à Group Push, consultez [Okta documentation](#).

Résolution des problèmes liés à la suppression de groupes IAM Identity Center

Pour résoudre ce problème avec les groupes IAM Identity Center supprimés, le groupe doit être supprimé d'Okta. Si nécessaire, ces groupes devront également être recréés dans Okta à l'aide de Group Push. Lorsque l'utilisateur est recréé dans Okta, il est également reprovisionné dans le IAM Identity Center via SCIM. Pour plus d'informations sur la suppression d'un groupe, consultez la [documentation Okta](#).

Erreur de provisionnement automatique dans Okta

Si le message d'erreur suivant s'affiche dans Okta :

Le provisionnement automatique de l'utilisateur Jane Doe vers l'application AWS IAM Identity Center a échoué : l'utilisateur correspondant est introuvable

Consultez [Okta documentation](#) pour plus d'informations.

Ressources supplémentaires

- Pour obtenir des conseils généraux de résolution des problèmes liés au SCIM, consultez [Résolution des problèmes liés à IAM Identity Center](#).

Les ressources suivantes peuvent vous aider à résoudre les problèmes au fur et à mesure que vous travaillez avec AWS :

- [AWS re:Post](#)- Trouvez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- [AWS Support](#)- Bénéficiez d'un support technique

Configuration du provisionnement SCIM entre OneLogin et IAM Identity Center

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis OneLogin IAM Identity Center à l'aide du protocole SCIM (System for Cross-domain Identity Management) v2.0. Pour de plus amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Note

OneLogin ne prend actuellement pas en charge le service de consommation d'assertions multiples (ACS) SAML URLs dans l' AWS IAM Identity Center application. Cette fonctionnalité SAML est requise pour tirer pleinement parti de la prise en [charge multirégionale](#) dans IAM Identity Center. Si vous envisagez de répliquer IAM Identity Center vers d'autres régions, sachez que l'utilisation d'une seule URL ACS peut affecter l'expérience utilisateur dans ces régions supplémentaires. Votre région principale continuera de fonctionner normalement. Nous vous recommandons de travailler avec votre fournisseur d'IdP pour activer cette fonctionnalité. Pour plus d'informations sur l'expérience utilisateur dans des régions supplémentaires dotées d'une seule URL ACS, consultez [the section called “Utilisation d'applications AWS gérées sans plusieurs ACS URLs”](#) et [the section called “Compte AWS résilience des accès sans plusieurs ACS URLs”](#).

Vous configurez cette connexion en OneLogin utilisant votre point de terminaison SCIM pour IAM Identity Center et un jeton porteur créé automatiquement par IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec OneLogin les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et OneLogin.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs et des groupes depuis IAM Identity Center OneLogin à l'aide du protocole SCIM.

Note

Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord le [Considérations relatives à l'utilisation du provisionnement automatique](#).

Rubriques

- [Conditions préalables](#)
- [Étape 1 : activer le provisionnement dans IAM Identity Center](#)
- [Étape 2 : configurer le provisionnement dans OneLogin](#)
- [\(Facultatif\) Étape 3 : Configuration des attributs utilisateur OneLogin pour le contrôle d'accès dans IAM Identity Center](#)
- [\(Facultatif\) Transmission d'attributs pour le contrôle d'accès](#)
- [Résolution des problèmes](#)

Conditions préalables

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- Un OneLogin compte. Si vous n'avez pas de compte existant, vous pourrez peut-être obtenir un essai gratuit ou un compte développeur sur le [OneLoginsite Web](#).
- [Un compte compatible avec IAM Identity Center \(gratuit\)](#). Pour plus d'informations, voir [Activer le centre d'identité IAM](#).
- Une connexion SAML entre votre OneLogin compte et IAM Identity Center. Pour plus d'informations, consultez la section [Activation de l'authentification unique entre OneLogin et AWS](#) sur le blog du réseau de AWS partenaires.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console [IAM Identity Center](#).
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez le point de terminaison SCIM et le jeton d'accès. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
 - a. Point de terminaison SCIM : par exemple, `https://scim.us-east-2.amazonaws.com/ /scim/v2 1111111111-2222-3333-4444-555555555555`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisirez ces valeurs pour configurer le provisionnement automatique dans votre IdP plus loin dans ce didacticiel.

5. Choisissez Fermer.

Vous avez maintenant configuré le provisionnement dans la console IAM Identity Center. Vous devez maintenant effectuer les tâches restantes à l'aide de la console OneLogin d'administration, comme décrit dans la procédure suivante.

Étape 2 : configurer le provisionnement dans OneLogin

Utilisez la procédure suivante dans la console OneLogin d'administration pour activer l'intégration entre IAM Identity Center et l'application IAM Identity Center. Cette procédure suppose que vous avez déjà configuré l'application AWS Single Sign-On OneLogin pour l'authentification SAML. Si vous n'avez pas encore créé cette connexion SAML, veuillez le faire avant de continuer, puis revenez ici pour terminer le processus de provisionnement SCIM. Pour plus d'informations sur la configuration de SAML avec OneLogin, consultez la section [Activation de l'authentification unique entre OneLogin et AWS](#) sur le blog du réseau de AWS partenaires.

Pour configurer le provisionnement dans OneLogin

1. Connectez-vous à OneLogin, puis accédez à Applications > Applications.
2. Sur la page Applications, recherchez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center. Choisissez-le, puis sélectionnez Configuration dans le volet de navigation.
3. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL de base SCIM dans OneLogin. Dans la procédure précédente, vous avez également copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ SCIM Bearer Token. OneLogin
4. À côté de Connexion API, cliquez sur Activer, puis sur Enregistrer pour terminer la configuration.
5. Dans le panneau de navigation, choisissez Provisioning (Approvisionnement).
6. Cochez les cases Activer le provisionnement, Créer un utilisateur, Supprimer un utilisateur et Mettre à jour un utilisateur, puis choisissez Enregistrer.
7. Dans le panneau de navigation, choisissez utilisateurs.
8. Cliquez sur Autres actions et choisissez Synchroniser les connexions. Vous devriez recevoir le message Synchronisation des utilisateurs avec l'authentification AWS unique.
9. Cliquez à nouveau sur Autres actions, puis choisissez Réappliquer les mappages d'autorisations. Vous devriez recevoir le message Les mappages sont réappliqués.
10. À ce stade, le processus de provisionnement doit commencer. Pour le confirmer, accédez à Activité > Événements et surveillez la progression. Les événements de provisionnement réussis, ainsi que les erreurs, doivent apparaître dans le flux d'événements.
11. Pour vérifier que vos utilisateurs et groupes ont tous été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs.

Vos utilisateurs synchronisés OneLogin apparaissent sur la page Utilisateurs. Vous pouvez également consulter vos groupes synchronisés sur la page Groupes.

12. Pour synchroniser automatiquement les modifications des utilisateurs avec IAM Identity Center, accédez à la page Provisioning, recherchez la section Exiger l'approbation de l'administrateur avant que cette action ne soit effectuée, désélectionnez Créer un utilisateur, Supprimer un utilisateur, and/or Mettre à jour un utilisateur, puis cliquez sur Enregistrer.

(Facultatif) Étape 3 : Configuration des attributs utilisateur OneLogin pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative OneLogin si vous choisissez de configurer les attributs que vous utiliserez dans IAM Identity Center pour gérer l'accès à vos AWS ressources. Les attributs que vous définissez OneLogin sont transmis dans une assertion SAML à IAM Identity Center. Vous allez ensuite créer un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmis OneLogin.

Avant de commencer cette procédure, vous devez d'abord activer la [Attributs pour le contrôle d'accès](#) fonctionnalité. Pour plus d'informations sur cette étape, consultez [Activer et configurer les attributs pour le contrôle d'accès](#).

Pour configurer les attributs utilisateur OneLogin pour le contrôle d'accès dans IAM Identity Center

1. Connectez-vous à OneLogin, puis accédez à Applications > Applications.
2. Sur la page Applications, recherchez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center. Choisissez-le, puis sélectionnez Paramètres dans le volet de navigation.
3. Dans la section Paramètres requis, procédez comme suit pour chaque attribut que vous souhaitez utiliser dans IAM Identity Center :
 - a. Choisissez +.
 - b. Dans Nom du champ `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`, entrez et remplacez **AttributeName** par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
 - c. Sous Drapeaux, cochez la case à côté de Inclure dans l'assertion SAML, puis choisissez Enregistrer.

- d. Dans le champ Valeur, utilisez la liste déroulante pour choisir les attributs OneLogin utilisateur. Par exemple, Department.
4. Choisissez Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Nameattribut` est défini sur `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Résolution des problèmes

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la configuration du provisionnement automatique avec OneLogin.

Les groupes ne sont pas fournis à IAM Identity Center

Par défaut, les groupes ne peuvent pas être approvisionnés depuis OneLogin IAM Identity Center. Assurez-vous d'avoir activé le provisionnement de groupe pour votre application IAM Identity Center dans OneLogin. Pour ce faire, connectez-vous à la console OneLogin d'administration et assurez-vous que l'option Inclure dans le provisionnement utilisateur est sélectionnée dans les propriétés de l'application IAM Identity Center (application IAM Identity Center > Paramètres > Groupes). Pour plus

de détails sur la création de groupes dans OneLogin, notamment sur la synchronisation des OneLogin rôles en tant que groupes dans SCIM, consultez le [OneLoginsite Web](#).

Rien n'est synchronisé depuis OneLogin IAM Identity Center, même si tous les paramètres sont corrects

Outre la remarque ci-dessus concernant l'approbation de l'administrateur, vous devrez réappliquer les mappages de droits pour que de nombreuses modifications de configuration prennent effet. Vous pouvez le trouver dans Applications > Applications > Application IAM Identity Center > Autres actions. Vous pouvez consulter les détails et les journaux de la plupart des actions OneLogin, y compris les événements de synchronisation, sous Activité > Événements.

J'ai supprimé ou désactivé un groupe dans OneLogin, mais il apparaît toujours dans IAM Identity Center

OneLogin ne prend actuellement pas en charge l'opération SCIM DELETE pour les groupes, ce qui signifie que le groupe continue d'exister dans IAM Identity Center. Vous devez donc supprimer le groupe directement d'IAM Identity Center pour vous assurer que toutes les autorisations correspondantes dans IAM Identity Center pour ce groupe sont supprimées.

J'ai supprimé un groupe dans IAM Identity Center sans le supprimer au préalable OneLogin et je rencontre maintenant des problèmes de user/group synchronisation

Pour remédier à cette situation, assurez-vous d'abord que vous ne disposez pas de règles ou de configurations de provisionnement de groupe redondantes. OneLogin Par exemple, un groupe directement affecté à une application ainsi qu'une règle qui publie pour le même groupe. Supprimez ensuite tous les groupes indésirables dans IAM Identity Center. Enfin OneLogin, actualisez les droits (application IAM Identity Center > Provisioning > Droits), puis réappliquez les mappages de droits (application IAM Identity Center > Autres actions). Pour éviter ce problème à l'avenir, effectuez d'abord la modification pour arrêter le provisionnement du groupe OneLogin, puis supprimez le groupe d'IAM Identity Center.

Utilisation de Ping Identity produits avec IAM Identity Center

Les Ping Identity produits suivants ont été testés avec IAM Identity Center.

Rubriques

- [PingFederate](#)

- [PingOne](#)

PingFederate

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis le PingFederate produit Ping Identity (ci-après « Ping ») dans IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Pour de plus amples informations, veuillez consulter [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

Vous configurez cette connexion à PingFederate l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec PingFederate les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et PingFederate.

Ce guide est basé sur la PingFederate version 10.2. Les étapes pour les autres versions peuvent varier. Contactez-nous Ping pour plus d'informations sur la configuration du provisionnement vers IAM Identity Center pour les autres versions de PingFederate.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs et des groupes depuis IAM Identity Center PingFederate à l'aide du protocole SCIM.

Note

Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord le [Considérations relatives à l'utilisation du provisionnement automatique](#). Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- [Conditions préalables](#)
- [Considérations](#)
- [Étape 1 : activer le provisionnement dans IAM Identity Center](#)
- [Étape 2 : configurer le provisionnement dans PingFederate](#)
- [\(Facultatif\) Étape 3 : configurer les attributs utilisateur dans PingFederate pour le contrôle d'accès dans IAM Identity Center](#)

- [\(Facultatif\) Transmission d'attributs pour le contrôle d'accès](#)
- [Résolution des problèmes](#)

Conditions préalables

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- Un PingFederate serveur en état de marche. Si vous n'avez pas de PingFederate serveur existant, vous pourrez peut-être obtenir un essai gratuit ou un compte développeur sur le site Web de [Ping Identity](#). La version d'essai inclut le téléchargement de licences et de logiciels ainsi que la documentation associée.
- Une copie du logiciel PingFederate IAM Identity Center Connector installé sur votre PingFederate serveur. Pour plus d'informations sur la façon d'obtenir ce logiciel, consultez la section [IAM Identity Center Connector](#) sur le Ping Identity site Web.
- [Un compte compatible avec IAM Identity Center \(gratuit\)](#). Pour plus d'informations, voir [Activer le centre d'identité IAM](#).
- Une connexion SAML entre votre PingFederate instance et IAM Identity Center. Pour obtenir des instructions sur la configuration de cette connexion, consultez la PingFederate documentation. En résumé, il est recommandé d'utiliser le connecteur IAM Identity Center pour configurer le « Browser SSO » dans PingFederate, en utilisant les fonctionnalités de « téléchargement » et d'« importation » de métadonnées situées aux deux extrémités pour échanger des métadonnées SAML entre IAM Identity Center PingFederate et IAM Identity Center.
- Si vous avez répliqué IAM Identity Center vers des régions supplémentaires, vous devez mettre à jour la configuration de votre fournisseur d'identité pour permettre l'accès aux applications AWS gérées et à Comptes AWS partir de ces régions. Pour en savoir plus, consultez [the section called "Étape 3 : Mettre à jour la configuration de l'IdP externe"](#). Consultez la PingFederate documentation pour plus de détails.

Considérations

Voici des considérations importantes PingFederate qui peuvent affecter la manière dont vous implémentez le provisionnement avec IAM Identity Center.

- Si un attribut (tel qu'un numéro de téléphone) est supprimé d'un utilisateur dans le magasin de données configuré dans PingFederate, cet attribut ne sera pas supprimé de l'utilisateur correspondant dans IAM Identity Center. Il s'agit d'une limitation connue dans la mise en

PingFederate's œuvre du fournisseur. Si un attribut est remplacé par une valeur différente (non vide) pour un utilisateur, cette modification sera synchronisée avec IAM Identity Center.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Après avoir rempli les conditions requises, ouvrez la console [IAM Identity Center](#).
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez le point de terminaison SCIM et le jeton d'accès. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
 - a. Point de terminaison SCIM : par exemple, `https://scim.us-east-2.amazonaws.com/ /scim/v2 1111111111-2222-3333-4444-555555555555`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisissez ces valeurs pour configurer le provisionnement automatique dans votre IdP plus loin dans ce didacticiel.

5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide de la console d'PingFederateadministration. Les étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans PingFederate

Utilisez la procédure suivante dans la console d'PingFederateadministration pour activer l'intégration entre IAM Identity Center et le connecteur IAM Identity Center. Cette procédure suppose que vous avez déjà installé le logiciel IAM Identity Center Connector. Si vous ne l'avez pas encore fait, reportez-vous à cette procédure [Conditions préalables](#), puis exécutez-la pour configurer le provisionnement SCIM.

Important

Si votre PingFederate serveur n'a pas encore été configuré pour le provisionnement SCIM sortant, vous devrez peut-être modifier le fichier de configuration pour activer le provisionnement. Pour plus d'informations, consultez la documentation Ping. En résumé, vous devez modifier le `pf.provisioner.mode` paramètre du `pingfederate-<version>/pingfederate/bin/run.properties` fichier à une valeur autre que `OFF` (valeur par défaut) et redémarrer le serveur s'il est en cours d'exécution. Par exemple, vous pouvez choisir de l'utiliser `STANDALONE` si vous ne disposez pas actuellement d'une configuration haute disponibilité avec PingFederate.

Pour configurer le provisionnement dans PingFederate

1. Connectez-vous à la console PingFederate d'administration.
2. Sélectionnez Applications en haut de la page, puis cliquez sur SP Connections.
3. Localisez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center, puis cliquez sur le nom de la connexion.
4. Sélectionnez le type de connexion dans les en-têtes de navigation sombres situés en haut de la page. Vous devriez voir que l'authentification unique du navigateur est déjà sélectionnée dans votre configuration précédente de SAML. Si ce n'est pas le cas, vous devez d'abord suivre ces étapes avant de pouvoir continuer.
5. Cochez la case Outbound Provisioning, choisissez le type IAM Identity Center Cloud Connector, puis cliquez sur Enregistrer. Si le connecteur IAM Identity Center Cloud n'apparaît pas en option, assurez-vous que vous avez installé le connecteur IAM Identity Center et que vous avez redémarré votre serveur. PingFederate
6. Cliquez sur Suivant à plusieurs reprises jusqu'à ce que vous arriviez sur la page de provisionnement sortant, puis cliquez sur le bouton Configurer le provisionnement.

7. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL SCIM de la PingFederate console. Dans la procédure précédente, vous avez également copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ Access Token de la PingFederate console. Cliquez sur Sauvegarder
8. Sur la page Configuration des canaux (Configurer les canaux), cliquez sur Créer.
9. Entrez un nom de canal pour ce nouveau canal de provisionnement (tel que **AWSIAMIdentityCenterchannel1**), puis cliquez sur Suivant.
10. Sur la page Source, choisissez le magasin de données actif que vous souhaitez utiliser pour votre connexion à IAM Identity Center, puis cliquez sur Suivant.

 Note

Si vous n'avez pas encore configuré de source de données, vous devez le faire maintenant. Consultez la documentation Ping du produit pour savoir comment choisir et configurer une source de données dans PingFederate.

11. Sur la page Paramètres source, vérifiez que toutes les valeurs sont correctes pour votre installation, puis cliquez sur Suivant.
12. Sur la page Emplacement de la source, entrez les paramètres appropriés à votre source de données, puis cliquez sur Suivant. Par exemple, si vous utilisez Active Directory comme annuaire LDAP :
 - a. Entrez le DN de base de votre forêt AD (tel que **DC=myforest,DC=mydomain,DC=com**).
 - b. Dans Utilisateurs > Nom distinctif du groupe, spécifiez un groupe unique contenant tous les utilisateurs que vous souhaitez attribuer à IAM Identity Center. Si aucun groupe unique de ce type n'existe, créez-le dans AD, revenez à ce paramètre, puis entrez le DN correspondant.
 - c. Spécifiez si vous souhaitez rechercher des sous-groupes (recherche imbriquée) et indiquez tout filtre LDAP requis.
 - d. Dans Groupes > Nom du groupe, spécifiez un groupe unique contenant tous les groupes que vous souhaitez attribuer à IAM Identity Center. Dans de nombreux cas, il peut s'agir du même DN que celui que vous avez spécifié dans la section Utilisateurs. Entrez les valeurs de recherche et de filtre imbriquées selon les besoins.
13. Sur la page Mappage des attributs, vérifiez les points suivants, puis cliquez sur Suivant :

- a. Le champ `UserName` doit être mappé à un attribut au format e-mail (`user@domain.com`). Elle doit également correspondre à la valeur que l'utilisateur utilisera pour se connecter à Ping. Cette valeur est à son tour renseignée dans la `nameId` réclamation SAML lors de l'authentification fédérée et utilisée pour établir une correspondance avec l'utilisateur dans IAM Identity Center. Par exemple, lorsque vous utilisez Active Directory, vous pouvez choisir de le spécifier `UserPrincipalName` comme `UserName`.
 - b. Les autres champs marqués d'un * doivent être mappés à des attributs non nuls pour vos utilisateurs.
14. Sur la page Activation et résumé, définissez le statut du canal sur Actif pour que la synchronisation démarre immédiatement après l'enregistrement de la configuration.
15. Vérifiez que toutes les valeurs de configuration de la page sont correctes, puis cliquez sur Terminé.
16. Sur la page Gérer les chaînes, cliquez sur Enregistrer.
17. À ce stade, le provisionnement commence. Pour confirmer l'activité, vous pouvez consulter le fichier `provisioner.log`, situé par défaut dans le `pingfederate-<version>/pingfederate/log` répertoire de votre PingFederate serveur.
18. Pour vérifier que les utilisateurs et les groupes ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés PingFederate apparaissent sur la page Utilisateurs. Vous pouvez également consulter les groupes synchronisés sur la page Groupes.

(Facultatif) Étape 3 : configurer les attributs utilisateur dans PingFederate pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative PingFederate si vous choisissez de configurer les attributs que vous utiliserez dans IAM Identity Center pour gérer l'accès à vos AWS ressources. Les attributs que vous définissez PingFederate sont transmis dans une assertion SAML à IAM Identity Center. Vous allez ensuite créer un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmis PingFederate.

Avant de commencer cette procédure, vous devez d'abord activer la [Attributs pour le contrôle d'accès](#) fonctionnalité. Pour plus d'informations sur cette étape, consultez [Activer et configurer les attributs pour le contrôle d'accès](#).

Pour configurer les attributs utilisateur PingFederate pour le contrôle d'accès dans IAM Identity Center

1. Connectez-vous à la console PingFederate d'administration.
 2. Choisissez Applications en haut de la page, puis cliquez sur SP Connections.
 3. Localisez l'application que vous avez créée précédemment pour établir votre connexion SAML avec IAM Identity Center, puis cliquez sur le nom de la connexion.
 4. Choisissez Browser SSO dans les en-têtes de navigation sombres situés en haut de la page. Cliquez ensuite sur Configurer le SSO du navigateur.
 5. Sur la page Configurer l'authentification unique du navigateur, choisissez Création d'assertions, puis cliquez sur Configurer la création d'assertions.
 6. Sur la page Configurer la création d'assertions, sélectionnez Attribute Contract.
 7. Sur la page Contrat d'attribut, sous la section Étendre le contrat, ajoutez un nouvel attribut en effectuant les étapes suivantes :
 - a. Dans la zone de texte, entrez `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`, remplacez **AttributeName** par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
 - b. Pour Format du nom d'attribut, sélectionnez `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.
 - c. Choisissez Ajouter, puis Next.
 8. Sur la page Mappage des sources d'authentification, choisissez l'instance d'adaptateur configurée avec votre application.
 9. Sur la page Exécution du contrat d'attribut, choisissez la source (magasin de données) et la valeur (attribut du magasin de données) pour le contrat d'attribut `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
- 
- Note**
- Si vous n'avez pas encore configuré de source de données, vous devez le faire maintenant. Consultez la documentation Ping du produit pour savoir comment choisir et configurer une source de données dans PingFederate.
10. Cliquez sur Suivant à plusieurs reprises jusqu'à ce que vous arriviez sur la page Activation et résumé, puis cliquez sur Enregistrer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un Attribute élément dont l'Nameattribut est défini sur `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément AttributeValue qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un Attribute élément distinct pour chaque balise.

Résolution des problèmes

Pour le dépannage général des systèmes SCIM et SAML PingFederate, consultez les sections suivantes :

- [Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe](#)
- [Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center](#)
- [Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe](#)
- Pour plus d'informations PingFederate, consultez [PingFederate la documentation](#).

Les ressources suivantes peuvent vous aider à résoudre les problèmes lorsque vous travaillez avec AWS :

- [AWS re:Post](#)- Trouvez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.

- [AWS Support](#)- Bénéficiez d'un support technique

PingOne

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations utilisateur depuis le PingOne produit Ping Identity (ci-après « Ping ») vers IAM Identity Center. Ce provisionnement utilise le protocole SCIM (System for Cross-Domain Identity Management) v2.0. Vous configurez cette connexion à PingOne l'aide de votre point de terminaison SCIM et de votre jeton d'accès IAM Identity Center. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage de vos attributs utilisateur avec PingOne les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et PingOne.

Les étapes suivantes vous expliquent comment activer le provisionnement automatique des utilisateurs depuis IAM Identity Center PingOne à l'aide du protocole SCIM.

Note

Avant de commencer à déployer SCIM, nous vous recommandons de consulter d'abord le [Considérations relatives à l'utilisation du provisionnement automatique](#). Passez ensuite en revue les autres considérations dans la section suivante.

Rubriques

- [Conditions préalables](#)
- [Considérations](#)
- [Étape 1 : activer le provisionnement dans IAM Identity Center](#)
- [Étape 2 : configurer le provisionnement dans PingOne](#)
- [\(Facultatif\) Étape 3 : Configuration des attributs utilisateur PingOne pour le contrôle d'accès dans IAM Identity Center](#)
- [\(Facultatif\) Transmission d'attributs pour le contrôle d'accès](#)
- [Résolution des problèmes](#)

Conditions préalables

Vous aurez besoin des éléments suivants avant de pouvoir commencer :

- Un PingOne abonnement ou un essai gratuit, avec des fonctionnalités d'authentification fédérée et de provisionnement. Pour plus d'informations sur la façon d'obtenir un essai gratuit, consultez le [Ping Identity](#) site Web.
- [Un compte compatible avec IAM Identity Center \(gratuit\)](#). Pour plus d'informations, voir [Activer le centre d'identité IAM](#).
- L'application PingOne IAM Identity Center a été ajoutée à votre portail PingOne d'administration. Vous pouvez obtenir l'application PingOne IAM Identity Center à partir du catalogue PingOne d'applications. Pour des informations générales, voir [Ajouter une application depuis le catalogue d'applications](#) sur le Ping Identity site Web.
- Une connexion SAML entre votre PingOne instance et IAM Identity Center. Une fois que l'application PingOne IAM Identity Center a été ajoutée à votre portail PingOne d'administration, vous devez l'utiliser pour configurer une connexion SAML entre votre PingOne instance et IAM Identity Center. Utilisez les fonctionnalités de « téléchargement » et d'« importation » des métadonnées situées aux deux extrémités pour échanger des métadonnées SAML entre IAM Identity PingOne Center et IAM. Pour obtenir des instructions sur la configuration de cette connexion, consultez la PingOne documentation.
- Si vous avez répliqué IAM Identity Center vers des régions supplémentaires, vous devez mettre à jour la configuration de votre fournisseur d'identité pour permettre l'accès aux applications AWS gérées et à Comptes AWS partir de ces régions. Pour en savoir plus, consultez [the section called "Étape 3 : Mettre à jour la configuration de l'IdP externe"](#). Consultez la PingOne documentation pour plus de détails.

Considérations

Voici des considérations importantes PingOne qui peuvent affecter la manière dont vous implémentez le provisionnement avec IAM Identity Center.

- PingOne ne prend pas en charge le provisionnement de groupes via SCIM. Contactez-nous Ping pour obtenir les dernières informations sur le soutien aux groupes dans SCIM for PingOne.
- Les utilisateurs peuvent continuer à être approvisionnés PingOne après avoir désactivé le provisionnement dans le PingOne portail d'administration. Si vous devez mettre fin au provisionnement immédiatement, supprimez le jeton porteur SCIM approprié, and/or désactivez-le [Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM](#) dans IAM Identity Center.
- Si un attribut d'un utilisateur est supprimé du magasin de données configuré dans PingOne, cet attribut ne sera pas supprimé de l'utilisateur correspondant dans IAM Identity Center. Il s'agit d'une

limitation connue dans la mise en PingOne's œuvre du fournisseur. Si un attribut est modifié, le changement sera synchronisé avec IAM Identity Center.

- Voici quelques remarques importantes concernant votre configuration SAML dans PingOne :
 - IAM Identity Center ne prend en charge emailAddress que le NameId format. Cela signifie que vous devez choisir un attribut utilisateur unique dans votre répertoire dans PingOne, non nul et formaté sous la forme d'un email/UPN (par exemple, user@domain.com) pour votre mappage SAML_SUBJECT dans. PingOne Email (Work) est une valeur raisonnable à utiliser pour tester les configurations avec le répertoire PingOne intégré.
 - Les utilisateurs qui se connectent PingOne avec une adresse e-mail contenant un caractère + peuvent ne pas être en mesure de se connecter à IAM Identity Center en raison d'erreurs telles que 'SAML_215' ou 'Invalid input'. Pour résoudre ce problème PingOne, choisissez l'option Advanced pour le mappage SAML_SUBJECT dans les mappages d'attributs. Définissez ensuite le format Name ID à envoyer à SP : to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress dans le menu déroulant.

Étape 1 : activer le provisionnement dans IAM Identity Center

Dans cette première étape, vous utilisez la console IAM Identity Center pour activer le provisionnement automatique.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Après avoir rempli les conditions requises, ouvrez la console [IAM Identity Center](#).
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.
4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez le point de terminaison SCIM et le jeton d'accès. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
 - a. Point de terminaison SCIM : par exemple, `https://scim.us-east-2.amazonaws.com/ /scim/v2 1111111111-2222-3333-4444-555555555555`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

 Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisirez ces valeurs pour configurer le provisionnement automatique dans votre IdP plus loin dans ce didacticiel.

5. Choisissez Fermer.

Maintenant que vous avez configuré le provisionnement dans la console IAM Identity Center, vous devez effectuer les tâches restantes à l'aide de l'application PingOne IAM Identity Center. Ces étapes sont décrites dans la procédure suivante.

Étape 2 : configurer le provisionnement dans PingOne

Utilisez la procédure suivante dans l'application PingOne IAM Identity Center pour activer le provisionnement avec IAM Identity Center. Cette procédure suppose que vous avez déjà ajouté l'application PingOne IAM Identity Center à votre portail PingOne d'administration. Si vous ne l'avez pas encore fait, reportez-vous à cette procédure [Conditions préalables](#), puis exécutez-la pour configurer le provisionnement SCIM.

Pour configurer le provisionnement dans PingOne

1. Ouvrez l'application PingOne IAM Identity Center que vous avez installée dans le cadre de la configuration de SAML pour PingOne (Applications > Mes applications). Consultez [Conditions préalables](#).
2. Faites défiler la page vers le bas. Sous Configuration utilisateur, choisissez le lien complet pour accéder à la configuration de configuration utilisateur de votre connexion.
3. Sur la page Instructions de provisionnement, choisissez Passer à l'étape suivante.
4. Dans la procédure précédente, vous avez copié la valeur du point de terminaison SCIM dans IAM Identity Center. Collez cette valeur dans le champ URL SCIM de l'application PingOne IAM Identity Center. Dans la procédure précédente, vous avez également copié la valeur du jeton d'accès dans IAM Identity Center. Collez cette valeur dans le champ ACCESS_TOKEN de l'application PingOne IAM Identity Center.
5. Pour REMOVE_ACTION, choisissez Désactivé ou Supprimé (voir le texte de description sur la page pour plus de détails).

6. Sur la page Mappage des attributs, choisissez une valeur à utiliser pour l'assertion SAML_SUBJECT (NameId), en suivant les instructions données [Considérations](#) plus haut sur cette page. Choisissez ensuite Passer à l'étape suivante.
7. Sur la page Personnalisation des PingOne applications - IAM Identity Center, apportez les modifications de personnalisation souhaitées (facultatif), puis cliquez sur Passer à l'étape suivante.
8. Sur la page Accès aux groupes, choisissez les groupes contenant les utilisateurs que vous souhaitez activer pour le provisionnement et l'authentification unique à IAM Identity Center. Choisissez Passer à l'étape suivante.
9. Faites défiler la page vers le bas et choisissez Terminer pour commencer le provisionnement.
10. Pour vérifier que les utilisateurs ont été correctement synchronisés avec IAM Identity Center, revenez à la console IAM Identity Center et sélectionnez Utilisateurs. Les utilisateurs synchronisés depuis PingOne apparaîtront sur la page Utilisateurs. Ces utilisateurs peuvent désormais être affectés à des comptes et à des applications au sein d'IAM Identity Center.

N'oubliez pas que PingOne cela ne prend pas en charge le provisionnement de groupes ou d'adhésions à des groupes via SCIM. Contactez-nous Ping pour plus d'informations.

(Facultatif) Étape 3 : Configuration des attributs utilisateur PingOne pour le contrôle d'accès dans IAM Identity Center

Il s'agit d'une procédure facultative PingOne si vous choisissez de configurer des attributs pour IAM Identity Center afin de gérer l'accès à vos AWS ressources. Les attributs que vous définissez PingOne sont transmis dans une assertion SAML à IAM Identity Center. Vous créez ensuite un ensemble d'autorisations dans IAM Identity Center pour gérer l'accès en fonction des attributs que vous avez transmis PingOne.

Avant de commencer cette procédure, vous devez d'abord activer la [Attributs pour le contrôle d'accès](#) fonctionnalité. Pour plus d'informations sur cette étape, consultez [Activer et configurer les attributs pour le contrôle d'accès](#).

Pour configurer les attributs utilisateur PingOne pour le contrôle d'accès dans IAM Identity Center

1. Ouvrez l'application PingOne IAM Identity Center que vous avez installée dans le cadre de la configuration de SAML pour PingOne (Applications > Mes applications).
2. Choisissez Modifier, puis passez à l'étape suivante jusqu'à ce que vous arriviez à la page Mappages d'attributs.

3. Sur la page Mappages d'attributs, choisissez Ajouter un nouvel attribut, puis procédez comme suit. Vous devez effectuer ces étapes pour chaque attribut que vous ajouterez pour être utilisé dans IAM Identity Center à des fins de contrôle d'accès.
 - a. Dans le champ Attribut de l'application, entrez `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`. Remplacez-le par le nom de l'attribut que vous attendez dans IAM Identity Center. Par exemple, `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`.
 - b. Dans le champ Attribut ou valeur littérale d'Identity Bridge, sélectionnez les attributs utilisateur PingOne dans votre annuaire. Par exemple, Email (Work).
4. Cliquez sur Suivant à quelques reprises, puis sur Terminer.

(Facultatif) Transmission d'attributs pour le contrôle d'accès

Vous pouvez éventuellement utiliser la [Attributs pour le contrôle d'accès](#) fonctionnalité d'IAM Identity Center pour transmettre un `Attribute` élément dont l'`Name` attribut est défini sur `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Cet élément vous permet de transmettre des attributs en tant que balises de session dans l'assertion SAML. Pour plus d'informations sur les balises de session, consultez la section [Transmission de balises de session AWS STS dans](#) le guide de l'utilisateur IAM.

Pour transmettre des attributs en tant que balises de session, incluez l'élément `AttributeValue` qui spécifie la valeur de la balise. Par exemple, pour transmettre la paire clé-valeur du `tagCostCenter = blue`, utilisez l'attribut suivant.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si vous devez ajouter plusieurs attributs, incluez un `Attribute` élément distinct pour chaque balise.

Résolution des problèmes

Pour le dépannage général des systèmes SCIM et SAML PingOne, consultez les sections suivantes :

- [Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe](#)
- [Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center](#)
- [Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe](#)
- Pour plus d'informations PingOne, consultez [PingOne la documentation](#).

Les ressources suivantes peuvent vous aider à résoudre les problèmes lorsque vous travaillez avec AWS :

- [AWS re:Post](#)- Trouvez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- [AWS Support](#)- Bénéficiez d'un support technique

Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut

Lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire Identity Center comme source d'identité par défaut. Vous n'avez donc pas besoin de choisir une source d'identité. Si votre organisation utilise un autre fournisseur d'identité tel que Microsoft Active Directory, Microsoft Entra ID, ou Okta envisagez d'intégrer cette source d'identité à IAM Identity Center au lieu d'utiliser la configuration par défaut.

Objectif

Dans ce didacticiel, vous allez utiliser le répertoire par défaut comme source d'identité et une instance d'organisation IAM Identity Center pour configurer et tester un utilisateur administratif. Cet utilisateur administratif crée et gère des utilisateurs et des groupes et accorde AWS l'accès avec des ensembles d'autorisations. Au cours des prochaines étapes, vous allez créer les éléments suivants :

- Un utilisateur administratif nommé *Nikki Wolf*
- Un groupe nommé *Admin team*
- Un ensemble d'autorisations nommé *AdminAccess*

Pour vérifier que tout a été créé correctement, vous allez vous connecter et définir le mot de passe de l'utilisateur administratif. Une fois ce didacticiel terminé, vous pouvez utiliser l'utilisateur administratif pour ajouter d'autres utilisateurs dans IAM Identity Center, créer des ensembles d'autorisations supplémentaires et configurer l'accès organisationnel aux applications. Si vous souhaitez autoriser les utilisateurs à accéder à l'application, vous pouvez également suivre l'[étape 1](#) de cette procédure et [configurer l'accès à l'application](#).

Conditions préalables

Les prérequis suivants sont nécessaires pour suivre ce didacticiel :

- [Activer IAM Identity Center](#) et disposez d'une [instance organisationnelle d'IAM Identity Center](#).
 - Si vous possédez une [instance de compte](#) d'IAM Identity Center, vous pouvez créer des utilisateurs et des groupes, ainsi que leur accorder l'accès aux applications. Pour plus d'informations, consultez la section [Accès aux applications](#).
- Connectez-vous à la console IAM Identity Center AWS Management Console et accédez-y en tant que :
 - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant l'utilisateur Compte AWS root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
 - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
 - Pour obtenir de l'aide supplémentaire pour vous connecter au AWS Management Console, consultez le [Connexion à AWS Guide](#).
- Vous pouvez configurer l'authentification multifactorielle pour les utilisateurs de votre IAM Identity Center. Pour de plus amples informations, veuillez consulter [Configuration de la MFA dans IAM Identity Center](#).

Étape 1 : ajouter un utilisateur

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le volet de navigation d'IAM Identity Center, choisissez Utilisateurs, puis sélectionnez Ajouter un utilisateur.
3. Sur la page Spécifier les détails de l'utilisateur, complétez les informations suivantes :
 - Nom d'utilisateur : pour ce didacticiel, entrez *nikkiw*.

Lorsque vous créez des utilisateurs, choisissez des noms d'utilisateur faciles à mémoriser. Vos utilisateurs doivent mémoriser leur nom d'utilisateur pour se connecter au portail AWS d'accès et vous ne pourrez pas le modifier ultérieurement.

- Mot de passe - Choisissez Envoyer un e-mail à cet utilisateur avec les instructions de configuration du mot de passe (recommandé).

Cette option envoie à l'utilisateur une adresse e-mail provenant d'Amazon Web Services, avec pour objet Invitation à rejoindre IAM Identity Center. L'e-mail provient de l'un `no-reply@signin.aws` ou `dono-reply@login.awsapps.com`. Ajoutez ces adresses e-mail à votre liste d'expéditeurs approuvés.

- Adresse e-mail - Entrez l'adresse e-mail de l'utilisateur à laquelle vous pouvez recevoir l'e-mail. Ensuite, saisissez-le à nouveau pour le confirmer. Chaque utilisateur doit avoir une adresse e-mail unique.
 - Prénom - Entrez le prénom de l'utilisateur. Dans le cadre de ce didacticiel, entrez *Nikki*.
 - Nom de famille - Entrez le nom de famille de l'utilisateur. Dans le cadre de ce didacticiel, entrez *Wolf*.
 - Nom d'affichage : la valeur par défaut est le prénom et le nom de famille de l'utilisateur. Si vous souhaitez modifier le nom d'affichage, vous pouvez saisir un autre nom. Le nom d'affichage est visible dans le portail de connexion et dans la liste des utilisateurs.
 - Complétez les informations facultatives si vous le souhaitez. Il n'est pas utilisé pendant ce didacticiel et vous pourrez le modifier ultérieurement.
4. Choisissez Suivant. La page Ajouter un utilisateur aux groupes apparaît. Nous allons créer un groupe auquel attribuer des autorisations administratives au lieu de les donner directement *Nikki*.

Choisissez Créer un groupe

Un nouvel onglet de navigateur s'ouvre pour afficher la page Créer un groupe.

- a. Sous Détails du groupe, dans Nom du groupe, entrez le nom du groupe. Nous recommandons un nom de groupe qui identifie le rôle du groupe. Dans le cadre de ce didacticiel, entrez *Admin team*.
- b. Choisissez Créer un groupe
- c. Fermez l'onglet du navigateur de groupes pour revenir à l'onglet du navigateur Ajouter un utilisateur

5. Dans la zone Groupes, sélectionnez le bouton Actualiser. Le *Admin team* groupe apparaît dans la liste.

Cochez la case à côté de *Admin team*, puis choisissez Next.

6. Sur la page Vérifier et ajouter un utilisateur, confirmez les points suivants :

- Les informations principales apparaissent comme vous le souhaitez
- Groupes affiche l'utilisateur ajouté au groupe que vous avez créé

Si vous souhaitez apporter des modifications, choisissez Modifier. Lorsque tous les détails sont corrects, choisissez Ajouter un utilisateur.

Un message de notification vous informe que l'utilisateur a été ajouté.

Vous allez ensuite ajouter des autorisations administratives pour le *Admin team* groupe afin qu'il *Nikki* ait accès aux ressources.

Étape 2 : ajouter des autorisations administratives

Important

Suivez ces étapes uniquement si vous avez activé une [instance d'organisation d'IAM Identity Center](#).

1. Dans le volet de navigation d'IAM Identity Center, sous Autorisations multi-comptes, sélectionnez. Comptes AWS
2. Sur la Comptes AWS page, la structure organisationnelle affiche votre organisation avec vos comptes situés en dessous dans la hiérarchie. Cochez la case correspondant à votre compte de gestion, puis sélectionnez Attribuer des utilisateurs ou des groupes.
3. Le flux de travail Attribuer des utilisateurs et des groupes s'affiche. Il se compose de trois étapes :
 - a. Pour l'étape 1 : Sélectionnez les utilisateurs et les groupes, choisissez le *Admin team* groupe que vous avez créé. Ensuite, sélectionnez Suivant.

- b. Pour l'étape 2 : Sélectionnez des ensembles d'autorisations, choisissez Créer un ensemble d'autorisations pour ouvrir un nouvel onglet qui vous indique les trois sous-étapes nécessaires à la création d'un ensemble d'autorisations.
- i. Pour l'étape 1 : Sélectionnez le type d'ensemble d'autorisations, procédez comme suit :
 - Dans Type d'ensemble d'autorisations, choisissez Ensemble d'autorisations prédéfini.
 - Dans Politique pour un ensemble d'autorisations prédéfini, sélectionnez AdministratorAccess.

Choisissez Suivant.

- ii. Pour l'étape 2 : Spécifiez les détails de l'ensemble d'autorisations, conservez les paramètres par défaut et choisissez Next.

Les paramètres par défaut créent un ensemble d'autorisations nommé *AdministratorAccess* avec une durée de session fixée à une heure. Vous pouvez modifier le nom de l'ensemble d'autorisations en saisissant un nouveau nom dans le champ Nom de l'ensemble d'autorisations.

- iii. Pour l'étape 3 : révision et création, vérifiez que le type d'ensemble d'autorisations utilise la politique AWS gérée AdministratorAccess. Choisissez Créer. Sur la page Ensembles d'autorisations, une notification apparaît pour vous informer que l'ensemble d'autorisations a été créé. Vous pouvez maintenant fermer cet onglet dans votre navigateur Web.

Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, vous êtes toujours à l'étape 2 : sélectionnez les ensembles d'autorisations à partir desquels vous avez lancé le flux de travail de création d'ensembles d'autorisations.

Dans la zone Ensembles d'autorisations, cliquez sur le bouton Actualiser. L'ensemble *AdministratorAccess* d'autorisations que vous avez créé apparaît dans la liste. Cochez la case correspondant à cet ensemble d'autorisations, puis choisissez Next.

- c. Sur la page Étape 3 : Révision et envoi des tâches, vérifiez que le *Admin team* groupe est sélectionné et que l'ensemble d'*AdministratorAccess* autorisations est sélectionné, puis choisissez Soumettre.

La page Compte AWS est mise à jour avec un message indiquant que vous êtes en cours de configuration. Patientez jusqu'à ce que le processus soit terminé.

Vous êtes renvoyé à la Comptes AWS page. Un message de notification vous informe que votre Compte AWS compte a été réapprovisionné et que l'ensemble d'autorisations mis à jour a été appliqué.

Félicitations !

Vous avez correctement configuré votre premier utilisateur, votre premier groupe et votre premier ensemble d'autorisations.

Dans la partie suivante de ce didacticiel, vous allez tester *Nikki's* l'accès en vous connectant au portail d' AWS accès avec leurs informations d'identification administratives et en définissant leur mot de passe. Déconnectez-vous de la console maintenant.

Étape 3 : Tester l'accès utilisateur

Maintenant qu'il *Nikki Wolf* s'agit d'un utilisateur de votre organisation, il peut se connecter et accéder aux ressources pour lesquelles il est autorisé en fonction de son ensemble d'autorisations. Pour vérifier que l'utilisateur est correctement configuré, à l'étape suivante, vous utiliserez les *Nikki's* informations d'identification pour vous connecter et configurer son mot de passe. Lorsque vous avez ajouté l'utilisateur *Nikki Wolf* à l'étape 1, vous avez choisi de *Nikki* recevoir un e-mail contenant les instructions de configuration du mot de passe. Il est temps d'ouvrir cet e-mail et de procéder comme suit :

1. Dans l'e-mail, sélectionnez le lien Accepter l'invitation pour accepter l'invitation.

Note

L'e-mail inclut également le nom *Nikki's* d'utilisateur et l'URL du portail d' AWS accès qu'ils utiliseront pour se connecter à l'organisation. Enregistrez ces informations pour une utilisation future.

Vous êtes redirigé vers la page d'inscription d'un nouvel utilisateur où vous pouvez définir un *Nikki 's* mot de passe et [enregistrer son appareil MFA](#).

- Après avoir défini le *Nikki 's* mot de passe, vous êtes dirigé vers la page de connexion. Entrez *nikkiw* et choisissez Suivant, puis entrez le *Nikki 's* mot de passe et choisissez Se connecter.
- Le portail AWS d'accès s'ouvre et affiche l'organisation et les applications auxquelles vous pouvez accéder.

Sélectionnez l'organisation pour la développer dans une liste Comptes AWS , puis sélectionnez le compte pour afficher les rôles que vous pouvez utiliser pour accéder aux ressources du compte.

Chaque ensemble d'autorisations comporte deux méthodes de gestion que vous pouvez utiliser, soit les clés de rôle, soit les clés d'accès.

- Rôle, par exemple *AdministratorAccess* - Ouvre le AWS Console Home.
 - Clés d'accès : fournit des informations d'identification que vous pouvez utiliser avec le AWS CLI ou le AWS SDK. Inclut les informations relatives à l'utilisation d'informations d'identification à court terme actualisées automatiquement ou de clés d'accès à court terme. Pour de plus amples informations, veuillez consulter [Obtenir les informations d'identification utilisateur d'IAM Identity Center pour le ou AWS CLI AWS SDKs](#).
- Cliquez sur le lien Rôle pour vous connecter au AWS Console Home.

Vous êtes connecté et vous avez accédé à la AWS Console Home page. Explorez la console et confirmez que vous disposez de l'accès attendu.

Étapes suivantes

Maintenant que vous avez créé un utilisateur administratif dans IAM Identity Center, vous pouvez :

- [Attribuer des applications](#)
- [Ajouter d'autres utilisateurs](#)
- [Attribuer des utilisateurs à des comptes](#)
- [Configurer des ensembles d'autorisations supplémentaires](#)

 Note

Vous pouvez attribuer plusieurs ensembles d'autorisations au même utilisateur. Pour suivre la meilleure pratique consistant à appliquer des autorisations de moindre privilège, après avoir créé votre utilisateur administratif, créez un ensemble d'autorisations plus restrictif et attribuez-le au même utilisateur. Ainsi, vous pouvez accéder à votre compte uniquement Compte AWS avec les autorisations dont vous avez besoin, plutôt qu'avec des autorisations administratives.

Une fois que vos utilisateurs ont [accepté leur invitation](#) à activer leur compte et qu'ils se sont connectés au portail d' AWS accès, les seuls éléments qui apparaissent dans le Comptes AWS portail concernent les rôles et les applications auxquels ils sont affectés.

Didacticiels vidéo

Comme ressource supplémentaire, vous pouvez utiliser ces didacticiels vidéo pour en savoir plus sur la configuration de fournisseurs d'identité externes :

- [Migration entre fournisseurs d'identité externes dans AWS IAM Identity Center](#)
- [Fédérer votre AWS IAM Identity Center instance existante avec Microsoft Entra ID](#)

Configurez votre personnel dans IAM Identity Center

IAM Identity Center est la AWS solution pour connecter les utilisateurs de votre personnel à des applications AWS gérées telles que Kiro et Amazon Quick, ainsi qu'à d'autres AWS ressources. Vous pouvez connecter votre fournisseur d'identité existant et synchroniser les utilisateurs et les groupes à partir de votre annuaire, ou créer et gérer vos utilisateurs directement dans IAM Identity Center.

Vous utilisez déjà IAM pour accéder à ? Comptes AWS

Vous n'avez pas besoin de modifier vos Compte AWS flux de travail actuels pour utiliser IAM Identity Center pour accéder aux applications AWS gérées. Si vous utilisez la [fédération avec IAM](#) pour l' Compte AWS accès, vos utilisateurs peuvent continuer à accéder Comptes AWS de la même manière qu'ils l'ont toujours fait, et vous pouvez continuer à utiliser vos flux de travail existants pour gérer cet accès.

Choisissez l'approche qui correspond le mieux à la stratégie de gestion des identités de votre entreprise et à l'infrastructure existante.

Rubriques

- [Utilisateurs, groupes et provisionnement dans IAM Identity Center](#)
- [Gérez votre source d'identité](#)
- [Gérer les utilisateurs dans le répertoire Identity Center](#)

Utilisateurs, groupes et provisionnement dans IAM Identity Center

IAM Identity Center vous permet de contrôler qui peut se connecter et à quelles ressources il peut accéder. Un utilisateur doit être configuré pour se connecter. Vous pouvez ensuite attribuer l'accès uniquement aux utilisateurs ou aux groupes provisionnés. Découvrez les utilisateurs, les groupes et le provisionnement dans IAM Identity Center.

Unicité du nom d'utilisateur et de l'adresse e-mail

IAM Identity Center exige que chaque utilisateur possède un nom d'utilisateur unique. Le nom d'utilisateur est l'identifiant principal de l'utilisateur. Le nom d'utilisateur ne doit pas nécessairement correspondre à l'adresse e-mail de l'utilisateur. IAM Identity Center exige que tous les noms d'utilisateur et adresses e-mail de vos utilisateurs soient uniques et non nuls.

Groupes

Les groupes sont une combinaison logique d'utilisateurs que vous définissez. Vous pouvez créer des groupes et y ajouter des utilisateurs. IAM Identity Center ne prend pas en charge les groupes imbriqués (un groupe au sein d'un groupe). Les groupes sont utiles lors de l'attribution de l'accès aux applications Comptes AWS et de leur attribution. Plutôt que d'attribuer des autorisations à chaque utilisateur individuellement, vous accordez des autorisations à un groupe. Plus tard, lorsque vous ajoutez ou supprimez des utilisateurs d'un groupe, l'utilisateur obtient ou perd l'accès dynamique aux comptes et aux applications que vous avez affectés au groupe.

Provisionnement d'utilisateurs et de groupes

Le provisionnement est le processus qui consiste à mettre les informations des utilisateurs et des groupes à la disposition d'IAM Identity Center et des applications AWS gérées ou des applications gérées par le client. Vous pouvez créer des utilisateurs et des groupes directement dans IAM Identity Center ou connecter votre source d'identité à IAM Identity Center. Avec IAM Identity Center, vous pouvez attribuer aux utilisateurs et aux groupes l'accès aux applications connectées et Comptes AWS.

Le provisionnement dans IAM Identity Center varie en fonction de la source d'identité que vous utilisez. Pour de plus amples informations, veuillez consulter [Gérez votre source d'identité](#).

Déprovisionnement des utilisateurs et des groupes

Le déprovisionnement est le processus de suppression des informations relatives aux utilisateurs et aux groupes d'IAM Identity Center.

Si vous utilisez Active Directory ou un fournisseur d'identité externe avec IAM Identity Center, vous devez supprimer les utilisateurs et les groupes de ces sources d'identité plutôt qu'IAM Identity Center. La suppression des utilisateurs et des groupes IAM Identity Center ne les supprimera pas complètement si votre source d'identité est Active Directory ou un fournisseur d'identité externe.

Si vous devez déprovisionner des utilisateurs ou des groupes IAM Identity Center, vous devez d'abord [supprimer toute attribution d'ensembles d'autorisations](#) ou d'applications aux utilisateurs ou aux groupes que vous souhaitez déprovisionner. Dans le cas contraire, vous aurez des ensembles d'autorisations et des attributions d'applications non attribués dans votre IAM Identity Center.

Gérez votre source d'identité

Votre source d'identité dans IAM Identity Center définit l'endroit où vos utilisateurs et vos groupes sont gérés. Après avoir configuré votre source d'identité, vous pouvez rechercher des utilisateurs ou des groupes pour leur accorder un accès par authentification unique aux applications Comptes AWS, ou aux deux.

Vous ne pouvez avoir qu'une seule source d'identité par organisation dans AWS Organizations. Vous pouvez choisir l'une des sources d'identité suivantes :

- [Fournisseur d'identité externe](#) : choisissez cette option si vous souhaitez gérer les utilisateurs dans un fournisseur d'identité externe (IdP) tel que Okta ou. Microsoft Entra ID
- [Votre Active Directory sur site ou AWS géré](#) : choisissez cette option si vous souhaitez connecter votre Active Directory (AD).
- [Répertoire du centre d'identité](#) : lorsque vous activez IAM Identity Center pour la première fois, il est automatiquement configuré avec un répertoire du centre d'identité comme source d'identité par défaut, sauf si vous choisissez une autre source d'identité. L'annuaire Identity Center vous permet de créer vos utilisateurs et groupes, et d'attribuer leur niveau d'accès à vos applications Comptes AWS et à vos applications.

Note

IAM Identity Center ne prend pas en charge SAMBA4 Simple AD en tant que source d'identité.

Rubriques

- [Considérations relatives à la modification de votre source d'identité](#)
- [Modifier la source de votre identité](#)
- [Attributs d'utilisateur et de groupe pris en charge dans IAM Identity Center](#)
- [Fournisseurs d'identité externes](#)
- [Microsoft ADannuaire](#)

Considérations relatives à la modification de votre source d'identité

Bien que vous puissiez modifier votre source d'identité à tout moment, nous vous recommandons de réfléchir à l'impact de cette modification sur votre déploiement actuel.

Si vous gérez déjà des utilisateurs et des groupes dans une source d'identité, le passage à une autre source d'identité peut supprimer toutes les attributions d'utilisateurs et de groupes que vous avez configurées dans IAM Identity Center. Dans ce cas, tous les utilisateurs, y compris l'utilisateur administratif d'IAM Identity Center, perdront l'accès par authentification unique à leurs applications Comptes AWS et à leurs applications.

Avant de modifier la source d'identité pour IAM Identity Center, prenez en compte les points suivants avant de poursuivre. Si vous souhaitez continuer à modifier votre source d'identité, reportez-vous à la section [Modifier la source de votre identité](#) pour plus d'informations.

Basculement entre le répertoire IAM Identity Center et Active Directory

Si vous gérez déjà des utilisateurs et des groupes dans Active Directory, nous vous recommandons d'envisager de connecter votre annuaire lorsque vous activez IAM Identity Center et que vous choisissez votre source d'identité. Faites-le avant de créer des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center et de procéder à des affectations.

Important

Lorsque vous modifiez votre type de source d'identité dans IAM Identity Center vers ou depuis Active Directory, sachez que l'ID du magasin d'identités va changer. Cela peut avoir les conséquences suivantes :

- L'URL de votre portail AWS d'accès par défaut va changer. Vous devrez communiquer la nouvelle URL à votre personnel et mettre à jour les signets, les listes d'autorisation du portail ou du pare-feu, ainsi que les configurations dans lesquelles cette URL est référencée. Nous vous recommandons d'effectuer cette modification dans le cadre d'une période de maintenance planifiée afin de minimiser les perturbations pour vos utilisateurs.
- Si vous utilisez une clé KMS gérée par le client pour le chiffrement au repos dans IAM Identity Center et que vous avez configuré la politique de clé KMS avec le contexte de chiffrement, sachez que le contexte de chiffrement de l'Identity Store va changer. Par exemple, dans l'ARN de l'Identity Store « `arn:aws:identitystore : :123456789012:identitystore/d-922763e9b3` », « `d-922763e9b3` »

est l'ID de l'Identity Store. Pour éviter toute interruption de service pendant cette transition, modifiez temporairement votre politique de clés KMS pour utiliser un modèle générique :
« `arn:aws:identitystore : :123456789012:identitystore/*` ».

Si vous gérez déjà des utilisateurs et des groupes dans le répertoire par défaut d'Identity Center, tenez compte des points suivants :

- Attributions supprimées et utilisateurs et groupes supprimés : le fait de remplacer votre source d'identité par Active Directory supprime vos utilisateurs et vos groupes de l'annuaire Identity Center. Cette modification supprime également vos assignations. Dans ce cas, une fois que vous êtes passé à Active Directory, vous devez synchroniser vos utilisateurs et vos groupes depuis Active Directory vers le répertoire Identity Center, puis réappliquer leurs attributions.

Si vous choisissez de ne pas utiliser Active Directory, vous devez créer vos utilisateurs et groupes dans le répertoire Identity Center, puis effectuer des assignations.

- Les attributions ne sont pas supprimées lorsque les identités sont supprimées : lorsque les identités sont supprimées dans le répertoire Identity Center, les attributions correspondantes sont également supprimées dans IAM Identity Center. Toutefois, dans Active Directory, lorsque des identités sont supprimées (que ce soit dans Active Directory ou dans les identités synchronisées), les attributions correspondantes ne sont pas supprimées.
- Aucune synchronisation sortante pour APIs — Si vous utilisez Active Directory comme source d'identité, nous vous recommandons d'utiliser les options [Créer, mettre à jour et supprimer](#) APIs avec prudence. IAM Identity Center ne prend pas en charge la synchronisation sortante. Par conséquent, votre source d'identité n'est pas automatiquement mise à jour en fonction des modifications que vous apportez aux utilisateurs ou aux groupes qui les utilisent. APIs
- L'URL du portail d'accès va changer — La modification de votre source d'identité entre IAM Identity Center et Active Directory modifie également l'URL du portail AWS d'accès.
- Si des utilisateurs sont supprimés ou désactivés dans la console IAM Identity Center à l'aide d'Identity Store APIs, les utilisateurs ayant des sessions actives peuvent continuer à accéder aux applications et aux comptes intégrés. Pour plus d'informations sur la durée de la session d'authentification et le comportement des utilisateurs, consultez [Comprendre les sessions d'authentification dans IAM Identity Center](#).

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultez [Microsoft ADannuaire](#).

Passage d'IAM Identity Center à un IdP externe

Si vous remplacez votre source d'identité d'IAM Identity Center par un fournisseur d'identité externe (IdP), tenez compte des points suivants :

- Les assignations et les adhésions fonctionnent avec des assertions correctes : vos attributions d'utilisateur, vos attributions de groupe et vos appartenances à des groupes continuent de fonctionner tant que le nouvel IdP envoie les assertions correctes (par exemple, le nom SAML). IDs Ces assertions doivent correspondre aux noms d'utilisateur et aux groupes d'IAM Identity Center.
- Aucune synchronisation sortante : IAM Identity Center ne prend pas en charge la synchronisation sortante. Votre IdP externe ne sera donc pas automatiquement mis à jour en fonction des modifications apportées aux utilisateurs et aux groupes dans IAM Identity Center.
- Provisionnement SCIM : si vous utilisez le provisionnement SCIM, les modifications apportées aux utilisateurs et aux groupes de votre fournisseur d'identité ne sont reflétées dans IAM Identity Center qu'une fois que ce dernier a envoyé ces modifications à IAM Identity Center. Consultez [Considérations relatives à l'utilisation du provisionnement automatique](#).
- Annulation : vous pouvez à tout moment rétablir votre source d'identité pour qu'elle utilise à nouveau IAM Identity Center. Consultez [Passage d'un IdP externe à IAM Identity Center](#).
- Les sessions utilisateur existantes sont révoquées à l'expiration de la durée de session : une fois que vous avez remplacé votre source d'identité par un fournisseur d'identité externe, les sessions utilisateur actives sont conservées pendant le reste de la durée maximale de session configurée dans la console. Par exemple, si la durée de session du portail d' AWS accès est définie sur huit heures et que vous avez modifié la source d'identité au cours de la quatrième heure, les sessions utilisateur actives persistent pendant quatre heures supplémentaires. Pour révoquer des sessions utilisateur, consultez [the section called “Mettre fin aux sessions actives pour les utilisateurs du personnel”](#).

Si des utilisateurs sont supprimés ou désactivés dans la console IAM Identity Center à l'aide d'Identity Store APIs, les utilisateurs ayant des sessions actives peuvent continuer à accéder aux applications et aux comptes intégrés. Pour plus d'informations sur la durée de la session d'authentification et le comportement des utilisateurs, consultez [Comprendre les sessions d'authentification dans IAM Identity Center](#).

 Note

Vous ne pouvez pas révoquer les sessions utilisateur depuis la console IAM Identity Center après avoir supprimé l'utilisateur.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultez [Fournisseurs d'identité externes](#).

Passage d'un IdP externe à IAM Identity Center

Si vous remplacez votre source d'identité par un fournisseur d'identité externe (IdP) par IAM Identity Center, tenez compte des points suivants :

- IAM Identity Center préserve toutes vos assignations.
- Forcer la réinitialisation du mot de passe — Les utilisateurs qui possédaient des mots de passe dans IAM Identity Center peuvent continuer à se connecter avec leurs anciens mots de passe. Pour les utilisateurs qui se trouvaient dans l'IdP externe et non dans IAM Identity Center, un administrateur doit forcer la réinitialisation du mot de passe.
- Les sessions utilisateur existantes sont révoquées à l'expiration de la durée de session : une fois que vous avez changé votre source d'identité en IAM Identity Center, les sessions utilisateur actives sont conservées pendant la durée restante de la durée maximale de session configurée dans la console. Par exemple, si la durée de la session du portail d' AWS accès est de huit heures et que vous avez modifié la source d'identité à la quatrième heure, les sessions utilisateur actives continuent de s'exécuter pendant quatre heures supplémentaires. Pour révoquer des sessions utilisateur, consultez [the section called “Mettre fin aux sessions actives pour les utilisateurs du personnel”](#).

Si des utilisateurs sont supprimés ou désactivés dans la console IAM Identity Center à l'aide d'Identity Store APIs, les utilisateurs ayant des sessions actives peuvent continuer à accéder aux applications et aux comptes intégrés. Pour plus d'informations sur la durée de la session d'authentification et le comportement des utilisateurs, consultez [Comprendre les sessions d'authentification dans IAM Identity Center](#).

 Note

Vous ne pourrez pas révoquer les sessions utilisateur depuis la console IAM Identity Center après avoir supprimé l'utilisateur.

- Support multirégional : si vous avez répliqué IAM Identity Center dans d'autres régions ou si vous envisagez de le faire, vous devez utiliser un fournisseur d'identité externe comme source d'identité. Pour plus d'informations, notamment sur les autres prérequis, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultez [Gérer les utilisateurs dans le répertoire Identity Center](#).

Passage d'un IdP externe à un autre IdP externe

Si vous utilisez déjà un IdP externe comme source d'identité pour IAM Identity Center et que vous changez d'IdP externe, tenez compte des points suivants :

- Les assignations et les adhésions fonctionnent avec des assertions correctes. IAM Identity Center conserve toutes vos assignations. Les attributions d'utilisateurs, les attributions de groupes et les appartenances à des groupes continuent de fonctionner tant que le nouvel IdP envoie les assertions correctes (par exemple, le nom SAML). IDs

Ces assertions doivent correspondre aux noms d'utilisateur dans IAM Identity Center lorsque vos utilisateurs s'authentifient via le nouvel IdP externe.

- Provisionnement du SCIM : si vous utilisez le SCIM pour le provisionnement dans IAM Identity Center, nous vous recommandons de consulter les informations spécifiques à l'IdP contenues dans ce guide et la documentation fournie par l'IdP afin de vous assurer que le nouveau fournisseur fait correspondre correctement les utilisateurs et les groupes lorsque le SCIM est activé.
- Les sessions utilisateur existantes sont révoquées à l'expiration de la durée de session : une fois que vous avez remplacé votre source d'identité par un autre fournisseur d'identité externe, les sessions utilisateur actives sont conservées pendant la durée restante de la durée maximale de session configurée dans la console. Par exemple, si la durée de la session du portail d' AWS accès est de huit heures et que vous avez modifié la source d'identité à la quatrième heure, les sessions utilisateur actives persistent pendant quatre heures supplémentaires. Pour révoquer des sessions utilisateur, consultez [the section called “Mettre fin aux sessions actives pour les utilisateurs du personnel”](#).

Si des utilisateurs sont supprimés ou désactivés dans la console IAM Identity Center à l'aide d'Identity Store APIs, les utilisateurs ayant des sessions actives peuvent continuer à accéder aux applications et aux comptes intégrés. Pour plus d'informations sur la durée de la session d'authentification et le comportement des utilisateurs, consultez [Comprendre les sessions d'authentification dans IAM Identity Center](#).

 Note

Vous ne pouvez pas révoquer les sessions utilisateur depuis la console IAM Identity Center après avoir supprimé l'utilisateur.

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultez [Fournisseurs d'identité externes](#).

Passage d'Active Directory à un IdP externe

Si vous remplacez votre source d'identité par un IdP externe par Active Directory, ou d'Active Directory par un IdP externe, tenez compte des points suivants :

- Les utilisateurs, les groupes et les attributions sont supprimés : tous les utilisateurs, groupes et attributions sont supprimés d'IAM Identity Center. Aucune information d'utilisateur ou de groupe n'est affectée ni dans l'IdP externe ni dans Active Directory.
- Approvisionnement des utilisateurs : si vous passez à un IdP externe, vous devez configurer IAM Identity Center pour approvisionner vos utilisateurs. Vous devez également configurer manuellement les utilisateurs et les groupes pour l'IdP externe avant de pouvoir configurer les attributions.
- Création d'attributions et de groupes : si vous passez à Active Directory, vous devez créer des attributions avec les utilisateurs et les groupes figurant dans votre annuaire dans Active Directory.
- Si des utilisateurs sont supprimés ou désactivés dans la console IAM Identity Center à l'aide d'Identity Store APIs, les utilisateurs ayant des sessions actives peuvent continuer à accéder aux applications et aux comptes intégrés. Pour plus d'informations sur la durée de la session d'authentification et le comportement des utilisateurs, consultez [Comprendre les sessions d'authentification dans IAM Identity Center](#).
- Support multirégional : si vous avez répliqué IAM Identity Center dans d'autres régions ou si vous envisagez de le faire, vous devez utiliser un fournisseur d'identité externe comme source d'identité.

Pour plus d'informations, notamment sur les autres prérequis, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

Pour plus d'informations sur la manière dont IAM Identity Center approvisionne les utilisateurs et les groupes, consultez [Microsoft ADannuaire](#).

Modifier la source de votre identité

La procédure suivante décrit comment passer d'un répertoire fourni par IAM Identity Center (le répertoire par défaut du centre d'identité) à Active Directory ou à un fournisseur d'identité externe, ou inversement. Avant de continuer, consultez les informations contenues dans [Considérations relatives à la modification de votre source d'identité](#). Pour effectuer cette procédure, vous aurez besoin d'une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Warning

En fonction de votre déploiement actuel, cette modification supprime toutes les attributions d'utilisateurs et de groupes que vous avez configurées dans IAM Identity Center. Cette modification supprimera également de votre Comptes AWS compte les rôles IAM définis par des autorisations. Par conséquent, vous devrez peut-être mettre à jour vos politiques en matière de ressources et vous assurer que cela ne perturbera pas votre accès aux AWS KMS clés et aux clusters Amazon EKS. Pour en savoir plus, veuillez consulter la section [Référencement des ensembles d'autorisations dans les politiques de ressources, les cartes de configuration du cluster Amazon EKS et les politiques AWS KMS clés](#).

Dans ce cas, tous les utilisateurs et groupes, y compris l'utilisateur administratif d'IAM Identity Center, perdront l'accès par authentification unique à leurs applications Comptes AWS et à leurs applications.

Pour modifier votre source d'identité

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité. Choisissez Actions, puis sélectionnez Modifier la source d'identité.

4. Sous Choisir la source d'identité, sélectionnez la source que vous souhaitez remplacer, puis choisissez Suivant.

Si vous passez à Active Directory, choisissez le répertoire disponible dans le menu de la page suivante.

 Important

La modification de votre source d'identité vers ou depuis Active Directory supprime les utilisateurs et les groupes de l'annuaire Identity Center. Cette modification supprime également toutes les attributions que vous avez configurées dans IAM Identity Center.

 Note

Si vous avez répliqué IAM Identity Center vers d'autres régions, vous ne pourrez pas modifier le type de source d'identité. Vous ne pouvez remplacer que l'IdP externe actuel par un autre. Pour modifier le type de source d'identité, vous devez d'abord supprimer toutes les régions supplémentaires. Pour de plus amples informations, consultez [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

Si vous passez à un fournisseur d'identité externe, nous vous recommandons de suivre les étapes décrites dans [Comment se connecter à un fournisseur d'identité externe](#).

5. Une fois que vous avez lu la clause de non-responsabilité et que vous êtes prêt à continuer, tapez ACCEPT.
6. Choisissez Modifier la source d'identité. Si vous remplacez votre source d'identité par Active Directory, passez à l'étape suivante.
7. Si vous remplacez votre source d'identité par Active Directory, vous accédez à la page Paramètres. Sur la page Paramètres, effectuez l'une des opérations suivantes :
 - Choisissez Démarrer la configuration guidée. Pour plus d'informations sur la façon de terminer le processus de configuration guidée, consultez [Configuration guidée](#).
 - Dans la section Source d'identité, choisissez Actions, puis sélectionnez Gérer la synchronisation pour configurer l'étendue de la synchronisation, ainsi que la liste des utilisateurs et des groupes à synchroniser.

Attributs d'utilisateur et de groupe pris en charge dans IAM Identity Center

Ce guide fournit une référence pour la prise en charge des attributs SCIM dans IAM Identity Center. Il répertorie les attributs d'utilisateur et de groupe issus de la spécification SCIM qui sont pris en charge dans le magasin d'identités IAM Identity Center et identifie les attributs et sous-attributs spécifiques qui ne sont pas pris en charge.

Les attributs sont des informations qui vous aident à définir et à identifier des objets d'utilisateur ou de groupe individuels, tels que `email`, `members`. IAM Identity Center prend en charge les attributs les plus couramment utilisés par le biais de la saisie manuelle et du provisionnement SCIM automatique.

- [Pour plus d'informations sur la spécification du système de gestion des identités interdomaines \(SCIM\), consultez `https://tools.ietf.org/html/rfc7642`.](https://tools.ietf.org/html/rfc7642)
- Pour plus d'informations sur le provisionnement manuel et automatique, consultez [Provisionnement lorsque les utilisateurs proviennent d'un IdP externe](#).
- Pour plus d'informations sur le mappage des attributs, consultez [Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes](#).

Comme IAM Identity Center prend en charge le SCIM pour les cas d'utilisation du provisionnement automatique, le répertoire Identity Center prend en charge tous les attributs d'utilisateur et de groupe répertoriés dans la spécification SCIM, à quelques exceptions près. Les sections suivantes décrivent les attributs qui ne sont pas pris en charge par IAM Identity Center.

Les objets utilisateur ne sont pas pris en charge

Tous les attributs du schéma utilisateur SCIM (<https://tools.ietf.org/html/rfc7643#section-8.3>) sont pris en charge dans le magasin d'identités IAM Identity Center, à l'exception des suivants :

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

Tous les sous-attributs des utilisateurs sont pris en charge, à l'exception des suivants :

- 'display' sous-attribut de n'importe quel attribut à valeurs multiples (par exemple, emails ou phoneNumbers)
- 'version' sous-attribut de l'attribut 'meta'

Objets de groupe non pris en charge

Tous les attributs du schéma de groupe SCIM (<https://tools.ietf.org/html/rfc7643#section-8.4>) sont pris en charge.

Tous les sous-attributs des groupes sont pris en charge, à l'exception des suivants :

- 'display' sous-attribut de n'importe quel attribut à valeurs multiples (par exemple, membres).

Fournisseurs d'identité externes

Avec IAM Identity Center, vous pouvez connecter les identités de votre personnel existantes à celles de fournisseurs d'identité externes (IdPs) via les protocoles SAML (Security Assertion Markup Language) 2.0 et SCIM (System for Cross-Domain Identity Management). Cela permet à vos utilisateurs de se connecter au portail AWS d'accès avec leurs informations d'identification professionnelles. Ils peuvent ensuite accéder aux comptes, rôles et applications qui leur sont assignés et hébergés en externe IdPs.

Par exemple, vous pouvez connecter un IdP externe tel que Okta ou à IAM Microsoft Entra ID Identity Center. Vos utilisateurs peuvent ensuite se connecter au portail d'accès AWS avec leurs informations d'identification existantes Okta ou leurs Microsoft Entra ID informations d'identification. Pour contrôler ce que vos utilisateurs peuvent faire une fois qu'ils sont connectés, vous pouvez leur attribuer des autorisations d'accès de manière centralisée pour tous les comptes et applications de votre AWS organisation. En outre, les développeurs peuvent simplement se connecter au AWS Command Line Interface (AWS CLI) à l'aide de leurs informations d'identification existantes et bénéficier de la génération et de la rotation automatiques des informations d'identification à court terme.

Si vous utilisez un annuaire autogéré dans Active Directory ou un AWS Managed Microsoft AD, consultez [Microsoft ADannuaire](#).

 Note

Le protocole SAML ne permet pas d'interroger l'IdP pour en savoir plus sur les utilisateurs et les groupes. Par conséquent, vous devez informer IAM Identity Center de l'existence de ces utilisateurs et groupes en les configurant dans IAM Identity Center.

Provisionnement lorsque les utilisateurs proviennent d'un IdP externe

Lorsque vous utilisez un IdP externe, vous devez configurer tous les utilisateurs et groupes concernés dans IAM Identity Center avant de pouvoir attribuer des tâches ou des applications. Comptes AWS Pour ce faire, vous pouvez configurer [Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM](#) pour vos utilisateurs et groupes, ou utiliser [Approvisionnement manuel](#). Quelle que soit la manière dont vous configurez les utilisateurs, IAM Identity Center redirige l' AWS Management Console interface de ligne de commande et l'authentification des applications vers votre IdP externe. IAM Identity Center accorde ensuite l'accès à ces ressources en fonction des politiques que vous créez dans IAM Identity Center. Pour plus d'informations sur le provisionnement, consultez [Provisionnement d'utilisateurs et de groupes](#).

Rubriques

- [Comment se connecter à un fournisseur d'identité externe](#)
- [Comment modifier les métadonnées d'un fournisseur d'identité externe dans IAM Identity Center](#)
- [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#)
- [Profil SCIM et implémentation de SAML 2.0](#)

Comment se connecter à un fournisseur d'identité externe

Il existe différents prérequis, considérations et procédures de provisionnement pour les applications externes prises en charge. IdPs Des step-by-step tutoriels sont disponibles pour plusieurs IdPs :

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)

- [Identité Ping](#)

Pour plus d'informations sur les considérations relatives aux applications externes IdPs prises en charge par IAM Identity Center, consultez [Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes](#).

La procédure suivante fournit un aperçu général de la procédure utilisée avec tous les fournisseurs d'identité externes.

Pour vous connecter à un fournisseur d'identité externe

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis Actions > Modifier la source d'identité.
4. Sous Choisir une source d'identité, sélectionnez Fournisseur d'identité externe, puis cliquez sur Suivant.
5. Sous Configurer le fournisseur d'identité externe, procédez comme suit :
 - a. Sous Métadonnées du fournisseur de services, choisissez Télécharger le fichier de métadonnées pour télécharger le fichier de métadonnées et l'enregistrer sur votre système. Le fichier de métadonnées SAML d'IAM Identity Center est requis par votre fournisseur d'identité externe.

 Note

Le fichier de métadonnées SAML que vous téléchargez contient à la fois un service ACS (Assertion Consumer Service) IPv4 réservé et un service ACS (Dualstack Assertion Consumer Service). URLs En outre, si votre centre d'identité IAM est répliqué dans des régions supplémentaires, le fichier de métadonnées contient ACS URLs pour chaque région supplémentaire. Si le nombre d'ACS de votre IdP externe est limité URLs, vous devrez supprimer les ACS inutiles. URLs Par exemple, si votre entreprise a complètement adopté les terminaux à double pile et n'utilise plus IP4v uniquement des terminaux, vous pouvez supprimer ces derniers. Une autre approche consiste à ne pas utiliser le fichier de métadonnées mais à copier-coller l'ACS URLs dans l'IdP externe.

- b. Sous Métadonnées du fournisseur d'identité, choisissez Choisir un fichier et recherchez le fichier de métadonnées que vous avez téléchargé auprès de votre fournisseur d'identité externe. Téléchargez ensuite le fichier. Ce fichier de métadonnées contient le certificat public x509 nécessaire utilisé pour approuver les messages envoyés par l'IdP.
- c. Choisissez Suivant.

 Important

La modification de votre source vers ou depuis Active Directory supprime toutes les attributions d'utilisateurs et de groupes existantes. Vous devez réappliquer les assignations manuellement une fois que vous avez correctement modifié votre source.

6. Une fois que vous avez lu la clause de non-responsabilité et que vous êtes prêt à continuer, entrez ACCEPT.
7. Choisissez Modifier la source d'identité. Un message d'état vous informe que vous avez correctement modifié la source d'identité.

Comment modifier les métadonnées d'un fournisseur d'identité externe dans IAM Identity Center

Vous pouvez modifier les métadonnées de votre fournisseur d'identité externe que vous avez précédemment fournies à l'IAM Identity Center. Ces modifications affectent la capacité de vos utilisateurs à se connecter et à accéder aux AWS ressources via IAM Identity Center. La procédure suivante décrit comment mettre à jour les métadonnées de votre IdP externe stockées dans IAM Identity Center. Pour effectuer cette procédure, vous aurez besoin d'une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Pour modifier les métadonnées d'un fournisseur d'identité externe

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité. Choisissez Actions, puis sélectionnez Gérer l'authentification.
4. Dans la section Métadonnées du fournisseur d'identité, choisissez Modifier les métadonnées de l'IdP. Vous pouvez apporter les modifications à l'URL de connexion à l'IdP et/ou à l'URL de

l'émetteur de l'IdP pour votre IdP externe sur cette page. Choisissez Enregistrer les modifications lorsque vous avez effectué toutes les modifications nécessaires.

Utilisation de la fédération d'identité SAML et SCIM avec des fournisseurs d'identité externes

IAM Identity Center met en œuvre les protocoles normalisés suivants pour la fédération des identités :

- SAML 2.0 pour l'authentification des utilisateurs
- SCIM pour le provisionnement

Tout fournisseur d'identité (IdP) qui implémente ces protocoles standard est censé interagir avec succès avec IAM Identity Center, avec les considérations spéciales suivantes :

- SAML
 - IAM Identity Center nécessite un format SAML NameID pour l'adresse e-mail (c'est-à-dire,).
`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
 - [La valeur du champ NameID dans les assertions doit être une chaîne conforme à la norme RFC 2822 \(https://tools.ietf.org/html/rfc2822\) addr-spec \(« »\) \(/rfc2822 #section -3.4.1\).](https://tools.ietf.org/html/rfc2822)
[name@domain.com https://tools.ietf.org/html](https://tools.ietf.org/html/rfc2822#section-3.4.1)
 - Le fichier de métadonnées ne doit pas comporter plus de 75 000 caractères.
 - Les métadonnées doivent contenir un EntityID, un certificat X509 et faire partie de SingleSignOnService l'URL de connexion.
 - Aucune clé de chiffrement n'est prise en charge.
 - IAM Identity Center ne prend pas en charge la signature des demandes d'authentification SAML envoyées à des entités externes. IdPs
 - L'IdP doit prendre en charge le service client à assertions multiples (ACS) URLs si vous envisagez de répliquer le centre d'identité IAM dans d'autres régions et de tirer pleinement parti des avantages d'un centre d'identité IAM multirégional. Pour de plus amples informations, veuillez consulter [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#). L'utilisation d'une seule URL ACS peut affecter l'expérience utilisateur dans d'autres régions. Votre région principale continuera de fonctionner normalement. Pour plus d'informations sur l'expérience utilisateur dans des régions supplémentaires dotées d'une seule URL ACS, consultez [the section](#)

called “Utilisation d'applications AWS gérées sans plusieurs ACS URLs” et the section called “Compte AWS résilience des accès sans plusieurs ACS URLs”.

- SCIM
 - La mise en œuvre du SCIM d'IAM Identity Center est basée sur les SCIM RFCs 7642 (<https://tools.ietf.org/html/rfc7642>), 7643 ([/rfc7643](https://tools.ietf.org/html/rfc7643)) et 7644 (<https://tools.ietf.org/html/rfc7644>), ainsi que sur les exigences d'interopérabilité énoncées dans le projet de <https://tools.ietf.org/html/mars-2020> du profil SCIM de base 1.0 (#rfc .section.4). FastFed https://openid.net/specs/fastfed-scim-1_0-02.html Toute différence entre ces documents et l'implémentation actuelle dans IAM Identity Center est décrite dans la section [Opérations d'API prises en charge](#) du guide du développeur de mise en œuvre d'IAM Identity Center SCIM.

IdPs qui ne sont pas conformes aux normes et aux considérations mentionnées ci-dessus ne sont pas prises en charge. Veuillez contacter votre IdP pour toute question ou précision concernant la conformité de ses produits à ces normes et considérations.

Si vous rencontrez des problèmes pour connecter votre IdP à IAM Identity Center, nous vous recommandons de vérifier :

- AWS CloudTrail enregistre en filtrant sur le nom de l'événement ExternalIdPDirectoryLogin
- Logs spécifiques à l'IDP, journaux and/or de débogage
- [Résolution des problèmes liés à IAM Identity Center](#)

Note

Certains IdPs, comme ceux présentés dans le [Tutoriels sur les sources d'identité IAM Identity Center](#), offrent une expérience de configuration simplifiée pour IAM Identity Center sous la forme d'une « application » ou d'un « connecteur » spécialement conçu pour IAM Identity Center. Si votre IdP propose cette option, nous vous recommandons de l'utiliser, en prenant soin de choisir l'élément spécialement conçu pour IAM Identity Center. D'autres éléments appelés « AWS », « AWS fédération » ou « noms génériques AWS » similaires peuvent utiliser des and/or points de terminaison d'autres approches de fédération et peuvent ne pas fonctionner comme prévu avec IAM Identity Center.

Profil SCIM et implémentation de SAML 2.0

SCIM et SAML sont des éléments importants à prendre en compte lors de la configuration d'IAM Identity Center.

Implémentation de SAML 2.0

IAM Identity Center prend en charge la fédération des identités avec le langage [SAML \(Security Assertion Markup Language\)](#) 2.0. Cela permet à IAM Identity Center d'authentifier les identités auprès de fournisseurs d'identité externes (IdPs). SAML 2.0 est un standard ouvert utilisé pour échanger des assertions SAML en toute sécurité. SAML 2.0 transmet des informations sur un utilisateur entre une autorité SAML (appelée fournisseur d'identité ou IdP) et un consommateur SAML (appelé fournisseur de services ou SP). Le service IAM Identity Center utilise ces informations pour fournir une authentification unique fédérée. L'authentification unique permet aux utilisateurs d'accéder aux applications Comptes AWS et de les configurer en fonction de leurs informations d'identification de fournisseur d'identité existantes.

IAM Identity Center ajoute des fonctionnalités IDP SAML à votre boutique IAM Identity Center ou à un fournisseur AWS Managed Microsoft AD d'identité externe. Les utilisateurs peuvent ensuite se connecter de manière unique aux services qui prennent en charge le protocole SAML, y compris les applications tierces telles que Microsoft 365Concur, AWS Management Console et. Salesforce

Le protocole SAML ne permet toutefois pas d'interroger l'IdP pour en savoir plus sur les utilisateurs et les groupes. Par conséquent, vous devez informer IAM Identity Center de l'existence de ces utilisateurs et groupes en les configurant dans IAM Identity Center.

profil SCIM

IAM Identity Center prend en charge la norme SCIM (System for Cross-Domain Identity Management) v2.0. Le SCIM synchronise les identités de votre IAM Identity Center avec celles de votre IdP. Cela inclut le provisionnement, les mises à jour et le déprovisionnement des utilisateurs entre votre fournisseur d'identité et IAM Identity Center.

Pour plus d'informations sur la mise en œuvre du SCIM, consultez [Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM](#). Pour plus de détails sur la mise en œuvre du SCIM par IAM Identity Center, consultez le guide du développeur de mise en œuvre du [SCIM d'IAM Identity Center](#).

Rubriques

- [Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM](#)
- [Rotation des certificats SAML 2.0](#)

Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM

IAM Identity Center prend en charge le provisionnement automatique (synchronisation) des informations sur les utilisateurs et les groupes depuis votre fournisseur d'identité (IdP) vers IAM Identity Center à l'aide du protocole System for Cross-domain Identity Management (SCIM) v2.0. Lorsque vous configurez la synchronisation SCIM, vous créez un mappage des attributs utilisateur de votre fournisseur d'identité (IdP) avec les attributs nommés dans IAM Identity Center. Cela entraîne la correspondance des attributs attendus entre IAM Identity Center et votre IdP. Vous configurez cette connexion dans votre IdP à l'aide de votre point de terminaison SCIM pour IAM Identity Center et d'un jeton porteur que vous créez dans IAM Identity Center.

Rubriques

- [Considérations relatives à l'utilisation du provisionnement automatique](#)
- [Comment surveiller l'expiration des jetons d'accès](#)
- [Générer un jeton d'accès](#)
- [Activer le provisionnement automatique](#)
- [Supprimer un jeton d'accès](#)
- [Désactiver le provisionnement automatique](#)
- [Faire pivoter un jeton d'accès](#)
- [Auditez et réconciliez les ressources provisionnées automatiquement](#)
- [Approvisionnement manuel](#)

Considérations relatives à l'utilisation du provisionnement automatique

Avant de commencer à déployer le SCIM, nous vous recommandons de prendre d'abord en compte les considérations importantes suivantes concernant son fonctionnement avec IAM Identity Center. Pour d'autres considérations relatives au provisionnement, consultez la section [Tutoriels sur les sources d'identité IAM Identity Center](#) applicable à votre IdP.

- Si vous fournissez une adresse e-mail principale, cette valeur d'attribut doit être unique pour chaque utilisateur. Dans certains IdPs cas, l'adresse e-mail principale peut ne pas être une adresse e-mail réelle. Par exemple, il peut s'agir d'un nom principal universel (UPN) qui ressemble uniquement à un e-mail. Ils IdPs peuvent avoir une adresse e-mail secondaire ou « autre » contenant la véritable adresse e-mail de l'utilisateur. Vous devez configurer le SCIM dans votre IdP pour associer l'adresse e-mail unique non NULL à l'attribut d'adresse e-mail principale du IAM Identity Center. Et vous devez associer l'identifiant de connexion unique non NULL de l'utilisateur à l'attribut de nom d'utilisateur IAM Identity Center. Vérifiez si votre IdP possède une valeur unique qui est à la fois l'identifiant de connexion et le nom e-mail de l'utilisateur. Dans ce cas, vous pouvez mapper ce champ IdP à la fois à l'adresse e-mail principale et au nom d'utilisateur de l'IAM Identity Center.
- Pour que la synchronisation SCIM fonctionne, chaque utilisateur doit avoir un prénom, un nom de famille, un nom d'utilisateur et une valeur de nom d'affichage spécifiés. Si l'une de ces valeurs est absente pour un utilisateur, celui-ci ne sera pas approvisionné.
- Si vous devez utiliser des applications tierces, vous devez d'abord mapper l'attribut de sujet SAML sortant à l'attribut de nom d'utilisateur. Si l'application tierce a besoin d'une adresse e-mail routable, vous devez fournir l'attribut e-mail à votre IdP.
- Les intervalles de mise en service et de mise à jour du SCIM sont contrôlés par votre fournisseur d'identité. Les modifications apportées aux utilisateurs et aux groupes de votre fournisseur d'identité ne sont reflétées dans IAM Identity Center qu'une fois que votre fournisseur d'identité a envoyé ces modifications à IAM Identity Center. Consultez votre fournisseur d'identité pour plus de détails sur la fréquence des mises à jour des utilisateurs et des groupes.
- Actuellement, les attributs à valeurs multiples (tels que plusieurs e-mails ou numéros de téléphone pour un utilisateur donné) ne sont pas fournis avec SCIM. Les tentatives de synchronisation d'attributs à valeurs multiples dans IAM Identity Center avec SCIM échoueront. Pour éviter les échecs, assurez-vous qu'une seule valeur est transmise pour chaque attribut. Si vous avez des utilisateurs dotés d'attributs à valeurs multiples, supprimez ou modifiez les mappages d'attributs dupliqués dans SCIM sur votre IdP pour la connexion à IAM Identity Center.
- Vérifiez que le mappage `externalId` SCIM de votre IdP correspond à une valeur unique, toujours présente et peu susceptible de changer pour vos utilisateurs. Par exemple, votre IdP peut fournir un identifiant garanti `objectId` ou autre qui n'est pas affecté par les modifications apportées aux attributs utilisateur tels que le nom et l'adresse e-mail. Si tel est le cas, vous pouvez mapper cette valeur au `externalId` champ SCIM. Cela garantit que vos utilisateurs ne perdront pas leurs AWS droits, attributions ou autorisations si vous devez modifier leur nom ou leur adresse e-mail.

- Utilisateurs qui n'ont pas encore été affectés à une application ou qui Compte AWS ne peuvent pas être approvisionnés dans IAM Identity Center. Pour synchroniser les utilisateurs et les groupes, assurez-vous qu'ils sont affectés à l'application ou à une autre configuration représentant la connexion de votre IdP à IAM Identity Center.
- Le comportement de déprovisionnement des utilisateurs est géré par le fournisseur d'identité et peut varier en fonction de sa mise en œuvre. Renseignez-vous auprès de votre fournisseur d'identité pour en savoir plus sur le déprovisionnement des utilisateurs.
- Après avoir configuré le provisionnement automatique avec SCIM pour votre IdP, vous ne pouvez plus ajouter ni modifier d'utilisateurs dans la console IAM Identity Center. Si vous devez ajouter ou modifier un utilisateur, vous devez le faire à partir de votre IdP externe ou de votre source d'identité.

Pour plus d'informations sur la mise en œuvre du SCIM par IAM Identity Center, consultez le guide du développeur de mise en œuvre du [SCIM d'IAM Identity Center](#).

Comment surveiller l'expiration des jetons d'accès

Les jetons d'accès SCIM sont générés avec une validité d'un an. Lorsque votre jeton d'accès SCIM doit expirer dans 90 jours ou moins, il vous AWS envoie des rappels dans la console IAM Identity Center et via le tableau de AWS Health bord pour vous aider à faire pivoter le jeton. En faisant pivoter le jeton d'accès SCIM avant son expiration, vous sécurisez en permanence le provisionnement automatique des informations sur les utilisateurs et les groupes. Si le jeton d'accès SCIM expire, la synchronisation des informations relatives aux utilisateurs et aux groupes entre votre fournisseur d'identité et IAM Identity Center s'arrête, de sorte que le provisionnement automatique ne peut plus effectuer de mises à jour ni créer et supprimer des informations. L'interruption du provisionnement automatique peut entraîner des risques de sécurité accrus et avoir un impact sur l'accès à vos services.

Les rappels de la console Identity Center sont conservés jusqu'à ce que vous fassiez pivoter le jeton d'accès SCIM et que vous supprimiez tous les jetons d'accès inutilisés ou expirés. Les événements du tableau de AWS Health bord sont renouvelés chaque semaine entre 90 et 60 jours, deux fois par semaine de 60 à 30 jours, trois fois par semaine de 30 à 15 jours et tous les jours pendant 15 jours jusqu'à l'expiration des jetons d'accès SCIM.

Générer un jeton d'accès

Utilisez la procédure suivante pour générer un nouveau jeton d'accès dans la console IAM Identity Center.

 Note

Cette procédure nécessite que vous ayez préalablement activé le provisionnement automatique. Pour de plus amples informations, veuillez consulter [Activer le provisionnement automatique](#).

Pour générer un nouveau jeton d'accès

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, sous Jetons d'accès, choisissez Générer un jeton.
4. Dans la boîte de dialogue Générer un nouveau jeton d'accès, copiez le nouveau jeton d'accès et enregistrez-le en lieu sûr.
5. Choisissez Fermer.

Activer le provisionnement automatique

Utilisez la procédure suivante pour activer le provisionnement automatique des utilisateurs et des groupes depuis votre IdP vers IAM Identity Center à l'aide du protocole SCIM.

 Note

Avant de commencer cette procédure, nous vous recommandons de passer d'abord en revue les considérations de provisionnement applicables à votre IdP. Pour plus d'informations, consultez le correspondant [Tutoriels sur les sources d'identité IAM Identity Center](#) à votre IdP.

Pour activer le provisionnement automatique dans IAM Identity Center

1. Une fois que vous avez rempli les conditions requises, ouvrez la console [IAM Identity Center](#).
2. Choisissez Paramètres dans le volet de navigation de gauche.
3. Sur la page Paramètres, recherchez la zone Informations de provisionnement automatique, puis choisissez Activer. Cela active immédiatement le provisionnement automatique dans IAM

Identity Center et affiche les informations nécessaires sur le point de terminaison SCIM et le jeton d'accès.

4. Dans la boîte de dialogue de provisionnement automatique entrant, copiez le point de terminaison SCIM et le jeton d'accès. Vous devrez les coller ultérieurement lorsque vous configurerez le provisionnement dans votre IdP.
 - a. Point de terminaison SCIM : par exemple, `https://scim.us-east-2.amazonaws.com/ /scim/v2 1111111111-2222-3333-4444-555555555555`
 - b. Jeton d'accès : choisissez Afficher le jeton pour copier la valeur.

 Warning

C'est le seul moment où vous pouvez obtenir le point de terminaison SCIM et le jeton d'accès. Assurez-vous de copier ces valeurs avant de continuer. Vous saisirez ces valeurs pour configurer le provisionnement automatique dans votre IdP plus loin dans ce didacticiel.

5. Choisissez Fermer.

Une fois cette procédure terminée, vous devez configurer le provisionnement automatique dans votre IdP. Pour plus d'informations, consultez le correspondant [Tutoriels sur les sources d'identité IAM Identity Center](#) à votre IdP.

Supprimer un jeton d'accès

Utilisez la procédure suivante pour supprimer un jeton d'accès existant dans la console IAM Identity Center.

Pour supprimer un jeton d'accès existant

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, sous Jetons d'accès, sélectionnez le jeton d'accès que vous souhaitez supprimer, puis choisissez Supprimer.

4. Dans la boîte de dialogue Supprimer le jeton d'accès, passez en revue les informations, tapez DELETE, puis choisissez Supprimer le jeton d'accès.

Désactiver le provisionnement automatique

Utilisez la procédure suivante pour désactiver le provisionnement automatique dans la console IAM Identity Center.

Important

Vous devez supprimer le jeton d'accès avant de commencer cette procédure. Pour de plus amples informations, veuillez consulter [Supprimer un jeton d'accès](#).

Pour désactiver le provisionnement automatique dans la console IAM Identity Center

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, choisissez Désactiver.
4. Dans la boîte de dialogue Désactiver le provisionnement automatique, passez en revue les informations, tapez DISABLE, puis choisissez Désactiver le provisionnement automatique.

Faire pivoter un jeton d'accès

Un annuaire IAM Identity Center prend en charge jusqu'à deux jetons d'accès à la fois. Pour générer un jeton d'accès supplémentaire avant toute rotation, supprimez tous les jetons d'accès expirés ou non utilisés.

Si votre jeton d'accès SCIM est sur le point d'expirer, vous pouvez utiliser la procédure suivante pour faire pivoter un jeton d'accès existant dans la console IAM Identity Center.

Pour faire pivoter un jeton d'accès

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres dans le volet de navigation de gauche.

2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer le provisionnement.
3. Sur la page Provisionnement automatique, sous Jetons d'accès, notez l'ID du jeton que vous souhaitez faire pivoter.
4. Suivez les étapes décrites [Générer un jeton d'accès](#) pour créer un nouveau jeton. Si vous avez déjà créé le nombre maximum de jetons d'accès SCIM, vous devez d'abord supprimer l'un des jetons existants.
5. Accédez au site Web de votre fournisseur d'identité et configurez le nouveau jeton d'accès pour le provisionnement SCIM, puis testez la connectivité à IAM Identity Center à l'aide du nouveau jeton d'accès SCIM. Une fois que vous avez confirmé que le provisionnement fonctionne correctement à l'aide du nouveau jeton, passez à l'étape suivante de cette procédure.
6. Suivez les étapes décrites [Supprimer un jeton d'accès](#) pour supprimer l'ancien jeton d'accès que vous avez indiqué précédemment. Vous pouvez également utiliser la date de création du jeton comme indication du jeton à supprimer.

Auditez et réconciliez les ressources provisionnées automatiquement

SCIM vous permet de provisionner automatiquement des utilisateurs, des groupes et des adhésions à des groupes depuis votre source d'identité vers IAM Identity Center. Ce guide vous aide à vérifier et à réconcilier ces ressources afin de garantir une synchronisation précise.

Pourquoi auditer vos ressources ?

Un audit régulier permet de garantir que vos contrôles d'accès restent précis et que votre fournisseur d'identité (IdP) reste correctement synchronisé avec IAM Identity Center. Cela est particulièrement important pour la conformité en matière de sécurité et la gestion des accès.

Ressources que vous pouvez auditer :

- Utilisateurs
- Groupes
- Adhésions à des groupes

Vous pouvez utiliser les [commandes AWS Identity Store API](#) ou [CLI](#) pour effectuer l'audit et le rapprochement. Les exemples suivants utilisent des AWS CLI commandes. Pour les alternatives à l'API, reportez-vous aux [opérations correspondantes](#) dans la référence de l'API Identity Store.

Comment auditer les ressources

Voici des exemples expliquant comment auditer ces ressources à l'aide de AWS CLI commandes.

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Accès administrateur à IAM Identity Center.
- AWS CLI installé et configuré. Pour plus d'informations, consultez le [guide de l'utilisateur de l'interface de ligne de AWS commande](#).
- Autorisations IAM requises pour les commandes Identity Store.

Étape 1 : Répertorier les ressources actuelles

Vous pouvez consulter vos ressources actuelles à l'aide du AWS CLI.

Note

Lorsque vous utilisez le AWS CLI, la pagination est gérée automatiquement, sauf indication contraire de votre part. `--no-paginate` Si vous appelez directement l'API (par exemple, à l'aide d'un SDK ou d'un script personnalisé), gérez-le `NextToken` dans la réponse. Cela vous permet de récupérer tous les résultats sur plusieurs pages.

Exemple pour les utilisateurs

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Exemple pour les groupes

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Exemple pour les adhésions à des groupes

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

```
--identity-store-id IDENTITY_STORE_ID
--group-id GROUP_ID
```

Étape 2 : comparer avec votre source d'identité

Comparez les ressources répertoriées avec votre source d'identité pour identifier les éventuelles incohérences, telles que :

- Ressources manquantes qui devraient être provisionnées dans IAM Identity Center.
- Ressources supplémentaires qui devraient être supprimées d'IAM Identity Center.

Exemple pour les utilisateurs

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Exemple pour les groupes

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Exemple pour les adhésions à des groupes

```
# Add missing members
```



```
aws identitystore create-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID \  
  --member-id '{"UserId": "USER_ID"}'  
  
# Remove extra members  
aws identitystore delete-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --membership-id MEMBERSHIP_ID
```

Considérations

- Les commandes sont soumises à des [quotas de service et à une limitation des API](#).
- Lorsque vous constatez de nombreuses différences lors du rapprochement, apportez de petites modifications graduelles à AWS Identity Store. Cela vous permet d'éviter les erreurs qui affectent plusieurs utilisateurs.
- La synchronisation SCIM peut annuler vos modifications manuelles. Vérifiez les paramètres de votre IdP pour comprendre ce comportement.

Approvisionnement manuel

Certains IdPs ne sont pas compatibles avec le système de gestion des identités interdomaines (SCIM) ou ont une implémentation SCIM incompatible. Dans ces cas, vous pouvez configurer manuellement les utilisateurs via la console IAM Identity Center. Lorsque vous ajoutez des utilisateurs à IAM Identity Center, assurez-vous que le nom d'utilisateur est identique à celui que vous avez dans votre IdP. Au minimum, vous devez disposer d'une adresse e-mail et d'un nom d'utilisateur uniques. Pour de plus amples informations, veuillez consulter [Unicité du nom d'utilisateur et de l'adresse e-mail](#).

Vous devez également gérer tous les groupes manuellement dans IAM Identity Center. Pour ce faire, vous devez créer les groupes et les ajouter à l'aide de la console IAM Identity Center. Ces groupes n'ont pas besoin de correspondre à ce qui existe dans votre IdP. Pour de plus amples informations, veuillez consulter [Groupes](#).

Rotation des certificats SAML 2.0

IAM Identity Center utilise des certificats pour établir une relation de confiance SAML entre IAM Identity Center et votre fournisseur d'identité externe (IdP). Lorsque vous ajoutez un IdP externe dans IAM Identity Center, vous devez également obtenir au moins un certificat public SAML 2.0 X.509

auprès de l'IdP externe. Ce certificat est généralement installé automatiquement lors de l'échange de métadonnées IDP SAML lors de la création de la confiance.

En tant qu'administrateur du centre d'identité IAM, vous devrez parfois remplacer les anciens certificats IdP par des certificats plus récents. Par exemple, il se peut que vous deviez remplacer un certificat IdP lorsque la date d'expiration du certificat approche. Le processus de remplacement d'un ancien certificat par un nouveau est appelé rotation des certificats.

Rubriques

- [Faire pivoter un certificat SAML 2.0](#)
- [Indicateurs du statut d'expiration des certificats](#)

Faire pivoter un certificat SAML 2.0

Vous devrez peut-être importer des certificats périodiquement afin de remplacer les certificats non valides ou expirés émis par votre fournisseur d'identité. Cela permet d'éviter toute interruption ou interruption de l'authentification. Tous les certificats importés sont automatiquement actifs. Les certificats ne doivent être supprimés qu'après avoir vérifié qu'ils ne sont plus utilisés par le fournisseur d'identité associé.

Vous devez également tenir compte du fait que certains IdPs peuvent ne pas prendre en charge plusieurs certificats. Dans ce cas, le fait d'alterner les certificats avec ces derniers IdPs peut entraîner une interruption de service temporaire pour vos utilisateurs. Le service est rétabli lorsque la confiance avec cet IdP a été rétablie avec succès. Planifiez cette opération avec soin en dehors des heures de pointe si possible.

Note

Pour des raisons de sécurité, dès que des signes de compromission ou de mauvaise gestion d'un certificat SAML existant apparaissent, vous devez immédiatement le supprimer et le faire pivoter.

La rotation d'un certificat IAM Identity Center est un processus en plusieurs étapes qui implique les étapes suivantes :

- Obtenir un nouveau certificat auprès de l'IdP
- Importation du nouveau certificat dans IAM Identity Center

- Activation du nouveau certificat dans l'IdP
- Supprimer l'ancien certificat

Utilisez toutes les procédures suivantes pour terminer le processus de rotation des certificats tout en évitant toute interruption de l'authentification.

Étape 1 : obtenir un nouveau certificat auprès de l'IdP

Accédez au site Web de l'IdP et téléchargez leur certificat SAML 2.0. Assurez-vous que le fichier de certificat est téléchargé au format PEM codé. La plupart des fournisseurs vous permettent de créer plusieurs certificats SAML 2.0 dans l'IdP. Il est probable qu'ils soient marqués comme désactivés ou inactifs.

Étape 2 : Importer le nouveau certificat dans IAM Identity Center

Utilisez la procédure suivante pour importer le nouveau certificat à l'aide de la console IAM Identity Center.

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer l'authentification.
3. Sur la page Gérer les certificats SAML 2.0, choisissez Importer le certificat.
4. Dans la boîte de dialogue Importer un certificat SAML 2.0, choisissez Choisir un fichier, accédez à votre fichier de certificat et sélectionnez-le, puis choisissez Importer un certificat.

À ce stade, IAM Identity Center fera confiance à tous les messages SAML entrants signés à partir des deux certificats que vous avez importés.

Étape 3 : activer le nouveau certificat dans l'IdP

Retournez sur le site Web de l'IdP et marquez le nouveau certificat que vous avez créé précédemment comme principal ou actif. À ce stade, tous les messages SAML signés par l'IdP doivent utiliser le nouveau certificat.

Étape 4 : Supprimer l'ancien certificat

Suivez la procédure ci-dessous pour terminer le processus de rotation des certificats pour votre IdP. Il doit toujours y avoir au moins un certificat valide répertorié, et il ne peut pas être supprimé.

 Note

Assurez-vous que votre fournisseur d'identité ne signe plus les réponses SAML avec ce certificat avant de le supprimer.

1. Sur la page Gérer les certificats SAML 2.0, sélectionnez le certificat que vous souhaitez supprimer. Sélectionnez Delete (Supprimer).
2. Dans la boîte de dialogue Supprimer le certificat SAML 2.0, tapez **DELETE** pour confirmer, puis choisissez Supprimer.
3. Retournez sur le site Web de l'IdP et effectuez les étapes nécessaires pour supprimer l'ancien certificat inactif.

Indicateurs du statut d'expiration des certificats

La page Gérer les certificats SAML 2.0 affiche des icônes d'indicateur de statut colorées dans la colonne Expire le jour à côté de chaque certificat de la liste. Ce qui suit décrit les critères utilisés par IAM Identity Center pour déterminer quelle icône est affichée pour chaque certificat.

- Rouge — Indique qu'un certificat a expiré.
- Jaune — Indique qu'un certificat expire dans 90 jours ou moins.
- Vert — Indique qu'un certificat est valide et le reste pendant au moins 90 jours supplémentaires.

Pour vérifier l'état actuel d'un certificat

1. Dans la [console IAM Identity Center](#), sélectionnez Paramètres.
2. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Gérer l'authentification.
3. Sur la page Gérer l'authentification SAML 2.0, sous Gérer les certificats SAML 2.0, vérifiez le statut des certificats dans la liste, comme indiqué dans la colonne Expire le.

Microsoft ADannuaire

Avec AWS IAM Identity Center, vous pouvez connecter un annuaire autogéré dans Active Directory (AD) ou un annuaire dans en AWS Managed Microsoft AD utilisant AWS Directory Service. Ce

répertoire Microsoft AD définit le pool d'identités que les administrateurs peuvent extraire lorsqu'ils utilisent la console IAM Identity Center pour attribuer un accès par authentification unique. Après avoir connecté votre annuaire d'entreprise à IAM Identity Center, vous pouvez autoriser vos utilisateurs ou groupes AD à accéder aux applications Comptes AWS, ou aux deux.

AWS Directory Service vous permet de configurer et d'exécuter un AWS Managed Microsoft AD répertoire autonome hébergé dans le AWS Cloud. Vous pouvez également l'utiliser Directory Service pour connecter vos AWS ressources à un AD autogéré existant. Pour que AWS Directory Service la configuration fonctionne avec votre AD autogéré, vous devez d'abord établir des relations de confiance afin d'étendre l'authentification au cloud.

IAM Identity Center utilise la connexion fournie par Directory Service pour effectuer une authentification directe sur l'instance AD source. Lorsque vous l'utilisez AWS Managed Microsoft AD comme source d'identité, IAM Identity Center peut travailler avec des utilisateurs depuis AWS Managed Microsoft AD ou vers n'importe quel domaine connecté via un AD Trust. Si vous souhaitez localiser vos utilisateurs dans quatre domaines ou plus, les utilisateurs doivent utiliser la DOMAIN \user syntaxe comme nom d'utilisateur lorsqu'ils se connectent à IAM Identity Center.

Remarques

- Comme étape préalable, assurez-vous que votre AD Connector ou votre répertoire dans AWS Managed Microsoft AD in Directory Service se trouve dans votre compte AWS Organizations de gestion.
- IAM Identity Center ne prend pas en charge Simple AD basé sur SAMBA 4 en tant qu'annuaire connecté.
- IAM Identity Center ne peut pas synchroniser les principes de sécurité étrangers (FSPs). Si un groupe AWS Managed Microsoft AD contient des membres d'un domaine approuvé FSPs, ces membres ne seront pas synchronisés.

Pour une démonstration du processus d'utilisation d'Active Directory comme source d'identité pour IAM Identity Center, regardez la YouTube vidéo suivante :

[Utilisation d'Active Directory comme source d'identité pour AWS IAM Identity Center | Amazon Web Services](#)

Considérations relatives à l'utilisation d'Active Directory

Si vous souhaitez utiliser Active Directory comme source d'identité, votre configuration doit répondre aux conditions préalables suivantes :

- Si vous utilisez AWS Managed Microsoft AD, vous devez activer IAM Identity Center dans le même Région AWS endroit où votre AWS Managed Microsoft AD annuaire est configuré. IAM Identity Center stocke les données d'attribution dans la même région que le répertoire. Pour administrer IAM Identity Center, vous devrez peut-être passer à la région dans laquelle IAM Identity Center est configuré. Notez également que le portail AWS d'accès utilise la même URL d'accès que votre annuaire.
- Utilisez un Active Directory résidant dans le compte de gestion :

Vous devez disposer d'un AD Connector ou d'un AWS Managed Microsoft AD annuaire AD Connector existant dans votre compte de gestion AWS Directory Service, et celui-ci doit résider dans votre compte AWS Organizations de gestion. Vous ne pouvez connecter qu'un seul répertoire AD Connector ou un seul annuaire AWS Managed Microsoft AD à la fois. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisez AWS Managed Microsoft AD. Pour en savoir plus, consultez :

- [Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center](#)
- [Connectez un annuaire autogéré dans Active Directory à IAM Identity Center](#)
- Utilisez un Active Directory résidant dans le compte administrateur délégué :

Si vous envisagez d'activer l'administrateur délégué d'IAM Identity Center et d'utiliser Active Directory comme source d'identité IAM Identity Center, vous pouvez utiliser un connecteur AD Connector ou un AWS Managed Microsoft AD annuaire existant configuré dans AWS Directory résidant dans le compte d'administrateur délégué.

Si vous décidez de remplacer la source d'identité d'IAM Identity Center par une autre source par Active Directory, ou de passer d'Active Directory à une autre source, le répertoire doit résider (appartenir à) le compte membre administrateur délégué d'IAM Identity Center, s'il en existe un ; sinon, il doit figurer dans le compte de gestion.

Connectez Active Directory et spécifiez un utilisateur

Si vous utilisez déjà Active Directory, les rubriques suivantes vous aideront à préparer la connexion de votre annuaire à IAM Identity Center.

Vous pouvez connecter un AWS Managed Microsoft AD annuaire ou un annuaire autogéré dans Active Directory avec IAM Identity Center.

 Note

IAM Identity Center ne prend pas en charge SAMBA4 Simple AD en tant que source d'identité.

AWS Managed Microsoft AD

1. Consultez les directives dans [Microsoft ADannuaire](#).
2. Suivez les étapes de [Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center](#).
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour de plus amples informations, veuillez consulter [Synchroniser un utilisateur administratif dans IAM Identity Center](#).

Annuaire autogéré dans Active Directory

1. Consultez les directives dans [Microsoft ADannuaire](#).
2. Suivez les étapes de [Connectez un annuaire autogéré dans Active Directory à IAM Identity Center](#).
3. Configurez Active Directory pour synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center. Pour de plus amples informations, veuillez consulter [Synchroniser un utilisateur administratif dans IAM Identity Center](#).

IdP externe

1. Consultez les directives dans [Fournisseurs d'identité externes](#).
2. Suivez les étapes de [Comment se connecter à un fournisseur d'identité externe](#).
3. Configurez votre IdP pour connecter les utilisateurs à IAM Identity Center.

 Note

Avant de configurer le provisionnement automatique par groupe de toutes les identités de votre personnel, depuis votre IdP vers IAM Identity Center, nous vous recommandons de

synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives dans IAM Identity Center.

Synchroniser un utilisateur administratif dans IAM Identity Center

Après avoir connecté votre Active Directory à IAM Identity Center, vous pouvez spécifier un utilisateur auquel vous souhaitez accorder des autorisations administratives, puis synchroniser cet utilisateur depuis votre annuaire avec IAM Identity Center.

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Utilisateurs, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Dans l'onglet Utilisateurs, sous Utilisateur, entrez le nom d'utilisateur exact et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, procédez comme suit :
 - a. Vérifiez que l'utilisateur auquel vous souhaitez accorder des autorisations administratives est spécifié.
 - b. Cochez la case située à gauche du nom d'utilisateur.
 - c. Sélectionnez Soumettre.
7. Sur la page Gérer la synchronisation, l'utilisateur que vous avez spécifié apparaît dans la liste Utilisateurs synchronisés.
8. Dans le panneau de navigation, choisissez utilisateurs.
9. Sur la page Utilisateurs, l'utilisateur que vous avez spécifié peut mettre un certain temps à apparaître dans la liste. Cliquez sur l'icône d'actualisation pour mettre à jour la liste des utilisateurs.

À ce stade, votre utilisateur n'a pas accès au compte de gestion. Vous allez configurer l'accès administratif à ce compte en créant un ensemble d'autorisations administratives et en affectant l'utilisateur à cet ensemble d'autorisations. Pour de plus amples informations, veuillez consulter [Crée un jeu d'autorisations](#).

Provisionnement lorsque les utilisateurs proviennent d'Active Directory

IAM Identity Center utilise la connexion fournie par le Directory Service pour synchroniser les informations relatives aux utilisateurs, aux groupes et aux membres entre votre répertoire source dans Active Directory et le magasin d'identités IAM Identity Center. Aucune information de mot de passe n'est synchronisée avec IAM Identity Center, car l'authentification des utilisateurs s'effectue directement depuis le répertoire source dans Active Directory. Ces données d'identité sont utilisées par les applications pour faciliter les scénarios de recherche, d'autorisation et de collaboration intégrés à l'application sans renvoyer l'activité LDAP au répertoire source dans Active Directory.

Pour plus d'informations ci-dessus sur le provisionnement, consultez [Provisionnement d'utilisateurs et de groupes](#).

Rubriques

- [Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center](#)
- [Connectez un annuaire autogéré dans Active Directory à IAM Identity Center](#)
- [Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes](#)
- [Synchronisation AD configurable par IAM Identity Center](#)

Connecter un annuaire AWS Managed Microsoft AD à IAM Identity Center

Utilisez la procédure suivante pour connecter un répertoire géré par AWS Directory Service à IAM Identity Center. AWS Managed Microsoft AD

Pour vous connecter AWS Managed Microsoft AD à IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).

Note

Assurez-vous que la console IAM Identity Center utilise l'une des régions dans lesquelles se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Cliquez sur Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, puis sélectionnez Actions > Modifier la source d'identité.

4. Sous Choisir une source d'identité, sélectionnez Active Directory, puis cliquez sur Suivant.
5. Sous Connect Active Directory, choisissez un répertoire dans la AWS Managed Microsoft AD liste, puis cliquez sur Next.
6. Sous Confirmer la modification, passez en revue les informations et lorsque vous êtes prêt, tapez ACCEPT, puis choisissez Modifier la source d'identité.

 Important

Pour spécifier un utilisateur dans Active Directory en tant qu'utilisateur administratif dans IAM Identity Center, vous devez d'abord synchroniser l'utilisateur auquel vous souhaitez accorder des autorisations administratives depuis Active Directory vers IAM Identity Center. Pour ce faire, suivez les étapes de [Synchroniser un utilisateur administratif dans IAM Identity Center](#).

Connectez un annuaire autogéré dans Active Directory à IAM Identity Center

Les utilisateurs de votre annuaire autogéré dans Active Directory (AD) peuvent également accéder par authentification unique au portail d'accès Comptes AWS et aux applications qui s'y trouvent. Pour configurer l'accès à authentification unique pour ces utilisateurs, vous pouvez effectuer l'une des opérations suivantes :

- Création d'une relation de confiance bidirectionnelle : lorsque des relations de confiance bidirectionnelles sont créées entre AWS Managed Microsoft AD et un annuaire autogéré dans AD, les utilisateurs de votre annuaire autogéré dans AD peuvent se connecter avec leurs informations d'identification d'entreprise à divers AWS services et applications métier. Les approbations unidirectionnelles ne fonctionnent pas avec IAM Identity Center.

AWS IAM Identity Center nécessite une confiance bidirectionnelle afin d'être autorisé à lire les informations relatives aux utilisateurs et aux groupes de votre domaine afin de synchroniser les métadonnées des utilisateurs et des groupes. IAM Identity Center utilise ces métadonnées pour attribuer l'accès à des ensembles d'autorisations ou à des applications. Les métadonnées des utilisateurs et des groupes sont également utilisées par les applications à des fins de collaboration, par exemple lorsque vous partagez un tableau de bord avec un autre utilisateur ou un autre groupe. La confiance accordée par Directory Service Microsoft Active Directory à votre domaine permet à IAM Identity Center de faire confiance à votre domaine pour l'authentification. La

confiance dans le sens opposé accorde des AWS autorisations pour lire les métadonnées des utilisateurs et des groupes.

Pour plus d'informations sur la configuration d'une confiance bidirectionnelle, voir [Quand créer une relation de confiance](#) dans le Guide d'AWS Directory Service administration.

 Note

Pour utiliser AWS des applications, telles que IAM Identity Center, pour lire les utilisateurs de l' Directory Service annuaire provenant de domaines approuvés, les Directory Service comptes doivent disposer d'autorisations sur l' `userAccountControl` attribut associé aux utilisateurs de confiance. Sans autorisations de lecture pour cet attribut, AWS les applications ne sont pas en mesure de déterminer si le compte est activé ou désactivé. L'accès en lecture à cet attribut est fourni par défaut lorsqu'une approbation est créée. Si vous refusez l'accès à cet attribut (ce n'est pas recommandé), vous empêcherez des applications telles qu'Identity Center de lire les utilisateurs fiables. La solution consiste à autoriser spécifiquement l'accès en lecture à l'`userAccountControl` attribut sur les comptes de AWS service sous l'unité d'organisation AWS réservée (préfixée par `AWS_`).

- Création d'un AD Connector — AD Connector est une passerelle d'annuaire qui peut rediriger les demandes d'annuaire vers votre AD autogéré sans mettre en cache aucune information dans le cloud. Pour plus d'informations, voir [Connect to a Directory](#) dans le Guide AWS Directory Service d'administration. Les points suivants doivent être pris en compte lors de l'utilisation d'AD Connector :
 - Si vous connectez IAM Identity Center à un annuaire AD Connector, toute future réinitialisation du mot de passe utilisateur devra être effectuée depuis AD. Cela signifie que les utilisateurs ne pourront pas réinitialiser leur mot de passe depuis le portail AWS d'accès.
 - Si vous utilisez AD Connector pour connecter votre service de domaine Active Directory à IAM Identity Center, IAM Identity Center n'a accès qu'aux utilisateurs et aux groupes du domaine unique auquel AD Connector est attaché. Si vous devez prendre en charge plusieurs domaines ou forêts, utilisez Directory Service Microsoft Active Directory.

 Note

IAM Identity Center ne fonctionne pas avec les annuaires Simple AD SAMBA4 basés sur Simple AD.

Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes

Les mappages d'attributs sont utilisés pour mapper les types d'attributs qui existent dans IAM Identity Center avec des attributs similaires dans votre source d'identité externe Google Workspace, tels que Microsoft Active Directory (AD), et Okta. IAM Identity Center extrait les attributs utilisateur de votre source d'identité et les associe aux attributs utilisateur IAM Identity Center.

Si votre centre d'identité IAM est synchronisé pour utiliser un fournisseur d'identité externe (IdP), par exemple Google Workspace Okta, ou Ping comme source d'identité, vous devrez mapper vos attributs dans votre IdP.

IAM Identity Center préremplit un ensemble d'attributs pour vous sous l'onglet Mappages d'attributs situé sur sa page de configuration. IAM Identity Center utilise ces attributs utilisateur pour remplir les assertions SAML (sous forme d'attributs SAML) qui sont envoyées à l'application. Ces attributs utilisateur sont à leur tour extraits de votre source d'identité. Chaque application détermine la liste des attributs SAML 2.0 dont elle a besoin pour une authentification unique réussie. Pour de plus amples informations, veuillez consulter [Associez les attributs de votre application aux attributs d'IAM Identity Center](#).

IAM Identity Center gère également un ensemble d'attributs pour vous dans la section Mappages d'attributs de votre page de configuration Active Directory si vous utilisez Active Directory comme source d'identité. Pour de plus amples informations, veuillez consulter [Mappage des attributs utilisateur entre IAM Identity Center et Microsoft AD l'annuaire](#).

Attributs du fournisseur d'identité externe pris en charge

Le tableau suivant répertorie tous les attributs de fournisseur d'identité (IdP) externes pris en charge et pouvant être mappés aux attributs que vous pouvez utiliser lors de la configuration [Attributs pour le contrôle d'accès](#) dans IAM Identity Center. Lorsque vous utilisez des assertions SAML, vous pouvez utiliser les attributs pris en charge par votre IdP.

Attributs pris en charge dans votre IdP

`${path:userName}`

`${path:name.familyName}`

`${path:name.givenName}`

Attributs pris en charge dans votre IdP

```
${path:displayName}
```

```
${path:nickName}
```

```
${path:emails[primary eq true].value}
```

```
${path:addresses[type eq "work"].streetAddress}
```

```
${path:addresses[type eq "work"].locality}
```

```
${path:addresses[type eq "work"].region}
```

```
${path:addresses[type eq "work"].postalCode}
```

```
${path:addresses[type eq "work"].country}
```

```
${path:addresses[type eq "work"].formatted}
```

```
${path:phoneNumbers[type eq "work"].value}
```

```
${path:userType}
```

```
${path:title}
```

```
${path:locale}
```

```
${path:timezone}
```

```
${path:enterprise.employeeNumber}
```

```
${path:enterprise.costCenter}
```

```
${path:enterprise.organization}
```

```
${path:enterprise.division}
```

```
${path:enterprise.department}
```

```
${path:enterprise.manager.value}
```

Mappages par défaut entre IAM Identity Center et Microsoft AD

Le tableau suivant répertorie les mappages par défaut des attributs utilisateur dans IAM Identity Center avec les attributs utilisateur de votre Microsoft AD annuaire. IAM Identity Center prend uniquement en charge la liste des attributs de l'attribut Utilisateur dans la colonne IAM Identity Center.

Attribut utilisateur dans IAM Identity Center	Correspond à cet attribut dans votre Active Directory
displayname	<code>\${displayname}</code>
emails[?primary].value *	<code>\${mail}</code>
externalid	<code>\${objectguid}</code>
name.givenname	<code>\${givenname}</code>
name.familyname	<code>\${sn}</code>
name.middlename	<code>\${initials}</code>
sid	<code>\${objectsid}</code>
username	<code>\${userprincipalname}</code>

* L'attribut e-mail dans IAM Identity Center doit être unique dans l'annuaire.

Attribut de groupe dans IAM Identity Center	Correspond à cet attribut dans votre Active Directory
externalid	<code>\${objectguid}</code>
description	<code>\${description}</code>
displayname	<code>\${samaccountname}@{associateddomain}</code>

Considérations

- Si vous n'avez aucune attribution pour vos utilisateurs et groupes dans IAM Identity Center lorsque vous activez la synchronisation AD configurable, les mappages par défaut des tableaux précédents sont utilisés. Pour plus d'informations sur la personnalisation de ces mappages, consultez [Configurez les mappages d'attributs pour votre synchronisation](#).
- Certains attributs d'IAM Identity Center ne peuvent pas être modifiés car ils sont immuables et mappés par défaut à des attributs d'annuaire Microsoft AD spécifiques.

Par exemple, « nom d'utilisateur » est un attribut obligatoire dans IAM Identity Center. Si vous associez « nom d'utilisateur » à un attribut d'annuaire AD avec une valeur vide, IAM Identity Center considérera cette windowsUpn valeur comme valeur par défaut pour « nom d'utilisateur ». Si vous souhaitez modifier le mappage d'attributs pour « nom d'utilisateur » par rapport à votre mappage actuel, vérifiez que les flux IAM Identity Center dépendants du « nom d'utilisateur » continueront de fonctionner comme prévu, avant d'effectuer la modification.

Microsoft ADAttributs pris en charge pour IAM Identity Center

Le tableau suivant répertorie tous les attributs d'Microsoft ADannuaire pris en charge et pouvant être mappés aux attributs utilisateur dans IAM Identity Center.

Attributs pris en charge dans votre annuaire Microsoft AD

`${samaccountname}`

`${description}`

`${objectguid}`

`${objectsid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

Attributs pris en charge dans votre annuaire Microsoft AD

```
${userprincipalname}
```

```
${displayname}
```

```
${distinguishedname}
```

```
${proxyaddresses[?type == "SMTP"].value}
```

```
${proxyaddresses[?type == "smtp"].value}
```

```
${useraccountcontrol}
```

```
${associateddomain}
```

Considérations

- Vous pouvez spécifier n'importe quelle combinaison d'attributs d'annuaire Microsoft AD pris en charge à mapper à un seul attribut mutable dans IAM Identity Center.

Attributs IAM Identity Center pris en charge pour Microsoft AD

Le tableau suivant répertorie tous les attributs IAM Identity Center pris en charge et pouvant être mappés aux attributs utilisateur de votre annuaire Microsoft AD. Après avoir configuré les mappages d'attributs de votre application, vous pouvez utiliser ces mêmes attributs IAM Identity Center pour les mapper aux attributs réels utilisés par cette application.

Attributs pris en charge dans IAM Identity Center pour Active Directory

```
${user:AD_GUID}
```

```
${user:AD_SID}
```

```
${user:email}
```

```
${user:familyName}
```

```
${user:givenName}
```


Attributs pris en charge dans IAM Identity Center pour Active Directory

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

Mappage des attributs utilisateur entre IAM Identity Center et Microsoft AD l'annuaire

Vous pouvez utiliser la procédure suivante pour spécifier la manière dont vos attributs utilisateur dans IAM Identity Center doivent correspondre aux attributs correspondants dans votre Microsoft AD annuaire.

Pour associer les attributs d'IAM Identity Center aux attributs de votre annuaire

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Attributs pour le contrôle d'accès, puis sélectionnez Gérer les attributs.
4. Sur la page Gérer l'attribut pour le contrôle d'accès, recherchez l'attribut que vous souhaitez mapper dans IAM Identity Center, puis tapez une valeur dans la zone de texte. Par exemple, vous souhaitez peut-être mapper l'attribut utilisateur IAM Identity Center **email** à l'attribut d'annuaire Microsoft AD. **`${mail}`**
5. Sélectionnez Enregistrer les modifications.

Synchronisation AD configurable par IAM Identity Center

La synchronisation Active Directory (AD) configurable par IAM Identity Center vous permet de configurer explicitement les identités dans Microsoft Active Directory qui sont automatiquement synchronisées dans IAM Identity Center et de contrôler le processus de synchronisation.

- Avec cette méthode de synchronisation, vous pouvez effectuer les opérations suivantes :
 - Contrôlez les limites des données en définissant explicitement les utilisateurs et les groupes dans Microsoft Active Directory qui sont automatiquement synchronisés dans IAM Identity

Center. Vous pouvez [ajouter des utilisateurs et des groupes](#) ou [supprimer des utilisateurs et des groupes](#) pour modifier l'étendue de la synchronisation à tout moment.

- Attribuez aux utilisateurs et aux groupes synchronisés un [accès](#) par authentification unique Comptes AWS ou un [accès aux applications](#). Les applications peuvent être des applications AWS gérées ou des applications gérées par le client.
- Contrôlez le processus de synchronisation en [interrompant et en reprenant la synchronisation selon les besoins](#). Cela vous permet de réguler la charge sur les systèmes de production.

Prérequis et considérations

Avant d'utiliser la synchronisation AD configurable, tenez compte des conditions préalables et des considérations suivantes :

- Spécification des utilisateurs et des groupes à synchroniser dans Active Directory

Avant de pouvoir utiliser IAM Identity Center pour attribuer à de nouveaux utilisateurs et groupes l'accès à Comptes AWS des applications AWS gérées ou à des applications gérées par le client, vous devez spécifier les utilisateurs et les groupes à synchroniser dans Active Directory, puis les synchroniser dans IAM Identity Center.

- Synchronisation AD configurable : IAM Identity Center ne recherche pas directement les utilisateurs et les groupes dans votre contrôleur de domaine. Au lieu de cela, vous devez d'abord spécifier la liste des utilisateurs et des groupes à synchroniser. Vous pouvez configurer cette liste, également appelée étendue de synchronisation, de l'une des manières suivantes, selon que vous avez des utilisateurs et des groupes déjà synchronisés dans IAM Identity Center ou que vous avez de nouveaux utilisateurs et groupes que vous synchronisez pour la première fois à l'aide de la synchronisation AD configurable.
- Utilisateurs et groupes existants : si certains de vos utilisateurs et groupes sont déjà synchronisés dans IAM Identity Center, l'étendue de synchronisation dans la synchronisation AD configurable est préremplie avec une liste de ces utilisateurs et groupes. Pour attribuer de nouveaux utilisateurs ou groupes, vous devez les ajouter spécifiquement à la zone de synchronisation. Pour de plus amples informations, veuillez consulter [Ajoutez des utilisateurs et des groupes à votre zone de synchronisation](#).
- Nouveaux utilisateurs et groupes : si vous souhaitez attribuer à de nouveaux utilisateurs et groupes l'accès aux Comptes AWS applications, vous devez spécifier les utilisateurs et les groupes à ajouter à l'étendue de synchronisation dans AD Sync configurable avant de pouvoir

utiliser IAM Identity Center pour effectuer l'attribution. Pour de plus amples informations, veuillez consulter [Ajoutez des utilisateurs et des groupes à votre zone de synchronisation](#).

- Attribuer des attributions à des groupes imbriqués dans Active Directory

Les groupes membres d'autres groupes sont appelés groupes imbriqués (ou groupes d'enfants).

- Synchronisation AD configurable : l'utilisation de la synchronisation AD configurable pour attribuer des attributions à un groupe dans Active Directory contenant des groupes imbriqués peut augmenter le nombre d'utilisateurs ayant accès aux applications Comptes AWS ou à celles-ci. Dans ce cas, l'attribution s'applique à tous les utilisateurs, y compris ceux des groupes imbriqués. Par exemple, si vous accordez l'accès au groupe A et que le groupe B est membre du groupe A, les membres du groupe B héritent également de cet accès.
- Mise à jour des workflows automatisés

Si vous avez des flux de travail automatisés qui utilisent les actions de l'API du magasin d'identités IAM Identity Center et les actions de l'API d'attribution d'IAM Identity Center pour attribuer aux nouveaux utilisateurs et groupes l'accès aux comptes et aux applications, et pour les synchroniser dans IAM Identity Center, vous devez ajuster ces flux de travail avant le 15 avril 2022 afin qu'ils fonctionnent comme prévu avec la synchronisation AD configurable. La synchronisation AD configurable modifie l'ordre dans lequel l'attribution et le provisionnement des utilisateurs et des groupes ont lieu, ainsi que la manière dont les requêtes sont effectuées.

- Synchronisation AD configurable : le provisionnement a lieu en premier et n'est pas effectué automatiquement. Au lieu de cela, vous devez d'abord ajouter explicitement des utilisateurs et des groupes au magasin d'identités en les ajoutant à votre étendue de synchronisation. Pour plus d'informations sur les étapes recommandées pour automatiser votre configuration de synchronisation pour une synchronisation AD configurable, consultez [Automatisez votre configuration de synchronisation pour une synchronisation AD configurable](#).

Rubriques

- [Comment fonctionne la synchronisation AD configurable](#)
- [Configurez les mappages d'attributs pour votre synchronisation](#)
- [Configuration de la première synchronisation entre Active Directory et IAM Identity Center](#)
- [Ajoutez des utilisateurs et des groupes à votre zone de synchronisation](#)
- [Supprimer des utilisateurs et des groupes de votre zone de synchronisation](#)

- [Pause et reprise de la synchronisation](#)
- [Automatisez votre configuration de synchronisation pour une synchronisation AD configurable](#)

Comment fonctionne la synchronisation AD configurable

IAM Identity Center actualise les données d'identité basées sur la publicité dans le magasin d'identités en utilisant le processus suivant. Pour en savoir plus sur les prérequis, consultez [Prérequis et considérations](#).

Création

Après avoir connecté votre annuaire autogéré dans Active Directory ou votre AWS Managed Microsoft AD annuaire géré par Directory Service IAM Identity Center, vous pouvez configurer de manière explicite les utilisateurs et les groupes Active Directory que vous souhaitez synchroniser dans le magasin d'identités IAM Identity Center. Les identités que vous choisirez seront synchronisées toutes les trois heures environ dans le magasin d'identités IAM Identity Center. Selon la taille de votre répertoire, le processus de synchronisation peut prendre plus de temps.

Les groupes membres d'autres groupes (appelés groupes imbriqués ou groupes enfants) sont également enregistrés dans le magasin d'identités.

Vous ne pouvez attribuer l'accès à de nouveaux utilisateurs ou groupes qu'après leur synchronisation dans la banque d'identités IAM Identity Center.

Mettre à jour

Les données d'identité de la banque d'identités d'IAM Identity Center restent actualisées en lisant régulièrement les données du répertoire source dans Active Directory. IAM Identity Center synchronise les données de votre Active Directory toutes les heures selon un cycle de synchronisation par défaut. La synchronisation des données dans IAM Identity Center peut prendre entre 30 minutes et 2 heures, en fonction de la taille de votre Active Directory.

Les objets d'utilisateur et de groupe inclus dans la zone de synchronisation et leurs appartenances sont créés ou mis à jour dans IAM Identity Center pour être mappés aux objets correspondants dans le répertoire source d'Active Directory. Pour les attributs utilisateur, seul le sous-ensemble d'attributs répertorié dans la section Attributs pour le contrôle d'accès de la console IAM Identity Center est mis à jour dans IAM Identity Center. Un cycle de synchronisation peut être nécessaire pour que les mises à jour d'attributs que vous effectuez dans Active Directory soient répercutées dans IAM Identity Center.

Vous pouvez également mettre à jour le sous-ensemble d'utilisateurs et de groupes que vous synchronisez dans la banque d'identités IAM Identity Center. Vous pouvez choisir d'ajouter de nouveaux utilisateurs ou groupes à ce sous-ensemble ou de les supprimer. Toutes les identités que vous ajoutez sont synchronisées lors de la prochaine synchronisation planifiée. Les identités que vous supprimez du sous-ensemble ne seront plus mises à jour dans la banque d'identités IAM Identity Center. Tout utilisateur qui n'est pas synchronisé pendant plus de 28 jours sera désactivé dans la banque d'identités IAM Identity Center. Les objets utilisateur correspondants seront automatiquement désactivés dans la banque d'identités IAM Identity Center lors du prochain cycle de synchronisation, sauf s'ils font partie d'un autre groupe qui fait toujours partie de la zone de synchronisation.

Suppression

Les utilisateurs et les groupes sont supprimés de la banque d'identités IAM Identity Center lorsque les objets d'utilisateur ou de groupe correspondants sont supprimés du répertoire source dans Active Directory. Vous pouvez également supprimer explicitement des objets utilisateur de la banque d'identités IAM Identity Center à l'aide de la console IAM Identity Center. Si vous utilisez la console IAM Identity Center, vous devez également supprimer les utilisateurs de la zone de synchronisation afin de vous assurer qu'ils ne seront pas resynchronisés dans IAM Identity Center lors du prochain cycle de synchronisation.

Vous pouvez également suspendre et relancer la synchronisation à tout moment. Si vous suspendez la synchronisation pendant plus de 28 jours, tous vos utilisateurs seront désactivés.

Configurez les mappages d'attributs pour votre synchronisation

Pour plus d'informations sur les attributs disponibles, consultez [Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes](#).

Pour configurer les mappages d'attributs dans IAM Identity Center avec votre annuaire

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sous Gérer la synchronisation, choisissez Afficher le mappage des attributs.
5. Sous Attributs utilisateur Active Directory, configurez les attributs du magasin d'identités IAM Identity Center et les attributs utilisateur Active Directory. Par exemple, vous souhaitez peut-

être mapper l'attribut de banque d'identités IAM Identity Center email à l'attribut d'annuaire des utilisateurs Active Directory. `${objectguid}`

 Note

Sous Attributs de groupe, les attributs de banque d'identités IAM Identity Center et les attributs de groupe Active Directory ne peuvent pas être modifiés.

6. Sélectionnez Enregistrer les modifications. Cela vous ramène à la page Gérer la synchronisation.

Configuration de la première synchronisation entre Active Directory et IAM Identity Center

Si vous synchronisez vos utilisateurs et groupes depuis Active Directory vers IAM Identity Center pour la première fois, procédez comme suit. Vous pouvez également suivre les étapes décrites dans la section [Modifier la source de votre identité](#) pour modifier votre source d'identité d'IAM Identity Center à Active Directory.

Configuration guidée

1. Ouvrez la [console IAM Identity Center](#).

 Note

Assurez-vous que la console IAM Identity Center utilise l'un des emplacements Régions AWS où se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Cliquez sur Paramètres.
3. En haut de la page, dans le message de notification, choisissez Démarrer la configuration guidée.
4. À l'étape 1, facultatif : configurez les mappages d'attributs, passez en revue les mappages d'attributs par défaut pour les utilisateurs et les groupes. Si aucune modification n'est requise, choisissez Next. Si des modifications sont nécessaires, apportez-les, puis choisissez Enregistrer les modifications.
5. À l'étape 2, facultatif : configurer l'étendue de la synchronisation, cliquez sur l'onglet Utilisateurs. Entrez ensuite le nom d'utilisateur exact de l'utilisateur que vous souhaitez ajouter à votre étendue de synchronisation et choisissez Ajouter. Ensuite, choisissez l'onglet Groupes. Entrez le nom exact du groupe que vous souhaitez ajouter à votre étendue de synchronisation et

choisissez Ajouter. Ensuite, choisissez Suivant. Si vous souhaitez ajouter des utilisateurs et des groupes à votre zone de synchronisation ultérieurement, n'apportez aucune modification et choisissez Next.

6. Dans Étape 3 : Vérifiez et enregistrez la configuration, confirmez vos mappages d'attributs dans Étape 1 : Mappages d'attributs et vos utilisateurs et groupes dans Étape 2 : Étendue de synchronisation. Choisissez Save configuration. Cela vous amène à la page Gérer la synchronisation.

Ajoutez des utilisateurs et des groupes à votre zone de synchronisation

 Note

Lorsque vous ajoutez des groupes à votre zone de synchronisation, synchronisez les groupes directement à partir du domaine local approuvé plutôt qu'à partir des groupes du AWS Managed Microsoft AD domaine. Les groupes synchronisés directement depuis le domaine sécurisé contiennent des objets utilisateur réels auxquels IAM Identity Center peut accéder et synchroniser avec succès.

Ajoutez vos utilisateurs et groupes Active Directory à IAM Identity Center en suivant ces étapes.

Pour ajouter des utilisateurs

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Utilisateurs, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Dans l'onglet Utilisateurs, sous Utilisateur, entrez le nom d'utilisateur exact et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, passez en revue l'utilisateur que vous souhaitez ajouter.
7. Sélectionnez Soumettre.
8. Dans le panneau de navigation, choisissez utilisateurs. Si l'utilisateur que vous avez spécifié n'apparaît pas dans la liste, cliquez sur l'icône d'actualisation pour mettre à jour la liste des utilisateurs.

Pour ajouter des groupes

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sur la page Gérer la synchronisation, choisissez l'onglet Groupes, puis sélectionnez Ajouter des utilisateurs et des groupes.
5. Cliquez sur l'onglet Groupes (Groupes). Sous Groupe, entrez le nom exact du groupe et choisissez Ajouter.
6. Sous Utilisateurs et groupes ajoutés, passez en revue le groupe que vous souhaitez ajouter.
7. Sélectionnez Soumettre.
8. Dans le panneau de navigation, choisissez Groupes . Si le groupe que vous avez spécifié n'apparaît pas dans la liste, cliquez sur l'icône d'actualisation pour mettre à jour la liste des groupes.

Supprimer des utilisateurs et des groupes de votre zone de synchronisation

Pour plus d'informations sur ce qui se passe lorsque vous supprimez des utilisateurs et des groupes de votre zone de synchronisation, consultez [Comment fonctionne la synchronisation AD configurable](#).

Pour supprimer des utilisateurs

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sélectionnez l'onglet Utilisateurs.
5. Sous Utilisateurs synchronisés, cochez la case à côté de l'utilisateur que vous souhaitez supprimer. Pour supprimer tous les utilisateurs, cochez la case à côté de Nom d'utilisateur.
6. Cliquez sur Supprimer.

Pour supprimer des groupes

1. Ouvrez la [console IAM Identity Center](#).

2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Cliquez sur l'onglet Groups (Groupes).
5. Sous Groupes dans l'étendue de synchronisation, cochez la case à côté de l'utilisateur que vous souhaitez supprimer. Pour supprimer tous les groupes, cochez la case à côté du nom du groupe.
6. Cliquez sur Supprimer.

Pause et reprise de la synchronisation

La suspension de votre synchronisation interrompt tous les futurs cycles de synchronisation et empêche que les modifications que vous apportez aux utilisateurs et aux groupes dans Active Directory ne soient reflétées dans IAM Identity Center. Lorsque vous reprenez la synchronisation, le cycle de synchronisation prend en compte ces modifications lors de la prochaine synchronisation planifiée.

Pour suspendre votre synchronisation

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sous Gérer la synchronisation, choisissez Suspendre la synchronisation.

Pour reprendre votre synchronisation

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer la synchronisation.
4. Sous Gérer la synchronisation, choisissez Reprendre la synchronisation.

 Note

Si vous voyez Suspendre la synchronisation au lieu de Reprendre la synchronisation, la synchronisation entre Active Directory et IAM Identity Center a déjà repris.

Automatisez votre configuration de synchronisation pour une synchronisation AD configurable

Pour garantir que votre flux de travail automatisé fonctionne comme prévu avec la synchronisation AD configurable, nous vous recommandons de suivre les étapes suivantes pour automatiser la configuration de votre synchronisation.

Pour automatiser votre configuration de synchronisation pour une synchronisation AD configurable

1. Dans Active Directory, créez un groupe de synchronisation parent contenant tous les utilisateurs et groupes que vous souhaitez synchroniser dans IAM Identity Center. Par exemple, vous pouvez donner un nom au groupe IAMIdentityCenterAllUsersAndGroups.
2. Dans IAM Identity Center, ajoutez le groupe de synchronisation parent à votre liste de synchronisation configurable. IAM Identity Center synchronisera tous les utilisateurs, groupes, sous-groupes et membres de tous les groupes contenus dans le groupe de synchronisation parent.
3. Utilisez les actions de l'API de gestion des utilisateurs et des groupes Active Directory fournies par Microsoft pour ajouter ou supprimer des utilisateurs et des groupes du groupe de synchronisation parent.

Gérer les utilisateurs dans le répertoire Identity Center

IAM Identity Center fournit les fonctionnalités suivantes à vos utilisateurs et groupes :

- Créer vos utilisateurs et groupes.
- Ajouter vos utilisateurs en tant que membres aux groupes.
- Attribuez aux groupes le niveau d'accès souhaité à vos applications Comptes AWS et à vos applications.

Pour gérer les utilisateurs et les groupes dans le magasin IAM Identity Center, AWS prend en charge les opérations d'API répertoriées dans [Identity Center Actions](#).

Provisionnement lorsque les utilisateurs se trouvent dans IAM Identity Center

Lorsque vous créez des utilisateurs et des groupes directement dans IAM Identity Center, le provisionnement est automatique. Ces identités sont immédiatement disponibles pour être utilisées pour effectuer des assignations et pour être utilisées par les applications. Pour de plus amples informations, veuillez consulter [Provisionnement d'utilisateurs et de groupes](#).

Modification de la source de votre identité

Si vous préférez gérer les utilisateurs dans AWS Managed Microsoft AD, vous pouvez arrêter d'utiliser votre répertoire Identity Center à tout moment et connecter IAM Identity Center à votre répertoire dans Microsoft AD en utilisant Directory Service. Pour plus d'informations, consultez les considérations relatives à [Basculement entre le répertoire IAM Identity Center et Active Directory](#).

Si vous préférez gérer les utilisateurs dans un fournisseur d'identité externe (IdP), vous pouvez connecter IAM Identity Center à votre IdP et activer le provisionnement automatique. Pour plus d'informations, consultez les considérations relatives à [Passage d'IAM Identity Center à un IdP externe](#).

Rubriques

- [Ajouter des utilisateurs à votre répertoire Identity Center](#)
- [Ajoutez des groupes à votre répertoire Identity Center](#)
- [Ajouter des utilisateurs à des groupes](#)
- [Supprimer des groupes dans IAM Identity Center](#)
- [Supprimer des utilisateurs dans IAM Identity Center](#)
- [Supprimer des utilisateurs des groupes](#)
- [Modifier les propriétés utilisateur du répertoire Identity Center](#)

Ajouter des utilisateurs à votre répertoire Identity Center

Les utilisateurs et les groupes que vous créez dans votre répertoire Identity Center sont uniquement disponibles dans IAM Identity Center. Utilisez la procédure suivante pour ajouter des utilisateurs à votre répertoire Identity Center. Vous pouvez également appeler l'opération AWS API [CreateUser](#) pour ajouter des utilisateurs.

Console

Pour ajouter un utilisateur

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Utilisateurs.
3. Choisissez Ajouter un utilisateur et fournissez les informations requises suivantes :
 - a. Nom d'utilisateur — Ce nom d'utilisateur est obligatoire pour se connecter au portail AWS d'accès et ne peut pas être modifié ultérieurement. Doit comporter entre 1 et 100 caractères.
 - b. Mot de passe — Vous pouvez soit envoyer un e-mail contenant les instructions de configuration du mot de passe (il s'agit de l'option par défaut), soit générer un mot de passe à usage unique. Si vous créez un utilisateur administratif et que vous choisissez d'envoyer un e-mail, assurez-vous de spécifier une adresse e-mail à laquelle vous pouvez accéder.
 - i. Envoyez un e-mail à cet utilisateur avec les instructions de configuration du mot de passe — Cette option envoie automatiquement à l'utilisateur une adresse e-mail provenant d'Amazon Web Services, avec comme objet Invitation à s'inscrire AWS IAM Identity Center. L'e-mail invite l'utilisateur au nom de votre entreprise à accéder au portail d'accès IAM Identity Center AWS et enregistre un mot de passe. L'invitation par e-mail expirera dans sept jours. Dans ce cas, vous pouvez renvoyer l'e-mail en choisissant Réinitialiser le mot de passe, puis en choisissant Envoyer un e-mail à l'utilisateur avec les instructions pour réinitialiser le mot de passe. Avant que l'utilisateur n'accepte l'invitation, vous verrez le lien de vérification Envoyer un e-mail, destiné à vérifier son adresse e-mail. Cependant, cette étape est facultative et disparaîtra une fois que l'utilisateur aura accepté l'invitation et enregistré un mot de passe.

Note

Dans certaines régions, IAM Identity Center envoie des e-mails aux utilisateurs utilisant Amazon Simple Email Service depuis une autre Région AWS région. Pour plus d'informations sur le mode d'envoi des e-mails, consultez [E-mails interrégionaux avec Amazon SES](#).

Tous les e-mails envoyés par le service IAM Identity Center proviendront soit de l'adresse `no-reply@signin.aws.com`, soit de `no-`

`reply@login.awsapps.com` Nous vous recommandons de configurer votre système de messagerie de manière à ce qu'il accepte les e-mails provenant de ces adresses d'expéditeur et qu'il ne les traite pas comme du courrier indésirable ou du spam.

- ii. Générez un mot de passe à usage unique que vous pouvez partager avec cet utilisateur — Cette option vous fournit l'URL du portail AWS d'accès et les détails du mot de passe que vous pouvez envoyer manuellement à l'utilisateur à partir de votre adresse e-mail. L'utilisateur devra vérifier son adresse e-mail. Vous pouvez lancer le processus en choisissant Envoyer le lien de vérification par e-mail. Le lien de vérification par e-mail expirera dans sept jours. Dans ce cas, vous pouvez renvoyer le lien de vérification par e-mail en choisissant Réinitialiser le mot de passe, puis en choisissant Générer un mot de passe à usage unique et partager le mot de passe avec l'utilisateur.
- c. Adresse e-mail — L'adresse e-mail doit être unique.
- d. Confirmer l'adresse e-mail
- e. Prénom : vous devez saisir un nom ici pour que le provisionnement automatique fonctionne. Pour de plus amples informations, veuillez consulter [Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM](#).
- f. Nom : vous devez saisir un nom ici pour que le provisionnement automatique fonctionne.
- g. Display name (Nom d'affichage)

 Note

(Facultatif) Le cas échéant, vous pouvez spécifier des valeurs pour des attributs supplémentaires tels que l'identifiant immuable Microsoft 365 de l'utilisateur afin de fournir à l'utilisateur un accès par authentification unique à certaines applications professionnelles.

- 4. Choisissez Suivant.
- 5. Le cas échéant, sélectionnez un ou plusieurs groupes auxquels vous souhaitez ajouter l'utilisateur, puis choisissez Next.
- 6. Passez en revue les informations que vous avez spécifiées pour l'étape 1 : Spécifier les détails de l'utilisateur et pour l'étape 2 : ajouter un utilisateur aux groupes (facultatif). Choisissez Modifier à chaque étape pour apporter des modifications. Après avoir confirmé

que les informations correctes sont spécifiées pour les deux étapes, choisissez Ajouter un utilisateur.

AWS CLI

Pour ajouter un utilisateur

La `create-user` commande suivante crée un nouvel utilisateur dans votre répertoire Identity Center.

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --display-name "John Doe" \  
  --emails "Type=work,Value=johndoe@example.com"
```

Sortie :

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

Note

Lorsque vous créez des utilisateurs à l'aide de la commande `create-user` CLI ou de l'opération [CreateUser](#) API, les utilisateurs n'ont pas de mot de passe. Vous pouvez mettre à jour les paramètres dans IAM Identity Center pour envoyer à ces utilisateurs un e-mail de vérification après leur première tentative de connexion afin qu'ils puissent configurer un mot de passe. Si vous n'activez pas ce paramètre, vous devez générer un mot de passe à usage unique et le partager avec l'utilisateur. Pour de plus amples informations, veuillez consulter [Envoyer un mot de passe à usage unique par e-mail aux utilisateurs créés avec l'API ou la CLI](#).

Ajoutez des groupes à votre répertoire Identity Center

Utilisez la procédure suivante pour ajouter des groupes à votre répertoire Identity Center. Vous pouvez également appeler l'opération AWS API [CreateGroup](#) pour ajouter des groupes.

Console

Pour ajouter un groupe

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Groupes.
3. Choisissez Créer un groupe.
4. Entrez un nom et une description du groupe (facultatif). La description doit fournir des détails sur les autorisations qui ont été ou seront attribuées au groupe. Sous Ajouter des utilisateurs au groupe (facultatif), recherchez les utilisateurs que vous souhaitez ajouter en tant que membres. Activez ensuite la case à cocher en regard de chacun d'entre eux.
5. Choisissez Créer un groupe.

AWS CLI

Pour ajouter un groupe

La `create-group` commande suivante crée un nouveau groupe dans votre répertoire Identity Center.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

Sortie :

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

Après avoir ajouté ce groupe à votre répertoire Identity Center, vous pouvez lui attribuer un accès par authentification unique. Pour de plus amples informations, veuillez consulter [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).

Ajouter des utilisateurs à des groupes

Utilisez la procédure suivante pour ajouter des utilisateurs en tant que membres d'un groupe que vous avez créé précédemment dans votre annuaire Identity Center. Vous pouvez également appeler l'opération AWS API [CreateGroupMembership](#) pour ajouter un utilisateur en tant que membre d'un groupe.

Console

Pour ajouter un utilisateur en tant que membre d'un groupe

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Groupes.
3. Choisissez le nom du groupe que vous souhaitez mettre à jour.
4. Sur la page des détails du groupe, sous Utilisateurs de ce groupe, choisissez Ajouter des utilisateurs au groupe.
5. Sur la page Ajouter des utilisateurs au groupe, sous Autres utilisateurs, recherchez les utilisateurs que vous souhaitez ajouter en tant que membres. Sélectionnez ensuite la case à cocher située à côté de chacun d'eux.
6. Sélectionnez Ajouter des utilisateurs.

AWS CLI

Pour ajouter un utilisateur en tant que membre d'un groupe

La `create-group-membership` commande suivante ajoute un utilisateur à un groupe de votre répertoire Identity Center.

```
aws identitystore create-group-membership \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \  
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Sortie :


```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

Supprimer des groupes dans IAM Identity Center

Lorsque vous supprimez un groupe dans le répertoire de votre IAM Identity Center, tous les utilisateurs membres de ce groupe sont privés de l'accès à ces derniers Comptes AWS et de leurs applications. Une fois qu'un groupe est supprimé, il ne peut pas être annulé. Utilisez la procédure suivante pour supprimer un groupe dans votre répertoire Identity Center.

Important

Les instructions de cette page s'appliquent à [AWS IAM Identity Center](#). Ils ne s'appliquent pas à [Gestion des identités et des accès AWS\(IAM\)](#). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la suppression de groupes dans IAM, consultez la section [Suppression d'un groupe d'utilisateurs IAM](#) dans le guide de l'Gestion des identités et des accès AWS utilisateur.

Console

Pour supprimer un groupe

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Groupes.
3. Vous pouvez supprimer un groupe de deux manières :
 - Sur la page Groupes, vous pouvez sélectionner plusieurs groupes à supprimer. Sélectionnez le nom du groupe que vous souhaitez supprimer, puis choisissez Supprimer le groupe.
 - Choisissez le nom du groupe que vous souhaitez supprimer. Sur la page des détails du groupe, choisissez Supprimer le groupe.
4. Il vous sera peut-être demandé de confirmer votre intention de supprimer le groupe.

- Si vous supprimez plusieurs groupes à la fois, confirmez votre intention **Delete** en saisissant du texte dans la boîte de dialogue Supprimer le groupe.
 - Si vous supprimez un seul groupe contenant des utilisateurs, confirmez votre intention en saisissant le nom du groupe que vous souhaitez supprimer dans la boîte de dialogue Supprimer le groupe.
5. Choisissez Supprimer un groupe. Si vous avez sélectionné plusieurs groupes à supprimer, choisissez Supprimer le nombre de groupes.

AWS CLI

Pour supprimer un groupe

La `delete-group` commande suivante supprime le groupe spécifié de votre répertoire Identity Center.

```
aws identitystore delete-group \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Supprimer des utilisateurs dans IAM Identity Center

Lorsque vous supprimez un utilisateur dans le répertoire de votre IAM Identity Center, il supprime son accès aux applications Comptes AWS et à ses applications. Une fois que vous avez supprimé un utilisateur, vous ne pouvez pas annuler cette action. Suivez la procédure ci-dessous pour supprimer un utilisateur de votre répertoire Identity Center.

Note

Lorsque vous désactivez l'accès d'un utilisateur ou que vous supprimez un utilisateur dans IAM Identity Center, cet utilisateur est immédiatement empêché de se connecter au portail d'AWS accès et ne pourra pas créer de nouvelles sessions de connexion. Pour de plus amples informations, veuillez consulter [Comprendre les sessions d'authentification dans IAM Identity Center](#).

⚠ Important

Les instructions de cette page s'appliquent à [AWS IAM Identity Center](#). Ils ne s'appliquent pas à [Gestion des identités et des accès AWS](#)(IAM). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la suppression d'utilisateurs dans IAM, consultez la section [Suppression d'un utilisateur IAM](#) dans le guide de l'[Gestion des identités et des accès AWS](#) utilisateur.

Console

Pour supprimer un utilisateur

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Utilisateurs.
3. Vous pouvez supprimer un utilisateur de deux manières :
 - Sur la page Utilisateurs, vous pouvez sélectionner plusieurs utilisateurs à supprimer. Sélectionnez le nom d'utilisateur que vous souhaitez supprimer, puis choisissez Supprimer les utilisateurs.
 - Choisissez le nom d'utilisateur que vous souhaitez supprimer. Sur la page des informations de l'utilisateur, choisissez Supprimer l'utilisateur.
4. Si vous supprimez plusieurs utilisateurs à la fois, confirmez votre intention **Delete** en saisissant du texte dans la boîte de dialogue Supprimer un utilisateur.
5. Choisissez Delete user (Supprimer l'utilisateur). Si vous avez sélectionné plusieurs utilisateurs à supprimer, choisissez Supprimer le nombre d'utilisateurs.

AWS CLI

Pour supprimer un utilisateur

La `delete-user` commande suivante supprime un utilisateur de votre répertoire Identity Center.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Supprimer des utilisateurs des groupes

Pour supprimer des membres d'un groupe, procédez comme suit. Vous pouvez également appeler l'opération AWS API [DeleteGroupMembership](#) pour supprimer un utilisateur d'un groupe.

Console

Pour supprimer un utilisateur d'un groupe

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Groupes.
3. Choisissez le groupe que vous souhaitez mettre à jour.
4. Sur la page des détails du groupe, sous Utilisateurs de ce groupe, choisissez les utilisateurs à supprimer.
5. Choisissez Supprimer les utilisateurs du groupe.
6. Dans la boîte de dialogue Supprimer des utilisateurs, choisissez Supprimer les utilisateurs du groupe pour vérifier que vous souhaitez supprimer l'accès des utilisateurs au compte et aux applications assignés au groupe.

AWS CLI

Pour supprimer un utilisateur d'un groupe

La `delete-group-membership` commande suivante supprime l'appartenance à un groupe.

```
aws identitystore delete-group-membership
--identity-store-id d-1234567890 \
--membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Modifier les propriétés utilisateur du répertoire Identity Center

Utilisez la procédure suivante pour modifier les propriétés d'un utilisateur dans votre répertoire Identity Center. Vous pouvez également appeler l'opération AWS API [UpdateUser](#) pour mettre à jour les propriétés de l'utilisateur.

Console

Pour modifier les propriétés de l'utilisateur dans IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Utilisateurs.
3. Choisissez l'utilisateur que vous souhaitez modifier.
4. Sur la page du profil utilisateur, à côté de Détails du profil, sélectionnez Modifier.
5. Sur la page Modifier les détails du profil, mettez à jour les propriétés selon vos besoins. Ensuite, choisissez Save changes (Enregistrer les modifications).

Note

(Facultatif) Vous pouvez modifier des attributs supplémentaires tels que le numéro d'employé et l'identifiant immuable Office 365 pour aider à mapper l'identité de l'utilisateur dans IAM Identity Center avec certaines applications professionnelles que les utilisateurs doivent utiliser.

Note

L'attribut Adresse e-mail est un champ modifiable et la valeur que vous fournissez doit être unique.

AWS CLI

Pour modifier les propriétés de l'utilisateur dans IAM Identity Center

La `update-user` commande suivante met à jour le surnom de l'utilisateur.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

Configurer l'accès du personnel aux AWS ressources

Configurez la manière dont les utilisateurs de votre personnel s'authentifient et accèdent aux AWS ressources via IAM Identity Center. Cette section couvre les composants suivants qui régissent l'accès des utilisateurs du personnel à votre AWS environnement :

- Sessions d'authentification : découvrez comment IAM Identity Center gère les différents types de sessions utilisateur, qu'il s'agisse de sessions de portail interactives ou de sessions d'applications en arrière-plan, et comment elles interagissent les unes avec les autres.
- Gestion de l'accès des utilisateurs : configurez la durée des sessions, désactivez les comptes utilisateurs et implémentez des blocages d'accès à l'échelle de l'organisation pour garantir la sécurité et la conformité.
- Gestion des mots de passe : pour les utilisateurs créés dans le répertoire Identity Center, définissez les exigences en matière de mot de passe, gérez la configuration des informations d'identification utilisateur et gérez les réinitialisations de mots de passe pour les utilisateurs.
- Authentification multifactorielle : pour les utilisateurs créés dans l'annuaire Identity Center, renforcez la sécurité grâce à la MFA à l'aide d'applications d'authentification, de clés de sécurité ou d'authenticateurs intégrés pour protéger les connexions des utilisateurs.

Rubriques

- [Comprendre les sessions d'authentification dans IAM Identity Center](#)
- [Configuration de la durée de session dans IAM Identity Center](#)
- [Désactiver l'accès des utilisateurs à IAM Identity Center Comptes AWS et aux applications](#)
- [Refuser l'accès aux utilisateurs avec des politiques de contrôle des services](#)
- [Gestion de l'accès des utilisateurs dans le répertoire Identity Center](#)

Comprendre les sessions d'authentification dans IAM Identity Center

Lorsqu'un utilisateur se connecte au [portail d'AWS accès](#), IAM Identity Center crée une session d'authentification qui représente l'identité vérifiée de l'utilisateur.

Une fois authentifié, l'utilisateur peut accéder à toutes les [applications AWS gérées](#) qui lui sont attribuées Comptes AWS et aux [applications gérées par le client](#) que les administrateurs lui ont accordé l'autorisation d'utiliser, sans connexion supplémentaire.

Types de sessions d'authentification

Sessions interactives pour les utilisateurs

Une fois qu'un utilisateur s'est connecté au portail AWS d'accès, IAM Identity Center crée une session interactive utilisateur. Cette session représente l'état authentifié de l'utilisateur au sein d'IAM Identity Center et sert de base à la création d'autres types de sessions. Les sessions interactives des utilisateurs peuvent durer la durée configurée dans IAM Identity Center, qui peut aller jusqu'à 90 jours.

Les sessions interactives des utilisateurs constituent le principal mécanisme d'authentification. Ils se terminent lorsque l'utilisateur se déconnecte ou lorsqu'un administrateur met fin à sa session. La durée de ces sessions doit être soigneusement configurée en fonction des exigences de sécurité de votre organisation.

Pour plus d'informations sur la configuration de la durée de session interactive de l'utilisateur, consultez [the section called "Configuration de la durée de session"](#).

Séances de candidature

Les sessions d'application sont les connexions authentifiées entre les utilisateurs et les applications AWS gérées (telles que Kiro ou Amazon Quick) établies par IAM Identity Center par le biais de l'authentification unique.

Par défaut, les sessions d'application ont une durée de vie d'une heure, mais elles sont automatiquement actualisées tant que la session interactive de l'utilisateur sous-jacente reste valide. Ce mécanisme d'actualisation fournit une expérience fluide aux utilisateurs tout en maintenant les contrôles de sécurité. Lorsqu'une session interactive d'un utilisateur prend fin, que ce soit par le biais d'une déconnexion de l'utilisateur ou d'une action de l'administrateur, les sessions de l'application se terminent lors de la prochaine tentative d'actualisation, généralement dans les 30 minutes.

Sessions d'arrière-plan pour les utilisateurs

Les sessions d'arrière-plan utilisateur sont des sessions de longue durée conçues pour les applications qui doivent exécuter des processus pendant des heures ou des jours sans interruption. Actuellement, ce type de session s'applique principalement à [Amazon SageMaker Studio](#), où les data

scientists peuvent exécuter des tâches de formation à l'apprentissage automatique qui prennent de nombreuses heures.

Pour plus d'informations sur la configuration de la durée des sessions utilisateur en arrière-plan, consultez la section [Sessions utilisateur en arrière-plan](#).

Séances Kiro

Vous pouvez étendre les sessions Kiro pour permettre aux développeurs utilisant Kiro in de IDEs conserver l'authentification pendant 90 jours au maximum. Cette fonctionnalité réduit les interruptions de connexion lorsque vous travaillez sur le code.

Ces sessions sont indépendantes des autres types de sessions et n'affectent pas les sessions interactives des utilisateurs ni les autres applications AWS gérées. Selon le moment où vous avez activé IAM Identity Center, cette fonctionnalité peut être activée par défaut.

Pour plus d'informations sur la configuration de sessions Kiro étendues, consultez [???](#).

Sessions de rôles IAM créées par l'IAM Identity Center

IAM Identity Center crée un type de session différent lorsque les utilisateurs accèdent au AWS Management Console ou AWS CLI. Dans ces cas, IAM Identity Center utilise la session de connexion pour obtenir une session IAM en assumant un rôle IAM spécifié dans le jeu d'autorisations de l'utilisateur.

Important

Contrairement aux sessions d'application, les sessions de rôle IAM fonctionnent indépendamment une fois établies. Ils persistent pendant la durée configurée dans le jeu d'autorisations, qui peut aller jusqu'à 12 heures, quel que soit le statut de la session de connexion initiale. Ce comportement garantit que les opérations CLI ou les sessions de console de longue durée ne se terminent pas de manière inattendue.

Comment mettre fin aux sessions utilisateur dans IAM Identity Center

Initié par l'utilisateur

Lorsqu'un utilisateur se déconnecte du portail d' AWS accès, la session de connexion se termine, ce qui l'empêche d'accéder à de nouvelles ressources.

Les sessions d'application existantes ne se terminent toutefois pas instantanément. Au lieu de cela, ils se termineront dans un délai d'environ 30 minutes, lorsqu'ils tenteront leur prochaine actualisation et constateront que la session de connexion n'est plus valide. Les sessions de rôle IAM existantes se poursuivent jusqu'à leur expiration en fonction de la configuration de l'ensemble d'autorisations, ce qui peut prendre jusqu'à 12 heures plus tard.

Initié par l'administrateur

Toute personne disposant des autorisations administratives IAM Identity Center au sein de votre organisation, généralement les administrateurs informatiques ou les équipes de sécurité, peut [mettre fin à la session d'un utilisateur](#). Cette action fonctionne de la même manière que si les utilisateurs se déconnectaient eux-mêmes, ce qui permet aux administrateurs de demander aux utilisateurs de se reconnecter en cas de besoin. Cette fonctionnalité est utile lorsque les politiques de sécurité changent ou lorsqu'une activité suspecte est détectée.

Lorsqu'un administrateur du IAM Identity Center [supprime un utilisateur](#) ou [désactive son accès](#), [celui-ci perd l'accès](#) au portail d'accès et ne peut pas se reconnecter pour démarrer une nouvelle application ou une nouvelle session de rôle IAM. AWS L'utilisateur perdra l'accès aux sessions d'application existantes dans les 30 minutes. Toutes les sessions de rôle IAM existantes se poursuivront en fonction de la durée de session configurée dans le jeu d'autorisations IAM Identity Center. La durée maximale de la session peut être de 12 heures.

Qu'advient-il de l'accès utilisateur lorsque vous mettez fin à une session ?

Cette référence fournit des informations détaillées sur le comportement des sessions IAM Identity Center lorsque des mesures administratives sont prises. Les tableaux de cette section indiquent la durée et les effets des actions de gestion des utilisateurs et des modifications des autorisations sur l'accès au portail AWS d'accès, aux applications et aux Compte AWS sessions.

Gestion des utilisateurs

Ce tableau récapitule la manière dont les modifications de gestion des utilisateurs affectent l'accès aux AWS ressources, aux sessions d'application et aux sessions de AWS compte.

Action	L'utilisateur perd l'accès à IAM Identity Center	L'utilisateur ne peut pas créer de nouvelles sessions d'application	L'utilisateur ne peut pas accéder aux sessions d'application existantes	L'utilisateur perd l'accès aux Compte AWS sessions existantes
Accès de l'utilisateur désactivé	En vigueur immédiatement	En vigueur immédiatement	Dans les 30 minutes	Dans un délai de 12 heures ou moins. La durée dépend de la durée d'expiration de la session de rôle IAM configurée pour l'ensemble d'autorisations.
Utilisateur supprimé	En vigueur immédiatement	En vigueur immédiatement	Dans les 30 minutes	Dans un délai de 12 heures ou moins. La durée dépend de la durée d'expiration de la session de rôle IAM configurée pour l'ensemble d'autorisations.
Session utilisateur révoquée	L'utilisateur doit se reconnecter pour retrouver l'accès	En vigueur immédiatement	Dans les 30 minutes	Dans un délai de 12 heures ou moins. La durée dépend de la durée d'expiration de la session de rôle IAM configurée

Action	L'utilisateur perd l'accès à IAM Identity Center	L'utilisateur ne peut pas créer de nouvelles sessions d'application	L'utilisateur ne peut pas accéder aux sessions d'application existantes	L'utilisateur perd l'accès aux Compte AWS sessions existantes
				pour l'ensemble d'autorisations.
L'utilisateur se déconnecte	L'utilisateur doit se reconnecter pour retrouver l'accès	En vigueur immédiatement	Dans les 30 minutes	Dans un délai de 12 heures ou moins. La durée dépend de la durée d'expiration de la session de rôle IAM configurée pour l'ensemble d'autorisations.

Appartenance à un groupe

Ce tableau résume la façon dont les modifications apportées aux autorisations des utilisateurs et à l'appartenance à des groupes affectent l'accès aux AWS ressources, aux sessions d'application et aux sessions de AWS compte.

Action	L'utilisateur perd l'accès à IAM Identity Center	L'utilisateur ne peut pas créer de nouvelles sessions d'application	L'utilisateur ne peut pas accéder aux sessions d'application existantes	L'utilisateur perd l'accès aux Compte AWS sessions existantes
Application ou Compte AWS accès supprimé de l'utilisateur	Non, l'utilisateur peut continuer à accéder à IAM Identity Center	En vigueur immédiatement	Dans un délai d'une heure	Dans un délai de 12 heures ou moins. La durée dépend de la durée

Action	L'utilisateur perd l'accès à IAM Identity Center	L'utilisateur ne peut pas créer de nouvelles sessions d'application	L'utilisateur ne peut pas accéder aux sessions d'application existantes	L'utilisateur perd l'accès aux Compte AWS sessions existantes
				d'expiration de la session de rôle IAM configurée pour l'ensemble d'autorisations.
Utilisateur supprimé du groupe auquel une application avait été attribuée ou Compte AWS	Non, l'utilisateur peut continuer à accéder à IAM Identity Center	Dans un délai d'une heure	Dans les 2 heures	Dans un délai de 12 heures ou moins. La durée dépend de la durée d'expiration de la session de rôle IAM configurée pour l'ensemble d'autorisations.
Application ou Compte AWS accès supprimé du groupe	Non, l'utilisateur peut continuer à accéder à IAM Identity Center	En vigueur immédiatement	Dans un délai d'une heure	Dans un délai de 12 heures ou moins. La durée dépend de la durée d'expiration de la session de rôle IAM configurée pour l'ensemble d'autorisations.

 Note

Le portail AWS d'accès AWS CLI reflétera les autorisations utilisateur mises à jour dans l'heure suivant l'ajout ou la suppression d'un utilisateur de ce groupe.

Présentation des différences de temps

- En vigueur immédiatement : actions qui nécessitent une nouvelle authentification immédiate.
- Dans un délai de 30 minutes à 2 heures : les sessions de candidature ont besoin de temps pour vérifier auprès d'IAM Identity Center et découvrir les modifications éventuelles.
- Dans un délai de 12 heures ou moins : les sessions de rôle IAM fonctionnent indépendamment et ne se terminent que lorsque leur durée configurée expire.

Déconnexion unique

IAM Identity Center ne prend pas en charge la déconnexion unique SAML (protocole qui déconnecte automatiquement les utilisateurs de toutes les applications connectées lorsqu'ils se déconnectent d'une application) initiée par un fournisseur d'identité qui fait office de source d'identité. En outre, il n'envoie pas de déconnexion unique SAML aux applications SAML 2.0 qui utilisent IAM Identity Center comme fournisseur d'identité.

Bonnes pratiques pour la gestion des sessions

Une gestion de session efficace nécessite une configuration et une surveillance réfléchies. Organisations doivent configurer des durées de session adaptées à leurs exigences de sécurité, en utilisant généralement des durées plus courtes pour les applications et les environnements sensibles.

La mise en œuvre de processus visant à mettre fin aux sessions lorsque les utilisateurs changent de rôle ou quittent l'organisation est essentielle pour maintenir les limites de sécurité. L'examen régulier des sessions actives doit être intégré aux pratiques de surveillance de la sécurité afin de détecter les comportements anormaux susceptibles d'indiquer des problèmes de sécurité, tels que des modèles d'accès inhabituels, des heures ou des emplacements de connexion inattendus, ou l'accès à des ressources en dehors des fonctions professionnelles normales.

Configuration de la durée de session dans IAM Identity Center

Vous pouvez configurer la durée de session pour les utilisateurs de votre personnel lorsqu'ils utilisent les applications Portail d'accès AWS et celles qui fonctionnent avec IAM Identity Center, y compris Kiro. IAM Identity Center propose les types de sessions suivants : sessions interactives utilisateur, sessions d'arrière-plan utilisateur et sessions étendues pour Kiro.

Rubriques

- [Sessions interactives pour les utilisateurs](#)
- [Sessions d'arrière-plan pour les utilisateurs](#)
- [Sessions prolongées pour Kiro](#)
- [Afficher et terminer les sessions actives pour les utilisateurs de votre personnel](#)
- [Considérations relatives à la durée de session pour l'utilisation des sources d'identité, de la AWS CLI et AWS SDKs](#)

Sessions interactives pour les utilisateurs

Les sessions interactives sont des sessions liées à la connexion d'un utilisateur au portail d' AWS accès ou à l'accès aux [applications AWS gérées](#). La durée de session d'authentification dans les applications Portail d'accès AWS est la durée maximale pendant laquelle un utilisateur peut se connecter sans se réauthentifier. Si vous mettez fin à une session active du portail d' AWS accès, cela met également fin à toutes les sessions de ces applications gérées.

La durée de session par défaut pour les sessions interactives des utilisateurs est de 8 heures. Vous pouvez définir une durée différente, allant d'un minimum de 15 minutes à un maximum de 90 jours. Les valeurs de durée personnalisées doivent être saisies en minutes et comprises entre 15 minutes et 129 600 minutes (90 jours). Pour de plus amples informations, veuillez consulter [Comprendre les sessions d'authentification dans IAM Identity Center](#).

Pour des considérations telles que la manière dont les sources d'identité IAM Identity Center peuvent affecter la durée de la session interactive de l'utilisateur, voir [the section called “Considérations relatives aux sources d'identité, à la AWS CLI et AWS SDKs”](#).

Pour configurer la durée d'une session interactive utilisateur

1. Ouvrez la console IAM Identity Center.

2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Authentification, à côté de Durée de la session, sélectionnez Configurer. La boîte de dialogue Configurer la durée de session apparaît.
5. Dans la boîte de dialogue Configurer la durée de session, sous Sessions interactives utilisateur, choisissez la durée de session maximale pour vos utilisateurs en sélectionnant la flèche déroulante. Choisissez la durée de la session, puis cliquez sur Enregistrer.

 Note

Les modifications apportées à la durée des sessions ne s'appliquent qu'aux nouvelles sessions. Les sessions en cours conservent leur durée initiale.

6. Vous revenez à l'onglet Authentification. Un message de notification vert apparaît au-dessus de l'onglet pour indiquer que les paramètres de session ont été correctement mis à jour.

Sessions d'arrière-plan pour les utilisateurs

Les sessions d'arrière-plan de l'utilisateur permettent à un utilisateur de lancer une tâche de longue durée sur une application AWS gérée telle qu'[Amazon SageMaker Studio](#), sans que cet utilisateur n'ait à rester connecté pendant l'exécution de la tâche. La tâche s'exécute immédiatement et utilise la fonctionnalité de [propagation d'identité fiable](#) d'IAM Identity Center pour garantir que les autorisations de l'utilisateur sont maintenues pendant que la tâche est exécutée en arrière-plan. La tâche peut continuer à s'exécuter même si l'utilisateur éteint son ordinateur, si sa session de connexion à IAM Identity Center expire ou s'il se déconnecte du portail d' AWS accès. Cette fonctionnalité permet aux scientifiques des données, aux ingénieurs en apprentissage automatique et à d'autres personnes de démarrer des flux de travail d'analyse et d'apprentissage automatique exécutés en arrière-plan sans intervention active de l'utilisateur.

Les sessions d'arrière-plan des utilisateurs sont activées par défaut pour les applications AWS gérées prises en charge telles qu'Amazon SageMaker Studio. Pour utiliser cette fonctionnalité, vous devez toutefois activer la propagation d'identités fiables dans Amazon SageMaker Studio lorsque vous créez ou mettez à jour un domaine. Pour plus d'informations, consultez [Activer la propagation d'identités fiables dans votre domaine Amazon SageMaker AI](#).

La durée de session par défaut pour les sessions d'arrière-plan des utilisateurs est de 7 jours. Vous pouvez définir une durée différente, allant d'un minimum de 15 minutes à un maximum de 90 jours.

Les valeurs de durée personnalisées doivent être saisies en minutes et comprises entre 15 minutes et 129 600 minutes (90 jours).

Gardez à l'esprit les considérations suivantes pour les sessions d'arrière-plan des utilisateurs :

- Une session d'arrière-plan utilisateur ne peut être créée que lorsqu'un utilisateur lance manuellement une tâche dans Amazon SageMaker Studio. Cette fonctionnalité n'est pas prise en charge pour les flux de travail automatisés et planifiés.
- Pour obtenir la liste des AWS régions qui prennent en charge les sessions d'arrière-plan des utilisateurs, consultez la section [AWS Régions prises en charge](#).
- Vous pouvez consulter les sessions d'arrière-plan des utilisateurs dans CloudTrail. Pour plus d'informations, consultez la section [Identification des détails de la session d'arrière-plan de l'utilisateur](#).
- Vous pouvez également mettre fin aux sessions actives d'un utilisateur de votre organisation. Pour plus d'informations, voir [Mettre fin aux sessions actives pour les utilisateurs de votre personnel](#).

Pour configurer la durée d'une session utilisateur en arrière-plan

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Authentification, à côté de Durée de la session, sélectionnez Configurer. La boîte de dialogue Configurer la durée de session apparaît.
5. Dans la boîte de dialogue Configurer la durée de session, si la case Activer les sessions utilisateur en arrière-plan n'est pas déjà cochée, sélectionnez-la. Décochez la case pour désactiver les sessions utilisateur en arrière-plan.

 Note

Les sessions en cours ne sont pas affectées si vous désactivez les sessions d'arrière-plan des utilisateurs.

6. Sous Sessions en arrière-plan de l'utilisateur, choisissez la durée maximale de session en sélectionnant la flèche déroulante. Choisissez la durée de la session, puis cliquez sur Enregistrer.

 Note

Les modifications apportées à la durée des sessions ne s'appliquent qu'aux nouvelles sessions. Les sessions en cours conservent leur durée initiale.

7. Vous revenez à l'onglet Authentification. Un message de notification vert apparaît au-dessus de l'onglet pour indiquer que les paramètres de session ont été correctement mis à jour.

 Note

Une application gérée par le client ne peut pas créer de session utilisateur en arrière-plan.

Sessions prolongées pour Kiro

Si vos développeurs utilisent Kiro dans le cadre d'un environnement de développement intégré (IDE), vous pouvez définir la durée de session de Kiro à 90 jours. Selon le moment où vous avez activé IAM Identity Center, la durée de session prolongée pour Kiro peut être activée par défaut. Cette session prolongée n'affecte pas la durée de session du portail d' AWS accès ou des autres applications AWS gérées.

Pour des considérations telles que la manière dont les sources d'identité IAM Identity Center peuvent affecter la durée prolongée de la session, voir [the section called “Considérations relatives aux sources d'identité, à la AWS CLI et AWS SDKs”](#).

 Note

Kiro est accessible à partir de consoles configurées en mode commercial Régions AWS qui sont activées par défaut. Si votre instance IAM Identity Center est située dans une région où Kiro n'est actuellement pas accessible, l'activation d'une durée de session prolongée de 90 jours ne remplacera pas le paramètre par défaut. Cela signifie que la durée de votre session reste inchangée, que vous activiez la durée de session prolongée de 90 jours ou non. Pour plus d'informations, consultez la [section AWS Régions prises en charge par Kiro](#).

Pour prolonger une session pour Kiro

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Authentification, à côté de Durée de la session, sélectionnez Configurer. La boîte de dialogue Configurer la durée de session apparaît.
5. Dans la boîte de dialogue Configurer la durée de session, cochez la case Activer les sessions étendues pour Kiro. Décochez la case pour désactiver les sessions prolongées pour Kiro.
6. Choisissez Enregistrer pour revenir à la page des paramètres.

Afficher et terminer les sessions actives pour les utilisateurs de votre personnel

En tant qu'administrateur du centre d'identité IAM, vous pouvez consulter la liste des sessions actives des utilisateurs de votre personnel et, si nécessaire, mettre fin à une ou plusieurs sessions pour un utilisateur. Par exemple, il se peut que vous deviez mettre fin aux sessions d'un utilisateur lorsque :

- L'utilisateur n'a plus besoin des sessions.
- L'utilisateur ne doit pas conserver son état d'authentification actuel. Cela peut se produire lorsqu'ils quittent l'entreprise ou que leurs autorisations changent.

Vous pouvez consulter et terminer ces sessions à l'aide de la console IAM Identity Center. Vos utilisateurs peuvent également consulter et terminer leurs propres sessions à l'aide du portail AWS d'accès. Pour plus d'informations sur la manière dont les utilisateurs de votre personnel peuvent consulter et terminer leurs sessions sans l'assistance d'un administrateur, consultez [Afficher et terminer votre session active](#).

Note

La fin d'une session active pour un utilisateur de l'IAM Identity Center ne met fin à aucune session de rôle IAM active dans le AWS Management Console bloc opératoire. AWS CLI Pour de plus amples informations, veuillez consulter [Comprendre les sessions d'authentification dans IAM Identity Center](#).

Pour mettre fin à une session active pour un utilisateur du personnel (console IAM Identity Center)

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs.
3. Sur la page Utilisateurs, choisissez le nom d'utilisateur de l'utilisateur dont vous souhaitez gérer les sessions. Cela vous amène à une page contenant les informations de l'utilisateur.
4. Sur la page de l'utilisateur, choisissez l'onglet Sessions actives. Le nombre entre parenthèses à côté de Sessions actives indique le nombre de sessions actives pour cet utilisateur.
5. Rechercher les sessions d'arrière-plan des utilisateurs (facultatif)

Pour rechercher des sessions par le nom de ressource Amazon (ARN) de la tâche qui utilise la session, dans la liste des types de session, choisissez Sessions d'arrière-plan utilisateur, puis entrez l'ARN de la tâche dans le champ de recherche.

Note

Vous ne pouvez mettre fin qu'aux sessions actives qui sont chargées. Si un utilisateur possède de nombreuses sessions, choisissez Charger des sessions plus actives pour afficher des sessions supplémentaires.

6. Cochez la case à côté de chaque session à laquelle vous souhaitez mettre fin, puis choisissez Terminer les sessions.
7. Une boîte de dialogue apparaît pour confirmer que vous mettez fin aux sessions actives de cet utilisateur. Passez en revue les informations, et si vous souhaitez continuer, tapez `confirm`, puis choisissez Terminer les sessions.
8. Vous êtes renvoyé sur la page de l'utilisateur. Un message de notification vert apparaît pour indiquer que les sessions sélectionnées se sont terminées avec succès.

Considérations relatives à la durée de session pour l'utilisation des sources d'identité, de la AWS CLI et AWS SDKs

Vous trouverez ci-dessous des considérations relatives à la configuration de la durée de session si vous utilisez Microsoft Active Directory (AD) ou un fournisseur d'identité externe (IdP) comme source d'identité, ou si vous utilisez des AWS Command Line Interface kits de développement AWS logiciel (SDKs) ou d'autres outils de AWS développement pour accéder aux AWS services par programmation.

Microsoft Active Directory, sessions interactives avec les utilisateurs et sessions étendues pour Kiro

Si vous utilisez Microsoft Active Directory (AD) comme source d'identité et que vous configurez la durée de session pour les sessions interactives des utilisateurs ou les sessions étendues pour Kiro, tenez compte des considérations suivantes.

Note

Ces considérations ne s'appliquent pas aux sessions d'arrière-plan des utilisateurs.

Que vous utilisiez AWS Managed Microsoft AD ou configuriez AD Connector AWS Directory Service, la durée de vie maximale des tickets Kerberos définis dans Microsoft AD peut affecter la durée de validité des sessions interactives utilisateur et des sessions étendues pour Kiro. Pour plus d'informations sur ce paramètre, consultez la section Durée de [vie maximale du ticket utilisateur](#) sur le site Web de Microsoft.

- **AWS Managed Microsoft AD:** Si vous utilisez AWS Managed Microsoft AD Configuré dans AWS Directory Service, la durée de vie maximale des tickets Kerberos des utilisateurs est fixée à 10 heures. Par conséquent, la durée de la session interactive de l'utilisateur est définie sur la plus courte des valeurs suivantes : le paramètre IAM Identity Center et 10 heures. Par exemple, si vous définissez la durée de la session interactive des utilisateurs sur 12 heures, vos utilisateurs doivent s'authentifier à nouveau dans le portail d' AWS accès au bout de 10 heures. La même limite de 10 heures s'applique aux sessions prolongées pour Kiro.
- **AD Connector :** si vous utilisez AD Connector configuré dans AWS Directory Service, la durée de vie maximale des tickets Kerberos utilisateur est définie dans Microsoft AD derrière l'AD Connector. La valeur par défaut est de 10 heures, et elle a le même effet sur les sessions interactives des utilisateurs et les sessions prolongées que pour AWS Managed Microsoft AD. Bien que cette limite puisse être configurable dans Microsoft AD, nous vous recommandons de consulter votre administrateur informatique pour prendre en compte les risques, notamment parce que ce paramètre peut affecter la durée de session pour d'autres applications clientes Microsoft AD.

Fournisseurs d'identité externes, sessions interactives pour les utilisateurs et sessions étendues pour Kiro

Si vous utilisez un fournisseur d'identité (IdP) externe et que vous configurez la durée de session pour les sessions interactives des utilisateurs ou les sessions étendues pour Kiro, tenez compte des considérations suivantes.

Note

Ces considérations ne s'appliquent pas aux sessions d'arrière-plan des utilisateurs.

IAM Identity Center utilise les `SessionNotOnOrAfter` attributs des assertions SAML pour déterminer la durée de validité de la session.

- Si `SessionNotOnOrAfter` aucune assertion SAML n'est transmise, la durée d'une session de portail d' AWS accès (interactive utilisateur) et d'une session prolongée n'est pas affectée par la durée de votre session IdP externe. Par exemple, si la durée de votre session IdP est de 24 heures et que vous définissez une durée de session de 18 heures dans IAM Identity Center, vos utilisateurs doivent s'authentifier à nouveau sur le portail d'accès au AWS bout de 18 heures. De même, si vous définissez une session prolongée de 90 jours pour Kiro, vos utilisateurs de Kiro doivent se réauthentifier après 90 jours.
- Si une assertion SAML `SessionNotOnOrAfter` est transmise, la valeur de durée de session est définie sur la durée la plus courte entre la session du portail d' AWS accès (interaction utilisateur) ou la durée de session prolongée et la durée de votre session IDP SAML. Si vous définissez une durée de session de 72 heures dans IAM Identity Center et que votre IdP a une durée de session de 18 heures, vos utilisateurs auront accès aux AWS ressources pendant les 18 heures définies dans votre IdP. De même, si vous définissez une session prolongée de 90 jours pour Kiro, vos utilisateurs de Kiro doivent se réauthentifier dans Kiro au bout de 18 heures.
- Si la durée de session de votre IdP est plus longue que celle définie dans IAM Identity Center, vos utilisateurs peuvent démarrer une nouvelle session IAM Identity Center sans avoir à saisir à nouveau leurs informations d'identification, sur la base de leur session de connexion toujours valide avec votre IdP.

AWS CLI et sessions du SDK

Si vous utilisez la AWS CLI ou d'autres outils de AWS développement pour accéder aux AWS services par programmation, les conditions préalables suivantes doivent être remplies pour définir la durée de session pour le portail d' AWS accès et les AWS applications gérées. AWS SDKs

- Vous devez [configurer la durée de session du portail d' AWS accès](#) dans la console IAM Identity Center.
- Vous devez définir un profil pour les paramètres d'authentification unique dans votre fichier de AWS configuration partagé. Ce profil est utilisé pour se connecter au portail AWS d'accès. Nous vous recommandons d'utiliser la configuration du fournisseur de jetons SSO. Avec cette configuration, votre AWS SDK ou outil peut récupérer automatiquement des jetons d'authentification actualisés. Pour plus d'informations, consultez la section [Configuration du fournisseur de jetons SSO](#) dans le Guide de référence du AWS SDK et des outils.
- Les utilisateurs doivent exécuter une version du AWS CLI ou un SDK qui prend en charge la gestion des sessions.

Versions minimales du AWS CLI qui prennent en charge la gestion des sessions

Vous trouverez ci-dessous les versions minimales AWS CLI qui prennent en charge la gestion des sessions.

- AWS CLI V2 2.9 ou version ultérieure
- AWS CLI V1 1.27.10 ou version ultérieure

Note

Pour les cas d'utilisation de l'accès au compte, si vos utilisateurs exécutent le AWS CLI, si vous actualisez votre ensemble d'autorisations juste avant l'expiration de la session IAM Identity Center et que la durée de la session est fixée à 20 heures alors que la durée de l'ensemble d'autorisations est fixée à 12 heures, la AWS CLI session dure au maximum 20 heures plus 12 heures pour un total de 32 heures. Pour plus d'informations sur la CLI IAM Identity Center, consultez la section [AWS CLI Command Reference](#).

Les versions minimales de SDKs celui-ci prennent en charge la gestion des sessions IAM Identity Center

Vous trouverez ci-dessous les versions minimales SDKs qui prennent en charge la gestion des sessions IAM Identity Center.

Kit SDK	Version minimale
Python	1,26,10
PHP	3,245,0
Ruby	aws-sdk-core 3,167,0
Java V2	AWS SDK pour Java v2 (2.18.13)
Go V2	SDK complet : version 011-11 et modules Go spécifiques : 1.18.0 credentials/v1.13.0, config/v
JS V2	2,1253,0
JS V3	version 3.210.0
C++	1,9,372
.NET	v3.7.400.0

Désactiver l'accès des utilisateurs à IAM Identity Center Comptes AWS et aux applications

Lorsque vous désactivez l'accès des utilisateurs dans votre annuaire IAM Identity Center, vous ne pouvez pas modifier leurs informations d'utilisateur, réinitialiser leur mot de passe, ajouter l'utilisateur à un groupe ou consulter son appartenance à un groupe. La désactivation de l'accès des utilisateurs les empêche de se connecter au portail AWS d'accès et ils n'auront plus accès aux applications qui leur sont attribuées Comptes AWS . Utilisez l'option Désactiver l'accès utilisateur pour supprimer l'accès temporaire lorsque vous devrez peut-être rétablir l'accès ultérieurement.

Utilisez la procédure suivante pour désactiver l'accès des utilisateurs dans votre répertoire Identity Center à l'aide de la console IAM Identity Center.

 Note

Lorsque vous désactivez l'accès d'un utilisateur ou que vous supprimez un utilisateur dans IAM Identity Center, cet utilisateur est immédiatement empêché de se connecter au portail d'AWS accès et ne pourra pas créer de nouvelles sessions de connexion. Pour de plus amples informations, veuillez consulter [Comprendre les sessions d'authentification dans IAM Identity Center](#).

Pour désactiver l'accès des utilisateurs dans IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).

 Important

Les instructions de cette page s'appliquent à [AWS IAM Identity Center](#). Ils ne s'appliquent pas à [Gestion des identités et des accès AWS](#)(IAM). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la désactivation des utilisateurs dans IAM, consultez la section [Gestion des utilisateurs IAM](#) dans le guide de l'[Gestion des identités et des accès AWS](#) utilisateur.

2. Choisissez Utilisateurs.
3. Sélectionnez le nom d'utilisateur de l'utilisateur dont vous souhaitez désactiver l'accès.
4. Sous le nom d'utilisateur de l'utilisateur dont vous souhaitez désactiver l'accès, dans la section Informations générales, choisissez Désactiver l'accès utilisateur.
5. Dans la boîte de dialogue Désactiver l'accès utilisateur, choisissez Désactiver l'accès utilisateur.

Refuser l'accès aux utilisateurs avec des politiques de contrôle des services

Pour refuser immédiatement l'accès aux appels d'API autorisés lorsque l'accès d'un utilisateur d'IAM Identity Center est désactivé ou que l'utilisateur est supprimé, vous pouvez :

1. [Ajoutez ou mettez à jour](#) la [politique en ligne](#) du ou des ensembles d'autorisations attribués à l'utilisateur en ajoutant un Deny effet explicite pour toutes les actions sur toutes les ressources.
2. Spécifiez la clé de `identitystore:user_id` condition `aws:user_id` ou.

Vous pouvez également utiliser une [politique de contrôle des services](#) pour refuser l'accès de l'utilisateur à tous les comptes membres de votre organisation.

Exemple Exemple de SCP pour refuser l'accès

Cette politique de refus bloque toutes les AWS actions pour un utilisateur spécifique, quelles que soient les autres autorisations qui lui ont été accordées par ailleurs. Cette politique prévaut sur toutes Allow les politiques.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```

Gestion de l'accès des utilisateurs dans le répertoire Identity Center

Découvrez comment gérer les mots de passe et l'authentification multifactorielle (MFA) pour les utilisateurs dans l'annuaire IAM Identity Center. Ces fonctionnalités de sécurité aident à protéger les comptes des utilisateurs.

Note

Ces fonctionnalités ne s'appliquent pas aux utilisateurs d'Active Directory ni aux utilisateurs de fournisseurs d'identité externes.

Les administrateurs peuvent gérer à la fois les mots de passe et le MFA via la console IAM Identity Center. Ces fonctionnalités de sécurité ne fonctionnent qu'avec le répertoire Identity Center intégré.

Gestion des mots de passe

La gestion des mots de passe inclut les fonctionnalités suivantes :

- Réinitialiser les mots de passe avec des instructions par e-mail
- Générez des mots de passe uniques

- Configurer la vérification automatique des e-mails pour les utilisateurs créés par l'API

AWS applique des exigences de sécurité fixes, notamment des règles de complexité et des restrictions de réutilisation des mots de passe.

MFA

Le MFA est activé par défaut et prend en charge jusqu'à huit appareils par utilisateur.

Les types d'appareils pris en charge sont les suivants :

- Applications d'authentification
- Clés de sécurité
- Authentificateurs biométriques intégrés

Les administrateurs peuvent enregistrer et gérer les appareils MFA pour les utilisateurs.

Rubriques

- [Configuration des mots de passe utilisateur](#)
- [MFA pour les utilisateurs de l'annuaire Identity Center](#)

Configuration des mots de passe utilisateur

Pour les utilisateurs créés dans le répertoire Identity Center, les administrateurs peuvent gérer les politiques de mots de passe, gérer les utilisateurs sans mot de passe initial et réinitialiser les mots de passe en cas de besoin. Ces fonctionnalités de gestion des mots de passe s'appliquent uniquement aux utilisateurs du répertoire Identity Center intégré. Si vous utilisez Active Directory ou un fournisseur d'identité externe, vous devez gérer les mots de passe dans ces systèmes.

Options de gestion des mots de passe

- Exigences relatives aux mots de passe : exigences de sécurité auxquelles les utilisateurs doivent satisfaire lorsqu'ils définissent ou modifient des mots de passe. Cela inclut les règles de complexité et les restrictions de réutilisation.
- Configuration d'un mot de passe à usage unique : configurez la vérification des e-mails pour les utilisateurs créés via une API ou une CLI qui n'ont pas de mot de passe initial. Vous pouvez également générer des mots de passe temporaires pour un accès immédiat.

- Réinitialisation des mots de passe : réinitialisez les mots de passe des utilisateurs dont l'accès est bloqué ou qui ont besoin de nouvelles informations d'identification. Vous pouvez envoyer des instructions de réinitialisation par e-mail ou générer des mots de passe à usage unique.

Rubriques

- [Exigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center](#)
- [Envoyer un mot de passe à usage unique par e-mail aux utilisateurs créés avec l'API ou la CLI](#)
- [Réinitialisation du mot de passe utilisateur IAM Identity Center pour un utilisateur final](#)

Exigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center

Note

Ces exigences s'appliquent uniquement aux utilisateurs créés dans le répertoire Identity Center. Si vous avez configuré une source d'identité autre qu'IAM Identity Center pour l'authentification, telle qu'un [fournisseur Active Directory d'identité externe](#), les politiques de mot de passe pour vos utilisateurs sont définies et appliquées dans ces systèmes, et non dans IAM Identity Center. Si votre source d'identité l'est AWS Managed Microsoft AD, consultez [Gérer les politiques de mot de passe AWS Managed Microsoft AD pour](#) plus d'informations.

Lorsque vous utilisez IAM Identity Center comme source d'identité, les utilisateurs doivent respecter les exigences de mot de passe suivantes pour définir ou modifier leur mot de passe :

- Les mots de passe distinguent majuscules et minuscules.
- Les mots de passe doivent comporter entre 8 et 64 caractères.
- Les mots de passe doivent contenir au moins un caractère appartenant à chacune des quatre catégories suivantes :
 - Lettres minuscules (a-z)
 - Lettres majuscules (A-Z)
 - Chiffres (0-9)
 - Caractères non alphanumériques (~!@#\$%^&* _-+=`|\\(){}[]:;'"<>,.?/)

- Les trois derniers mots de passe ne peuvent pas être réutilisés.
- Les mots de passe connus du public grâce à un ensemble de données divulgué par un tiers ne peuvent pas être utilisés.

Envoyer un mot de passe à usage unique par e-mail aux utilisateurs créés avec l'API ou la CLI

Lorsque vous créez des utilisateurs à l'aide de l'opération [CreateUser](#) API ou de la commande `create-user` CLI, les utilisateurs n'ont pas de mot de passe. Vous pouvez mettre à jour les paramètres dans IAM Identity Center pour envoyer un e-mail de vérification à ces utilisateurs après leur première tentative de connexion, si vous avez spécifié un e-mail pour l'utilisateur lors de sa création. Après avoir reçu l'e-mail de vérification, l'utilisateur doit définir un mot de passe pour se connecter.

Si vous n'activez pas ce paramètre, vous devez [générer un mot de passe à usage unique](#) et le partager avec les utilisateurs que vous créez à l'aide de l'CreateUser API ou de la commande `create-user` CLI.

Pour envoyer un e-mail de vérification d'adresse e-mail aux utilisateurs créés à l'aide de l'CreateUser API ou de la commande `create-user` CLI

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification standard, choisissez Configurer.
5. Dans la boîte de dialogue Configurer l'authentification standard, cochez la case Envoyer un e-mail OTP. Ensuite, choisissez Enregistrer. Le statut passe de Désactivé à Activé.

Réinitialisation du mot de passe utilisateur IAM Identity Center pour un utilisateur final

Cette procédure est destinée aux administrateurs qui doivent réinitialiser le mot de passe d'un utilisateur dans le répertoire IAM Identity Center. Vous allez utiliser la console IAM Identity Center pour réinitialiser les mots de passe.

Considérations relatives aux fournisseurs d'identité et aux types d'utilisateurs

- Microsoft Active Directory ou fournisseur externe : si vous connectez IAM Identity Center à Microsoft Active Directory ou à un fournisseur externe, les réinitialisations du mot de passe utilisateur doivent être effectuées depuis Active Directory ou depuis le fournisseur externe. Cela signifie que les mots de passe de ces utilisateurs ne peuvent pas être réinitialisés depuis la console IAM Identity Center.
- Utilisateurs du répertoire IAM Identity Center : si vous êtes un utilisateur d'IAM Identity Center, vous pouvez réinitialiser votre propre mot de passe IAM Identity Center, voir. [Réinitialisation du mot de passe utilisateur de votre portail d' AWS accès](#)

Pour réinitialiser le mot de passe d'un utilisateur final d'IAM Identity Center

Important

Les instructions de cette page s'appliquent à [AWS IAM Identity Center](#). Ils ne s'appliquent pas à [Gestion des identités et des accès AWS\(IAM\)](#). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des instructions sur la modification des mots de passe des utilisateurs IAM, consultez la section [Gestion des mots de passe des utilisateurs IAM](#) dans le guide de l'Gestion des identités et des accès AWS utilisateur.

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Utilisateurs.
3. Sélectionnez le nom d'utilisateur de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.
4. Sur la page des informations de l'utilisateur, choisissez Réinitialiser le mot de passe.
5. Dans la boîte de dialogue Réinitialiser le mot de passe, sélectionnez l'une des options suivantes, puis choisissez Réinitialiser le mot de passe :
 - a. Envoyez un e-mail à l'utilisateur avec des instructions pour réinitialiser le mot de passe — Cette option envoie automatiquement à l'utilisateur une adresse e-mail provenant d'Amazon Web Services qui lui explique comment réinitialiser son mot de passe.

 Warning

Pour des raisons de sécurité, vérifiez que l'adresse e-mail de cet utilisateur est correcte avant de sélectionner cette option. Si cet e-mail de réinitialisation du mot de passe devait être envoyé à une adresse e-mail incorrecte ou mal configurée, un destinataire malveillant pourrait l'utiliser pour obtenir un accès non autorisé à votre AWS environnement.

- b. Générez un mot de passe à usage unique et partagez-le avec l'utilisateur — Cette option vous fournit les détails du mot de passe que vous pouvez envoyer manuellement à l'utilisateur à partir de votre adresse e-mail.

MFA pour les utilisateurs de l'annuaire Identity Center

 Important

Le MFA dans IAM Identity Center n'est actuellement pas pris en charge pour les fournisseurs d'identité [externes](#).

IAM Identity Center est préconfiguré avec l'authentification multifactorielle (MFA) activée par défaut, de sorte que tous les utilisateurs doivent se connecter avec l'authentification MFA en plus de leur nom d'utilisateur et de leur mot de passe. Cela garantit que les utilisateurs doivent se connecter au portail AWS d'accès en utilisant les deux facteurs suivants :

- Leurs nom d'utilisateur et mot de passe. C'est le premier facteur et les utilisateurs le savent.
- Il s'agit d'un code, d'une clé de sécurité ou de données biométriques. Il s'agit du deuxième facteur et c'est quelque chose que les utilisateurs possèdent (possession) ou sont (biométrie). Le deuxième facteur peut être soit un code d'authentification généré par son appareil mobile, soit une clé de sécurité connectée à son ordinateur, soit le scan biométrique de l'utilisateur.

Ensemble, ces multiples facteurs renforcent la sécurité en empêchant tout accès non autorisé à vos AWS ressources à moins qu'un défi MFA valide n'ait été relevé avec succès.

Chaque utilisateur peut enregistrer jusqu'à deux applications d'authentification virtuelles, qui sont des applications d'authentification par mot de passe à usage unique installées sur votre appareil mobile

ou votre tablette, et six authenticateurs FIDO, qui incluent des authenticateurs intégrés et des clés de sécurité, pour un total de huit appareils MFA. En savoir plus sur [Types de MFA disponibles pour IAM Identity Center](#).

Rubriques

- [Types de MFA disponibles pour IAM Identity Center](#)
- [Configuration de la MFA dans IAM Identity Center](#)
- [Enregistrer un appareil MFA pour les utilisateurs](#)
- [Modification du nom et suppression des appareils MFA dans IAM Identity Center](#)

Types de MFA disponibles pour IAM Identity Center

L'authentification multifactorielle (MFA) est un mécanisme simple et efficace pour renforcer la sécurité de vos utilisateurs. Le premier facteur d'un utilisateur, son mot de passe, est un secret qu'il mémorise, également appelé facteur de connaissance. Les autres facteurs peuvent être des facteurs liés à la possession (quelque chose que vous possédez, comme une clé de sécurité) ou des facteurs inhérents (quelque chose que vous êtes, comme un scan biométrique). Nous vous recommandons vivement de configurer le MFA pour ajouter un niveau de sécurité supplémentaire à votre compte.

Le MFA IAM Identity Center prend en charge les types d'appareils suivants. Tous les types de MFA sont pris en charge à la fois pour l'accès à la console via un navigateur et pour l'utilisation de la AWS CLI version v2 avec IAM Identity Center.

- [FIDO2 authenticateurs](#), y compris les authenticateurs intégrés et les clés de sécurité
- [Applications d'authentification virtuelle](#)
- Votre propre [RAYON MFA](#) implémentation connectée via AWS Managed Microsoft AD

Un utilisateur peut avoir jusqu'à huit appareils MFA, dont deux applications d'authentification virtuelle et six authenticateurs FIDO, enregistrés auprès d'un utilisateur. Compte AWS Vous pouvez également configurer les paramètres MFA pour exiger l'authentification MFA chaque fois qu'ils tentent de se connecter depuis un nouvel appareil ou un nouveau navigateur, ou lorsqu'ils se connectent depuis une adresse IP inconnue. Pour plus d'informations sur la configuration des paramètres MFA pour vos utilisateurs, consultez [Choisissez les types de MFA pour l'authentification des utilisateurs](#) et [Configurer l'application des dispositifs MFA](#)

FIDO2 authenticateurs

[FIDO2](#) est une norme qui inclut CTAP2. [WebAuthn](#) est basée sur la cryptographie à clé publique. Les informations d'identification FIDO résistent au hameçonnage car elles sont uniques au site Web sur lequel elles ont été créées, par exemple. AWS

AWS prend en charge les deux formats les plus courants pour les authenticateurs FIDO : les authenticateurs intégrés et les clés de sécurité. Voir ci-dessous pour plus d'informations sur les types les plus courants d'authenticateurs FIDO.

Rubriques

- [Authenticateurs intégrés](#)
- [Clés de sécurité](#)
- [Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authenticateurs FIDO](#)

Authenticateurs intégrés

De nombreux ordinateurs et téléphones portables modernes sont dotés d'authenticateurs intégrés, tels que TouchID sur Macbook ou un appareil photo compatible avec Windows Hello. Si votre appareil est doté d'un authenticateur intégré compatible avec Fido, vous pouvez utiliser votre empreinte digitale, votre visage ou le code PIN de votre appareil comme deuxième facteur.

Clés de sécurité

Les clés de sécurité sont des authenticateurs matériels externes compatibles avec FIDO que vous pouvez acheter et connecter à votre appareil via USB, BLE ou NFC. Lorsque le MFA vous est demandé, il vous suffit de faire un geste avec le capteur de la touche. Parmi les clés de sécurité, citons les clés feitiennes, YubiKeys et les clés de sécurité les plus courantes créent des informations d'identification FIDO liées à l'appareil. Pour une liste de toutes les clés de sécurité certifiées FIDO, consultez la section Produits certifiés [FIDO](#).

Gestionnaires de mots de passe, fournisseurs de clés d'accès et autres authenticateurs FIDO

Plusieurs fournisseurs tiers prennent en charge l'authentification FIDO dans les applications mobiles, en tant que fonctionnalité dans les gestionnaires de mots de passe, les cartes à puce dotées d'un mode FIDO et d'autres formats. Ces appareils compatibles avec FIDO peuvent fonctionner avec IAM Identity Center, mais nous vous recommandons de tester vous-même un authenticateur FIDO avant d'activer cette option pour le MFA.

 Note

Certains authentificateurs FIDO peuvent créer des informations d'identification FIDO détectables appelées clés d'accès. Les clés d'accès peuvent être liées à l'appareil qui les a créées, ou elles peuvent être synchronisées et sauvegardées dans un cloud. Par exemple, vous pouvez enregistrer une clé d'accès à l'aide d'Apple Touch ID sur un Macbook compatible, puis vous connecter à un site depuis un ordinateur portable Windows à l'aide de Google Chrome avec votre clé d'accès dans iCloud en suivant les instructions à l'écran lors de la connexion. Pour plus d'informations sur les appareils compatibles avec les clés d'accès synchronisées et sur l'interopérabilité actuelle des clés d'accès entre les systèmes d'exploitation et les navigateurs, consultez la section [Support](#) des appareils sur passkeys.dev, une ressource gérée par l'Alliance FIDO et le World Wide Web Consortium (W3C).

Applications d'authentification virtuelle

Les applications d'authentification sont essentiellement des authentificateurs tiers basés sur un mot de passe à usage unique (OTP). Vous pouvez utiliser une application d'authentification installée sur votre appareil mobile ou votre tablette en tant qu'appareil MFA autorisé. L'application d'authentification tierce doit être conforme à la RFC 6238, qui est un algorithme de mot de passe à usage unique (TOTP) basé sur des normes et basé sur le temps capable de générer des codes d'authentification à six chiffres.

Lorsqu'ils sont invités à saisir le MFA, les utilisateurs doivent saisir un code valide provenant de leur application d'authentification dans la zone de saisie présentée. Chaque dispositif MFA attribué à un utilisateur doit être unique. Deux applications d'authentification peuvent être enregistrées pour un utilisateur donné.

Applications d'authentification testées

Toute application conforme au TOTP fonctionnera avec le MFA d'IAM Identity Center. Le tableau suivant répertorie les applications d'authentification tierces les plus connues parmi lesquelles choisir.

Système d'exploitation	Application d'authentification testée
Android	Authy , Duo Mobile , Microsoft Authenticator , Google Authenticator

Système d'exploitation	Application d'authentification testée
iOS	Authy , Duo Mobile , Microsoft Authenticator , Google Authenticator

RAYON MFA

Le [Remote Authentication Dial-In User Service \(RADIUS\)](#) est un protocole client-serveur standard qui assure l'authentification, l'autorisation et la gestion de la comptabilité afin que les utilisateurs puissent se connecter aux services réseau. Directory Service inclut un client RADIUS qui se connecte au serveur RADIUS sur lequel vous avez implémenté votre solution MFA. Pour plus d'informations, voir [Activer l'authentification multifactorielle pour AWS Managed Microsoft AD](#).

Vous pouvez utiliser RADIUS MFA ou MFA dans IAM Identity Center pour les connexions des utilisateurs au portail utilisateur, mais pas les deux. La MFA dans IAM Identity Center est une alternative à la MFA RADIUS dans les cas où vous souhaitez une authentification AWS native à deux facteurs pour accéder au portail.

Lorsque vous activez l'authentification multifacteur dans IAM Identity Center, vos utilisateurs ont besoin d'un appareil MFA pour se connecter au portail d'accès. AWS Si vous avez déjà utilisé RADIUS MFA, l'activation de la MFA dans IAM Identity Center remplace efficacement la MFA RADIUS pour les utilisateurs qui se connectent au portail d'accès. AWS Cependant, le MFA RADIUS continue de poser des problèmes aux utilisateurs lorsqu'ils se connectent à toutes les autres applications compatibles Directory Service, telles qu'Amazon RDS for SQL Server.

Si votre MFA est désactivé sur la console IAM Identity Center et que vous avez configuré RADIUS MFA avec, Directory Service RADIUS MFA régit la connexion au portail d'accès. AWS Cela signifie qu'IAM Identity Center revient à la configuration RADIUS MFA si la MFA est désactivée.

Configuration de la MFA dans IAM Identity Center

Vous pouvez configurer les fonctionnalités d'authentification multifactorielle (MFA) dans IAM Identity Center lorsque votre source d'identité est configurée avec le magasin d'identités d'IAM Identity Center, AWS Managed Microsoft AD ou AD Connector. Le MFA dans IAM Identity Center n'est actuellement pas pris en charge pour les fournisseurs d'identité [externes](#).

Vous trouverez ci-dessous des recommandations générales de la MFA, en fonction des paramètres de votre centre d'identité IAM et des préférences organisationnelles.

- Les utilisateurs sont invités à enregistrer plusieurs authentificateurs de sauvegarde pour tous les types de MFA activés. Cette pratique permet d'éviter la perte d'accès en cas de panne ou d'égarement d'un dispositif MFA.
- Ne choisissez pas l'option Exiger qu'ils fournissent un mot de passe à usage unique envoyé par e-mail si vos utilisateurs doivent se connecter au portail AWS d'accès pour accéder à leur courrier électronique. Par exemple, vos utilisateurs peuvent utiliser Microsoft 365 le portail AWS d'accès pour lire leurs e-mails. Dans ce cas, les utilisateurs ne pourront pas récupérer le code de vérification et ne pourront pas se connecter au portail AWS d'accès. Pour de plus amples informations, veuillez consulter [Configurer l'application des dispositifs MFA](#).
- Si vous utilisez déjà le protocole RADIUS MFA que vous avez configuré Directory Service, vous n'avez pas besoin d'activer le MFA dans IAM Identity Center. Le MFA dans IAM Identity Center est une alternative au MFA RADIUS pour les Microsoft Active Directory utilisateurs d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [RAYON MFA](#).
- La YouTube vidéo suivante donne un aperçu du MFA et de l'IAM Identity Center :

[IAM Identity Center : Authentification multifactorielle par défaut pour les nouvelles instances](#)

Rubriques

- [Inviter les utilisateurs à utiliser le MFA](#)
- [Choisissez les types de MFA pour l'authentification des utilisateurs](#)
- [Configurer l'application des dispositifs MFA](#)
- [Autoriser les utilisateurs à enregistrer leurs propres appareils MFA](#)

Inviter les utilisateurs à utiliser le MFA

Vous pouvez suivre les étapes suivantes pour déterminer à quelle fréquence les utilisateurs du personnel sont invités à utiliser l'authentification multifactorielle (MFA) chaque fois qu'ils tentent de se connecter au portail d' AWS accès. Avant de commencer, nous vous recommandons de comprendre le [Types de MFA disponibles pour IAM Identity Center](#).

Important

Les instructions de cette section s'appliquent à [AWS IAM Identity Center](#). Ils ne s'appliquent pas à [Gestion des identités et des accès AWS\(IAM\)](#). Les utilisateurs, les groupes et les informations d'identification utilisateur d'IAM Identity Center sont différents des informations d'identification des utilisateurs, des groupes et des utilisateurs IAM. Si vous recherchez des

instructions sur la désactivation de l'authentification multifacteur pour les utilisateurs d'IAM, consultez la section [Désactivation des appareils MFA](#) dans le guide de l'utilisateur. Gestion des identités et des accès AWS

 Note

Si vous utilisez un IdP externe, la section Authentification multifactorielle ne sera pas disponible. Votre IdP externe gère les paramètres MFA, plutôt que IAM Identity Center les gère.

Pour configurer le MFA

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Inviter les utilisateurs à utiliser la MFA, choisissez l'un des modes d'authentification suivants en fonction du niveau de sécurité dont votre entreprise a besoin :

- Chaque fois qu'ils se connectent (toujours activé)

Dans ce mode (paramètre par défaut), IAM Identity Center exige que les utilisateurs possédant un appareil MFA enregistré soient invités à chaque fois qu'ils se connectent. Il s'agit du paramètre le plus sécurisé qui garantit l'application des politiques de votre organisation ou de conformité en exigeant que le MFA soit utilisé chaque fois qu'ils se connectent au portail d'AWS accès. Par exemple, la norme PCI DSS recommande vivement l'authentification MFA lors de chaque connexion afin d'accéder aux applications prenant en charge les transactions de paiement à haut risque.

- Uniquement lorsque leur contexte de connexion change (sensible au contexte)

Dans ce mode, IAM Identity Center offre aux utilisateurs la possibilité de faire confiance à leur appareil lors de la connexion. Une fois qu'un utilisateur indique qu'il souhaite faire confiance à un appareil, IAM Identity Center lui demande une seule fois de saisir le MFA et analyse le contexte de connexion (tel que l'appareil, le navigateur et l'emplacement) pour les connexions

ultérieures de l'utilisateur. Pour les connexions suivantes, IAM Identity Center détermine si l'utilisateur se connecte avec un contexte précédemment approuvé. Si le contexte de connexion de l'utilisateur change, IAM Identity Center l'invite à saisir le MFA en plus de son adresse e-mail et de son mot de passe.

Ce mode est facile à utiliser pour les utilisateurs qui se connectent fréquemment depuis leur lieu de travail, mais il est moins sécurisé que l'option Always-on. Les utilisateurs ne sont invités à utiliser le MFA que si leur contexte de connexion change.

- Jamais (désactivé)

Dans ce mode, tous les utilisateurs se connectent uniquement avec leur nom d'utilisateur et leur mot de passe standard. Le choix de cette option désactive le MFA d'IAM Identity Center et n'est pas recommandé.

Lorsque l'authentification MFA est désactivée pour votre annuaire Identity Center pour les utilisateurs, vous ne pouvez pas gérer les appareils MFA dans leurs informations d'utilisateur, et les utilisateurs du répertoire Identity Center ne peuvent pas gérer les appareils MFA depuis le portail d'accès. AWS

 Note

Si vous utilisez déjà RADIUS MFA avec Directory Service et que vous souhaitez continuer à l'utiliser comme type de MFA par défaut, vous pouvez laisser le mode d'authentification désactivé pour contourner les fonctionnalités MFA dans IAM Identity Center. Le passage du mode désactivé au mode contextuel ou permanent remplacera les paramètres MFA RADIUS existants. Pour de plus amples informations, veuillez consulter [RAYON MFA](#).

6. Sélectionnez Save Changes (Enregistrer les modifications).

Rubriques connexes

- [Choisissez les types de MFA pour l'authentification des utilisateurs](#)
- [Configurer l'application des dispositifs MFA](#)
- [Autoriser les utilisateurs à enregistrer leurs propres appareils MFA](#)

Choisissez les types de MFA pour l'authentification des utilisateurs

Utilisez la procédure suivante pour choisir les types d'appareils avec lesquels vos utilisateurs peuvent s'authentifier lorsqu'ils sont invités à utiliser l'authentification multifactorielle (MFA) sur le portail d'accès. AWS

Pour configurer les types de MFA pour vos utilisateurs

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Les utilisateurs peuvent s'authentifier avec ces types de MFA, choisissez l'un des types d'authentification MFA suivants en fonction des besoins de votre entreprise. Pour de plus amples informations, veuillez consulter [Types de MFA disponibles pour IAM Identity Center](#).
 - Clés de sécurité et authenticateurs intégrés
 - Applications d'authentification
6. Sélectionnez Enregistrer les modifications.

Configurer l'application des dispositifs MFA

Utilisez la procédure suivante pour déterminer si vos utilisateurs doivent disposer d'un dispositif MFA enregistré lorsqu'ils se connectent au portail d' AWS accès.

Pour plus d'informations sur l'authentification multifacteur dans IAM, consultez la section Authentification [AWS multifactorielle](#) dans IAM.

Pour configurer l'application des dispositifs MFA pour vos utilisateurs

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.

5. Sur la page Configurer l'authentification multifactorielle, sous Si un utilisateur ne possède pas encore d'appareil MFA enregistré, choisissez l'une des options suivantes en fonction des besoins de votre entreprise :

- Demandez-leur d'enregistrer un appareil MFA lors de la connexion

Il s'agit du paramètre par défaut lorsque vous configurez pour la première fois le MFA pour IAM Identity Center. Utilisez cette option lorsque vous souhaitez demander aux utilisateurs qui ne possèdent pas encore d'appareil MFA enregistré d'inscrire eux-mêmes un appareil lors de la connexion après une authentification par mot de passe réussie. Cela vous permet de sécuriser les AWS environnements de votre entreprise grâce à la MFA sans avoir à inscrire et à distribuer des dispositifs d'authentification individuels à vos utilisateurs. Lors de l'auto-inscription, vos utilisateurs peuvent enregistrer n'importe quel appareil parmi les appareils disponibles que [Types de MFA disponibles pour IAM Identity Center](#) vous avez précédemment activés. Une fois l'enregistrement terminé, les utilisateurs ont la possibilité de donner un nom convivial à leur appareil MFA nouvellement inscrit, après quoi IAM Identity Center redirige l'utilisateur vers sa destination d'origine. En cas de perte ou de vol de l'appareil de l'utilisateur, vous pouvez simplement le supprimer de son compte, et IAM Identity Center demandera à l'utilisateur d'enregistrer lui-même un nouvel appareil lors de sa prochaine connexion.

- Demandez-leur de fournir un mot de passe à usage unique envoyé par e-mail pour se connecter

Utilisez cette option lorsque vous souhaitez que des codes de vérification soient envoyés aux utilisateurs par e-mail. Étant donné que le courrier électronique n'est pas lié à un appareil spécifique, cette option ne répond pas aux normes de l'industrie en matière d'authentification multifactorielle. Mais cela améliore la sécurité par rapport au simple fait d'avoir un mot de passe. La vérification par e-mail ne sera demandée que si l'utilisateur n'a pas enregistré d'appareil MFA. Si la méthode d'authentification sensible au contexte a été activée, l'utilisateur aura la possibilité de marquer l'appareil sur lequel il reçoit l'e-mail comme étant fiable. Par la suite, ils ne seront pas tenus de vérifier un code e-mail lors de futures connexions à partir de cette combinaison d'appareil, de navigateur et d'adresse IP.

 Note

Si vous utilisez Active Directory comme source d'identité activée par votre IAM Identity Center, l'adresse e-mail sera toujours basée sur l'attribut `email` Active Directory.

Les mappages d'attributs Active Directory personnalisés ne remplaceront pas ce comportement.

- Bloquer leur connexion

Utilisez l'option Bloquer leur connexion lorsque vous souhaitez obliger chaque utilisateur à utiliser le MFA avant qu'il ne puisse se connecter. AWS

 Important

Si votre méthode d'authentification est configurée en fonction du contexte, un utilisateur peut cocher la case Ceci est un appareil fiable sur la page de connexion. Dans ce cas, cet utilisateur ne sera pas invité à utiliser le MFA même si le paramètre Bloquer sa connexion est activé. Si vous souhaitez que ces utilisateurs soient invités, remplacez votre méthode d'authentification par Always On.

- Autorisez-les à se connecter

Utilisez cette option pour indiquer que les appareils MFA ne sont pas nécessaires pour que vos utilisateurs puissent se connecter au portail d' AWS accès. Les utilisateurs qui ont choisi d'enregistrer des appareils MFA seront toujours invités à le faire.

6. Sélectionnez Enregistrer les modifications.

Autoriser les utilisateurs à enregistrer leurs propres appareils MFA

Les administrateurs d'IAM Identity Center peuvent autoriser les utilisateurs à enregistrer eux-mêmes leurs propres appareils MFA.

Pour permettre aux utilisateurs d'enregistrer leurs propres appareils MFA

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Dans la section Authentification multifactorielle, choisissez Configurer.
5. Sur la page Configurer l'authentification multifactorielle, sous Qui peut gérer les appareils MFA, choisissez Les utilisateurs peuvent ajouter et gérer leurs propres appareils MFA.
6. Sélectionnez Enregistrer les modifications.

 Note

Après avoir configuré l'auto-enregistrement pour vos utilisateurs, vous souhaitez peut-être leur envoyer un lien vers la procédure [Enregistrement de votre appareil à la MFA](#). Cette rubrique fournit des instructions sur la façon de configurer leurs propres dispositifs MFA.

Enregistrer un appareil MFA pour les utilisateurs

Les administrateurs d'IAM Identity Center peuvent configurer un nouveau dispositif MFA auquel un utilisateur spécifique pourra accéder dans la console IAM Identity Center. Les administrateurs doivent avoir un accès physique au dispositif MFA de l'utilisateur pour l'enregistrer. Par exemple, si vous configurez l'authentification multifacteur pour un utilisateur qui utilisera un appareil MFA exécuté sur un smartphone, vous aurez besoin d'un accès physique au smartphone pour terminer le processus d'enregistrement. Vous pouvez également autoriser les utilisateurs à configurer et à gérer leurs propres appareils MFA. Pour de plus amples informations, veuillez consulter [Autoriser les utilisateurs à enregistrer leurs propres appareils MFA](#).

Pour enregistrer un appareil MFA

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le volet de navigation de gauche, choisissez Utilisateurs. Choisissez un utilisateur dans la liste. Ne cochez pas la case à côté de l'utilisateur pour cette étape.
3. Sur la page des informations utilisateur, choisissez l'onglet Appareils MFA, puis sélectionnez Enregistrer un appareil MFA.
4. Sur la page Enregistrer un appareil MFA, sélectionnez l'un des types de périphériques MFA suivants et suivez les instructions :
 - Application Authenticator
 1. Sur la page Configurer l'application d'authentification, IAM Identity Center affiche les informations de configuration du nouveau dispositif MFA, notamment un code QR graphique. Le graphique est une représentation de la clé secrète qui peut être saisie manuellement sur les appareils qui ne prennent pas en charge les codes QR.
 2. À l'aide du périphérique MFA physique, procédez comme suit :
 - a. Ouvrez une application d'authentification MFA compatible. Pour obtenir la liste des applications testées que vous pouvez utiliser avec les appareils MFA, consultez. [Applications d'authentification virtuelle](#) Si l'application MFA prend en charge plusieurs

- comptes (plusieurs appareils MFA), choisissez l'option permettant de créer un nouveau compte (un nouvel appareil MFA).
- b. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des opérations suivantes sur la page Configurer l'application d'authentification :
 - i. Choisissez Afficher le code QR, puis utilisez l'application pour scanner le code QR. Par exemple, vous pouvez choisir l'icône de l'appareil photo ou une option similaire à Scanner le code. Utilisez ensuite l'appareil photo de l'appareil pour scanner le code.
 - ii. Choisissez Afficher la clé secrète, puis saisissez cette clé secrète dans votre application MFA.

 Important

Lorsque vous configurez un dispositif MFA pour IAM Identity Center, nous vous recommandons d'enregistrer une copie du code QR ou de la clé secrète dans un endroit sûr. Cela peut être utile si l'utilisateur désigné perd le téléphone ou doit réinstaller l'application d'authentification MFA. Si l'une de ces situations se produit, vous pouvez rapidement reconfigurer l'application pour qu'elle utilise la même configuration MFA. Cela évite à l'utilisateur de créer un nouveau dispositif MFA dans IAM Identity Center.

3. Sur la page Configurer l'application d'authentification, sous Code d'authentification, saisissez le mot de passe à usage unique qui apparaît actuellement sur le dispositif MFA physique.

 Important

Envoyez votre demande immédiatement après avoir généré le code. Si vous générez le code puis attendez trop longtemps pour soumettre la demande, le dispositif MFA est correctement associé à l'utilisateur. Mais le dispositif MFA n'est pas synchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez resynchroniser le dispositif.

4. Choisissez Assign MFA (Affecter le MFA). Le dispositif MFA peut désormais commencer à générer des mots de passe à usage unique et est maintenant prêt à être utilisé avec. AWS

- Clé de sécurité

1. Sur la page Enregistrer la clé de sécurité de votre utilisateur, suivez les instructions fournies par votre navigateur ou votre plateforme.

 Note

L'expérience ici varie en fonction des différents systèmes d'exploitation et navigateurs. Veuillez donc suivre les instructions affichées par votre navigateur ou votre plateforme. Une fois que l'appareil de votre utilisateur a été enregistré avec succès, vous aurez la possibilité d'associer un nom d'affichage convivial à l'appareil nouvellement inscrit de votre utilisateur. Si vous souhaitez modifier cela, choisissez Renommer, entrez le nouveau nom, puis cliquez sur Enregistrer. Si vous avez activé l'option permettant aux utilisateurs de gérer leurs propres appareils, l'utilisateur verra ce nom convivial sur le portail AWS d'accès.

Modification du nom et suppression des appareils MFA dans IAM Identity Center

Les administrateurs d'IAM Identity Center peuvent utiliser les procédures suivantes pour renommer ou supprimer le dispositif MFA d'un utilisateur.

Pour renommer un appareil MFA

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le volet de navigation de gauche, choisissez Utilisateurs. Choisissez l'utilisateur dans la liste. Ne cochez pas la case à côté de l'utilisateur pour cette étape.
3. Sur la page des informations utilisateur, choisissez l'onglet Appareils MFA, sélectionnez l'appareil, puis choisissez Renommer.
4. Lorsque vous y êtes invité, entrez le nouveau nom, puis choisissez Renommer.

Pour supprimer un appareil MFA

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le volet de navigation de gauche, choisissez Utilisateurs. Choisissez l'utilisateur dans la liste.

3. Sur la page des informations utilisateur, choisissez l'onglet Appareils MFA, sélectionnez l'appareil, puis choisissez Supprimer.
4. Pour confirmer, tapez DELETE, puis sélectionnez Supprimer.

Configuration de l'accès aux applications

Vous pouvez ainsi contrôler les personnes autorisées à accéder à vos applications par authentification unique. AWS IAM Identity Center Les utilisateurs peuvent accéder facilement à ces applications une fois qu'ils ont utilisé les informations d'identification de leur annuaire pour se connecter.

IAM Identity Center communique en toute sécurité avec ces applications grâce à une relation de confiance entre IAM Identity Center et le fournisseur de services de l'application. Cette confiance peut être créée de différentes manières, selon le type d'application.

IAM Identity Center prend en charge deux types d'applications : les [applications AWS gérées et les applications gérées par le client](#). AWS les applications gérées sont configurées directement depuis les consoles d'application pertinentes ou via l'application APIs. Les applications gérées par le client doivent être ajoutées à la console IAM Identity Center et configurées avec les métadonnées appropriées à la fois pour IAM Identity Center et pour le fournisseur de services.

Après avoir configuré les applications pour qu'elles fonctionnent avec IAM Identity Center, vous pouvez gérer les utilisateurs ou les groupes qui accèdent aux applications. Par défaut, aucun utilisateur n'est affecté aux applications.

Vous pouvez également accorder à vos employés l'accès AWS Management Console au formulaire spécifique Compte AWS de votre organisation. Pour de plus amples informations, veuillez consulter [Configurer l'accès à Comptes AWS](#).

Rubriques

- [AWS applications gérées](#)
- [Applications gérées par le client](#)
- [Vue d'ensemble de la propagation d'identités fiables](#)
- [Configuration de votre propre application OAuth 2.0](#)
- [Rotation des certificats IAM Identity Center](#)
- [Comprendre les propriétés de l'application dans la console IAM Identity Center](#)
- [Attribuer un accès utilisateur aux applications dans la console IAM Identity Center](#)
- [Supprimer l'accès des utilisateurs aux applications SAML 2.0](#)
- [Associez les attributs de votre application aux attributs d'IAM Identity Center](#)

AWS applications gérées

AWS IAM Identity Center rationalise et simplifie la tâche consistant à connecter les utilisateurs de votre personnel à des applications AWS gérées telles que Kiro et Amazon Quick. Avec IAM Identity Center, vous pouvez connecter votre fournisseur d'identité existant une seule fois et synchroniser les utilisateurs et les groupes à partir de votre annuaire, ou créer et gérer vos utilisateurs directement dans IAM Identity Center. En fournissant un point de fédération unique, IAM Identity Center élimine le besoin de configurer la fédération ou la synchronisation des utilisateurs et des groupes pour chaque application et réduit vos efforts administratifs. Vous bénéficiez également d'une [vue commune des attributions des utilisateurs et des groupes](#).

Pour un tableau des AWS applications qui fonctionnent avec IAM Identity Center, voir [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#).

Contrôle de l'accès aux applications AWS gérées

L'accès aux applications AWS gérées est contrôlé de deux manières :

- Entrée initiale dans l'application

IAM Identity Center gère cela par le biais d'assignments à l'application. Par défaut, les affectations sont obligatoires pour les applications AWS gérées. Si vous êtes administrateur d'applications, vous pouvez choisir d'exiger ou non des affectations à une application.

Si des attributions sont requises, lorsque les utilisateurs se connectent à l'application Portail d'accès AWS, seuls les utilisateurs affectés à l'application directement ou par le biais d'une attribution de groupe peuvent voir la vignette de l'application.

Si aucune attribution n'est requise, vous pouvez autoriser tous les utilisateurs d'IAM Identity Center à accéder à l'application. Dans ce cas, l'application gère l'accès aux ressources et la vignette de l'application est visible par tous les utilisateurs qui consultent le Portail d'accès AWS.

Important

Si vous êtes administrateur d'IAM Identity Center, vous pouvez utiliser la console IAM Identity Center pour supprimer des attributions aux applications AWS gérées. Avant de supprimer des attributions, nous vous recommandons de vous concerter avec l'administrateur de l'application. Vous devez également vous coordonner avec

l'administrateur de l'application si vous envisagez de modifier le paramètre qui détermine si des affectations sont requises ou d'automatiser les affectations d'applications.

- Accès aux ressources de l'application

L'application gère cela par le biais d'affectations de ressources indépendantes qu'elle contrôle.

AWS les applications gérées fournissent une interface utilisateur administrative que vous pouvez utiliser pour gérer l'accès aux ressources de l'application. Par exemple, les administrateurs Quick peuvent assigner aux utilisateurs l'accès aux tableaux de bord en fonction de leur appartenance à un groupe. La plupart des applications AWS gérées offrent également une AWS Management Console expérience qui vous permet d'attribuer des utilisateurs à l'application. L'expérience de console de ces applications peut intégrer les deux fonctions, afin de combiner les capacités d'attribution des utilisateurs avec la capacité de gérer l'accès aux ressources de l'application.

Partage d'informations d'identité

Considérations relatives au partage des informations d'identité dans Comptes AWS

IAM Identity Center prend en charge les attributs les plus couramment utilisés dans toutes les applications. Ces attributs incluent le prénom et le nom de famille, le numéro de téléphone, l'adresse e-mail, l'adresse et la langue préférée. Examinez attentivement quelles applications et quels comptes peuvent utiliser ces informations personnelles identifiables.

Vous pouvez contrôler l'accès à ces informations de l'une des manières suivantes :

- Vous pouvez choisir d'activer l'accès uniquement dans le compte AWS Organizations de gestion ou dans tous les comptes de AWS Organizations.
- Vous pouvez également utiliser les politiques de contrôle des services (SCPs) pour contrôler quelles applications peuvent accéder aux informations dans quels comptes AWS Organizations.

Par exemple, si vous activez l'accès uniquement dans le compte de AWS Organizations gestion, les applications des comptes membres n'ont pas accès aux informations. Toutefois, si vous activez l'accès dans tous les comptes, vous pouvez interdire l'accès SCPs à toutes les applications, à l'exception de celles que vous souhaitez autoriser.

Les politiques de contrôle des services sont une fonctionnalité de AWS Organizations. Pour obtenir des instructions sur la connexion d'un SCP, consultez les [politiques de contrôle de service relatives à l'attachement et au détachement](#) du guide de l'AWS Organizations utilisateur.

Configuration d'IAM Identity Center pour partager les informations d'identité

IAM Identity Center fournit une banque d'identités qui contient les attributs des utilisateurs et des groupes, à l'exception des informations de connexion. Vous pouvez utiliser l'une des méthodes suivantes pour maintenir à jour les utilisateurs et les groupes de votre banque d'identités IAM Identity Center :

- Utilisez le magasin d'identités IAM Identity Center comme source d'identité principale. Si vous choisissez cette méthode, vous gérez vos utilisateurs, leurs identifiants de connexion et les groupes depuis la console IAM Identity Center ou AWS Command Line Interface (AWS CLI). Pour de plus amples informations, veuillez consulter [Gérer les utilisateurs dans le répertoire Identity Center](#).
- Configurez le provisionnement (synchronisation) des utilisateurs et des groupes provenant de l'une des sources d'identité suivantes vers votre banque d'identités IAM Identity Center :
 - Active Directory — Pour plus d'informations, consultez [Microsoft ADannuaire](#).
 - Fournisseur d'identité externe : pour plus d'informations, consultez [Fournisseurs d'identité externes](#).

Si vous choisissez cette méthode de provisionnement, vous continuez à gérer vos utilisateurs et vos groupes depuis votre source d'identité, et ces modifications sont synchronisées avec le magasin d'identités IAM Identity Center.

Quelle que soit la source d'identité que vous choisissez, IAM Identity Center peut partager les informations relatives aux utilisateurs et aux groupes avec les applications AWS gérées. Ainsi, vous pouvez connecter une source d'identité à IAM Identity Center une seule fois, puis partager les informations d'identité avec plusieurs applications du AWS Cloud. Il n'est donc plus nécessaire de configurer indépendamment la fédération et le provisionnement des identités pour chaque application. Cette fonctionnalité de partage permet également de donner facilement à vos utilisateurs l'accès à de nombreuses applications de différentes manières Comptes AWS.

Limiter l'utilisation des applications AWS gérées

Lorsque vous activez IAM Identity Center pour la première fois, il devient disponible en tant que source d'identité pour les applications AWS gérées sur tous les comptes de votre AWS Organizations

compte. Pour restreindre les applications, vous devez implémenter des politiques de contrôle des services (SCPs). SCPs sont une fonctionnalité AWS Organizations que vous pouvez utiliser pour contrôler de manière centralisée les autorisations maximales que peuvent avoir les identités (utilisateurs et rôles) au sein de votre organisation. Vous pouvez l'utiliser SCPs pour bloquer l'accès aux informations des utilisateurs et des groupes IAM Identity Center et pour empêcher le démarrage de l'application, sauf pour les comptes désignés. Pour plus d'informations, voir [Politiques de contrôle des services \(SCPs\)](#) dans le guide de AWS Organizations l'utilisateur.

L'exemple de SCP suivant bloque l'accès aux informations des utilisateurs et des groupes IAM Identity Center et empêche le démarrage de l'application, sauf pour les comptes désignés (111111111111 et 222222222222) :

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS applications gérées que vous pouvez utiliser avec IAM Identity Center

IAM Identity Center vous permet de connecter votre source d'identité existante ou de créer des utilisateurs une seule fois. Cela permet aux administrateurs d'applications de gérer l'accès aux applications AWS gérées suivantes sans fédération séparée ni synchronisation entre les utilisateurs et les groupes.

Toutes les applications AWS gérées figurant dans le tableau suivant s'intègrent aux [instances organisationnelles d'IAM Identity Center](#). Le tableau fournit également des informations sur les points suivants pour une application AWS gérée prise en charge :

- Si l'application s'intègre également aux instances de compte d'IAM Identity Center
- Si l'application peut permettre une propagation d'identité fiable via IAM Identity Center
- Si l'application prend en charge le centre d'identité IAM configuré avec une clé KMS gérée par le client
- Si l'application prend en charge le déploiement dans d'autres régions d'IAM Identity Center

Note

Les applications qui prennent en charge le déploiement dans des régions supplémentaires d'IAM Identity Center prennent également en charge IAM Identity Center configuré avec une clé KMS gérée par le client. Chaque application AWS gérée répertoriée ici prend en charge le déploiement dans la région principale. Pour de plus amples informations, veuillez consulter [the section called “Déploiement et gestion d'applications AWS gérées sur plusieurs Régions AWS”](#).

AWS applications gérées qui s'intègrent à IAM Identity Center

AWS application gérée	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center	Supporte le centre d'identité IAM configuré avec une clé KMS gérée par le client	Prend en charge le déploiement dans des régions supplémentaires d'IAM Identity Center
Amazon Athena SQL	Oui	Oui	Oui	Non
Amazon CodeCatalyst	Oui	Non	Oui	Non

AWS application gérée	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center	Supporte le centre d'identité IAM configuré avec une clé KMS gérée par le client	Prend en charge le déploiement dans des régions supplémentaires d'IAM Identity Center
Amazon DataZone	Oui	Oui	Oui	Non
Fonctionnalités d'Amazon EKS	Oui	Oui	Oui	Non
Amazon EMR sur EC2	Oui	Oui	Oui	Non
Amazon EMR on EKS	Oui	Oui	Oui	Non
Amazon EMR sans serveur	Oui	Oui	Oui	Non
Amazon EMR Studio	Oui	Oui	Oui	Non
Amazon Kendra	Non	Non	Oui	Non
Amazon Managed Grafana	Non	Non	Oui	Non
Amazon Monitron	Non	Non	Non	Non
Amazon OpenSearch Service	Oui	Oui	Oui	Non

AWS application gérée	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center	Supporte le centre d'identité IAM configuré avec une clé KMS gérée par le client	Prend en charge le déploiement dans des régions supplémentaires d'IAM Identity Center
Amazon OpenSearch Service Serverless Service	Oui	Oui	Oui	Non
Amazon Q Business	Oui	Oui	Oui	Non
Amazon Quick	Oui	Oui	Oui	Non
Amazon Redshift	Oui ²	Oui	Oui	Oui
Amazon S3 Access Grants	Oui	Oui	Oui	Oui
Amazon SageMaker Studio	Non	Oui	Oui	Non
Amazon SageMaker Unified Studio	Oui	Oui	Oui	Non
Amazon WorkMail	Oui	Oui	Oui	Non
Amazon WorkSpaces	Oui	Non	Oui	Non
Amazon WorkSpaces Secure Browser	Non	Non	Oui	Non

AWS application gérée	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center	Supporte le centre d'identité IAM configuré avec une clé KMS gérée par le client	Prend en charge le déploiement dans des régions supplémentaires d'IAM Identity Center
AWS App Studio	Oui	Non	Non	Non
AWS Deadline Cloud	Oui	Non	Oui	Oui
AWS Glue	Oui	Oui	Oui	Non
AWS IoT Events	Non	Non	Non	Non
AWS IoT SiteWise	Non	Non	Non	Non
AWS Lake Formation	Oui	Oui	Oui	Oui
AWS re:Post privé	Oui	Non	Oui	Non
AWS Supply Chain	Oui	Non	Oui	Non
AWS Systems Manager	Non	Non	Oui	Oui - Fleet Manager Remote Desktop

AWS application gérée	Intégré aux instances de compte d'IAM Identity Center	Permet une propagation d'identité fiable via IAM Identity Center	Supporte le centre d'identité IAM configuré avec une clé KMS gérée par le client	Prend en charge le déploiement dans des régions supplémentaires d'IAM Identity Center
AWS Transfer Family applications Web	Oui	Oui	Oui	Non
AWS Transformation	Oui	Non	Oui	Non
Accès vérifié par AWS	Non	Non	Oui	Non
Kiro	¹ Oui	Oui	Oui	Non
Approbation multipartite	Non	Oui	Oui	Non
OpenSearch user interface (Dashboards)	Oui	Oui	Oui	Non

¹ Pour Kiro, les instances de compte d'IAM Identity Center sont prises en charge, sauf si vos utilisateurs ont besoin d'accéder à l'ensemble complet des fonctionnalités de Kiro sur les sites Web. AWS Pour plus d'informations, consultez la section [Configuration de Kiro](#) dans le guide de l'utilisateur de Kiro.

² Pour Amazon Redshift, les instances de compte d'IAM Identity Center sont prises en charge, à l'exception des applications telles que Query Editor v2 qui nécessitent des ensembles d'autorisations, qui ne sont pas prises en charge par les instances de compte.

 Note

Certains AWS services tels qu'Amazon Connect ne AWS Client VPN figurent pas dans ce tableau, bien que vous puissiez les utiliser avec IAM Identity Center. En effet, elles s'intègrent à IAM Identity Center exclusivement à l'aide de SAML et sont donc classées dans la catégorie des applications [gérées par le client](#).

Démarrage rapide : Configuration d'IAM Identity Center pour tester les applications AWS gérées

Si votre administrateur ne vous a pas encore donné accès à IAM Identity Center, vous pouvez suivre les étapes décrites dans cette rubrique pour configurer IAM Identity Center afin de tester les applications AWS gérées. Vous apprendrez comment activer IAM Identity Center, créer un utilisateur directement dans IAM Identity Center et affecter cet utilisateur à une application AWS gérée.

Cette rubrique décrit les étapes de démarrage rapide permettant d'activer IAM Identity Center de l'une des manières suivantes :

- Avec AWS Organizations : si vous choisissez cette option, une instance d'organisation d'IAM Identity Center est créée.
- Uniquement dans votre cas spécifique Compte AWS : si vous choisissez cette option, une instance de compte d'IAM Identity Center est créée.

Pour plus d'informations sur ces types d'instances, consultez [Instances d'organisation et de compte d'IAM Identity Center](#).

Conditions préalables

Avant d'activer IAM Identity Center, vérifiez les points suivants :

- Vous avez un Compte AWS — Si vous n'en avez pas Compte AWS, consultez la section [Commencer avec un Compte AWS](#) dans le Guide de référence de gestion de AWS compte.
- L'application AWS gérée fonctionne avec IAM Identity Center : consultez la liste des [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#) pour vérifier que l'application AWS gérée que vous souhaitez tester fonctionne avec IAM Identity Center.

- Vous avez examiné les considérations régionales : assurez-vous que l'application AWS gérée que vous souhaitez tester est prise en charge dans l' Région AWS endroit où vous activez IAM Identity Center. Pour plus d'informations, consultez la documentation de l'application AWS gérée.

 Note

Vous devez déployer votre application AWS gérée dans la même région où vous prévoyez d'activer IAM Identity Center.

Configuration d'une instance organisationnelle d'IAM Identity Center pour tester les applications AWS gérées

 Note

Cette rubrique décrit comment activer IAM Identity Center avec AWS Organizations, méthode recommandée pour activer IAM Identity Center.

Confirmez vos autorisations

Pour activer IAM Identity Center avec AWS Organizations, vous devez vous connecter à la console de AWS gestion en utilisant l'une des méthodes suivantes :

- Un utilisateur disposant d'autorisations administratives dans le Compte AWS cadre duquel IAM Identity Center sera activé. AWS Organizations
- L'utilisateur root (déconseillé sauf s'il n'existe aucun autre utilisateur administratif).

 Important

L'utilisateur root a accès à tous les AWS services et ressources du compte. Pour des raisons de sécurité, à moins que vous ne disposiez d'aucune autre information d'identification, n'utilisez pas les informations d'identification root de votre compte pour accéder aux AWS ressources. Ces informations d'identification offrent un accès illimité au compte et sont difficiles à révoquer.

Étape 1. Activez IAM Identity Center avec AWS Organizations

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
 - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
 - Utilisez-le déjà AWS avec un appareil autonome Compte AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Sur la page d'accueil de la console de AWS gestion, sélectionnez le service IAM Identity Center ou accédez à la console [IAM Identity Center](#).
3. Choisissez Activer, puis activez IAM Identity Center avec AWS Organizations. Ce faisant, vous créez une [instance d'organisation](#) d'IAM Identity Center.

Étape 2. Création d'un utilisateur administratif dans IAM Identity Center

Cette procédure décrit comment créer un utilisateur directement dans le répertoire intégré d'Identity Center. Ce répertoire n'est connecté à aucun autre répertoire que votre administrateur pourrait utiliser pour gérer les utilisateurs du personnel. Après avoir créé l'utilisateur dans IAM Identity Center, vous devez spécifier de nouvelles informations d'identification pour cet utilisateur. Lorsque vous vous connectez en tant qu'utilisateur pour tester votre application AWS gérée, vous vous connectez avec les nouvelles informations d'identification, et non avec les informations d'identification existantes que vous utilisez pour accéder aux ressources de l'entreprise.

Note

Nous vous recommandons d'utiliser cette méthode pour créer des utilisateurs à des fins de test uniquement.

1. Dans le volet de navigation de la console IAM Identity Center, sélectionnez Utilisateurs, puis Ajouter un utilisateur.
2. Suivez les instructions de la console pour ajouter l'utilisateur. Gardez la case Envoyer un e-mail à cet utilisateur avec les instructions de configuration du mot de passe sélectionnée et assurez-vous de spécifier une adresse e-mail à laquelle vous avez accès.

3. Dans le volet de navigation, choisissez Comptes AWS, cochez la case à côté de votre compte, puis choisissez Attribuer des utilisateurs ou des groupes.
4. Choisissez l'onglet Utilisateurs, cochez la case à côté de l'utilisateur que vous venez d'ajouter, puis cliquez sur Suivant.
5. Choisissez Créer un ensemble d'autorisations, puis suivez les instructions de la console pour créer le jeu d'autorisations AdministratorAccess prédéfini.
6. Lorsque vous avez terminé, le nouvel ensemble d'autorisations apparaît dans la liste. Fermez l'onglet Ensembles d'autorisations dans la fenêtre de votre navigateur, revenez à l'onglet Attribuer des utilisateurs et des groupes, puis cliquez sur l'icône d'actualisation à côté de Créer un ensemble d'autorisations.
7. Dans l'onglet du navigateur Attribuer des utilisateurs et des groupes, le nouvel ensemble d'autorisations apparaît dans la liste. Cochez la case à côté du nom de l'ensemble d'autorisations, choisissez Suivant, puis Soumettre.
8. Déconnectez-vous de la console .

Étape 3. Connectez-vous au portail d' AWS accès en tant qu'utilisateur administratif

Le portail AWS d'accès est un portail Web qui permet à l'utilisateur que vous avez créé d'accéder à la console AWS de gestion. Avant de pouvoir vous connecter au portail AWS d'accès, vous devez accepter l'invitation à rejoindre IAM Identity Center et activer vos informations d'identification utilisateur.

1. Vérifiez dans votre e-mail la ligne d'objet de l'invitation à rejoindre AWS IAM Identity Center.
2. Choisissez Accepter l'invitation et suivez les instructions de la page d'inscription pour définir un nouveau mot de passe, vous connecter et enregistrer un appareil MFA pour votre utilisateur.
3. Après avoir enregistré votre appareil MFA, le portail d' AWS accès s'ouvre.
4. Dans le portail AWS d'accès, sélectionnez votre Compte AWS et choisissez AdministratorAccess. Vous êtes redirigé vers la console AWS de gestion.

Étape 4 : Configurer l'application AWS gérée pour utiliser IAM Identity Center

1. Lorsque vous êtes connecté à la console AWS de gestion, ouvrez la console de l'application AWS gérée que vous comptez utiliser.

2. Suivez les instructions de la console pour configurer l'application AWS gérée afin qu'elle utilise IAM Identity Center. Au cours de ce processus, vous pouvez affecter l'utilisateur que vous avez créé à l'application.

Configuration d'une instance de compte d'IAM Identity Center pour tester les applications AWS gérées

Note

Une instance de compte d'IAM Identity Center limite votre déploiement à une seule Compte AWS instance. Vous devez activer cette instance de la même manière Région AWS que l' AWS application que vous souhaitez tester.

Confirmez votre application

Toutes les applications AWS gérées qui fonctionnent avec IAM Identity Center peuvent être utilisées avec les instances organisationnelles d'IAM Identity Center. Toutefois, seules certaines de ces applications peuvent être utilisées avec des instances de compte d'IAM Identity Center. Consultez la liste des [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#).

Étape 1. Activation d'une instance de compte d'IAM Identity Center

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
 - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
 - Utilisez-le déjà AWS avec un appareil autonome Compte AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Sur la page d'accueil de la console de AWS gestion, sélectionnez le service IAM Identity Center ou accédez à la console [IAM Identity Center](#).
3. Sélectionnez Activer.
4. Sur la AWS Organizations page Activer le centre d'identité IAM avec, choisissez activer une instance de compte d'IAM Identity Center.

5. Sur la page Activer l'instance de compte d'IAM Identity Center, passez en revue les informations et ajoutez éventuellement les balises que vous souhaitez associer à cette instance de compte. Puis choisissez Enable.

Étape 2. Création d'un utilisateur dans IAM Identity Center

Cette procédure décrit comment créer un utilisateur directement dans le répertoire intégré d'Identity Center. Ce répertoire n'est connecté à aucun autre répertoire que votre administrateur pourrait utiliser pour gérer les utilisateurs du personnel. Après avoir créé l'utilisateur dans IAM Identity Center, vous devez spécifier de nouvelles informations d'identification pour cet utilisateur. Lorsque vous vous connectez en tant qu'utilisateur pour tester votre application AWS gérée, vous vous connectez avec les nouvelles informations d'identification. Les nouvelles informations d'identification ne vous permettront pas d'accéder aux autres ressources de l'entreprise.

Note

Nous vous recommandons d'utiliser cette méthode pour créer des utilisateurs à des fins de test uniquement.

1. Dans le volet de navigation de la console IAM Identity Center, sélectionnez Utilisateurs, puis Ajouter un utilisateur.
2. Suivez les instructions de la console pour ajouter l'utilisateur. Gardez la case Envoyer un e-mail à cet utilisateur avec les instructions de configuration du mot de passe sélectionnée et assurez-vous de spécifier une adresse e-mail à laquelle vous avez accès.
3. Déconnectez-vous de la console .

Étape 3. Connectez-vous au portail d' AWS accès en tant qu'utilisateur de votre IAM Identity Center

Le portail AWS d'accès est un portail Web qui permet à l'utilisateur que vous avez créé d'accéder à la console AWS de gestion. Avant de pouvoir vous connecter au portail AWS d'accès, vous devez accepter l'invitation à rejoindre IAM Identity Center et activer vos informations d'identification utilisateur.

1. Vérifiez dans votre e-mail la ligne d'objet de l'invitation à rejoindre AWS IAM Identity Center.
2. Choisissez Accepter l'invitation et suivez les instructions de la page d'inscription pour définir un nouveau mot de passe, vous connecter et enregistrer un appareil MFA pour votre utilisateur.

3. Après avoir enregistré votre appareil MFA, le portail d' AWS accès s'ouvre. Lorsque des applications sont disponibles, vous les trouverez sous l'onglet Applications.

 Note

AWS les applications qui prennent en charge les instances de compte permettent aux utilisateurs de se connecter aux applications sans avoir besoin d'autorisations supplémentaires. Par conséquent, l'onglet Comptes restera vide.

Étape 4 : Configurer l'application AWS gérée pour utiliser IAM Identity Center

1. Lorsque vous êtes connecté à la console AWS de gestion, ouvrez la console de l'application AWS gérée que vous comptez utiliser.
2. Suivez les instructions de la console pour configurer l'application AWS gérée afin qu'elle utilise IAM Identity Center. Au cours de ce processus, vous pouvez affecter l'utilisateur que vous avez créé à l'application.

Afficher et modifier les détails d'une application AWS gérée

Une fois que vous avez connecté une application AWS gérée à IAM Identity Center à l'aide de la console ou APIs pour l'application, l'application est enregistrée auprès d'IAM Identity Center. Une fois qu'une application est enregistrée auprès d'IAM Identity Center, vous pouvez consulter et modifier les détails de l'application dans la console IAM Identity Center.

Les informations relatives à l'application indiquent si des affectations d'utilisateurs et de groupes sont requises et, le cas échéant, des utilisateurs et des groupes assignés et des applications fiables pour la propagation des identités. Pour plus d'informations sur la propagation d'identités fiables, consultez [Vue d'ensemble de la propagation d'identités fiables](#).

Pour afficher et modifier les informations relatives à une application AWS gérée dans la console IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Choisissez l'onglet AWS géré.
4. Choisissez le lien de l'application gérée que vous souhaitez ouvrir et afficher.

5. Si vous souhaitez modifier les informations relatives à une application AWS gérée, choisissez Action, puis Modifier les détails.
6. Vous pouvez modifier le nom d'affichage et la description de l'application, ainsi que la méthode d'attribution des utilisateurs et des groupes.
 - a. Pour modifier le nom d'affichage, entrez le nom souhaité dans le champ Nom d'affichage et choisissez Enregistrer les modifications.
 - b. Pour modifier la description, entrez la description souhaitée dans le champ Description et choisissez Enregistrer les modifications.
 - c. Pour modifier la méthode d'attribution des utilisateurs et des groupes, effectuez les modifications souhaitées et choisissez Enregistrer les modifications. Pour de plus amples informations, veuillez consulter [the section called "Utilisateurs, groupes et provisionnement"](#).

Désactivation d'une application AWS gérée

Pour empêcher les utilisateurs de s'authentifier auprès d'une application AWS gérée, vous pouvez désactiver l'application dans la console IAM Identity Center.

Pour désactiver une application AWS gérée

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Sur la page Applications, sous Applications AWS gérées, choisissez l'application que vous souhaitez désactiver.
4. Une fois l'application sélectionnée, choisissez Actions, puis sélectionnez Désactiver.
5. Dans la boîte de dialogue Désactiver l'application, choisissez Désactiver.
6. Dans la liste des applications AWS gérées, le statut de l'application apparaît comme Inactif.

Note

Si une application AWS gérée est désactivée, vous pouvez rétablir la capacité des utilisateurs à s'authentifier auprès de l'application en choisissant Actions puis Activer.

Activation de sessions de console à identité améliorée

Une session à identité améliorée pour la console améliore la session de AWS console d'un utilisateur en fournissant un contexte utilisateur supplémentaire pour personnaliser l'expérience de cet utilisateur. Cette fonctionnalité est actuellement prise en charge pour les utilisateurs de Kiro Pro [sur les AWS applications et les sites Web](#).

Vous pouvez activer les sessions de console à identité améliorée sans modifier les modèles d'accès existants ni la fédération dans la AWS console. Si vos utilisateurs se connectent à la AWS console via IAM (par exemple, s'ils se connectent en tant qu'utilisateurs IAM ou via un accès fédéré avec IAM), ils peuvent continuer à utiliser ces méthodes. Si vos utilisateurs se connectent au portail AWS d'accès, ils peuvent continuer à utiliser leurs informations d'identification utilisateur IAM Identity Center.

Rubriques

- [Prérequis et considérations](#)
- [Comment activer les identity-enhanced-console sessions](#)
- [Comment fonctionnent les sessions de console à identité améliorée](#)

Prérequis et considérations

Avant d'activer les sessions de console à identité améliorée, passez en revue les conditions préalables et les considérations suivantes :

- Si vos utilisateurs accèdent à Kiro sur des AWS applications et des sites Web via un abonnement Kiro Pro, vous devez activer les sessions de console à identité améliorée.

Note

Les utilisateurs de Kiro peuvent accéder à Kiro sans sessions d'identification améliorée, mais ils n'auront pas accès à leurs abonnements Kiro Pro.

- Les sessions de console à identité améliorée nécessitent une [instance organisationnelle](#) d'IAM Identity Center.
- L'intégration à Kiro n'est pas prise en charge si vous activez IAM Identity Center dans le cadre d'un opt-in. Région AWS

- Pour activer les sessions de console à identité améliorée, vous devez disposer des autorisations suivantes :
 - `sso:CreateApplication`
 - `sso:GetSharedSsoConfiguration`
 - `sso:ListApplications`
 - `sso:PutApplicationAssignmentConfiguration`
 - `sso:PutApplicationAuthenticationMethod`
 - `sso:PutApplicationGrant`
 - `sso:PutApplicationAccessScope`
 - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
 - `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- Pour permettre à vos utilisateurs d'utiliser des sessions de console à identité améliorée, vous devez leur accorder `sts:setContext` autorisation dans le cadre d'une politique basée sur l'identité. Pour plus d'informations, consultez la [section Autorisation des utilisateurs à utiliser les sessions de console à identité améliorée](#).

Comment activer les identity-enhanced-console sessions

Vous pouvez activer les sessions de console à identité améliorée dans la console Kiro ou dans la console IAM Identity Center.

Activer les sessions de console à identité améliorée dans la console Kiro

Avant d'activer les sessions de console à identité améliorée, vous devez disposer d'une instance d'organisation d'IAM Identity Center connectée à une source d'identité. Si vous avez déjà configuré IAM Identity Center, passez à l'étape 3.

1. Ouvrez la console IAM Identity Center. Choisissez Activer et créez une instance d'organisation d'IAM Identity Center. Pour plus d'informations, consultez [Activer IAM Identity Center](#).
2. Connectez votre source d'identité à IAM Identity Center et connectez les utilisateurs à IAM Identity Center. Vous pouvez connecter votre source d'identité existante à IAM Identity Center ou utiliser le répertoire Identity Center si vous n'utilisez pas déjà une autre source d'identité. Pour de plus amples informations, veuillez consulter [Tutoriels sur les sources d'identité IAM Identity Center](#).

3. Une fois que vous avez terminé de configurer IAM Identity Center, ouvrez la console Kiro et suivez les étapes décrites dans la section [Abonnements](#) du guide de l'utilisateur de Kiro. Assurez-vous d'activer les sessions de console à identité améliorée.

 Note

Si vous ne disposez pas des autorisations suffisantes pour activer les sessions de console à identité améliorée, vous devrez peut-être demander à un administrateur IAM Identity Center d'effectuer cette tâche pour vous dans la console IAM Identity Center. Pour en savoir plus, consultez la procédure suivante.

Activer les sessions de console à identité améliorée dans la console IAM Identity Center

Si vous êtes administrateur d'IAM Identity Center, un autre administrateur peut vous demander d'activer les sessions de console à identité améliorée dans la console IAM Identity Center.

1. Ouvrez la console IAM Identity Center.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Activer les sessions à identité améliorée, choisissez Activer.
4. Dans le deuxième message, sélectionnez Activer.
5. Une fois que vous avez terminé d'activer les sessions de console à identité améliorée, un message de confirmation apparaît en haut de la page Paramètres.
6. Dans la section Détails, le statut des sessions améliorées par identité est Activé.

Comment fonctionnent les sessions de console à identité améliorée

IAM Identity Center améliore la session de console actuelle d'un utilisateur pour inclure l'ID utilisateur IAM Identity Center actif et l'ID de session IAM Identity Center.

Les sessions de console à identité améliorée incluent les trois valeurs suivantes :

- ID utilisateur du magasin d'identités ([boutique d'identité : UserId](#)) : cette valeur est utilisée pour identifier de manière unique un utilisateur dans la source d'identité connectée à IAM Identity Center.

- ARN du répertoire du magasin d'identités ([boutique d'identité : IdentityStoreArn](#)) : cette valeur est l'ARN du magasin d'identités connecté à IAM Identity Center et dans lequel vous pouvez rechercher des attributs. `identitystore:UserId`
- ID de session IAM Identity Center : cette valeur indique si la session IAM Identity Center de l'utilisateur est toujours valide.

Les valeurs sont les mêmes, mais obtenues de différentes manières et ajoutées à différents moments du processus, en fonction de la manière dont l'utilisateur se connecte :

- IAM Identity Center (portail AWS d'accès) : dans ce cas, l'ID utilisateur et les valeurs ARN du magasin d'identités de l'utilisateur sont déjà fournis dans la session IAM Identity Center active. IAM Identity Center améliore la session en cours en ajoutant uniquement l'ID de session.
- Autres méthodes de connexion : si l'utilisateur se connecte en AWS tant qu'utilisateur IAM, avec un rôle IAM ou en tant qu'utilisateur fédéré avec IAM, aucune de ces valeurs n'est fournie. IAM Identity Center améliore la session en cours en ajoutant l'ID utilisateur de la banque d'identités, l'ARN du répertoire de la banque d'identités et l'ID de session.

Applications gérées par le client

IAM Identity Center agit comme un service d'identité central pour les utilisateurs et les groupes de votre personnel. Si vous utilisez déjà un fournisseur d'identité (IdP), IAM Identity Center peut s'intégrer à votre IdP afin que vous puissiez configurer vos utilisateurs et vos groupes dans IAM Identity Center et utiliser votre IdP pour l'authentification. Avec une connexion unique, IAM Identity Center représente votre IdP devant Services AWS plusieurs et permet à OAuth vos applications 2.0 de demander l'accès aux données de ces services au nom de vos utilisateurs. Vous pouvez également utiliser IAM Identity Center pour attribuer à vos utilisateurs l'accès aux applications [SAML 2.0](#). Cela inclut des AWS services tels qu'Amazon Connect et Amazon AWS Client VPN, qui s'intègrent à IAM Identity Center exclusivement à l'aide de SAML et sont donc classés dans la catégorie des applications gérées par le client.

- Si votre application prend en charge les jetons Web JSON (JWTs), vous pouvez utiliser la fonction de propagation d'identité sécurisée d'IAM Identity Center pour permettre à votre application de demander l'accès aux données Services AWS au nom de vos utilisateurs. La propagation fiable des identités repose sur le cadre d'autorisation OAuth 2.0 et inclut une option permettant aux applications d'échanger des jetons d'identité provenant d'un serveur d'autorisation OAuth 2.0

externe contre des jetons émis par IAM Identity Center et reconnus par Services AWS. Pour de plus amples informations, veuillez consulter [Cas d'utilisation de propagation d'identité fiables](#).

- Si votre application prend en charge le protocole SAML 2.0, vous pouvez la connecter à une [instance organisationnelle d'IAM Identity Center](#). Vous pouvez utiliser IAM Identity Center pour attribuer l'accès à votre application SAML 2.0.

Note

Lorsque vous intégrez des applications gérées par le client à une instance IAM Identity Center qui utilise une [clé KMS gérée par le client](#), vérifiez si l'application invoque le service IAM Identity Center APIs pour confirmer si l'application a besoin d'autorisations relatives aux clés KMS. Suivez les instructions relatives à l'octroi d'autorisations clés KMS pour les flux de travail personnalisés figurant dans les [politiques clés KMS de base](#) du guide de l'utilisateur d'IAM Identity Center.

Rubriques

- [Accès par authentification unique aux applications SAML 2.0 et OAuth 2.0](#)
- [Configuration d'applications SAML 2.0 gérées par le client](#)

Accès par authentification unique aux applications SAML 2.0 et OAuth 2.0

IAM Identity Center vous permet de fournir à vos utilisateurs un accès par authentification unique aux applications SAML 2.0 ou OAuth 2.0. Les rubriques suivantes fournissent une présentation générale de SAML 2.0 et OAuth 2.0.

Rubriques

- [SAML 2.0](#)
- [OAuth 2.0](#)

SAML 2.0

SAML 2.0 est une norme industrielle utilisée pour échanger en toute sécurité des assertions SAML qui transmettent des informations sur un utilisateur entre une autorité SAML (appelée fournisseur d'identité ou IdP) et un consommateur SAML 2.0 (appelé fournisseur de services ou SP). IAM Identity

Center utilise ces informations pour fournir un accès d'authentification unique fédéré aux utilisateurs autorisés à utiliser les applications du AWS portail d'accès.

 Note

IAM Identity Center ne prend pas en charge la validation des signatures des demandes d'authentification SAML entrantes provenant d'applications SAML.

OAuth 2,0

OAuth Le 2.0 est un protocole qui permet aux applications d'accéder aux données des utilisateurs et de les partager en toute sécurité sans partager de mots de passe. Cette fonctionnalité fournit aux utilisateurs un moyen sécurisé et standardisé d'autoriser les applications à accéder à leurs ressources. L'accès est facilité par différents flux de subventions OAuth 2.0.

IAM Identity Center permet aux applications qui s'exécutent sur des clients publics de récupérer des informations d'identification temporaires pour accéder Comptes AWS et fournir des services par programmation au nom de leurs utilisateurs. Les clients publics sont généralement des ordinateurs de bureau, des ordinateurs portables ou d'autres appareils mobiles utilisés pour exécuter des applications localement. Les exemples d' AWS applications exécutées sur des clients publics incluent le AWS Command Line Interface (AWS CLI) et AWS Toolkit les kits de développement AWS logiciel (SDKs). Pour permettre à ces applications d'obtenir des informations d'identification, IAM Identity Center prend en charge certaines parties des flux OAuth 2.0 suivants :

- [Octroi de code d'autorisation avec clé de preuve pour l'échange de code \(PKCE\) \(RFC 6749 et RFC 7636\)](#)
- Octroi d'autorisation d'appareil ([RFC 8628](#))

 Note

Ces types de subventions ne peuvent être utilisés Services AWS que s'ils prennent en charge cette fonctionnalité. Il est possible que ces services ne prennent pas en charge ce type de subvention du tout Régions AWS. Reportez-vous à la documentation pertinente Services AWS pour les différences régionales.

OpenID Connect (OIDC) est un protocole d'authentification basé sur le OAuth framework 2.0. L'OIDC indique comment utiliser la OAuth version 2.0 pour l'authentification. Par le biais du [service IAM Identity Center OIDC APIs](#), une application enregistre un client OAuth 2.0 et utilise l'un de ces flux pour obtenir un jeton d'accès qui fournit des autorisations à IAM Identity Center protected. APIs Une application définit les [étendues d'accès](#) pour déclarer l'utilisateur d'API auquel elle est destinée. Une fois que vous, en tant qu'administrateur du centre d'identité IAM, avez configuré votre source d'identité, les utilisateurs finaux de votre application doivent terminer un processus de connexion, s'ils ne l'ont pas déjà fait. Vos utilisateurs finaux doivent ensuite donner leur accord pour autoriser l'application à effectuer des appels d'API. Ces appels d'API sont effectués à l'aide des autorisations des utilisateurs. En réponse, IAM Identity Center renvoie un jeton d'accès à l'application contenant les étendues d'accès auxquelles les utilisateurs ont consenti.

Utilisation d'un flux de subventions OAuth 2.0

OAuth Les flux de subventions 2.0 ne sont disponibles que par le biais d'applications AWS gérées qui les prennent en charge. Pour utiliser un flux OAuth 2.0, votre instance d'IAM Identity Center et toutes les applications AWS gérées prises en charge que vous utilisez doivent être déployées en une seule Région AWS fois. Reportez-vous à la documentation de chacune Service AWS pour déterminer la disponibilité régionale des applications AWS gérées et l'instance d'IAM Identity Center que vous souhaitez utiliser.

Pour utiliser une application qui utilise un flux OAuth 2.0, l'utilisateur final doit saisir l'URL à laquelle l'application se connectera et s'enregistrera auprès de votre instance d'IAM Identity Center. Selon l'application, en tant qu'administrateur, vous devez fournir à vos utilisateurs l'URL du portail AWS d'accès ou l'URL de l'émetteur de votre instance d'IAM Identity Center. Vous trouverez ces deux paramètres sur la page des paramètres de la [console IAM Identity Center](#). Pour plus d'informations sur la configuration d'une application cliente, reportez-vous à la documentation de cette application.

L'expérience de l'utilisateur final en matière de connexion à une application et de fourniture de son consentement varie selon que l'application utilise le [Octroi de code d'autorisation avec PKCE](#) ou [Octroi d'autorisation d'appareil](#).

Octroi de code d'autorisation avec PKCE

Ce flux est utilisé par les applications qui s'exécutent sur un appareil doté d'un navigateur.

1. Une fenêtre de navigateur s'ouvre.
2. Si l'utilisateur ne s'est pas authentifié, le navigateur le redirige pour terminer l'authentification utilisateur.

3. Après authentification, l'utilisateur s'affiche sur un écran de consentement qui affiche les informations suivantes :
 - Le nom de l'application
 - Les étendues d'accès que l'application demande le consentement pour utiliser
4. L'utilisateur peut annuler le processus de consentement ou donner son consentement et l'application procède à l'accès en fonction des autorisations de l'utilisateur.

Octroi d'autorisation d'appareil

Ce flux peut être utilisé par les applications qui s'exécutent sur un appareil avec ou sans navigateur. Lorsque l'application lance le flux, elle présente une URL et un code utilisateur que l'utilisateur doit vérifier ultérieurement dans le flux. Le code utilisateur est nécessaire car l'application qui initie le flux est peut-être exécutée sur un appareil différent de celui sur lequel l'utilisateur donne son consentement. Le code garantit que l'utilisateur consent au flux qu'il a initié sur l'autre appareil.

Note

Si des clients l'utilisent `device.sso.region.amazonaws.com`, vous devez mettre à jour votre flux d'autorisation afin d'utiliser Proof Key for Code Exchange (PKCE). Pour plus d'informations, consultez [la section Configuration de l'authentification IAM Identity Center AWS CLI à l'aide du](#) guide de l'AWS Command Line Interface utilisateur.

1. Lorsque le flux est lancé à partir d'un appareil doté d'un navigateur, une fenêtre de navigateur s'ouvre. Lorsque le flux est lancé à partir d'un appareil sans navigateur, l'utilisateur doit ouvrir un navigateur sur un autre appareil et accéder à l'URL présentée par l'application.
2. Dans les deux cas, si l'utilisateur ne s'est pas authentifié, le navigateur le redirige pour terminer l'authentification de l'utilisateur.
3. Après authentification, l'utilisateur s'affiche sur un écran de consentement qui affiche les informations suivantes :
 - Le nom de l'application
 - Les étendues d'accès que l'application demande le consentement pour utiliser
 - Le code utilisateur que l'application a présenté à l'utilisateur
4. L'utilisateur peut annuler le processus de consentement ou donner son consentement et l'application procède à l'accès en fonction des autorisations de l'utilisateur.

Étendue d'accès

Une étendue définit l'accès à un service accessible via un flux OAuth 2.0. Les étendues permettent au service, également appelé serveur de ressources, de regrouper les autorisations liées aux actions et aux ressources du service, et elles spécifient les opérations grossières que OAuth les clients 2.0 peuvent demander. Lorsqu'un client OAuth 2.0 s'enregistre auprès du [service IAM Identity Center OIDC](#), il précise les limites dans lesquelles il doit déclarer les actions prévues, pour lesquelles l'utilisateur doit donner son consentement.

OAuth Les clients 2.0 utilisent scope les valeurs définies dans [la section 3.3 de OAuth 2.0 \(RFC 6749\)](#) pour spécifier les autorisations demandées pour un jeton d'accès. Les clients peuvent spécifier un maximum de 25 étendues lorsqu'ils demandent un jeton d'accès. Lorsqu'un utilisateur donne son consentement lors d'une attribution de code d'autorisation avec PKCE ou Device Authorization Grant flow, IAM Identity Center encode les étendues dans le jeton d'accès qu'il renvoie.

AWS ajoute des champs d'application à IAM Identity Center pour qu'ils soient pris en charge.

Services AWS Le tableau suivant répertorie les étendues prises en charge par le service IAM Identity Center OIDC lorsque vous enregistrez un client public.

Étendue d'accès prise en charge par le service IAM Identity Center OIDC lors de l'enregistrement d'un client public

Scope	Description	Services pris en charge par
sso:account:access	Accédez aux comptes gérés par IAM Identity Center et aux ensembles d'autorisations.	IAM Identity Center
codewhisperer:analysis	Activez l'accès à l'analyse du code Kiro.	ID de constructeur AWS et IAM Identity Center
codewhisperer:completions	Activez l'accès aux suggestions de code en ligne de Kiro.	ID de constructeur AWS et IAM Identity Center
codewhisperer:conversations	Activez l'accès au chat Kiro.	ID de constructeur AWS et IAM Identity Center

Scope	Description	Services pris en charge par
<code>codewhisperer:taskassist</code>	Activez l'accès à Kiro Agent pour le développement de logiciels.	ID de constructeur AWS et IAM Identity Center
<code>codewhisperer:transformations</code>	Activez l'accès à l'agent Kiro pour la transformation du code.	ID de constructeur AWS et IAM Identity Center
<code>codecatalyst:read_write</code>	Lisez et écrivez sur vos CodeCatalyst ressources Amazon pour accéder à toutes vos ressources existantes.	ID de constructeur AWS et IAM Identity Center
<code>verified_access:application:connect</code>	Activer Accès vérifié par AWS	Accès vérifié par AWS
<code>redshift:connect</code>	Connect à Amazon Redshift	Amazon Redshift
<code>datazone:domain:access</code>	Accédez à votre rôle d'exécution de DataZone domaine	Amazon DataZone
<code>nosqlworkbench:datamodeladviser</code>	Création et lecture de modèles de données	NoSQL Workbench
<code>transform:read_write</code>	Permettre l'accès à l'agent de AWS transformation pour la transformation du code	AWS Transformation

Configuration d'applications SAML 2.0 gérées par le client

Si vous utilisez des applications gérées par le client qui prennent en charge le [protocole SAML 2.0](#), vous pouvez fédérer votre IdP à IAM Identity Center via SAML 2.0 et utiliser IAM Identity Center pour gérer l'accès des utilisateurs à ces applications. Vous pouvez sélectionner une application SAML 2.0

dans un catalogue d'applications couramment utilisées dans la console IAM Identity Center, ou vous pouvez configurer votre propre application SAML 2.0.

 Note

Si vous avez des applications gérées par le client compatibles avec la OAuth version 2.0 et que vos utilisateurs doivent y accéder depuis ces applications Services AWS, vous pouvez utiliser la propagation d'identité sécurisée. Grâce à la propagation sécurisée des identités, un utilisateur peut se connecter à une application, et cette application peut transmettre l'identité de l'utilisateur dans les demandes d'accès aux données Services AWS.

Rubriques

- [Configuration d'une application à partir du catalogue d'applications IAM Identity Center](#)
- [Configurez votre propre application SAML 2.0](#)

Configuration d'une application à partir du catalogue d'applications IAM Identity Center

Vous pouvez utiliser le catalogue d'applications de la console IAM Identity Center pour ajouter de nombreuses applications SAML 2.0 couramment utilisées qui fonctionnent avec IAM Identity Center. Les exemples incluent Salesforce, Box et Microsoft 365.

La plupart des applications fournissent des informations détaillées sur la façon de configurer la confiance entre IAM Identity Center et le fournisseur de services de l'application. Ces informations sont disponibles sur la page de configuration de l'application, une fois que vous l'avez sélectionnée dans le catalogue. Après avoir configuré l'application, vous pouvez attribuer l'accès à des utilisateurs ou à des groupes dans IAM Identity Center selon vos besoins.

Utilisez cette procédure pour configurer une relation de confiance SAML 2.0 entre IAM Identity Center et le fournisseur de services de votre application.

Avant de commencer cette procédure, il est utile de disposer du fichier d'échange de métadonnées du fournisseur de services afin de configurer plus efficacement la confiance. Si vous ne possédez pas ce fichier, vous pouvez toujours utiliser cette procédure pour le configurer manuellement.

Pour ajouter et configurer une application à partir du catalogue d'applications

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.

3. Choisissez l'onglet Gérée par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférences de configuration, choisissez Je souhaite sélectionner une application dans le catalogue.
6. Sous Catalogue d'applications, commencez à taper le nom de l'application que vous souhaitez ajouter dans le champ de recherche.
7. Choisissez le nom de l'application dans la liste lorsqu'elle apparaît dans les résultats de recherche, puis cliquez sur Suivant.
8. Sur la page Configurer l'application, les champs Nom d'affichage et Description sont préremplis avec les informations pertinentes pour l'application. Vous pouvez modifier ces informations.
9. Sous les métadonnées du IAM Identity Center, procédez comme suit :
 - a. Dans le fichier de métadonnées SAML d'IAM Identity Center, choisissez Télécharger pour télécharger les métadonnées du fournisseur d'identité.
 - b. Sous le certificat IAM Identity Center, choisissez Télécharger le certificat pour télécharger le certificat du fournisseur d'identité.

 Note

Vous aurez besoin de ces fichiers ultérieurement lorsque vous configurerez l'application sur le site Web du fournisseur de services. Suivez les instructions de ce fournisseur.

10. (Facultatif) Sous Propriétés de l'application, vous pouvez spécifier l'URL de démarrage de l'application, l'état du relais et la durée de la session. Pour de plus amples informations, veuillez consulter [Comprendre les propriétés de l'application dans la console IAM Identity Center](#).
11. Sous Métadonnées de l'application, effectuez l'une des opérations suivantes :
 - a. Si vous avez un fichier de métadonnées, choisissez Télécharger le fichier de métadonnées SAML de l'application. Sélectionnez ensuite Choisir un fichier pour rechercher et sélectionner le fichier de métadonnées.
 - b. Si vous n'avez pas de fichier de métadonnées, choisissez Tapez manuellement vos valeurs de métadonnées, puis fournissez l'URL de l'application ACS et les valeurs d'audience SAML de l'application.
12. Sélectionnez Soumettre. Vous êtes redirigé vers la page de détails de l'application que vous venez d'ajouter.

Configurez votre propre application SAML 2.0

Vous pouvez configurer vos propres applications qui autorisent la fédération d'identités à l'aide de SAML 2.0 et les ajouter à IAM Identity Center. La plupart des étapes de configuration de vos propres applications SAML 2.0 sont identiques à celles de configuration d'une application SAML 2.0 à partir du catalogue d'applications de la console IAM Identity Center. Toutefois, vous devez également fournir des mappages d'attributs SAML supplémentaires pour vos propres applications SAML 2.0. Ces mappages permettent à IAM Identity Center de remplir correctement l'assertion SAML 2.0 pour votre application. Vous pouvez fournir ce mappage d'attributs SAML supplémentaire lorsque vous configurez l'application pour la première fois. Vous pouvez également fournir des mappages d'attributs SAML 2.0 sur la page de détails de l'application dans la console IAM Identity Center.

Utilisez la procédure suivante pour configurer une relation de confiance SAML 2.0 entre IAM Identity Center et le fournisseur de services de votre application SAML 2.0. Avant de commencer cette procédure, vérifiez que vous avez le certificat et les fichiers d'échange de métadonnées du fournisseur de services afin de finaliser la configuration de l'approbation.

Pour configurer votre propre application SAML 2.0

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Choisissez l'onglet Gérée par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférence de configuration, choisissez J'ai une application que je souhaite configurer.
6. Sous Type d'application, choisissez SAML 2.0.
7. Choisissez Suivant.
8. Sur la page Configurer l'application, sous Configurer l'application, entrez un nom d'affichage pour l'application, tel que **MyApp**. Entrez ensuite une description.
9. Sous les métadonnées du IAM Identity Center, procédez comme suit :
 - a. Dans le fichier de métadonnées SAML d'IAM Identity Center, choisissez Télécharger pour télécharger les métadonnées du fournisseur d'identité.
 - b. Sous le certificat IAM Identity Center, choisissez Télécharger pour télécharger le certificat du fournisseur d'identité.

 Note

Vous aurez besoin de ces fichiers par la suite pour configurer l'application personnalisée sur le site web du fournisseur de services.

10. (Facultatif) Sous Propriétés de l'application, vous pouvez également spécifier l'URL de démarrage de l'application, l'état du relais et la durée de la session. Pour de plus amples informations, veuillez consulter [Comprendre les propriétés de l'application dans la console IAM Identity Center](#).
11. Sous Métadonnées de l'application, choisissez Tapez manuellement vos valeurs de métadonnées. Indiquez ensuite l'URL ACS de l'application et les valeurs d'audience SAML de l'application.
12. Sélectionnez Soumettre. Vous êtes redirigé vers la page de détails de l'application que vous venez d'ajouter.

Vue d'ensemble de la propagation d'identités fiables

La propagation fiable des identités est une fonctionnalité d'IAM Identity Center qui permet aux administrateurs d' Services AWS accorder des autorisations en fonction des attributs de l'utilisateur tels que les associations de groupes. Avec la propagation d'identité sécurisée, le contexte d'identité est ajouté à un rôle IAM pour identifier l'utilisateur qui demande l'accès aux AWS ressources. Ce contexte est propagé à d'autres Services AWS.

Le contexte d'identité comprend les informations Services AWS utilisées pour prendre des décisions d'autorisation lorsqu'ils reçoivent des demandes d'accès. Ces informations incluent des métadonnées qui identifient le demandeur (par exemple, un utilisateur du IAM Identity Center), l'accès Service AWS auquel l'accès est demandé (par exemple, Amazon Redshift) et l'étendue de l'accès (par exemple, accès en lecture seule). Le destinataire Service AWS utilise ce contexte, ainsi que toutes les autorisations attribuées à l'utilisateur, pour autoriser l'accès à ses ressources.

Avantages d'une propagation d'identité fiable

La propagation fiable des identités permet aux administrateurs d' Services AWS accorder des autorisations sur des ressources, telles que des données, en utilisant les identités d'entreprise de votre personnel. En outre, ils peuvent vérifier qui a accédé à quelles données en consultant les journaux de service ou AWS CloudTrail. Si vous êtes administrateur d'IAM Identity Center,

d'autres Service AWS administrateurs peuvent vous demander d'activer la propagation sécurisée des identités.

Permettre une propagation d'identité fiable

Le processus d'activation de la propagation d'identités fiables implique les deux étapes suivantes :

1. Activez IAM Identity Center et connectez votre source d'identités existante à IAM Identity Center : vous continuerez à gérer les identités de vos employés dans votre source d'identités existante ; la connexion à IAM Identity Center crée une référence à votre personnel que tous peuvent partager Services AWS dans votre cas d'utilisation. Les propriétaires de données pourront également l'utiliser dans de futurs cas d'utilisation.
2. Connectez le Services AWS cas d'utilisation à IAM Identity Center : l'administrateur de chaque Service AWS cas d'utilisation de propagation d'identité sécurisée suit les instructions de la documentation du service correspondant pour connecter le service à IAM Identity Center.

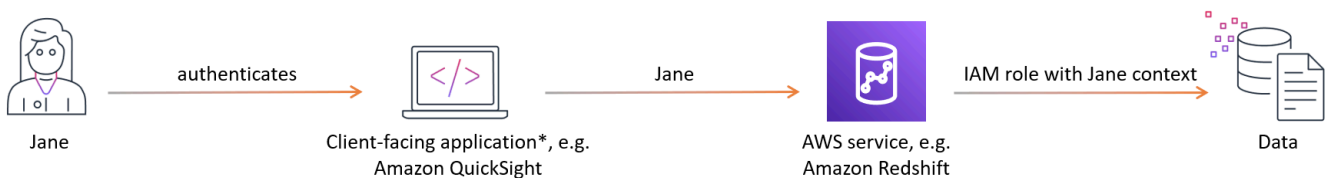
Note

Si votre cas d'utilisation implique une application développée par un tiers ou un client, vous activez la propagation fiable des identités en configurant une relation de confiance entre le fournisseur d'identité qui authentifie les utilisateurs de l'application et IAM Identity Center. Cela permet à votre application de tirer parti du flux de propagation d'identité sécurisé décrit précédemment.

Pour de plus amples informations, veuillez consulter [Utilisation d'applications dotées d'un émetteur de jetons fiable](#).

Comment fonctionne la propagation fiable des identités

Le schéma suivant montre le flux de travail de haut niveau pour la propagation d'identités fiables :



1. Les utilisateurs s'authentifient à l'aide d'une application orientée client, par exemple Quick.

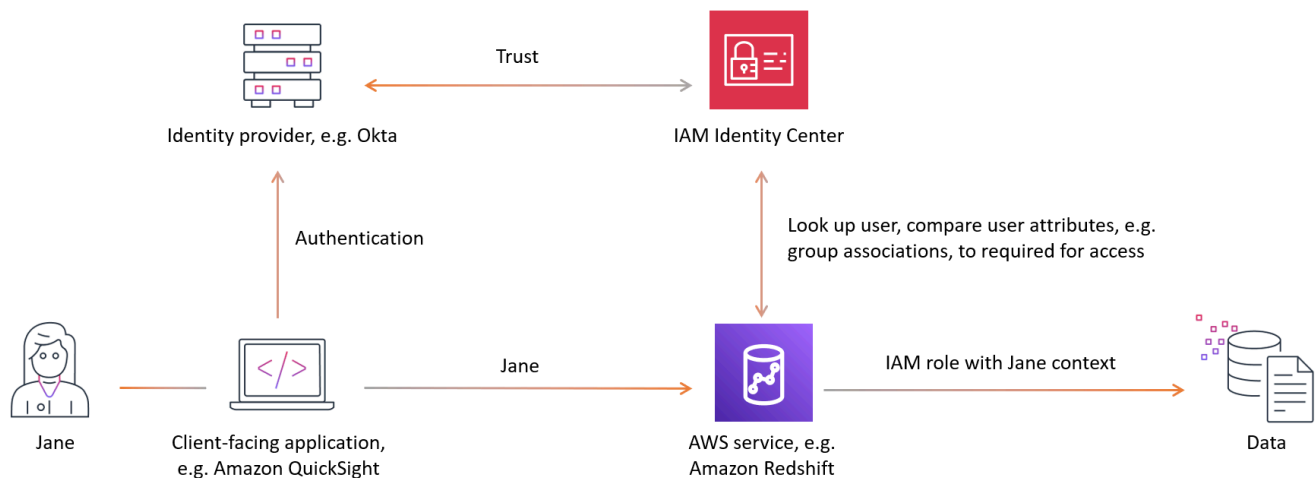
2. L'application orientée client demande l'accès pour utiliser et Service AWS pour interroger des données et inclut des informations sur l'utilisateur.

Note

Certains cas d'utilisation de propagation d'identités fiables impliquent des outils qui interagissent avec Services AWS l'utilisation de pilotes de service. Vous pouvez savoir si cela s'applique à votre cas d'utilisation dans le [guide d'utilisation](#).

3. Service AWS Vérifie l'identité de l'utilisateur auprès d'IAM Identity Center et compare les attributs de l'utilisateur, tels que ses associations de groupe, avec ceux requis pour l'accès. L'accès Service AWS est autorisé tant que l'utilisateur ou son groupe dispose des autorisations nécessaires.
4. Services AWS peuvent enregistrer l'identifiant de l'utilisateur dans AWS CloudTrail et dans leurs journaux de service. Consultez la documentation du service pour plus de détails.

L'image suivante fournit une vue d'ensemble des étapes décrites précédemment dans le processus de propagation des identités fiables :



Rubriques

- [Prérequis et considérations](#)
- [Cas d'utilisation de propagation d'identité fiables](#)
- [Services d'autorisation](#)

Prérequis et considérations

Avant de configurer la propagation sécurisée des identités, passez en revue les conditions préalables et les considérations suivantes.

Rubriques

- [Conditions préalables](#)
- [Considérations](#)
- [Considérations relatives aux applications gérées par le client](#)

Conditions préalables

Pour utiliser la propagation d'identité sécurisée, assurez-vous que votre environnement répond aux exigences suivantes :

- Activer et approvisionner IAM Identity Center
 - Pour utiliser la propagation d'identité sécurisée, vous devez activer IAM Identity Center au même Région AWS endroit où les AWS applications et services auxquels vos utilisateurs auront accès sont activés. Pour plus d'informations, consultez [Activer IAM Identity Center](#).
 - L'instance d'organisation IAM Identity Center est recommandée - Nous vous recommandons d'utiliser une [instance d'organisation](#) d'IAM Identity Center que vous activez dans le compte de gestion de. AWS Organizations Vous pouvez [déléguer l'administration](#) d'une instance d'organisation d'IAM Identity Center à un compte membre. Si vous choisissez une [instance de compte](#) d'IAM Identity Center, toutes les instances auxquelles vous souhaitez Services AWS que les utilisateurs accèdent grâce à une propagation d'identité sécurisée doivent se trouver dans le même Compte AWS endroit où vous activez IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances de compte d'IAM Identity Center](#).
- Connectez votre fournisseur d'identité existant à IAM Identity Center et configurez vos utilisateurs et groupes dans IAM Identity Center. Pour de plus amples informations, veuillez consulter [Tutoriels sur les sources d'identité IAM Identity Center](#).
- Connectez les applications et services AWS gérés dans votre cas d'utilisation de propagation d'identité fiable à IAM Identity Center. Pour utiliser une propagation d'identité fiable, les applications AWS gérées doivent être connectées à IAM Identity Center.

Considérations

Tenez compte des considérations suivantes lors de la configuration et de l'utilisation de la propagation d'identité sécurisée :

- Organisation ou instance de compte d'IAM Identity Center
 - Une [instance organisationnelle](#) d'IAM Identity Center vous donnera le maximum de contrôle et de flexibilité pour étendre vos cas d'utilisation à plusieurs Comptes AWS, utilisateurs et Services AWS. Si vous ne parvenez pas à utiliser une instance d'organisation, votre cas d'utilisation peut être pris en charge par les instances de compte d'IAM Identity Center. Pour en savoir plus sur les instances de compte de support d'IAM Identity Center figurant Services AWS dans votre cas d'utilisation, consultez [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#).
- Les autorisations multi-comptes (ensembles d'autorisations) ne sont pas requises
 - La propagation fiable des identités ne vous oblige pas à configurer des autorisations [multi-comptes \(ensembles d'autorisations\)](#). Vous pouvez activer IAM Identity Center et l'utiliser uniquement pour une propagation d'identité fiable.

Considérations relatives aux applications gérées par le client

Votre personnel peut bénéficier d'une propagation d'identité fiable, même si vos utilisateurs interagissent avec des applications destinées aux clients qui ne sont pas gérées par AWS, par exemple, Tableau ou par vos applications développées sur mesure. Les utilisateurs de ces applications ne sont peut-être pas approvisionnés dans IAM Identity Center. Pour permettre une reconnaissance et une autorisation fluides de l'accès des utilisateurs aux AWS ressources, IAM Identity Center vous permet de configurer une relation de confiance entre le fournisseur d'identité authentifiant vos utilisateurs et IAM Identity Center. Pour de plus amples informations, veuillez consulter [Utilisation d'applications dotées d'un émetteur de jetons fiable](#).

En outre, la configuration de la propagation d'identité sécurisée pour votre application nécessitera :

- Votre application doit utiliser le framework OAuth 2.0 pour l'authentification. La propagation d'identités fiables ne prend pas en charge les intégrations SAML 2.0.
- Votre candidature doit être reconnue par IAM Identity Center. Suivez les instructions spécifiques à votre [cas d'utilisation](#).

Cas d'utilisation de propagation d'identité fiables

En tant qu'administrateur du centre d'identité IAM, il peut vous être demandé d'aider à configurer la propagation sécurisée des identités depuis les applications destinées aux utilisateurs vers. Services AWS Pour appuyer cette demande, vous aurez besoin des informations suivantes :

- Avec quelle application orientée client vos utilisateurs interagiront-ils ?
- Quels Services AWS sont ceux utilisés pour interroger les données et pour autoriser l'accès aux données ?
- Qui Service AWS autorise l'accès aux données ?

Votre rôle dans la mise en place de cas d'utilisation de propagation d'identité fiables qui n'impliquent pas d'applications tierces ou d'applications développées sur mesure est de :

1. [Activez IAM Identity Center.](#)
2. [Connectez votre source d'identité existante à IAM Identity Center.](#)

Les étapes restantes de la configuration de l'identité sécurisée pour ces cas d'utilisation sont effectuées dans les applications connectées Services AWS et. Les administrateurs des applications connectées Services AWS doivent consulter les guides d'utilisation respectifs pour obtenir des conseils complets spécifiques au service.

Votre rôle dans la mise en place d'une propagation d'identité fiable dans les cas d'utilisation impliquant des applications tierces ou des applications développées sur mesure inclut les étapes de [Activer IAM Identity Center connexion à votre source d'identités](#), ainsi que les étapes suivantes :

1. Configuration de la connexion de votre fournisseur d'identité (IdP) à l'application tierce ou développée sur mesure.
2. Permettre à IAM Identity Center de reconnaître l'application tierce ou développée sur mesure.
3. Configuration de votre IdP en tant qu'émetteur de jetons de confiance dans IAM Identity Center. Pour de plus amples informations, veuillez consulter [Utilisation d'applications dotées d'un émetteur de jetons fiable](#).

Les administrateurs des applications connectées Services AWS doivent se référer aux guides d'utilisation respectifs pour obtenir des conseils complets spécifiques aux services.

Cas d'utilisation de l'analytique, du data lakehouse et de l'apprentissage automatique

Vous pouvez activer des cas d'utilisation de propagation fiables à l'aide des services d'analyse et d'apprentissage automatique suivants :

- Amazon Redshift - Pour obtenir des conseils, consultez. [Propagation d'identité fiable avec Amazon Redshift](#)
- Amazon EMR - Pour obtenir des conseils, consultez. [Propagation d'identité fiable avec Amazon EMR](#)
- Amazon Athena - Pour obtenir des conseils, consultez. [Propagation d'identité fiable avec Amazon Athena](#)
- SageMaker Studio - Pour obtenir des conseils, voir [Propagation d'identité fiable avec Amazon SageMaker Studio](#).

Cas d'utilisation supplémentaires

Vous pouvez activer le centre d'identité IAM et la propagation d'identités fiables avec les options supplémentaires Services AWS suivantes :

- Amazon Q Business : pour obtenir des conseils, consultez :
 - [Flux de travail d'administration pour les applications utilisant IAM Identity Center](#).
 - [Configuration d'une application Amazon Q Business à l'aide d'IAM Identity Center](#).
 - [Configurez Amazon Q Business avec la propagation d'identité fiable d'IAM Identity Center](#).
- Amazon OpenSearch Service : pour obtenir des conseils, consultez :
 - [Support de propagation d'identité fiable d'IAM Identity Center pour Amazon OpenSearch Service](#).
 - [Interface OpenSearch utilisateur centralisée \(tableaux de bord\) avec Amazon OpenSearch Service](#).
- AWS Transfer Family- pour obtenir des conseils, voir :
 - [Applications Web Transfer Family](#).

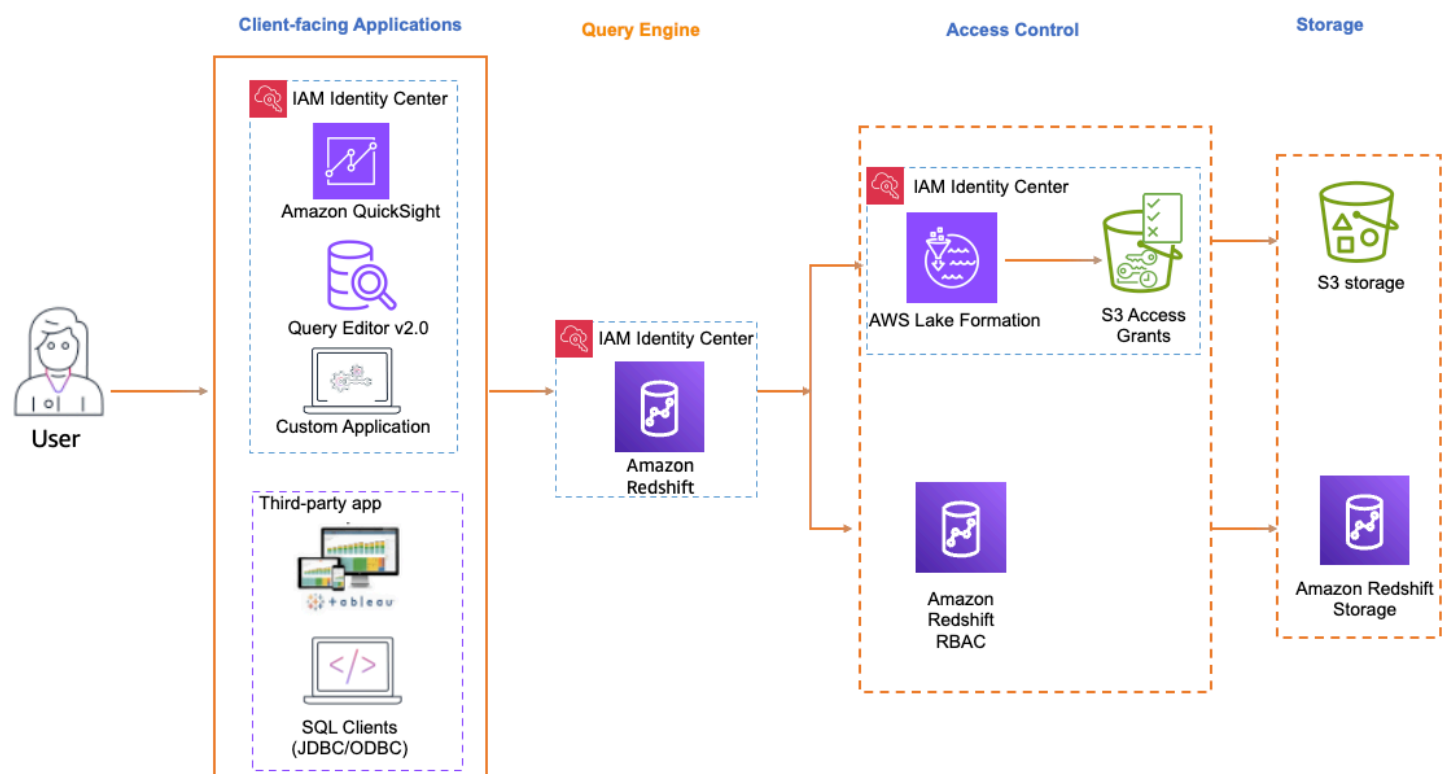
Rubriques

- [Propagation d'identité fiable avec Amazon Redshift](#)
- [Propagation d'identité fiable avec Amazon EMR](#)
- [Propagation d'identité fiable avec Amazon Athena](#)

- [Propagation d'identité fiable avec Amazon SageMaker Studio](#)

Propagation d'identité fiable avec Amazon Redshift

Les étapes à suivre pour activer la propagation fiable des identités varient selon que vos utilisateurs interagissent avec des applications AWS gérées ou des applications gérées par le client. Le schéma suivant montre une configuration de propagation d'identité fiable pour les applications orientées client (AWS gérées ou externes) qui interrogent les données Amazon Redshift avec un contrôle d'accès fourni soit par Amazon Redshift, soit par des services d'autorisation, tels qu'Amazon S3. AWS Lake Formation Access Grants



Lorsque la propagation fiable des identités vers Amazon Redshift est activée, les administrateurs de Redshift peuvent configurer Redshift pour créer automatiquement des rôles pour IAM Identity Center en tant que fournisseur d'identité, associer les rôles Redshift aux groupes d'IAM Identity Center et utiliser le contrôle d'accès basé sur les rôles Redshift pour accorder l'accès.

Applications destinées aux clients prises en charge

AWS applications gérées

Les applications AWS gérées orientées client suivantes prennent en charge la propagation fiable des identités vers Amazon Redshift :

- [Amazon Redshift Query Editor V2](#)
- [Rapide](#)

 Note

Si vous utilisez Amazon Redshift Spectrum pour accéder à des bases de données ou à des tables AWS Glue Data Catalog externes, pensez [à configurer Lake Formation](#) [et Amazon Access Grants](#) S3 pour fournir un contrôle d'accès précis.

Applications gérées par le client

Les applications gérées par le client suivantes prennent en charge la propagation fiable des identités vers Amazon Redshift :

- Tableau Desktop compris TableauServer, et Tableau Prep
 - Pour permettre aux utilisateurs de propager des identités de manière fiable Tableau, consultez la section [Intégrer Tableau et Okta utiliser Amazon Redshift à l'aide d'IAM Identity Center](#) sur le blog AWS Big Data.
- Clients SQL (DBeaver et DBVisualizer)
 - Pour permettre une propagation d'identité fiable pour les utilisateurs de clients SQL (DBeaver et DBVisualizer), consultez la section [Intégrer le fournisseur d'identité \(IdP\) à Amazon Redshift Query Editor V2 et le client SQL à l'aide d'IAM Identity Center pour une authentification unique fluide](#) sur le blog Big Data.AWS

Configuration d'une propagation d'identité fiable avec Amazon Redshift Query Editor V2

La procédure suivante explique comment assurer une propagation d'identité fiable depuis Amazon Redshift Query Editor V2 vers Amazon Redshift.

Conditions préalables

Avant de commencer ce didacticiel, vous devez configurer les éléments suivants :

1. [Activez IAM Identity Center](#). [L'instance d'organisation](#) est recommandée. Pour de plus amples informations, veuillez consulter [Prérequis et considérations](#).
2. [Approvisionnez les utilisateurs et les groupes de votre source d'identités dans IAM Identity Center](#).

L'activation de la propagation fiable des identités inclut les tâches effectuées par un administrateur IAM Identity Center dans la console IAM Identity Center et les tâches effectuées par un administrateur Amazon Redshift dans la console Amazon Redshift.

Tâches effectuées par l'administrateur de l'IAM Identity Center

Les tâches suivantes devaient être effectuées par l'administrateur de l'IAM Identity Center :

1. Créez un [rôle IAM](#) dans le compte où se trouve le cluster Amazon Redshift ou l'instance Serverless avec la politique d'autorisation suivante. Pour plus d'informations, consultez la section [Création d'un rôle IAM](#).
- Les exemples de politique suivants incluent les autorisations nécessaires pour terminer ce didacticiel. Pour utiliser cette politique, remplacez celle de *italicized placeholder text* l'exemple de politique par vos propres informations. Pour obtenir des instructions supplémentaires, voir [Créer une politique](#) ou [Modifier une politique](#).

Politique d'autorisation :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ],
}
```

```

    {
      "Sid": "AllowIDCPPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource": [
        "arn:aws:sso::instance/Your-IAM-Identity-Center-Instance-ID",
        "arn:aws:sso::111122223333:application/Your-IAM-Identity-Center-Instance-ID/*"
      ]
    }
  ]
}

```

Politique de confiance :

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

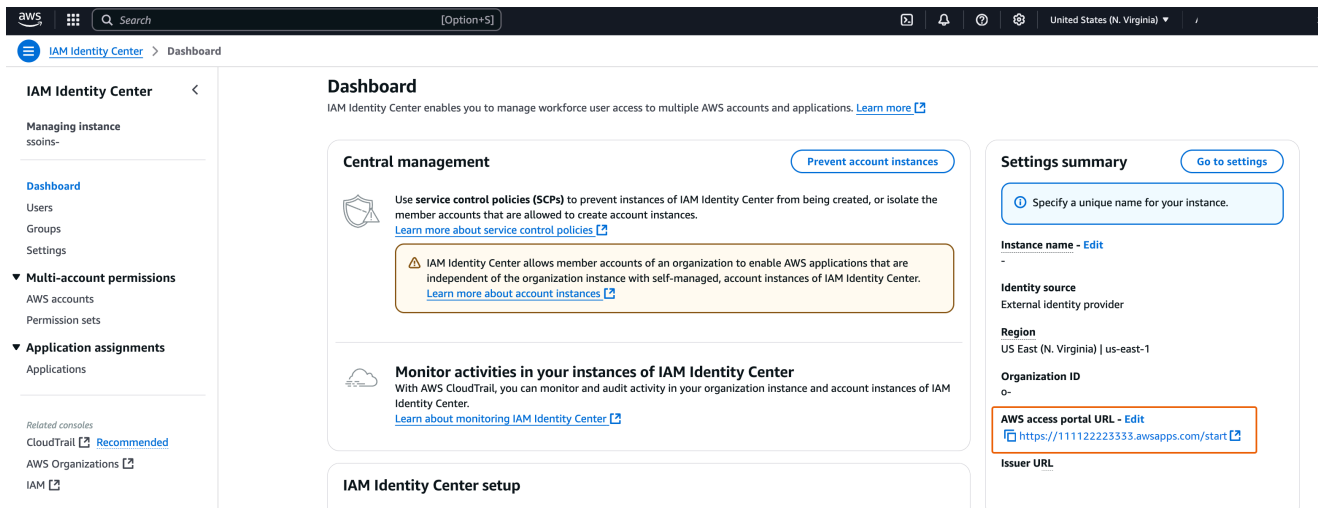
2. Créez un ensemble d'autorisations dans le compte AWS Organizations de gestion sur lequel IAM Identity Center est activé. Vous l'utiliserez à l'étape suivante pour autoriser les utilisateurs fédérés à accéder à Redshift Query Editor V2.
 - a. Accédez à la console IAM Identity Center, sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
 - b. Choisissez Create permission set (Créer un jeu d'autorisations).
 - c. Choisissez Ensemble d'autorisations personnalisé, puis cliquez sur Suivant.
 - d. Dans Politiques AWS gérées, sélectionnez **AmazonRedshiftQueryEditorV2ReadSharing**.
 - e. Sous Stratégie intégrée, ajoutez la politique suivante :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}
```

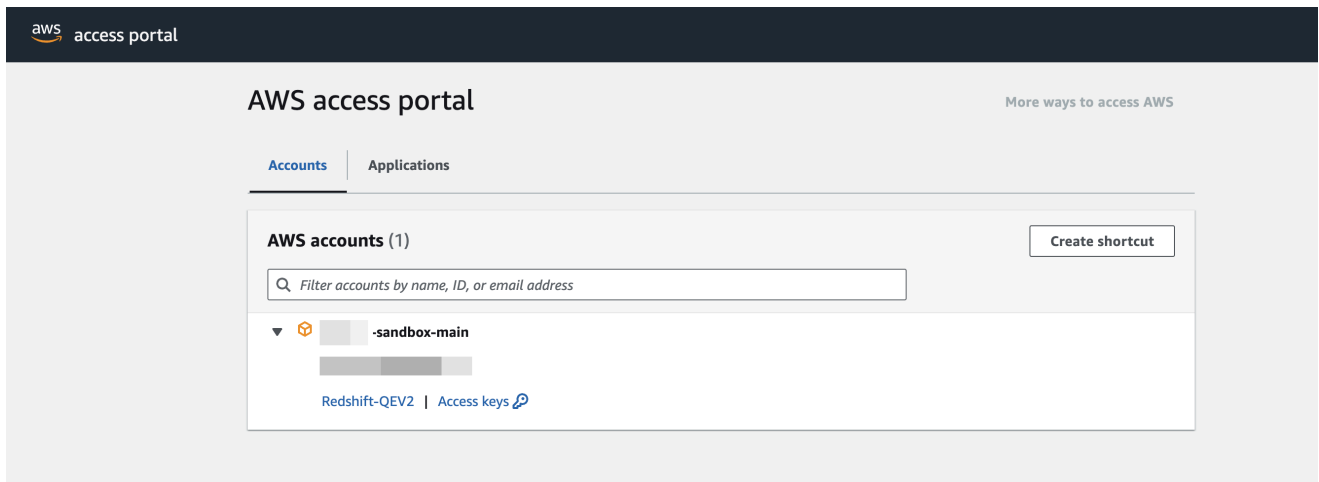
- f. Sélectionnez Suivant, puis attribuez un nom au nom de l'ensemble d'autorisations. Par exemple, **Redshift-Query-Editor-V2**.
 - g. Sous État du relais — facultatif, définissez l'état du relais par défaut sur l'URL de l'éditeur de requêtes V2, en utilisant le format :`https://your-region.console.aws.amazon.com/sqlworkbench/home`.
 - h. Vérifiez les paramètres et choisissez Créer.

- i. Accédez au tableau de bord du centre d'identité IAM et copiez l'URL du portail AWS d'accès depuis la section Récapitulatif des paramètres.



- j. Ouvrez une nouvelle fenêtre de navigation privée et collez l'URL.

Cela vous redirigera vers votre portail AWS d'accès, garantissant que vous vous connectez avec un utilisateur d'IAM Identity Center.



Pour plus d'informations sur l'ensemble d'autorisations, consultez [Gérer Comptes AWS avec des ensembles d'autorisations](#).

3. Permettez aux utilisateurs fédérés d'accéder à Redshift Query Editor V2.
 - a. Dans le compte AWS Organizations de gestion, ouvrez la console IAM Identity Center.
 - b. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
 - c. Sur la Comptes AWS page, sélectionnez Compte AWS celui auquel vous souhaitez attribuer l'accès.

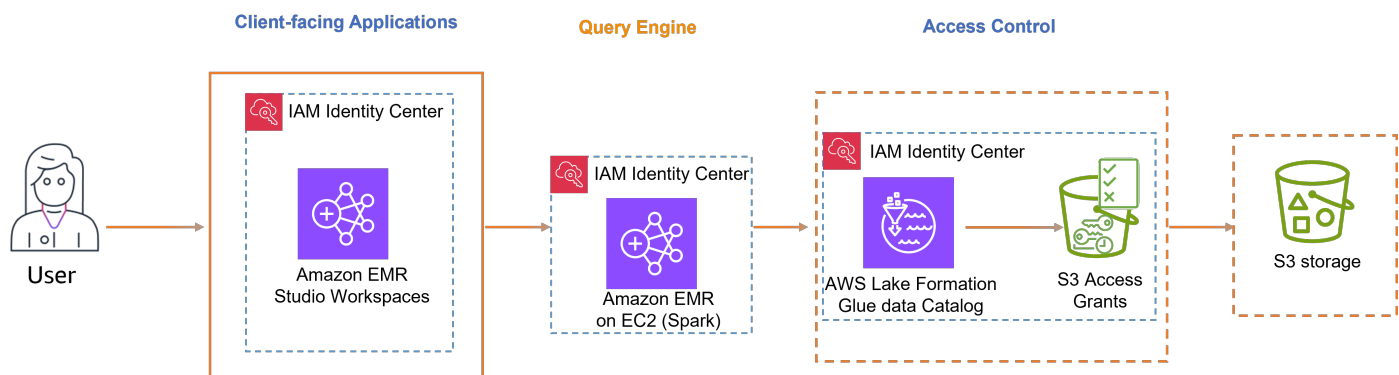
- d. Choisissez Attribuer des utilisateurs ou des groupes.
- e. Sur la page Attribuer des utilisateurs et des groupes, choisissez les utilisateurs et/ou les groupes pour lesquels vous souhaitez créer l'ensemble d'autorisations. Ensuite, choisissez Suivant.
- f. Sur la page Attribuer des ensembles d'autorisations, choisissez le jeu d'autorisations que vous avez créé à l'étape précédente. Ensuite, choisissez Suivant.
- g. Sur la page Réviser et soumettre les devoirs, passez en revue vos sélections et choisissez Soumettre.

Tâches effectuées par un administrateur Amazon Redshift

Pour permettre une propagation d'identité fiable vers Amazon Redshift, un administrateur de cluster Amazon Redshift ou un administrateur Amazon Redshift Serverless doit effectuer un certain nombre de tâches dans la console Amazon Redshift. Pour plus d'informations, consultez [Intégrer le fournisseur d'identité \(IdP\) à Amazon Redshift Query Editor V2 et au client SQL à l'aide d'IAM Identity Center pour une authentification unique fluide](#) sur le blog Big Data.AWS

Propagation d'identité fiable avec Amazon EMR

Le schéma suivant montre une configuration de propagation d'identité fiable pour Amazon EMR Studio à l'aide d'Amazon EMR sur Amazon EC2 avec un contrôle d'accès fourni par Amazon S3. AWS Lake Formation Access Grants



Applications destinées aux clients prises en charge

- Amazon EMR Studio

Pour activer la propagation d'identités fiables, procédez comme suit :

- [Configurez Amazon EMR](#) en Studio tant qu'application orientée client pour le cluster Amazon EMR.
- Configurez le [cluster Amazon EMR sur Amazon EC2](#) avec. Apache Spark
- Recommandé : [AWS Lake Formation](#) et [Amazon S3 Access Grants](#) pour fournir un contrôle d'accès précis AWS Glue Data Catalog et des emplacements de données sous-jacents dans S3.

Configuration d'une propagation d'identité fiable avec Amazon EMR Studio

La procédure suivante explique comment configurer Amazon EMR Studio pour une propagation d'identité fiable dans les requêtes adressées à un groupe de travail Amazon Athena ou à un cluster Amazon EMR en cours d'exécution. Apache Spark

Conditions préalables

Avant de commencer ce didacticiel, vous devez configurer les éléments suivants :

1. [Activez IAM Identity Center](#). [L'instance d'organisation](#) est recommandée. Pour de plus amples informations, veuillez consulter [Prérequis et considérations](#).
2. [Approvisionnez les utilisateurs et les groupes de votre source d'identités dans IAM Identity Center](#).

Pour terminer la configuration de la propagation d'identité sécurisée depuis Amazon EMR Studio, l'administrateur d'EMR Studio doit effectuer les étapes suivantes.

Étape 1. Création des rôles IAM requis pour EMR Studio

Au cours de cette étape, l'Studioadministrateur Amazon EMR crée un rôle de service IAM et un rôle d'utilisateur IAM pour EMR. Studio

1. [Création d'un rôle de service EMR Studio : EMR Studio assume ce rôle](#) IAM pour gérer en toute sécurité les espaces de travail et les blocs-notes, se connecter aux clusters et gérer les interactions de données.
 - a. Accédez à la console IAM (<https://console.aws.amazon.com/iam/>) et créez un rôle IAM.
 - b. Sélectionnez Service AWS comme entité de confiance, puis choisissez Amazon EMR. Joignez les politiques suivantes pour définir les autorisations et la relation de confiance du rôle.

Pour utiliser ces politiques, remplacez celles de *italicized placeholder text* l'exemple de politique par vos propres informations. Pour obtenir des instructions supplémentaires, voir [Créer une politique](#) ou [Modifier une politique](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    },
    {
      "Sid": "BucketActions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    }
  ]
}
```

```
}
]
}
```

Pour une référence de toutes les autorisations de rôle de service, voir Autorisations de [rôle de service EMR Studio](#).

2. [Créez un rôle utilisateur EMR Studio pour l'authentification IAM Identity Center](#) : EMR Studio assume ce rôle lorsqu'un utilisateur se connecte via IAM Identity Center pour gérer des espaces de travail, des clusters EMR, des jobs et des référentiels git. Ce rôle est utilisé pour lancer le flux de travail de propagation des identités fiables.

Note

Le rôle d'utilisateur EMR Studio n'a pas besoin d'inclure d'autorisations pour accéder aux emplacements Amazon S3 des tables dans AWS Glue Catalog. AWS Lake Formation les autorisations et les emplacements enregistrés des lacs seront utilisés pour recevoir des autorisations temporaires.

L'exemple de politique suivant peut être utilisé dans un rôle permettant à un utilisateur d'EMR Studio d'utiliser les groupes de travail Athena pour exécuter des requêtes.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
```

```

        "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
    }
},
{
    "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
            "ec2:CreateAction": "CreateSecurityGroup"
        }
    }
},
{
    "Sid": "AllowSecretManagerListSecrets",
    "Action": [
        "secretsmanager:ListSecrets"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
    "Effect": "Allow",
    "Action": "secretsmanager:CreateSecret",
    "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
    }
},
{
    "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
    "Effect": "Allow",
    "Action": "secretsmanager:TagResource",

```

```

        "Resource": "arn:aws:secretsmanager::*:secret:emr-studio-*"
    },
    {
        "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ListAndLocationPermissions",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::*"
    },
    {
        "Sid": "AllowS3ReadOnlyAccessToLogs",
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowAthenaQueryExecutions",
        "Effect": "Allow",
        "Action": [
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution",
            "athena:ListQueryExecutions",
            "athena:GetQueryResultsStream",
            "athena:ListWorkGroups",
            "athena:GetWorkGroup",

```

```

        "athena:CreatePreparedStatement",
        "athena:GetPreparedStatement",
        "athena>DeletePreparedStatement"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowGlueSchemaManipulations",
    "Effect": "Allow",
    "Action": [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowQueryEditorToAccessWorkGroup",
    "Effect": "Allow",
    "Action": "athena:GetWorkGroup",
    "Resource": "arn:aws:athena:*:111122223333:workgroup*"
},
{
    "Sid": "AllowConfigurationForWorkspaceCollaboration",
    "Action": [
        "elasticmapreduce:UpdateEditor",
        "elasticmapreduce:PutWorkspaceAccess",
        "elasticmapreduce>DeleteWorkspaceAccess",
        "elasticmapreduce:ListWorkspaceAccessIdentities"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "elasticmapreduce:ResourceTag/creatorUserId":
                "${aws:userId}"
        }
    }
},
{
    "Sid": "DescribeNetwork",

```



```
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ListIAMRoles",
        "Effect": "Allow",
        "Action": [
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AssumeRole",
        "Effect": "Allow",
        "Action": [
            "sts:AssumeRole"
        ],
        "Resource": "*"
    }
]
```

La politique de confiance suivante permet à EMR Studio d'assumer ce rôle :

 Note

Des autorisations supplémentaires sont nécessaires pour exploiter les espaces de travail EMR Studio et les Notebooks EMR. Voir [Créer des politiques d'autorisation pour les utilisateurs d'EMR Studio](#) pour plus d'informations.

Vous trouverez de plus amples informations à l'aide des liens suivants :

- [Définir des autorisations IAM personnalisées à l'aide de politiques gérées par le client](#)
- [Autorisations relatives aux rôles du service EMR Studio](#)

Étape 2. Créez et configurez votre studio EMR

Au cours de cette étape, vous allez créer un Amazon EMR Studio dans la console EMR Studio et utiliser les rôles IAM que vous y avez créés. [Étape 1. Création des rôles IAM requis pour EMR Studio](#)

1. Accédez à la console EMR Studio, sélectionnez Create Studio et l'option Configuration personnalisée. Vous pouvez créer un nouveau compartiment S3 ou utiliser un compartiment existant. Vous pouvez cocher la case pour chiffrer les fichiers de l'espace de travail avec vos propres clés KMS. Pour de plus amples informations, veuillez consulter [AWS Key Management Service](#).

The screenshot shows the 'Create Studio' page in the AWS EMR Studio console. The top navigation bar includes the AWS logo, a search bar, and the region 'United States (N. Virginia)'. The breadcrumb trail is 'Amazon EMR > EMR Studio: Studios > Create Studio'. The main content area is titled 'Create a Studio' and includes an 'Info' link. It is divided into two sections: 'Setup options' and 'Studio settings'. In the 'Setup options' section, there are three radio buttons: 'Interactive workloads', 'Batch jobs', and 'Custom' (which is selected). The 'Studio settings' section includes a 'Studio name' field with the value 'Studio_1', a 'Description - optional' text area, and an 'S3 location for Workspace storage' section. In the S3 location section, 'Create new bucket' is selected, and a note indicates that a new bucket will be created with the location 's3://aws-emr-studio-225989353012-us-east-1/1735848818523'. There is also an unchecked checkbox for 'Encrypt Workspace files with your own AWS KMS key'.

2. Sous Rôle de service pour permettre à Studio d'accéder à vos ressources, sélectionnez le rôle [Étape 1. Création des rôles IAM requis pour EMR Studio](#) de service créé dans le menu.
3. Choisissez IAM Identity Center sous Authentification. Sélectionnez le rôle d'utilisateur créé dans [Étape 1. Création des rôles IAM requis pour EMR Studio](#).

Service role to let Studio access your AWS resources

AmazonEMRStudio_

[View permission details](#)

Authentication Info

Authentication

Choose an authentication method for your Studio.

☐ AWS Identity and Access Management (IAM)
Authenticate with single sign-on using IAM identity federation or IAM credentials.

☒ **IAM Identity Center (AWS Single Sign-On)**
Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).

User role

Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#).

emrstudio-userrole-idc

[Create IAM role](#)

Connect EMR Studio to IAM Identity Center

instance of IAM Identity Center

Manage access to EMR Studio by assigning users and groups from your Identity Center directory.

[arn:aws:sso::instance:ssoins-](#)

4. Cochez la case Propagation d'identité fiable. Choisissez Uniquement les utilisateurs et les groupes assignés dans la section Accès aux applications, ce qui vous permettra de n'autoriser que les utilisateurs et les groupes autorisés à accéder à ce studio.
5. (Facultatif) - Vous pouvez configurer le VPC et le sous-réseau si vous utilisez ce studio avec des clusters EMR.

Trusted identity propagation Info

Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

The following features aren't supported from a Studio with trusted identity propagation: creating EMR on EC2 clusters without a template, using EMR Serverless applications, launching EMR on EKS clusters, using a runtime role, and enabling SQL Explorer or Workspace collaboration.

Application access Info

Choose who can access your application

Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ All users and groups
Any user or group from your IAM Identity Center directory can access this application.

Networking and security - optional

VPC Info

Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

Select a VPC

Subnets Info

Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

6. Vérifiez tous les détails et sélectionnez Create Studio.
7. Après avoir configuré un cluster Athena WorkGroup ou EMR, connectez-vous à l'URL du Studio pour :
 - a. Exécutez des requêtes Athena avec l'éditeur de requêtes.

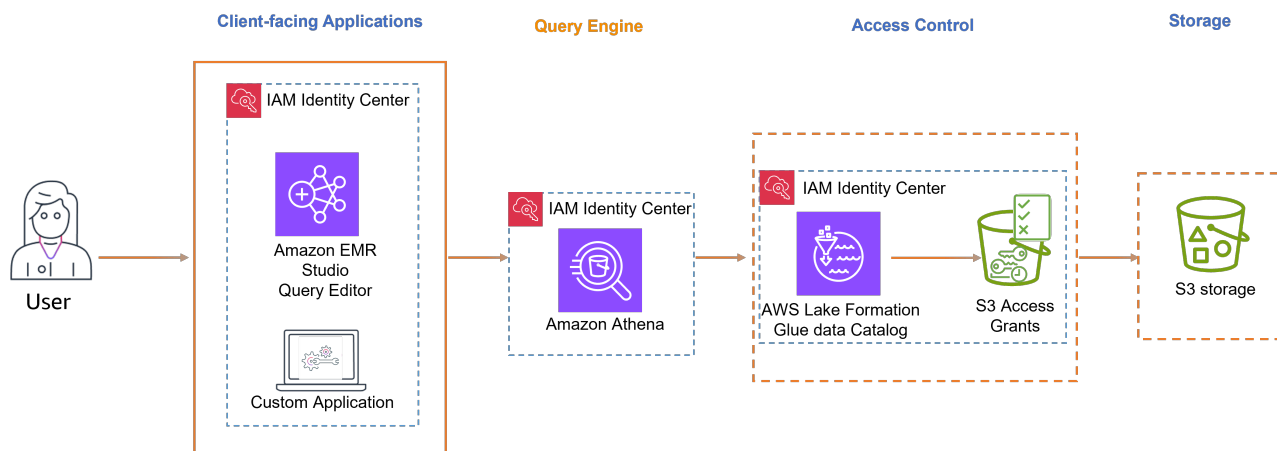
- b. Exécutez des tâches Spark dans l'espace de travail à l'aide du Jupyter bloc-notes.

Propagation d'identité fiable avec Amazon Athena

Les étapes à suivre pour activer la propagation fiable des identités varient selon que vos utilisateurs interagissent avec des applications AWS gérées ou des applications gérées par le client. Le schéma suivant montre une configuration de propagation d'identité fiable pour les applications orientées client (AWS gérées ou externes) qui utilisent Amazon Athena pour AWS interroger les données Amazon S3 avec un contrôle d'accès fourni par Amazon S3 et AWS Lake Formation Amazon S3. Access Grants

Note

- La propagation fiable des identités avec Amazon Athena nécessite l'utilisation de Trino.
- Les clients Apache Spark et SQL connectés à Amazon Athena via les pilotes ODBC et JDBC ne sont pas pris en charge.



AWS applications gérées

L'application AWS gérée orientée client suivante prend en charge la propagation sécurisée des identités avec Athena :

- Amazon EMR Studio

Pour activer la propagation d'identités fiables, procédez comme suit :

- [Configurez Amazon EMR](#) en Studio tant qu'application orientée client pour Athena. L'éditeur de requêtes d'EMR Studio est nécessaire pour exécuter les requêtes Athena lorsque la propagation sécurisée des identités est activée.
- [Configurez le groupe de travail Athena](#).
- [Configurez AWS Lake Formation](#) pour activer un contrôle d'accès précis pour les AWS Glue tables en fonction de l'utilisateur ou du groupe dans IAM Identity Center.
- [Configurez Amazon S3 Access Grants](#) pour permettre un accès temporaire aux emplacements de données sous-jacents dans S3.

 Note

Lake Formation et Amazon S3 Access Grants sont tous deux requis pour le contrôle d'accès aux résultats des requêtes Athena AWS Glue Data Catalog et pour ceux-ci dans Amazon S3.

Applications gérées par le client

Pour activer la propagation d'identité fiable pour les utilisateurs d'applications développées sur mesure, reportez-vous à la section [Accès Services AWS par programmation à l'aide de la propagation d'identité sécurisée](#) dans le blog sur la AWS sécurité.

Configuration d'une propagation d'identité fiable avec les groupes de travail Amazon Athena

La procédure suivante explique comment configurer les groupes de travail Amazon Athena pour une propagation d'identité fiable.

Conditions préalables

Avant de commencer ce didacticiel, vous devez configurer les éléments suivants :

1. [Activez IAM Identity Center](#). [L'instance d'organisation](#) est recommandée. Pour de plus amples informations, veuillez consulter [Prérequis et considérations](#).
2. [Approvisionnez les utilisateurs et les groupes de votre source d'identités dans IAM Identity Center](#).
3. Cette configuration nécessite [Amazon EMR Studio](#) et [Amazon S3 Access Grants](#). [AWS Lake Formation](#)

Configuration d'une propagation d'identité fiable avec Athena

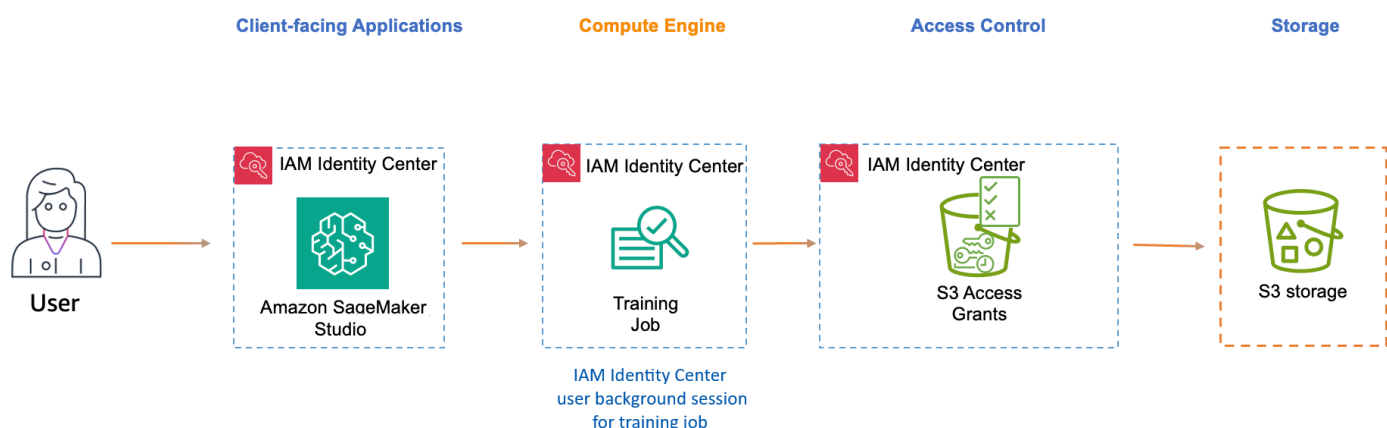
Pour configurer la propagation sécurisée des identités avec Athena, l'administrateur d'Athena doit :

1. Passez en revue [les considérations et les limites liées à l'utilisation des groupes de travail Athena compatibles avec IAM Identity Center](#).
2. [Créez un groupe de travail Athena compatible avec IAM Identity Center](#).

Propagation d'identité fiable avec Amazon SageMaker Studio

[Amazon SageMaker Studio](#) s'intègre à IAM Identity Center et prend en charge les [sessions d'arrière-plan des utilisateurs](#) et la propagation d'identités fiables. Les sessions utilisateur en arrière-plan permettent à un utilisateur de lancer une tâche de longue durée sur SageMaker Studio, sans qu'il soit obligé de rester connecté pendant l'exécution de la tâche. La tâche s'exécute immédiatement et en arrière-plan, en utilisant les autorisations de l'utilisateur à l'origine de la tâche. La tâche peut continuer à s'exécuter même si l'utilisateur éteint son ordinateur, si sa session de connexion à IAM Identity Center expire ou s'il se déconnecte du portail d' AWS accès. La durée de session par défaut pour les sessions d'arrière-plan des utilisateurs est de 7 jours, mais vous pouvez spécifier une durée maximale de 90 jours. La propagation fiable des identités permet de fournir un accès précis à des AWS ressources telles que les compartiments Amazon S3 en fonction de l'identité de l'utilisateur ou de son appartenance à un groupe.

Le schéma suivant montre une configuration de propagation d'identité fiable pour SageMaker Studio, avec accès aux données stockées dans un compartiment Amazon S3. Les sessions d'arrière-plan utilisateur sont activées pour IAM Identity Center, ce qui permet à la tâche de formation SageMaker Studio de s'exécuter en arrière-plan. Le contrôle d'accès aux données d'entraînement est fourni par Amazon S3Access Grants.



AWS application gérée

L'application AWS gérée orientée client suivante prend en charge la propagation d'identités fiables :

- [Amazon SageMaker Studio](#)

Pour activer la propagation d'identité fiable et les sessions d'arrière-plan des utilisateurs, procédez comme suit :

- [Configurez SageMaker Studio en tant qu'application orientée client.](#)
- [Configurez Amazon S3 Access Grants](#) pour permettre un accès temporaire aux emplacements de données sous-jacents dans Amazon S3.

Configuration d'une propagation d'identité fiable avec SageMaker Studio

La procédure suivante explique comment configurer SageMaker Studio pour une propagation d'identité fiable et des sessions d'arrière-plan utilisateur.

Conditions préalables

Avant de commencer ce didacticiel, vous devez effectuer les tâches suivantes :

1. [Activez IAM Identity Center.](#) Une instance d'organisation est requise. Pour de plus amples informations, veuillez consulter [Prérequis et considérations.](#)
2. [Approvisionnez les utilisateurs et les groupes de votre source d'identités dans IAM Identity Center.](#)
3. [Vérifiez que les sessions d'arrière-plan des utilisateurs sont activées](#) dans la console IAM Identity Center. Par défaut, les sessions utilisateur en arrière-plan sont activées et leur durée est fixée à 7 jours. Vous pouvez modifier cette durée.

Pour configurer une propagation d'identité fiable depuis SageMaker Studio, l'administrateur de SageMaker Studio doit effectuer les étapes suivantes.

Étape 1 : activer la propagation d'identités fiables dans un domaine SageMaker Studio nouveau ou existant

SageMaker Studio utilise des domaines pour organiser les profils utilisateur, les applications et les ressources associées. Pour activer la propagation d'identités fiables, vous devez créer un domaine SageMaker Studio ou modifier un domaine existant comme décrit dans la procédure suivante.

1. Ouvrez la console SageMaker AI, accédez à Domains et effectuez l'une des opérations suivantes.
 - Créez un nouveau domaine SageMaker Studio à l'aide de [Configuration pour les organisations](#).

Choisissez Configurer pour les organisations, puis procédez comme suit :

- Choisissez AWS Identity Center comme méthode d'authentification.
- Cochez la case Activer la propagation d'identités fiables pour tous les utilisateurs de ce domaine.
- Modifiez un domaine SageMaker Studio existant.
 - Sélectionnez un domaine existant qui utilise IAM Identity Center pour l'authentification.

 Important

La propagation d'identités fiables n'est prise en charge que dans les domaines SageMaker Studio qui utilisent IAM Identity Center pour l'authentification. Si le domaine utilise IAM pour l'authentification, vous ne pouvez pas modifier la méthode d'authentification et, par conséquent, vous ne pouvez pas activer la propagation d'identité fiable.

- [Modifiez les paramètres du domaine](#). Modifiez les paramètres d'authentification et d'autorisation pour activer la propagation d'identités fiables.
2. Passez à l'[étape 2 : configurer le rôle d'exécution du domaine par défaut](#). Ce rôle est requis pour que les utilisateurs d'un domaine SageMaker Studio puissent accéder à d'autres AWS services tels qu'Amazon S3.

Étape 2 : Configuration du rôle d'exécution du domaine par défaut et de la politique de confiance des rôles

Un rôle d'exécution de domaine est un [rôle IAM](#) qu'un domaine SageMaker Studio assume au nom de tous les utilisateurs du domaine. Les autorisations que vous attribuez à ce rôle déterminent les actions que SageMaker Studio peut effectuer.

1. Pour créer ou sélectionner un rôle d'exécution de domaine, effectuez l'une des opérations suivantes :

- Créez ou sélectionnez un rôle à l'aide de [Configuration pour les organisations](#).
 - Ouvrez la console SageMaker AI et suivez les instructions de la console à l'étape 2 : Configurer les rôles et les activités de machine learning pour créer un nouveau rôle d'exécution de domaine ou sélectionner un rôle existant.
 - Effectuez le reste des étapes de configuration pour créer votre domaine SageMaker Studio.
 - Créez un rôle d'exécution manuellement.
 - Ouvrez la console IAM et [créez vous-même le rôle d'exécution](#).
2. [Mettez à jour la politique de confiance](#) attachée au rôle d'exécution du domaine afin qu'elle inclue les deux actions suivantes : [sts:AssumeRole](#) et [sts:SetContext](#). Pour plus d'informations sur la façon de trouver le rôle d'exécution pour votre domaine SageMaker Studio, voir [Obtenir le rôle d'exécution du domaine](#).

Une politique de confiance spécifie l'identité qui peut assumer un rôle. Cette politique est requise pour permettre au service SageMaker Studio d'assumer le rôle d'exécution du domaine. Ajoutez ces deux actions afin qu'elles apparaissent comme suit dans votre politique.

```
{  
  
  "Version": "2012-10-17",  
  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": [  
          "sagemaker.amazonaws.com"  
        ]  
      },  
      "Action": [  
        "sts:AssumeRole",  
        "sts:SetContext"  
      ]  
    }  
  ]  
}
```

Étape 3 : vérifier les autorisations Amazon S3 Access Grant requises pour le rôle d'exécution du domaine

Pour utiliser Amazon S3 Access Grants, vous devez avoir une politique d'autorisation attachée (sous forme de politique intégrée ou de politique gérée par le client) à votre rôle d'exécution de domaine SageMaker Studio contenant les autorisations suivantes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```

Si aucune politique ne contient ces autorisations, suivez les instructions de la section [Ajouter et supprimer des autorisations d'identité IAM](#) dans le Guide de l'Gestion des identités et des accès AWS utilisateur.

Étape 4 : Attribuer des groupes et des utilisateurs au domaine

Attribuez des groupes et des utilisateurs au domaine SageMaker Studio en suivant les étapes décrites dans [Ajouter des groupes et des utilisateurs](#).

Étape 5 : configurer les autorisations d'accès Amazon S3

Pour configurer les subventions d'accès Amazon S3, suivez les étapes décrites dans [Configuration des subventions d'accès Amazon S3 pour une propagation d'identité fiable via IAM Identity Center](#). Suivez les step-by-step instructions pour effectuer les tâches suivantes :

1. Créez une instance Amazon S3 Access Grants.
2. Enregistrez un emplacement dans cette instance.

3. Créez des autorisations pour permettre à des utilisateurs ou à des groupes spécifiques de l'IAM Identity Center d'accéder à des emplacements ou à des sous-ensembles Amazon S3 désignés (par exemple, des préfixes spécifiques) au sein de ces sites.

Étape 6 : Soumettre un projet de SageMaker formation et consulter les détails de la session d'arrière-plan de l'utilisateur

Dans SageMaker Studio, lancez un nouveau bloc-notes Jupyter et soumettez une tâche de formation. Pendant l'exécution de la tâche, effectuez les étapes suivantes pour afficher les informations de session et vérifier que le contexte de session d'arrière-plan de l'utilisateur est actif.

1. Ouvrez la console IAM Identity Center.
2. Choisissez Utilisateurs.
3. Sur la page Utilisateurs, choisissez le nom d'utilisateur de l'utilisateur dont vous souhaitez gérer les sessions. Cela vous amène à une page contenant les informations de l'utilisateur.
4. Sur la page de l'utilisateur, choisissez l'onglet Sessions actives. Le nombre entre parenthèses à côté de Sessions actives indique le nombre de sessions actives pour cet utilisateur.
5. Pour rechercher des sessions par le nom de ressource Amazon (ARN) de la tâche qui utilise la session, dans la liste des types de session, choisissez Sessions d'arrière-plan utilisateur, puis entrez l'ARN de la tâche dans le champ de recherche.

Voici un exemple de la façon dont une tâche de formation utilisant une session d'arrière-plan utilisateur apparaît dans l'onglet Sessions actives d'un utilisateur.

Active sessions (5) End sessions

You can end any of the active sessions in this list. The list shows all active sessions initiated by wei_zhang [Learn more](#)

Find sessions by client or used by Session type: All

☐ Client	☐ Session type	☐ Used by	☐ IP address
☐ -	User background se...	arn:aws:sagemaker:us-west-2:777788889999:training-job/trustedidprop-trjob-12345a6b	-

Étape 7 : Afficher les CloudTrail journaux pour vérifier la propagation fiable de l'identité dans CloudTrail

Lorsque la propagation d'identités fiables est activée, les actions apparaissent dans les journaux d'événements CloudTrail situés sous l'élément `onBehalfOf`. Le `userId` reflète l'ID de l'utilisateur de

l'IAM Identity Center qui a initié la tâche de formation. L' CloudTrail événement suivant capture le processus de propagation d'identités fiables.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAI23456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAI23456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
          },
          "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
          }
        },
        "onBehalfOf": {
          "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
          "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/
d-1234567890"
        }
      },
    },
  },

```

Considérations relatives à l'exécution

Si un administrateur définit `MaxRuntimeInSeconds` des tâches de formation ou de traitement de longue durée inférieures à la durée de la session d'arrière-plan de l'utilisateur, SageMaker Studio exécute le travail pendant la durée minimale de la session d'arrière-plan de l'utilisateur `MaxRuntimeInSeconds` ou pendant la durée minimale de la session d'arrière-plan de l'utilisateur.

Pour plus d'informations `MaxRuntimeInSeconds`, consultez les instructions relatives au `CreateTrainingJob` [StoppingCondition](#) paramètre dans le Amazon SageMaker API Reference.

Services d'autorisation

Dans tous les [cas d'utilisation d'Analytics et de data lakehouse](#), vous pouvez obtenir des contrôles d'accès précis en utilisant :

- AWS Lake Formation - pour obtenir des conseils, voir [Configuration AWS Lake Formation avec IAM Identity Center](#).
- Amazon S3 Access Grants : pour obtenir des conseils, consultez [Configuration des subventions d'accès Amazon S3 avec IAM Identity Center](#).

Configuration AWS Lake Formation avec IAM Identity Center

[AWS Lake Formation](#) est un service géré qui simplifie la création et la gestion de lacs de données sur AWS. Il automatise la collecte, le catalogage et la sécurité des données, en fournissant un référentiel centralisé pour le stockage et l'analyse de différents types de données. Lake Formation propose des contrôles d'accès précis et s'intègre à divers services AWS d'analyse, permettant aux entreprises de configurer, de sécuriser et d'extraire efficacement des informations de leurs lacs de données.

Suivez ces étapes pour permettre à Lake Formation d'accorder des autorisations de données en fonction de l'identité de l'utilisateur à l'aide d'IAM Identity Center et d'une propagation d'identité fiable.

Conditions préalables

Avant de commencer ce didacticiel, vous devez configurer les éléments suivants :

- [Activez IAM Identity Center](#). [L'instance d'organisation](#) est recommandée. Pour de plus amples informations, veuillez consulter [Prérequis et considérations](#).

Étapes pour configurer une propagation d'identité fiable

1. Intégrez IAM Identity Center en AWS Lake Formation suivant les instructions de la section [Connecting Lake Formation with IAM Identity Center](#).

⚠ Important

Si vous ne disposez pas de AWS Glue Data Catalog tables, vous devez les créer afin de les utiliser AWS Lake Formation pour accorder l'accès aux utilisateurs et aux groupes IAM Identity Center. Voir [Création d'objets dans AWS Glue Data Catalog](#) pour plus d'informations.

2. Enregistrez les emplacements des lacs de données.

[Enregistrez les emplacements S3](#) où les données des tables Glue sont stockées. Lake Formation fournira ainsi un accès temporaire aux emplacements S3 requis lorsque les tables sont demandées, éliminant ainsi le besoin d'inclure des autorisations S3 dans le rôle de service (par exemple, le rôle de service Athena configuré sur le). WorkGroup

- Accédez aux emplacements des lacs de données dans la section Administration du volet de navigation de la AWS Lake Formation console. Sélectionnez Enregistrer l'emplacement.

Cela permettra à Lake Formation de fournir des informations d'identification IAM temporaires avec les autorisations nécessaires pour accéder aux emplacements de données S3.

The screenshot shows the 'Register location' page in the AWS Lake Formation console. The page is titled 'Register location' and has a breadcrumb trail: 'AWS Lake Formation > Data lake locations > Register location'. The main content area is divided into several sections:

- Amazon S3 location**: A section with the heading 'Register an Amazon S3 path as the storage location for your data lake.' Below this is the 'Amazon S3 path' section, which includes a text input field containing 's3://awsids-aibi-sandbox-storage' and a 'Browse' button.
- Review location permissions - strongly recommended**: A section with the text 'Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.' Below this is a 'Review location permissions' button.
- IAM role**: A section with the text 'To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.' Below this is a dropdown menu showing 'LakeFormationDataLocationRole'.
- Enable Data Catalog Federation**: A checkbox labeled 'Enable Data Catalog Federation' with the text 'Checking this box will allow Lake Formation to assume a role to access tables in a federated database.' It is currently unchecked.
- Permission mode**: A section with the text 'Select the permission mode you want to use to manage access.' Below this are two radio button options: 'Hybrid access mode' (selected) and 'Lake Formation'. The 'Hybrid access mode' option is highlighted with a blue border and includes a 'Learn more' link. The 'Lake Formation' option is labeled 'Only Lake Formation permissions are enforced.'

At the bottom right of the page, there are two buttons: 'Cancel' and 'Register location'.

- Entrez le chemin S3 des emplacements de données des AWS Glue tables dans le champ Amazon S3 path.
- Dans la section Rôle IAM, ne sélectionnez pas le rôle lié au service si vous souhaitez l'utiliser dans le cadre d'une propagation d'identité sécurisée. Créez un rôle distinct avec les autorisations suivantes.

Pour utiliser ces politiques, remplacez celles de *italicized placeholder text* l'exemple de politique par vos propres informations. Pour obtenir des instructions supplémentaires, voir [Créer une politique](#) ou [Modifier une politique](#). La politique d'autorisation doit accorder l'accès à l'emplacement S3 spécifié dans le chemin :

i. Politique d'autorisation :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessServiceRolePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
    }
  ]
}
```

```

        "Resource": [
            "arn:aws:s3:::*"
        ]
    }
]
}

```

- ii. Relation de confiance : Cela devrait inclure `sts:SetContext` ce qui est nécessaire pour la propagation d'une identité fiable.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

 Note

Le rôle IAM créé par l'assistant est un rôle lié à un service et n'inclut pas. `sts:SetContext`

- d. Après avoir créé le rôle IAM, sélectionnez Enregistrer l'emplacement.

Propagation d'identité fiable grâce à Lake Formation Comptes AWS

AWS Lake Formation prend en charge l'utilisation de [AWS Resource Access Manager \(RAM\)](#) pour partager des tables entre elles Comptes AWS et fonctionne avec une propagation d'identité

fiable lorsque le compte du donateur et le compte du bénéficiaire se trouvent dans la même AWS Organizations instance organisationnelle d'IAM Identity Center. Région AWS Voir [Partage de données entre comptes dans Lake Formation](#) pour plus d'informations.

Configuration des subventions d'accès Amazon S3 avec IAM Identity Center

[Amazon S3 Access Grants](#) offre la flexibilité nécessaire pour accorder un contrôle d'accès précis basé sur l'identité aux sites S3. Vous pouvez utiliser Amazon S3 Access Grants pour accorder l'accès au compartiment Amazon S3 directement aux utilisateurs et aux groupes de votre entreprise. Suivez ces étapes pour activer S3 Access Grants avec IAM Identity Center et obtenir une propagation d'identité fiable.

Conditions préalables

Avant de commencer ce didacticiel, vous devez configurer les éléments suivants :

- [Activez IAM Identity Center](#). [L'instance d'organisation](#) est recommandée. Pour de plus amples informations, veuillez consulter [Prérequis et considérations](#).

Configuration des autorisations d'accès S3 pour une propagation d'identité fiable via IAM Identity Center

Si vous possédez déjà une Access Grants instance Amazon S3 avec un emplacement enregistré, procédez comme suit :

1. [Associez votre instance IAM Identity Center](#).
2. [Créez une subvention](#).

Si vous n'avez pas Access Grants encore créé d'Amazon S3, procédez comme suit :

1. [Création d'une Access Grants instance S3](#) : vous pouvez créer une Access Grants instance S3 par Région AWS. Lorsque vous créez l'Access Grants instance S3, assurez-vous de cocher la case Ajouter une instance IAM Identity Center et de fournir l'ARN de votre instance IAM Identity Center. Sélectionnez Suivant.

L'image suivante montre la page Créer une Access Grants instance S3 dans la Access Grants console Amazon S3 :

Step 1 **Create S3 Access Grants instance** Info

Step 2 Register S3 Buckets or prefixes as locations

Step 3 Create grant

Step 4 Review and finish

Create S3 Access Grants instance Info

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance Info

AWS Region
You can create one S3 Access Grants instance per AWS Region per account.
US East (N. Virginia) us-east-1

☒ **Add IAM Identity Center instance in US East (N. Virginia) us-east-1 - optional**
You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN
You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

Enter IAM Identity Center instance ARN
Format: arn:aws:sso::instance/<instanceidentifier>

Choosing **Next** will create the S3 Access Grants instance and proceed to the next step.

Cancel **Next**

- Enregistrer un emplacement - Après avoir créé et [créé une Access Grants instance Amazon S3](#) Région AWS dans un compte, vous [enregistrez un emplacement S3](#) dans cette instance. Un Access Grants emplacement S3 associe la région S3 par défaut (S3://), un compartiment ou un préfixe à un rôle IAM. S3 Access Grants assume ce rôle Amazon S3 pour vendre des informations d'identification temporaires au bénéficiaire qui accède à cet emplacement particulier. Vous devez d'abord enregistrer au moins un emplacement dans votre Access Grants instance S3 avant de pouvoir créer une autorisation d'accès.

Pour l'étendue de localisations `s3://`, spécifiez, qui inclut tous vos compartiments de cette région. Il s'agit de l'étendue de localisation recommandée pour la plupart des cas d'utilisation. Si vous avez un cas d'utilisation de gestion avancée des accès, vous pouvez définir l'étendue de localisation en fonction d'un compartiment `s3://bucket` ou d'un préfixe spécifique au sein d'un compartiment `s3://bucket/prefix-with-path`. Pour plus d'informations, consultez [Enregistrer un emplacement](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Note

Assurez-vous que les emplacements S3 des AWS Glue tables auxquelles vous souhaitez accorder l'accès sont inclus dans ce chemin.

La procédure vous oblige à configurer un rôle IAM pour l'emplacement. Ce rôle doit inclure les autorisations d'accès à la zone de localisation. Vous pouvez utiliser l'assistant de console S3 pour créer le rôle. Vous devez spécifier l'ARN de votre Access Grants instance S3 dans les

politiques relatives à ce rôle IAM. La valeur par défaut de l'ARN de votre Access Grants instance S3 est `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`.

L'exemple de politique d'autorisation suivant donne à Amazon S3 des autorisations pour le rôle IAM que vous avez créé. Et l'exemple de politique de confiance qui suit permet au principal du Access Grants service S3 d'assumer le rôle IAM.

a. Stratégie d'autorisation

Pour utiliser ces politiques, remplacez celles de *italicized placeholder text* l'exemple de politique par vos propres informations. Pour obtenir des instructions supplémentaires, voir [Créer une politique](#) ou [Modifier une politique](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3::*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
          "s3:AccessGrantsInstanceArn": [
            "arn:aws:s3:::access-grants/instance-id"
          ]
        }
      }
    }
  ],
}
```

```

{
  "Sid": "ObjectLevelWritePermissions",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:AbortMultipartUpload"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "111122223333"
    },
    "ArnEquals": {
      "s3:AccessGrantsInstanceArn": [
        "arn:aws:s3:::access-grants/instance-id"
      ]
    }
  }
},
{
  "Sid": "BucketLevelReadPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "111122223333"
    },
    "ArnEquals": {
      "s3:AccessGrantsInstanceArn": [
        "arn:aws:s3:::access-grants/instance-id"
      ]
    }
  }
}

```

```

    },
    {
      "Sid": "OptionalKMSPermissionsForSSEEncryption",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

b. Politique d'approbation

Dans la politique de confiance du rôle IAM, accordez au service S3 Access Grants (access-grants.s3.amazonaws.com) l'accès au rôle IAM que vous avez créé. Pour ce faire, vous pouvez créer un fichier JSON contenant les instructions suivantes. Pour ajouter la politique d'approbation à votre compte, consultez [Création d'un rôle à l'aide de politiques d'approbation personnalisées](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-  
ARN"
        }
      }
    }
  ]
}

```

```

    },
    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Action": "sts:SetContext",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders":
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
        }
      }
    }
  ]
}

```

Création d'une subvention d'accès Amazon S3

Si vous possédez une Access Grants instance Amazon S3 avec un emplacement enregistré et que vous y avez associé votre instance IAM Identity Center, vous pouvez [créer une subvention](#). Sur la page Create Grant de la console S3, procédez comme suit :

Créer un octroi

1. Sélectionnez l'emplacement créé à l'étape précédente. Vous pouvez réduire la portée de la subvention en ajoutant un sous-préfixe. Le sous-préfixe peut être un bucket/prefix, ou un objet du compartiment. Pour plus d'informations, consultez la section [Sous-préfixe](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.
2. Sous Autorisations et accès, sélectionnez Lire et/ou Écrire en fonction de vos besoins.
3. Dans Type Granter, choisissez Directory Identity form IAM Identity Center.
4. Indiquez l'ID d'utilisateur ou de groupe IAM Identity Center. Vous trouverez l'utilisateur et le groupe IDs dans les [sections Utilisateur et Groupe](#) de la console IAM Identity Center. Sélectionnez Suivant.

- Sur la page Révision et finition, passez en revue les paramètres du S3, Access Grant puis sélectionnez Create Grant.

L'image suivante montre la page Create Grant dans la Access Grants console Amazon S3 :

The screenshot shows the 'Create Grant' page in the AWS S3 console. The page is titled 'Create Grant' and includes an 'Info' link. It contains several sections:

- Grant**: A brief description of the grant.
- Grant scope**: A description of the grant scope and a note about the default location.
- Location**: A text input field containing 's3://', with a 'Browse locations' button and a 'Register location' button.
- Location ID**: A text input field.
- IAM role**: A link to 's3accessgrants_role_for_awsids-aii-sandbox-storage'.
- Subprefix - optional**: A text input field containing 'bucket-name/prefix/*'.
- Grant scope**: A text input field containing 's3://', with a checkbox 'The grant scope is an object'.
- Permissions and access**: A warning box stating 'The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.'
- Permissions**: Two checkboxes, 'Read' and 'Write', both of which are checked.
- Grantee type**: Two radio buttons, 'Directory identity from IAM Identity Center' (selected) and 'IAM principal'.
- Directory identity type**: Two radio buttons, 'User' and 'Group' (selected).
- IAM Identity Center group ID**: A text input field containing 'Enter group ID'.

Configuration de votre propre application OAuth 2.0

La propagation fiable des identités permet à une application gérée par le client de demander l'accès aux données AWS des services au nom d'un utilisateur. La gestion de l'accès aux données est basée sur l'identité de l'utilisateur, de sorte que les administrateurs peuvent accorder l'accès en fonction de l'appartenance des utilisateurs et des groupes aux utilisateurs existants. L'identité de l'utilisateur, les actions effectuées en son nom et les autres événements sont enregistrés dans des journaux et CloudTrail des événements spécifiques au service.

Grâce à la propagation sécurisée des identités, un utilisateur peut se connecter à une application gérée par le client, et cette application peut transmettre l'identité de l'utilisateur dans les demandes d'accès aux données Services AWS.

Important

Pour accéder à un Service AWS, les applications gérées par le client doivent obtenir un jeton auprès d'un émetteur de jetons fiable, externe à IAM Identity Center. Un émetteur de jetons

de confiance est un serveur d'autorisation OAuth 2.0 qui crée des jetons signés. Ces jetons autorisent les applications qui lancent des demandes d'accès à Services AWS (réception d'applications). Pour de plus amples informations, veuillez consulter [Utilisation d'applications dotées d'un émetteur de jetons fiable](#).

Rubriques

- [Configurez des applications OAuth 2.0 gérées par le client pour une propagation fiable des identités](#)
- [Spécifier les applications fiables](#)
- [Utilisation d'applications dotées d'un émetteur de jetons fiable](#)

Configurez des applications OAuth 2.0 gérées par le client pour une propagation fiable des identités

Pour configurer une application OAuth 2.0 gérée par le client pour une propagation d'identité fiable, vous devez d'abord l'ajouter à IAM Identity Center. Utilisez la procédure suivante pour ajouter votre application à IAM Identity Center.

Rubriques

- [Étape 1 : Sélectionnez le type de demande](#)
- [Étape 2 : Spécifier les détails de l'application](#)
- [Étape 3 : Spécifier les paramètres d'authentification](#)
- [Étape 4 : Spécifier les informations d'identification de l'application](#)
- [Étape 5 : révision et configuration](#)

Étape 1 : Sélectionnez le type de demande

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Choisissez l'onglet Gérée par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférence de configuration, choisissez J'ai une application que je souhaite configurer.

6. Sous Type d'application, choisissez OAuth 2.0.
7. Choisissez Next pour passer à la page suivante, [Étape 2 : Spécifier les détails de l'application](#).

Étape 2 : Spécifier les détails de l'application

1. Sur la page Spécifier les détails de l'application, sous Nom et description de l'application, entrez un nom d'affichage pour l'application, tel que **MyApp**. Entrez ensuite une description.
2. Sous Méthode d'attribution des utilisateurs et des groupes, choisissez l'une des options suivantes :

- Exiger des attributions : autorisez uniquement les utilisateurs et les groupes IAM Identity Center affectés à cette application à accéder à l'application.

Visibilité de la vignette de l'application : seuls les utilisateurs affectés à l'application directement ou par le biais d'une attribution de groupe peuvent voir la vignette de l'application dans le portail AWS d'accès, à condition que la visibilité de l'application dans le portail AWS d'accès soit définie sur Visible.

- Pas besoin d'assignments : autorisez tous les utilisateurs et groupes autorisés d'IAM Identity Center à accéder à cette application.

Visibilité de la vignette de l'application : la vignette de l'application est visible par tous les utilisateurs qui se connectent au portail AWS d'accès, sauf si la visibilité de l'application dans le portail d' AWS accès est définie sur Non visible.

3. Sous portail AWS d'accès, entrez l'URL à laquelle les utilisateurs peuvent accéder à l'application et spécifiez si la vignette de l'application sera visible ou non dans le portail AWS d'accès. Si vous choisissez Non visible, même les utilisateurs assignés ne peuvent pas voir la vignette de l'application.
4. Sous Balises (facultatif), choisissez Ajouter une nouvelle balise, puis spécifiez les valeurs de clé et de valeur (facultatif).

Pour plus d'informations sur les balises, consultez [Ressources de balisage AWS IAM Identity Center](#).

5. Choisissez Next, puis passez à la page suivante [Étape 3 : Spécifier les paramètres d'authentification](#).

Étape 3 : Spécifier les paramètres d'authentification

Pour ajouter une application gérée par le client compatible avec la OAuth version 2.0 à IAM Identity Center, vous devez spécifier un émetteur de jetons fiable. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui crée des jetons signés. Ces jetons autorisent les applications qui lancent des demandes (demandes d'applications) pour accéder aux applications gérées par AWS (réception d'applications).

1. Sur la page Spécifier les paramètres d'authentification, sous Émetteurs de jetons fiables, effectuez l'une des opérations suivantes :

- Pour utiliser un émetteur de jetons de confiance existant :

Cochez la case à côté du nom de l'émetteur de jetons de confiance que vous souhaitez utiliser.

- Pour ajouter un nouvel émetteur de jetons de confiance :

1. Choisissez Créer un émetteur de jetons approuvés.
2. Un nouvel onglet de navigateur s'ouvre. Suivez les étapes 5 à 8 dans [Comment ajouter un émetteur de jetons fiable à la console IAM Identity Center](#).
3. Après avoir effectué ces étapes, retournez dans la fenêtre du navigateur que vous utilisez pour configurer votre application et sélectionnez l'émetteur de jetons de confiance que vous venez d'ajouter.
4. Dans la liste des émetteurs de jetons de confiance, cochez la case à côté du nom de l'émetteur de jetons de confiance que vous venez d'ajouter.

Après avoir sélectionné un émetteur de jetons de confiance, la section Configurer les émetteurs de jetons de confiance sélectionnés apparaît.

2. Sous Configurer les émetteurs de jetons fiables sélectionnés, entrez la réclamation Aud. La réclamation Aud identifie le public cible (destinataires) du jeton généré par l'émetteur du jeton de confiance. Pour de plus amples informations, veuillez consulter [Réclamation d'aide](#).
3. Pour éviter que vos utilisateurs n'aient à s'authentifier à nouveau lorsqu'ils utilisent cette application, sélectionnez Activer l'octroi de jetons d'actualisation. Lorsqu'elle est sélectionnée, cette option actualise le jeton d'accès à la session toutes les 60 minutes, jusqu'à ce que la session expire ou que l'utilisateur y mette fin.
4. Choisissez Next, puis passez à la page suivante [Étape 4 : Spécifier les informations d'identification de l'application](#).

Étape 4 : Spécifier les informations d'identification de l'application

Suivez les étapes de cette procédure pour spécifier les informations d'identification que votre application utilise pour effectuer des actions d'échange de jetons avec des applications fiables. Ces informations d'identification sont utilisées dans une politique basée sur les ressources. La politique exige que vous spécifiez un principal autorisé à effectuer les actions spécifiées dans la stratégie. Vous devez spécifier un principal, même si les applications fiables se trouvent dans les mêmes applications Compte AWS.

Note

Lorsque vous définissez des autorisations à l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège.

Cette politique nécessite l'action de [CreateTokenWithIAM](#) l'API. Pour plus d'informations sur cette politique et un exemple que vous pouvez adapter en fonction des besoins de votre environnement, consultez [Exemple de politique basée sur les ressources pour IAM Identity Center IAM Identity Center](#).

1. Sur la page Spécifier les informations d'identification de l'application, effectuez l'une des opérations suivantes :
 - Pour définir rapidement un ou plusieurs rôles IAM :
 1. Choisissez Entrez un ou plusieurs rôles IAM.
 2. Sous Enter IAM roles, spécifiez le Amazon Resource Name (ARN) d'un rôle IAM existant. Pour spécifier l'ARN, utilisez la syntaxe suivante. La partie de la région de l'ARN est vide, car les ressources IAM sont globales.

```
arn:aws:iam::account:role/role-name-with-path
```

Pour plus d'informations, consultez la section [Accès entre comptes à l'aide de politiques basées sur les ressources](#) et [IAM ARNs](#) dans le guide de l'utilisateur. Gestion des identités et des accès AWS

- Pour modifier manuellement la politique (obligatoire si vous spécifiez des informations autres que les informations AWS d'identification) :
 1. Sélectionnez Modifier la politique de l'application.
 2. Modifiez votre politique en tapant ou en collant du texte dans la zone de texte JSON.
 3. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés lors de la validation des politiques. Pour plus d'informations, consultez la section [Validation des politiques IAM](#) dans le guide de l'Gestion des identités et des accès AWS utilisateur.
- 2. Choisissez Next et passez à la page suivante, [Étape 5 : révision et configuration](#).

Étape 5 : révision et configuration

1. Sur la page Révision et configuration, passez en revue les choix que vous avez faits. Pour apporter des modifications, choisissez la section de configuration souhaitée, choisissez Modifier, puis apportez les modifications requises.
2. Lorsque vous avez terminé, choisissez Ajouter une application.
3. L'application que vous avez ajoutée apparaît dans la liste des applications gérées par le client.
4. Après avoir configuré votre application gérée par le client dans IAM Identity Center, vous devez spécifier une ou plusieurs applications Services AWS, ou applications fiables, pour la propagation des identités. Cela permet aux utilisateurs de se connecter à votre application gérée par le client et d'accéder aux données de l'application sécurisée.

Pour de plus amples informations, veuillez consulter [Spécifier les applications fiables](#).

Spécifier les applications fiables

Après avoir [configuré votre application gérée par le client](#), vous devez spécifier un ou plusieurs AWS services fiables, ou applications fiables, pour la propagation des identités. Spécifiez un AWS service contenant des données auxquelles les utilisateurs de vos applications gérées par le client doivent accéder. Lorsque vos utilisateurs se connectent à votre application gérée par le client, cette application transmet l'identité de vos utilisateurs à l'application sécurisée.

Utilisez la procédure suivante pour sélectionner un service, puis spécifiez les applications individuelles à approuver pour ce service.

1. Ouvrez la [console IAM Identity Center](#).

2. Choisissez Applications.
3. Choisissez l'onglet Gérée par le client.
4. Dans la liste des applications gérées par le client, sélectionnez l'application OAuth 2.0 pour laquelle vous souhaitez lancer des demandes d'accès. Il s'agit de l'application à laquelle vos utilisateurs se connectent.
5. Sur la page Détails, sous Applications approuvées pour la propagation d'identité, choisissez Spécifier les applications approuvées.
6. Sous Type d'installation, sélectionnez Applications individuelles et spécifiez l'accès, puis choisissez Suivant.
7. Sur la page Sélectionner un service, choisissez le AWS service qui possède des applications auxquelles votre application gérée par le client peut faire confiance pour la propagation des identités, puis choisissez Next.

Le service que vous sélectionnez définit les applications fiables. Vous allez sélectionner les applications à l'étape suivante.

8. Sur la page Sélectionner des applications, choisissez Applications individuelles, cochez la case correspondant à chaque application pouvant recevoir des demandes d'accès, puis choisissez Suivant.
9. Sur la page Configurer l'accès, sous Méthode de configuration, effectuez l'une des opérations suivantes :
 - Sélectionnez l'accès pour chaque application : sélectionnez cette option pour configurer différents niveaux d'accès pour chaque application. Choisissez l'application pour laquelle vous souhaitez configurer le niveau d'accès, puis choisissez Modifier l'accès. Dans Niveau d'accès à appliquer, modifiez les niveaux d'accès selon vos besoins, puis sélectionnez Enregistrer les modifications.
 - Appliquer le même niveau d'accès à toutes les applications : sélectionnez cette option si vous n'avez pas besoin de configurer les niveaux d'accès pour chaque application.
10. Choisissez Suivant.
11. Sur la page Vérifier la configuration, passez en revue les choix que vous avez effectués. Pour apporter des modifications, choisissez la section de configuration souhaitée, choisissez Modifier l'accès, puis apportez les modifications requises.
12. Lorsque vous avez terminé, choisissez Trust applications.

Utilisation d'applications dotées d'un émetteur de jetons fiable

Les émetteurs de jetons fiables vous permettent d'utiliser la propagation d'identité fiable avec des applications qui s'authentifient en dehors de. AWS Avec des émetteurs de jetons fiables, vous pouvez autoriser ces applications à faire des demandes d'accès aux applications AWS gérées au nom de leurs utilisateurs.

Les rubriques suivantes décrivent le fonctionnement des émetteurs de jetons fiables et fournissent des conseils de configuration.

Rubriques

- [Vue d'ensemble des émetteurs de jetons fiables](#)
- [Conditions préalables et considérations pour les émetteurs de jetons fiables](#)
- [Détails de la réclamation de JTI](#)
- [Paramètres de configuration des émetteurs de jetons fiables](#)
- [Configuration d'un émetteur de jetons de confiance](#)
- [Sessions de rôles IAM améliorées](#)

Vue d'ensemble des émetteurs de jetons fiables

La propagation d'identités fiables fournit un mécanisme qui permet aux applications qui s'authentifient AWS à l'extérieur de faire des demandes au nom de leurs utilisateurs en utilisant un émetteur de jetons fiable. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui crée des jetons signés. Ces jetons autorisent les applications qui lancent des demandes (demandes d'applications) pour accéder à Services AWS (recevoir des applications). Les applications demandeuses lancent des demandes d'accès au nom des utilisateurs authentifiés par l'émetteur de jetons de confiance. Les utilisateurs sont connus à la fois de l'émetteur du jeton sécurisé et de l'IAM Identity Center.

Services AWS qui reçoivent des demandes gèrent l'autorisation précise de leurs ressources en fonction de leurs utilisateurs et de leur appartenance à un groupe, comme indiqué dans le répertoire Identity Center. Services AWS ne peut pas utiliser directement les jetons provenant de l'émetteur de jetons externe.

Pour résoudre ce problème, IAM Identity Center fournit à l'application demandeuse, ou à un AWS pilote utilisé par l'application demandeuse, un moyen d'échanger le jeton émis par l'émetteur du jeton approuvé contre un jeton généré par IAM Identity Center. Le jeton généré par IAM Identity Center

fait référence à l'utilisateur IAM Identity Center correspondant. L'application demandeuse, ou le pilote, utilise le nouveau jeton pour lancer une demande à l'application réceptrice. Étant donné que le nouveau jeton fait référence à l'utilisateur correspondant dans IAM Identity Center, l'application réceptrice peut autoriser l'accès demandé en fonction de l'utilisateur ou de son appartenance à un groupe tel que représenté dans IAM Identity Center.

Important

Le choix d'un serveur d'autorisation OAuth 2.0 à ajouter en tant qu'émetteur de jetons de confiance est une décision de sécurité qui nécessite un examen attentif. Choisissez uniquement des émetteurs de jetons fiables en qui vous avez confiance pour effectuer les tâches suivantes :

- Authentifiez l'utilisateur indiqué dans le jeton.
- Autorisez l'accès de cet utilisateur à l'application réceptrice.
- Générez un jeton qu'IAM Identity Center peut échanger contre un jeton créé par IAM Identity Center.

Conditions préalables et considérations pour les émetteurs de jetons fiables

Avant de configurer un émetteur de jetons fiable, passez en revue les conditions préalables et les considérations suivantes.

- Configuration d'un émetteur de jetons fiable

Vous devez configurer un serveur d'autorisation OAuth 2.0 (l'émetteur de jetons de confiance). Bien que l'émetteur de jetons de confiance soit généralement le fournisseur d'identité que vous utilisez comme source d'identité pour IAM Identity Center, il n'est pas nécessaire que ce soit le cas. Pour plus d'informations sur la configuration de l'émetteur de jetons de confiance, consultez la documentation du fournisseur d'identité concerné.

Note

Vous pouvez configurer jusqu'à 10 émetteurs de jetons fiables à utiliser avec IAM Identity Center, à condition de mapper l'identité de chaque utilisateur de l'émetteur de jetons de confiance à un utilisateur correspondant dans IAM Identity Center.

- Le serveur d'autorisation OAuth 2.0 (l'émetteur de jetons de confiance) qui crée le jeton doit disposer d'un point de terminaison de découverte [OpenID Connect \(OIDC\)](#) que IAM Identity Center peut utiliser pour obtenir des clés publiques afin de vérifier les signatures des jetons. Pour de plus amples informations, veuillez consulter [URL du point de terminaison de découverte OIDC \(URL de l'émetteur\)](#).
- Tokens émis par l'émetteur de jetons de confiance

Les jetons émis par l'émetteur de jetons de confiance doivent répondre aux exigences suivantes :

- Le jeton doit être signé et au format [JSON Web Token \(JWT\)](#) à l'aide de l' RS256algorithme.
- Le jeton doit contenir les allégations suivantes :
 - [Émetteur](#) (iss) — Entité qui a émis le jeton. Cette valeur doit correspondre à la valeur configurée dans le point de terminaison de découverte OIDC (URL de l'émetteur) dans l'émetteur de jetons de confiance.
 - [Sujet](#) (sous) — L'utilisateur authentifié.
 - [Audience](#) (aud) — Destinataire prévu du jeton. Il s'agit de Service AWS celui qui sera accessible une fois le jeton échangé contre un jeton auprès d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Réclamation d'aide](#).
 - [Délai d'expiration](#) (exp) : délai après lequel le jeton expire.
- Le jeton peut être un jeton d'identité ou un jeton d'accès.
- Le jeton doit avoir un attribut qui peut être mappé de manière unique à un utilisateur du IAM Identity Center.

 Note

L'utilisation d'une clé de signature personnalisée pour JWTs from n'Microsoft Entra IDest pas prise en charge. Pour utiliser des jetons provenant Microsoft Entra ID d'un émetteur de jetons fiable, vous ne pouvez pas utiliser de clé de signature personnalisée.

- Réclamations facultatives

IAM Identity Center prend en charge toutes les revendications facultatives définies dans la RFC 7523. Pour plus d'informations, consultez [la section 3 : Format JWT et exigences de traitement](#) de cette RFC.

Par exemple, le jeton peut contenir une réclamation [JTI \(JWT ID\)](#). Cette réclamation, lorsqu'elle est présente, empêche les jetons portant le même JTI d'être réutilisés pour des échanges de jetons. Pour plus d'informations sur les réclamations de la JTI, consultez [Détails de la réclamation de JTI](#).

- Configuration du centre d'identité IAM pour fonctionner avec un émetteur de jetons fiable

Vous devez également activer IAM Identity Center, configurer la source d'identité pour IAM Identity Center et configurer les utilisateurs correspondant aux utilisateurs figurant dans le répertoire de l'émetteur de jetons de confiance.

Pour ce faire, vous devez effectuer l'une des opérations suivantes :

- Synchronisez les utilisateurs dans IAM Identity Center à l'aide du protocole SCIM (System for Cross-Domain Identity Management) 2.0.
- Créez les utilisateurs directement dans IAM Identity Center.

Détails de la réclamation de JTI

Si IAM Identity Center reçoit une demande d'échange d'un jeton qu'IAM Identity Center a déjà échangé, la demande échoue. Pour détecter et empêcher la réutilisation d'un jeton pour des échanges de jetons, vous pouvez inclure une réclamation JTI. IAM Identity Center protège contre la réédition de jetons en fonction des revendications contenues dans le jeton.

Les serveurs d'autorisation OAuth 2.0 n'ajoutent pas tous une réclamation JTI aux jetons. Certains serveurs d'autorisation OAuth 2.0 peuvent ne pas vous autoriser à ajouter une JTI en tant que réclamation personnalisée. OAuth Les serveurs d'autorisation 2.0 qui prennent en charge l'utilisation d'une réclamation JTI peuvent ajouter cette réclamation uniquement aux jetons d'identité, aux jetons d'accès uniquement, ou aux deux. Pour plus d'informations, consultez la documentation de votre serveur d'autorisation OAuth 2.0.

Pour plus d'informations sur la création d'applications qui échangent des jetons, consultez la documentation de l'API IAM Identity Center. Pour plus d'informations sur la configuration d'une application gérée par le client afin d'obtenir et d'échanger les jetons appropriés, consultez la documentation de l'application.

Paramètres de configuration des émetteurs de jetons fiables

Les sections suivantes décrivent les paramètres requis pour configurer et utiliser un émetteur de jetons fiable.

Rubriques

- [URL du point de terminaison de découverte OIDC \(URL de l'émetteur\)](#)
- [Mappage d'attribut](#)
- [Réclamation d'aide](#)

URL du point de terminaison de découverte OIDC (URL de l'émetteur)

Lorsque vous ajoutez un émetteur de jetons fiable à la console IAM Identity Center, vous devez spécifier l'URL du point de terminaison de découverte OIDC. Cette URL est généralement désignée par son URL relative, `/.well-known/openid-configuration`. Dans la console IAM Identity Center, cette URL est appelée URL de l'émetteur.

Note

Vous devez coller l'URL du point de terminaison de découverte jusqu'au bout et sans `.well-known/openid-configuration`. Si elle `.well-known/openid-configuration` est incluse dans l'URL, la configuration de l'émetteur de jetons de confiance ne fonctionnera pas. Comme IAM Identity Center ne valide pas cette URL, si celle-ci n'est pas correctement formée, la configuration de l'émetteur de jetons de confiance échouera sans notification. L'URL du point de terminaison de découverte OIDC doit être accessible uniquement via les ports 80 et 443.

IAM Identity Center utilise cette URL pour obtenir des informations supplémentaires sur l'émetteur du jeton de confiance. Par exemple, IAM Identity Center utilise cette URL pour obtenir les informations requises pour vérifier les jetons générés par l'émetteur de jetons de confiance. Lorsque vous ajoutez un émetteur de jetons de confiance à IAM Identity Center, vous devez spécifier cette URL. Pour trouver l'URL, consultez la documentation du fournisseur de serveur d'autorisation OAuth 2.0 que vous utilisez pour générer des jetons pour votre application, ou contactez directement le fournisseur pour obtenir de l'aide.

Mappage d'attribut

Les mappages d'attributs permettent à IAM Identity Center de faire correspondre l'utilisateur représenté dans un jeton émis par un émetteur de jeton fiable à un seul utilisateur dans IAM Identity Center. Vous devez spécifier le mappage des attributs lorsque vous ajoutez l'émetteur de jetons de confiance à IAM Identity Center. Ce mappage d'attributs est utilisé dans une réclamation dans

le jeton généré par l'émetteur du jeton fiable. La valeur de la réclamation est utilisée pour effectuer une recherche dans IAM Identity Center. La recherche utilise l'attribut spécifié pour récupérer un seul utilisateur dans IAM Identity Center, qui sera utilisé comme utilisateur dans AWS le centre. La réclamation que vous choisissez doit être mappée à un attribut dans une liste fixe d'attributs disponibles dans la banque d'identités IAM Identity Center. Vous pouvez choisir l'un des attributs de la banque d'identités IAM Identity Center suivants : nom d'utilisateur, e-mail et identifiant externe. La valeur de l'attribut que vous spécifiez dans IAM Identity Center doit être unique pour chaque utilisateur.

Réclamation d'aide

Une réclamation AUD identifie le public (destinataires) auquel un jeton est destiné. Lorsque l'application demandant l'accès s'authentifie par le biais d'un fournisseur d'identité qui n'est pas fédéré à IAM Identity Center, ce fournisseur d'identité doit être configuré en tant qu'émetteur de jetons de confiance. L'application qui reçoit la demande d'accès (l'application réceptrice) doit échanger le jeton généré par l'émetteur du jeton approuvé contre un jeton généré par IAM Identity Center.

Pour plus d'informations sur la façon d'obtenir les valeurs de réclamation en dollars australiens pour l'application réceptrice telles qu'elles sont enregistrées auprès de l'émetteur de jetons de confiance, consultez la documentation de votre émetteur de jetons de confiance ou contactez l'administrateur de l'émetteur de jetons de confiance pour obtenir de l'aide.

Configuration d'un émetteur de jetons de confiance

Pour permettre la propagation d'identités fiables pour une application qui s'authentifie en externe auprès d'IAM Identity Center, un ou plusieurs administrateurs doivent configurer un émetteur de jetons fiable. Un émetteur de jetons de confiance est un serveur d'autorisation OAuth 2.0 qui émet des jetons aux applications qui initient des demandes (demandes d'applications). Les jetons autorisent ces applications à initier des demandes au nom de leurs utilisateurs à une application réceptrice (une Service AWS).

Rubriques

- [Coordination des rôles et responsabilités administratifs](#)
- [Tâches de configuration d'un émetteur de jetons de confiance](#)
- [Comment ajouter un émetteur de jetons fiable à la console IAM Identity Center](#)
- [Comment afficher ou modifier les paramètres de l'émetteur de jetons de confiance dans la console IAM Identity Center](#)

- [Processus de configuration et flux de demandes pour les applications utilisant un émetteur de jetons fiable](#)

Coordination des rôles et responsabilités administratifs

Dans certains cas, un seul administrateur peut effectuer toutes les tâches nécessaires à la configuration d'un émetteur de jetons de confiance. Si plusieurs administrateurs exécutent ces tâches, une étroite coordination est requise. Le tableau suivant décrit comment plusieurs administrateurs peuvent se coordonner pour configurer un émetteur de jetons fiable et configurer le AWS service pour l'utiliser.

Note

L'application peut être n'importe quel AWS service intégré à IAM Identity Center et prenant en charge la propagation fiable des identités.

Pour de plus amples informations, veuillez consulter [Tâches de configuration d'un émetteur de jetons de confiance](#).

Role	Effectue ces tâches	Se coordonne avec
Administrateur du centre d'identité IAM	Ajoute l'IdP externe en tant qu'émetteur de jetons de confiance à la console IAM Identity Center. Permet de configurer le mappage d'attributs correct entre IAM Identity Center et l'IdP externe. Informe l'administrateur du AWS service lorsque l'émetteur du jeton sécurisé est ajouté à la console IAM Identity Center.	Administrateur d'un IdP externe (émetteur de jetons de confiance) AWS administrateur de service
Administrateur d'un IdP externe (émetteur)	Configure l'IdP externe pour émettre des jetons.	Administrateur du centre d'identité IAM

Role	Effectue ces tâches	Se coordonne avec
de jetons de confiance)	Permet de configurer le mappage d'attributs correct entre IAM Identity Center et l'IdP externe. Fournit le nom du public (réclamation Aud) à l'administrateur du AWS service.	AWS administrateur de service
AWS administrateur de service	Vérifie la présence de l'émetteur de jetons de confiance dans la console de AWS service. L'émetteur du jeton sécurisé sera visible dans la console de AWS service une fois que l'administrateur d'IAM Identity Center l'aura ajouté à la console IAM Identity Center. Configure le AWS service pour qu'il utilise l'émetteur de jetons de confiance.	Administrateur du centre d'identité IAM Administrateur d'un IdP externe (émetteur de jetons de confiance)

Tâches de configuration d'un émetteur de jetons de confiance

Pour configurer un émetteur de jetons fiable, un administrateur du centre d'identité IAM, un administrateur d'IdP externe (émetteur de jetons de confiance) et un administrateur de l'application doivent effectuer les tâches suivantes.

Note

L'application peut être n'importe quel AWS service intégré à IAM Identity Center et prenant en charge la propagation fiable des identités.

1. Ajouter l'émetteur de jeton fiable à IAM Identity Center : l'administrateur du centre d'identité IAM [ajoute l'émetteur de jeton fiable à l'aide de la console IAM](#) Identity Center ou. [APIs](#) Cette configuration nécessite de spécifier les éléments suivants :

- Nom de l'émetteur de jetons de confiance.
 - URL du point de terminaison de découverte OIDC (dans la console IAM Identity Center, cette URL est appelée URL de l'émetteur). Le point de terminaison de découverte doit être accessible via les ports 80 et 443 uniquement.
 - Mappage d'attributs pour la recherche par l'utilisateur. Ce mappage d'attributs est utilisé dans une réclamation dans le jeton généré par l'émetteur du jeton fiable. La valeur de la réclamation est utilisée pour effectuer une recherche dans IAM Identity Center. La recherche utilise l'attribut spécifié pour récupérer un seul utilisateur dans IAM Identity Center.
2. Connecter le AWS service à IAM Identity Center : l'administrateur du AWS service doit connecter l'application à IAM Identity Center à l'aide de la console de l'application ou de l'application. APIs

Une fois que l'émetteur du jeton sécurisé est ajouté à la console IAM Identity Center, il est également visible dans la console de AWS service et peut être sélectionné par l'administrateur du AWS service.

3. Configurer l'utilisation de l'échange de jetons : dans la console de AWS service, l'administrateur du AWS service configure le AWS service pour accepter les jetons émis par l'émetteur de jetons de confiance. Ces jetons sont échangés contre des jetons générés par IAM Identity Center. Cela nécessite de spécifier le nom de l'émetteur de jetons de confiance indiqué à l'étape 1 et la valeur de réclamation Aud correspondant au AWS service.

L'émetteur de jetons de confiance place la valeur de réclamation Aud dans le jeton qu'il émet pour indiquer que le jeton est destiné à être utilisé par le AWS service. Pour obtenir cette valeur, contactez l'administrateur de l'émetteur du jeton de confiance.

Comment ajouter un émetteur de jetons fiable à la console IAM Identity Center

Dans une organisation qui compte plusieurs administrateurs, cette tâche est exécutée par un administrateur du IAM Identity Center. Si vous êtes l'administrateur de l'IAM Identity Center, vous devez choisir l'IdP externe à utiliser comme émetteur de jetons de confiance.

Pour ajouter un émetteur de jetons fiable à la console IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Émetteurs de jetons fiables, choisissez Créer un émetteur de jetons de confiance.

5. Sur la page Configurer un IdP externe pour émettre des jetons fiables, sous Détails de l'émetteur de jetons fiables, procédez comme suit :
 - Pour l'URL de l'émetteur, spécifiez l'[URL de découverte OIDC de l'IdP externe](#) qui émettra des jetons pour une propagation d'identité fiable. Vous devez spécifier l'URL du point de terminaison de découverte jusqu'au bout et sans `.well-known/openid-configuration`. L'administrateur de l'IdP externe peut fournir cette URL.

 Note

Remarque Cette URL doit correspondre à l'URL figurant dans la réclamation de l'émetteur (iss) dans les jetons émis pour une propagation d'identité fiable.

- Pour Nom de l'émetteur de jeton fiable, entrez un nom pour identifier cet émetteur de jeton fiable dans IAM Identity Center et dans la console de l'application.
6. Sous Attributs de carte, procédez comme suit :
 - Pour l'attribut du fournisseur d'identité, sélectionnez un attribut dans la liste à mapper à un attribut de la banque d'identités IAM Identity Center.
 - Pour l'attribut IAM Identity Center, sélectionnez l'attribut correspondant pour le mappage des attributs.
 7. Sous Tags (facultatif), choisissez Ajouter une nouvelle balise, spécifiez une valeur pour Key, et éventuellement pour Value.

Pour plus d'informations sur les balises, consultez [Ressources de balisage AWS IAM Identity Center](#).

8. Choisissez Créer un émetteur de jetons approuvés.
9. Une fois que vous avez créé l'émetteur de jetons approuvés, contactez l'administrateur de l'application pour lui communiquer le nom de l'émetteur de jetons approuvés, afin qu'il puisse confirmer que cet émetteur est visible dans la console appropriée.
10. L'administrateur de l'application doit sélectionner cet émetteur de jeton sécurisé dans la console applicable pour permettre aux utilisateurs d'accéder à l'application à partir d'applications configurées pour la propagation d'identités fiables.

Comment afficher ou modifier les paramètres de l'émetteur de jetons de confiance dans la console IAM Identity Center

Après avoir ajouté un émetteur de jetons de confiance à la console IAM Identity Center, vous pouvez consulter et modifier les paramètres appropriés.

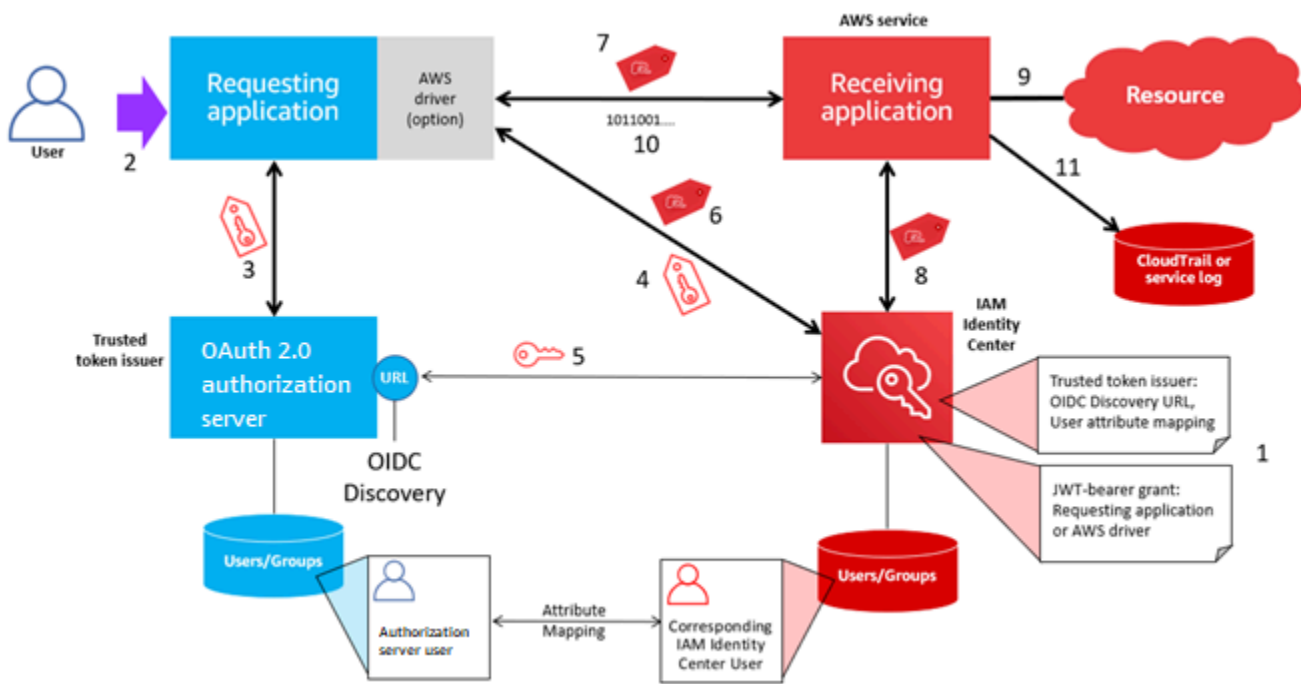
Si vous envisagez de modifier les paramètres de l'émetteur de jetons de confiance, gardez à l'esprit que les utilisateurs risquent de perdre l'accès à toutes les applications configurées pour utiliser l'émetteur de jetons de confiance. Pour éviter de perturber l'accès des utilisateurs, nous vous recommandons de vous coordonner avec les administrateurs de toutes les applications configurées pour utiliser l'émetteur de jetons approuvé avant de modifier les paramètres.

Pour consulter ou modifier les paramètres de l'émetteur de jetons de confiance dans la console IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Authentification.
4. Sous Émetteurs de jetons fiables, sélectionnez l'émetteur de jetons de confiance que vous souhaitez consulter ou modifier.
5. Sélectionnez Actions, puis Edit (Modifier).
6. Sur la page Modifier l'émetteur de jetons de confiance, consultez ou modifiez les paramètres selon vos besoins. Vous pouvez modifier le nom de l'émetteur du jeton fiable, les mappages d'attributs et les balises.
7. Sélectionnez Enregistrer les modifications.
8. Dans la boîte de dialogue Modifier l'émetteur de jetons de confiance, vous êtes invité à confirmer que vous souhaitez apporter des modifications. Choisissez Confirmer.

Processus de configuration et flux de demandes pour les applications utilisant un émetteur de jetons fiable

Cette section décrit le processus de configuration et le flux de demandes pour les applications qui utilisent un émetteur de jetons fiable pour la propagation d'identités fiables. Le schéma suivant donne un aperçu de ce processus.



Les étapes suivantes fournissent des informations supplémentaires sur ce processus.

1. Configurez IAM Identity Center et l'application AWS gérée réceptrice pour qu'ils utilisent un émetteur de jetons fiable. Pour plus d'informations, consultez [Tâches de configuration d'un émetteur de jetons de confiance](#).
2. Le flux de demandes commence lorsqu'un utilisateur ouvre l'application demandeuse.
3. L'application demandeuse demande un jeton à l'émetteur de jetons de confiance pour initier des demandes à l'application AWS gérée réceptrice. Si l'utilisateur ne s'est pas encore authentifié, ce processus déclenche un flux d'authentification. Le jeton contient les informations suivantes :
 - Le sujet (Sub) de l'utilisateur.
 - Attribut utilisé par IAM Identity Center pour rechercher l'utilisateur correspondant dans IAM Identity Center.
 - Une réclamation d'audience (Aud) contenant une valeur que l'émetteur de jetons de confiance associe à l'application AWS gérée réceptrice. Si d'autres réclamations sont présentes, elles ne sont pas utilisées par IAM Identity Center.
4. L'application demandeuse, ou le AWS pilote qu'elle utilise, transmet le jeton à IAM Identity Center et demande que le jeton soit échangé contre un jeton généré par IAM Identity Center. Si vous utilisez un AWS pilote, vous devrez peut-être le configurer pour ce cas d'utilisation. Pour plus d'informations, consultez la documentation de l'application AWS gérée correspondante.

5. IAM Identity Center utilise le point de terminaison OIDC Discovery pour obtenir la clé publique qu'il peut utiliser pour vérifier l'authenticité du jeton. IAM Identity Center effectue ensuite les opérations suivantes :
 - Vérifie le jeton.
 - Effectue une recherche dans le répertoire Identity Center. Pour ce faire, IAM Identity Center utilise l'attribut mappé spécifié dans le jeton.
 - Vérifie que l'utilisateur est autorisé à accéder à l'application réceptrice. Si l'application AWS gérée est configurée pour exiger des affectations aux utilisateurs et aux groupes, l'utilisateur doit disposer d'une attribution directe ou basée sur un groupe à l'application ; sinon, la demande est refusée. Si l'application AWS gérée est configurée pour ne pas nécessiter d'assignation d'utilisateur ou de groupe, le traitement se poursuit.

 Note

AWS les services ont une configuration de paramètres par défaut qui détermine si des attributions sont requises pour les utilisateurs et les groupes. Nous vous recommandons de ne pas modifier le paramètre Exiger des attributions pour ces applications si vous prévoyez de les utiliser dans le cadre d'une propagation d'identité sécurisée. Même si vous avez configuré des autorisations détaillées qui permettent aux utilisateurs d'accéder à des ressources spécifiques de l'application, la modification du paramètre Exiger des attributions peut entraîner un comportement inattendu, notamment une interruption de l'accès des utilisateurs à ces ressources.

- Vérifie que l'application demandeuse est configurée pour utiliser des étendues valides pour l'application AWS gérée réceptrice.
6. Si les étapes de vérification précédentes sont réussies, IAM Identity Center crée un nouveau jeton. Le nouveau jeton est un jeton opaque (crypté) qui inclut l'identité de l'utilisateur correspondant dans IAM Identity Center, le public (Aud) de l'application AWS gérée réceptrice et les étendues que l'application demandeuse peut utiliser lorsqu'elle adresse des demandes à l'application AWS gérée réceptrice.
 7. L'application demandeuse, ou le pilote qu'elle utilise, lance une demande de ressource à l'application réceptrice et transmet le jeton généré par IAM Identity Center à l'application réceptrice.
 8. L'application réceptrice appelle IAM Identity Center pour obtenir l'identité de l'utilisateur et les étendues codées dans le jeton. Il peut également faire des demandes pour obtenir les attributs des utilisateurs ou les appartenances à des groupes d'utilisateurs à partir du répertoire Identity Center.

9. L'application réceptrice utilise sa configuration d'autorisation pour déterminer si l'utilisateur est autorisé à accéder à la ressource d'application demandée.
10. Si l'utilisateur est autorisé à accéder à la ressource d'application demandée, l'application réceptrice répond à la demande.
11. L'identité de l'utilisateur, les actions effectuées en son nom et les autres événements sont enregistrés dans les journaux et CloudTrail événements de l'application réceptrice. La manière spécifique dont ces informations sont enregistrées varie en fonction de l'application.

Sessions de rôles IAM améliorées

Le [AWS Security Token Service](#) (STS) permet à une application d'obtenir une session de rôle IAM améliorée en termes d'identité. Les sessions de rôle à identité améliorée ont un contexte d'identité ajouté qui porte un identifiant utilisateur à celui Service AWS qu'elles appellent. Services AWS peut rechercher les appartenances aux groupes et les attributs de l'utilisateur dans IAM Identity Center et les utiliser pour autoriser l'accès de l'utilisateur aux ressources.

AWS les applications obtiennent des sessions de rôle à identité améliorée en adressant des requêtes à l'action de l' AWS STS [AssumeRole](#) API et en transmettant une assertion de contexte avec l'identifiant de l'utilisateur (userId) dans le ProvidedContexts paramètre de la demande à. AssumeRole L'assertion de contexte est obtenue à partir de la idToken demande reçue en réponse à une demande adressée SSO OIDC à [CreateTokenWithIAM](#). Lorsqu'une AWS application utilise une session de rôle à identité améliorée pour accéder à une ressource, elle CloudTrail enregistre la userId session initiatrice et l'action entreprise. Pour de plus amples informations, veuillez consulter [Journalisation des sessions de rôle IAM améliorée en termes d'identité](#).

Rubriques

- [Types de sessions de rôle IAM à identité améliorée](#)
- [Journalisation des sessions de rôle IAM améliorée en termes d'identité](#)

Types de sessions de rôle IAM à identité améliorée

AWS STS peut créer deux types différents de sessions de rôle IAM à identité améliorée, en fonction de l'assertion de contexte fournie à la demande. AssumeRole Les applications qui ont obtenu des jetons d'identification auprès d'IAM Identity Center peuvent ajouter sts:identity_context (recommandé) ou sts:audit_context (pris en charge pour des raisons de rétrocompatibilité) aux sessions de rôle IAM. Une session de rôle IAM à identité améliorée ne peut comporter qu'une seule de ces assertions de contexte, et non les deux.

Sessions de rôle IAM à identité améliorée créées avec **sts:identity_context**

Lorsqu'une session de rôle à identité améliorée contient `sts:identity_context` l'appelé, cela Service AWS détermine si l'autorisation des ressources est basée sur l'utilisateur représenté dans la session de rôle ou si elle est basée sur le rôle. Services AWS qui prennent en charge l'autorisation basée sur l'utilisateur fournissent à l'administrateur de l'application des contrôles permettant d'attribuer l'accès à l'utilisateur ou aux groupes dont l'utilisateur est membre.

Services AWS qui ne prennent pas en charge l'autorisation basée sur l'utilisateur ignorent `sts:identity_context`. CloudTrail enregistre l'`userId` de l'utilisateur IAM Identity Center avec toutes les actions entreprises par le rôle. Pour de plus amples informations, veuillez consulter [Journalisation des sessions de rôle IAM améliorée en termes d'identité](#).

Pour obtenir ce type de session de rôle à identité améliorée auprès des applications AWS STS, les applications fournissent la valeur du `sts:identity_context` champ dans la [AssumeRole](#) demande à l'aide du paramètre de `ProvidedContexts` demande. Utilisez `arn:aws:iam::aws:contextProvider/IdentityCenter` comme valeur pour `ProviderArn`.

Pour plus d'informations sur le comportement de l'autorisation, consultez la documentation relative à la réception Service AWS.

Sessions de rôle IAM à identité améliorée créées avec **sts:audit_context**

Dans le passé, `sts:audit_context` était utilisé pour permettre d' Services AWS enregistrer l'identité de l'utilisateur sans l'utiliser pour prendre une décision d'autorisation. Services AWS sont désormais en mesure d'utiliser un seul contexte - `sts:identity_context` - pour y parvenir ainsi que pour prendre des décisions d'autorisation. Nous vous recommandons d'utiliser `sts:identity_context` la propagation sécurisée des identités dans tous les nouveaux déploiements.

Journalisation des sessions de rôle IAM améliorée en termes d'identité

Lorsqu'une demande est adressée à une session Service AWS utilisant un rôle IAM amélioré, le centre d'identité IAM de l'utilisateur `userId` est connecté à CloudTrail l'élément. `OnBehalfOf` La manière dont les événements sont enregistrés CloudTrail varie en fonction du Service AWS. Tous n' Services AWS enregistrent pas l'`onBehalfOf` élément.

Voici un exemple de connexion à une demande envoyée à une session Service AWS utilisant un rôle à identité améliorée. CloudTrail

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
  }
}
```

Rotation des certificats IAM Identity Center

IAM Identity Center utilise des certificats pour établir une relation de confiance SAML entre IAM Identity Center et le fournisseur de services de votre application. Lorsque vous ajoutez une application dans IAM Identity Center, un certificat IAM Identity Center est automatiquement créé pour être utilisé avec cette application pendant le processus de configuration. Par défaut, ce certificat IAM Identity Center généré automatiquement est valide pour une période de cinq ans.

En tant qu'administrateur d'IAM Identity Center, vous devrez parfois remplacer les anciens certificats par des certificats plus récents pour une application donnée. Par exemple, il se peut que vous deviez remplacer un certificat lorsque sa date d'expiration approche. Le processus de remplacement d'un ancien certificat par un nouveau est appelé rotation des certificats.

Considérations relatives à la rotation d'un certificat

Avant de commencer le processus de rotation d'un certificat dans IAM Identity Center, tenez compte des points suivants :

- Le processus de rotation des certifications nécessite que vous rétablissiez la confiance entre IAM Identity Center et le fournisseur de services. Pour rétablir la confiance, utilisez les procédures fournies dans [Rotation d'un certificat IAM Identity Center](#).
- La mise à jour du certificat auprès du fournisseur de services peut entraîner une interruption de service temporaire pour vos utilisateurs jusqu'à ce que la confiance soit rétablie avec succès. Planifiez cette opération avec soin en dehors des heures de pointe si possible.

Rotation d'un certificat IAM Identity Center

La rotation d'un certificat IAM Identity Center est un processus en plusieurs étapes qui implique les étapes suivantes :

- Génération d'un nouveau certificat
- Ajouter le nouveau certificat sur le site Web du fournisseur de services
- Activer le nouveau certificat
- Supprimer le certificat inactif

Utilisez toutes les procédures suivantes dans l'ordre suivant pour terminer le processus de rotation des certificats pour une application donnée.

Étape 1 : générer un nouveau certificat

Les nouveaux certificats IAM Identity Center que vous générez peuvent être configurés pour utiliser les propriétés suivantes :

- Période de validité — Spécifie le temps imparti (en mois) avant l'expiration d'un nouveau certificat IAM Identity Center.
- Taille de clé — Détermine le nombre de bits qu'une clé doit utiliser avec son algorithme cryptographique. Vous pouvez définir cette valeur sur 1024 bits RSA ou 2048 bits RSA. Pour des informations générales sur le fonctionnement de la taille des clés en cryptographie, consultez la section [Taille des clés](#).

- **Algorithme** — Spécifie l'algorithme utilisé par IAM Identity Center lors de la signature de l'assertion/réponse SAML. Vous pouvez définir cette valeur sur SHA-1 ou SHA-256. AWS recommande d'utiliser le protocole SHA-256 dans la mesure du possible, sauf si votre fournisseur de services exige le protocole SHA-1. Pour des informations générales sur le fonctionnement des algorithmes de cryptographie, voir Cryptographie à [clé publique](#).

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Dans la liste des applications, sélectionnez l'application pour laquelle vous souhaitez générer un nouveau certificat.
4. Sur la page des détails de l'application, choisissez l'onglet Configuration. Sous les métadonnées du centre d'identité IAM, sélectionnez Gérer le certificat. Si vous n'avez pas d'onglet Configuration ou si le paramètre de configuration n'est pas disponible, il n'est pas nécessaire de faire pivoter le certificat pour cette application.
5. Sur la page du certificat IAM Identity Center, sélectionnez Générer un nouveau certificat.
6. Dans la boîte de dialogue Générer un nouveau certificat IAM Identity Center, spécifiez les valeurs appropriées pour la période de validité, l'algorithme et la taille de la clé. Choisissez ensuite Generate.

Étape 2 : mise à jour du site Web du fournisseur de services

Suivez la procédure ci-dessous pour rétablir la confiance avec le fournisseur de services de l'application.

Important

Lorsque vous téléchargez le nouveau certificat auprès du fournisseur de services, il est possible que vos utilisateurs ne soient pas en mesure de s'authentifier. Pour corriger cette situation, définissez le nouveau certificat comme actif, comme décrit à l'étape suivante.

1. Dans la [console IAM Identity Center](#), choisissez l'application pour laquelle vous venez de générer un nouveau certificat.
2. Sur la page des détails de l'application, choisissez Modifier la configuration.

3. Choisissez Afficher les instructions, puis suivez les instructions du site Web de votre fournisseur de services d'application spécifique pour ajouter le certificat nouvellement généré.

Étape 3 : activer le nouveau certificat

Jusqu'à deux certificats peuvent être attribués à une application. IAM Identity Center utilisera la certification définie comme active pour signer toutes les assertions SAML.

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Dans la liste des applications, sélectionnez votre application.
4. Sur la page des détails de l'application, choisissez l'onglet Configuration. Sous les métadonnées du centre d'identité IAM, sélectionnez Gérer le certificat.
5. Sur la page du certificat IAM Identity Center, sélectionnez le certificat que vous souhaitez définir comme actif, choisissez Actions, puis sélectionnez Définir comme actif.
6. Dans la boîte de dialogue Définir le certificat sélectionné comme actif, confirmez que vous comprenez que le fait de définir un certificat comme actif peut nécessiter le rétablissement de la confiance, puis choisissez Rendre actif.

Étape 4 : Supprimer l'ancien certificat

Suivez la procédure ci-dessous pour terminer le processus de rotation des certificats pour votre demande. Vous ne pouvez supprimer qu'un certificat dont l'état est inactif.

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Dans la liste des applications, sélectionnez votre application.
4. Sur la page des détails de l'application, sélectionnez l'onglet Configuration. Sous les métadonnées du centre d'identité IAM, sélectionnez Gérer le certificat.
5. Sur la page du certificat IAM Identity Center, sélectionnez le certificat que vous souhaitez supprimer. Choisissez Actions, puis Delete (Supprimer).
6. Dans la boîte de dialogue Supprimer le certificat, choisissez Supprimer.

Indicateurs du statut d'expiration des certificats

Dans la console IAM Identity Center, la page Applications affiche des icônes d'indicateur d'état dans les propriétés de chaque application. Ces icônes s'affichent dans la colonne Expire le jour à côté de chaque certificat de la liste. Ce qui suit décrit les critères utilisés par IAM Identity Center pour déterminer l'icône qui s'affiche pour chaque certificat.

- Rouge — Indique qu'un certificat est actuellement expiré.
- Jaune — Indique qu'un certificat expirera dans 90 jours ou moins.
- Vert — Indique qu'un certificat est actuellement valide et le restera pendant au moins 90 jours supplémentaires.

Pour vérifier le statut d'un certificat

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Dans la liste des applications, vérifiez le statut des certificats de la liste, comme indiqué dans la colonne Expire le.

Comprendre les propriétés de l'application dans la console IAM Identity Center

Dans IAM Identity Center, vous pouvez personnaliser l'expérience utilisateur en configurant l'URL de démarrage de l'application, l'état du relais et la durée de session.

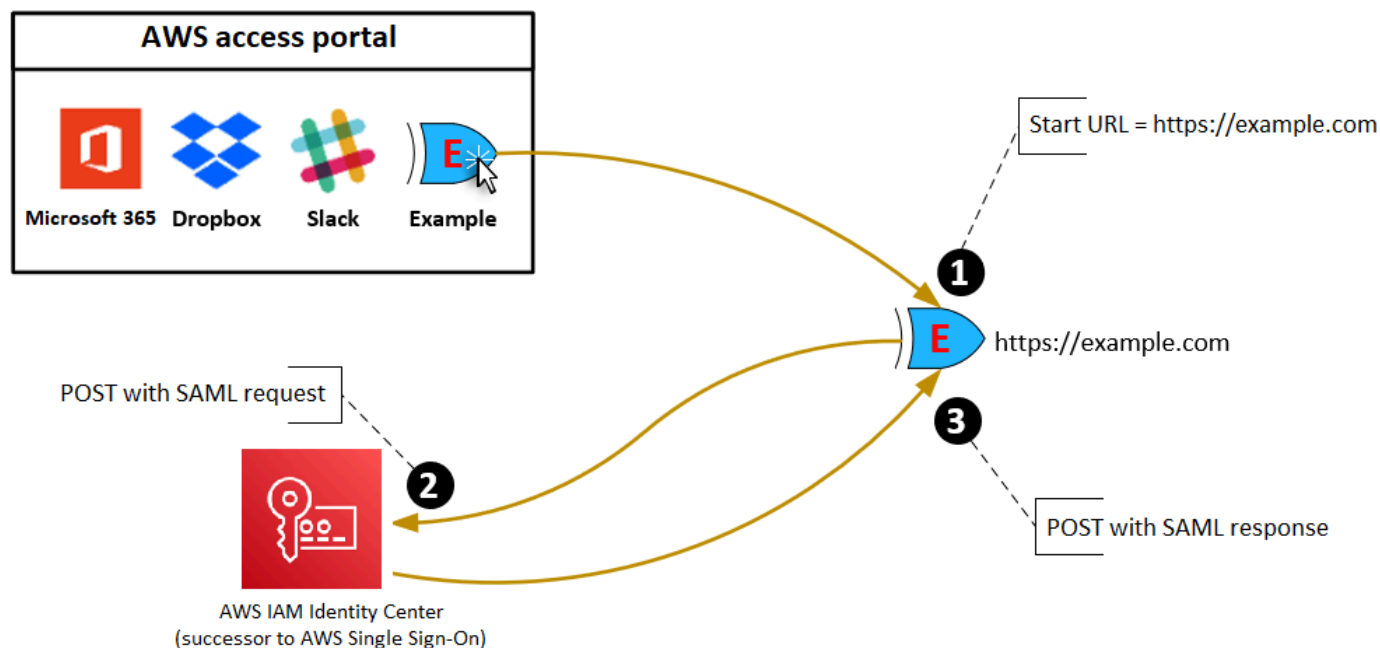
URL de démarrage de l'application

Vous utilisez une URL de lancement d'application pour démarrer le processus de fédération avec votre application. L'utilisation typique concerne une application qui prend uniquement en charge la liaison initiée par le fournisseur de services (SP).

Les étapes et le schéma suivants illustrent le flux de travail d'authentification par URL de démarrage de l'application lorsqu'un utilisateur choisit une application dans le portail AWS d'accès :

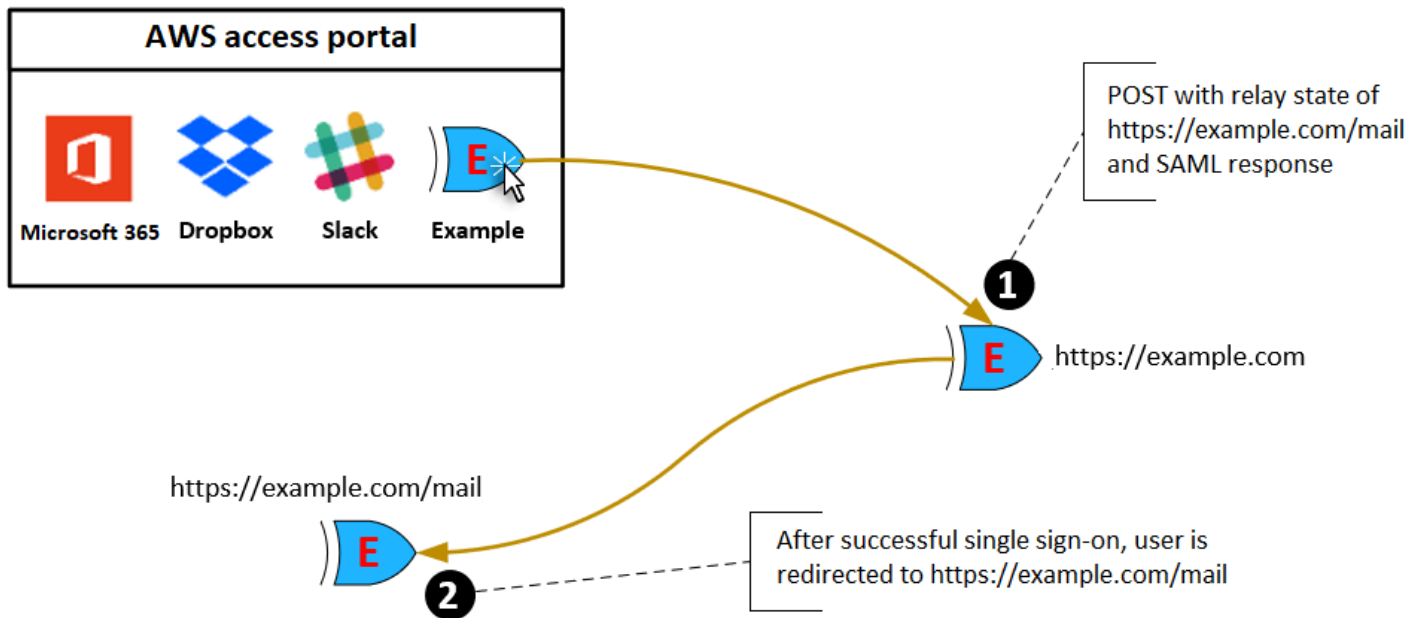
1. Le navigateur de l'utilisateur redirige la demande d'authentification en utilisant la valeur de l'URL de démarrage de l'application (dans ce cas <https://example.com>).

2. L'application envoie un HTML POST identifiant SAMLRequest à IAM Identity Center.
3. IAM Identity Center envoie ensuite un message HTML POST avec un SAMLResponse retour à l'application.



État du relais

Pendant le processus d'authentification de la fédération, l'état de relais redirige les utilisateurs au sein de l'application. Pour SAML 2.0, cette valeur est transmise, sans modification, à l'application. Une fois les propriétés de l'application configurées, IAM Identity Center envoie la valeur de l'état du relais avec une réponse SAML à l'application.



Durée de la session

La durée de session est la durée pendant laquelle une session utilisateur de l'application est valide. Pour SAML 2.0, cela est utilisé pour définir la `SessionNotOnOrAfter` date de l'élément de l'assertion SAML. `saml2:AuthNStatement`

La durée de session peut être interprétée par les applications de l'une des manières suivantes :

- Les applications peuvent l'utiliser pour déterminer la durée maximale autorisée pour la session de l'utilisateur. Les applications peuvent générer une session utilisateur d'une durée plus courte. Cela peut se produire lorsque l'application prend uniquement en charge les sessions utilisateur avec une durée plus courte que la durée de session configurée.
- Les applications peuvent l'utiliser comme durée exacte et ne pas permettre aux administrateurs de configurer la valeur. Cela peut se produire lorsque l'application prend uniquement en charge une durée de session spécifique.

Pour plus d'informations sur la façon dont la durée de la session est utilisée, consultez la documentation de votre application spécifique.

Attribuer un accès utilisateur aux applications dans la console IAM Identity Center

Vous pouvez attribuer aux utilisateurs un accès par authentification unique aux applications SAML 2.0 du catalogue d'applications ou aux applications SAML 2.0 personnalisées.

Considérations relatives aux tâches de groupe :

- Attribuez l'accès directement aux groupes. Pour simplifier l'administration des autorisations d'accès, nous vous recommandons d'attribuer l'accès directement à des groupes plutôt qu'à des utilisateurs individuels. Avec les groupes, vous pouvez accorder ou refuser des autorisations à des groupes d'utilisateurs, au lieu d'appliquer ces autorisations à chaque individu. Si un utilisateur est transféré dans une autre organisation, il vous suffit de le déplacer vers un autre groupe. L'utilisateur reçoit alors automatiquement les autorisations requises pour la nouvelle organisation.
- Les groupes imbriqués ne sont pas pris en charge. Lors de l'attribution d'un accès utilisateur aux applications, IAM Identity Center ne prend pas en charge l'ajout d'utilisateurs à des groupes imbriqués. Si un utilisateur est ajouté à un groupe imbriqué, il peut recevoir un message « Vous n'avez aucune application » lors de la connexion. Les attributions doivent être effectuées par rapport au groupe immédiat dont l'utilisateur est membre.

Pour attribuer un accès aux applications à un utilisateur ou à un groupe

Important

Pour les applications AWS gérées, vous devez ajouter des utilisateurs directement depuis les consoles d'applications concernées ou via le APIs.

1. Ouvrez la [console IAM Identity Center](#).

Note

Si vous gérez des utilisateurs dans AWS Managed Microsoft AD, assurez-vous que la console IAM Identity Center utilise la AWS région dans laquelle se trouve votre AWS Managed Microsoft AD annuaire avant de passer à l'étape suivante.

2. Choisissez Applications.

3. Dans la liste des applications, choisissez le nom de l'application à laquelle vous souhaitez attribuer l'accès.
4. Sur la page des détails de l'application, dans la section Utilisateurs assignés, choisissez Attribuer des utilisateurs.
5. Dans la boîte de dialogue Attribuer des utilisateurs, entrez un nom d'affichage utilisateur ou un nom de groupe. Vous pouvez spécifier plusieurs utilisateurs ou groupes en sélectionnant les comptes applicables tels qu'ils apparaissent dans les résultats de recherche.
6. Choisissez Assign users (Affecter des utilisateurs).

Supprimer l'accès des utilisateurs aux applications SAML 2.0

Utilisez cette procédure pour supprimer l'accès des utilisateurs aux applications SAML 2.0 du catalogue d'applications ou aux applications SAML 2.0 personnalisées. Pour plus d'informations sur les sessions d'authentification et leur durée, consultez [Comprendre les sessions d'authentification dans IAM Identity Center](#).

Pour supprimer l'accès d'un utilisateur à une application

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Dans la liste des applications, choisissez l'application dont vous souhaitez supprimer l'accès utilisateur.
4. Sur la page des détails de l'application, dans la section Utilisateurs assignés, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer, puis cliquez sur le bouton Supprimer l'accès.
5. Dans la boîte de dialogue Remove access (Supprimer l'accès), vérifiez le nom de l'utilisateur ou du groupe. Choisissez ensuite Remove access (Supprimer l'accès).

Associez les attributs de votre application aux attributs d'IAM Identity Center

Certains fournisseurs de services ont besoin d'assertions SAML personnalisées pour transmettre des données supplémentaires concernant les connexions des utilisateurs. Dans ce cas, utilisez la procédure suivante pour spécifier comment les attributs utilisateur de vos applications doivent correspondre aux attributs correspondants dans IAM Identity Center.

Pour mapper les attributs d'une application à des attributs dans IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Applications.
3. Dans la liste des applications, choisissez l'application pour laquelle vous souhaitez mapper les attributs.
4. Sur la page des détails de l'application, sélectionnez Actions, puis sélectionnez Modifier le mappage d'attributs.
5. Choisissez Ajouter un nouveau mappage d'attributs.
6. Dans la première zone de texte, entrez l'attribut de l'application.
7. Dans la deuxième zone de texte, entrez l'attribut dans IAM Identity Center que vous souhaitez associer à l'attribut de l'application. Par exemple, vous souhaitez peut-être mapper l'attribut de l'application **Username** à l'attribut **email** utilisateur IAM Identity Center. Pour consulter la liste des attributs utilisateur autorisés dans IAM Identity Center, consultez le tableau dans [Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes](#).
8. Dans la troisième colonne du tableau, choisissez le format approprié pour l'attribut dans le menu.
9. Sélectionnez Enregistrer les modifications.

Configurer l'accès à Comptes AWS

AWS IAM Identity Center est intégré à AWS Organizations, ce qui vous permet de gérer de manière centralisée les autorisations sur plusieurs comptes Comptes AWS sans configurer manuellement chacun de vos comptes. Vous pouvez définir des autorisations et les attribuer aux utilisateurs du personnel afin de contrôler leur accès à des informations spécifiques à Comptes AWS l'aide d'une [instance organisationnelle](#) d'IAM Identity Center. [Les instances de compte](#) d'IAM Identity Center ne prennent pas en charge l'accès aux comptes.

Compte AWS types

Il existe deux types d' Comptes AWS entrées AWS Organizations :

- Compte de gestion - Le Compte AWS compte utilisé pour créer l'organisation.
- Comptes de membres : les Comptes AWS autres comptes appartiennent à une organisation.

Pour plus d'informations sur les Compte AWS types, reportez-vous à [AWS Organizations la section Terminologie et concepts](#) du guide de AWS Organizations l'utilisateur.

Vous pouvez également choisir d'enregistrer un compte membre en tant qu'administrateur délégué pour IAM Identity Center. Les utilisateurs de ce compte peuvent effectuer la plupart des tâches administratives d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Administration déléguée](#).

Pour chaque tâche et chaque type de compte, le tableau suivant indique si la tâche administrative d'IAM Identity Center peut être exécutée par les utilisateurs du compte.

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Lire les utilisateurs ou les groupes (lire le groupe lui-même et les membres du groupe)	 Oui	 Oui	 Oui

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Ajouter, modifier ou supprimer des utilisateurs ou des groupes	 Non	 Oui	 Oui
Activer ou désactiver l'accès utilisateur	 Non	 Oui	 Oui
Activer, désactiver ou gérer les attributs entrants	 Non	 Oui	 Oui
Modifier ou gérer les sources d'identité	 Non	 Oui	 Oui
Création, modification ou suppression d'applications gérées par le client	 Non	 Oui	 Oui
Création, modification ou suppression d'applications AWS gérées	 Oui	 Oui	 Oui

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Configuration de la MFA	 Non	 Oui	 Oui
Gérer les ensembles d'autorisations non provisionnés dans le compte de gestion	 Non	 Oui	 Oui
Gérer les ensembles d'autorisations fournis dans le compte de gestion	 Non	 Non	 Oui
Activer IAM Identity Center	 Non	 Non	 Oui
Supprimer la configuration du centre d'identité IAM	 Non	 Non	 Oui
Activer ou désactiver l'accès utilisateur dans le compte de gestion	 Non	 Non	 Oui

Tâches administratives d'IAM Identity Center	Compte membre	Compte administrateur délégué	Compte de gestion
Enregistrer ou désenregistrer un compte membre en tant qu'administrateur délégué	 Non	 Non	 Oui

*Reportez-vous aux meilleures pratiques en matière d'administration déléguée concernant les affectations d'utilisateurs et de groupes au compte de gestion.

Attribution d'un accès Compte AWS

Vous pouvez utiliser des ensembles d'autorisations pour simplifier la façon dont vous attribuez l'accès aux utilisateurs et aux groupes de votre organisation Comptes AWS. Les ensembles d'autorisations sont stockés dans IAM Identity Center et définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Vous pouvez créer un ensemble d'autorisations unique et l'attribuer à plusieurs Comptes AWS au sein de votre organisation. Vous pouvez également attribuer plusieurs ensembles d'autorisations au même utilisateur.

Pour plus d'informations sur les jeux d'autorisations, consultez [Création, gestion et suppression des jeux d'autorisations](#).

Note

Vous pouvez également attribuer à vos utilisateurs un accès par authentification unique aux applications. Pour plus d'informations, consultez [Configuration de l'accès aux applications](#).

Expérience de l'utilisateur final

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à toutes les applications Comptes AWS et applications qui leur sont assignées via un portail Web. Le portail AWS d'accès est différent du [AWS Management Console](#), qui est un ensemble de consoles de service permettant de gérer les AWS ressources.

Lorsque vous créez un ensemble d'autorisations, le nom que vous spécifiez pour l'ensemble d'autorisations apparaît dans le portail AWS d'accès en tant que rôle disponible. Les utilisateurs se connectent AWS au portail d'accès Compte AWS, choisissent un, puis le rôle. Après avoir choisi le rôle, ils peuvent accéder aux AWS services en utilisant AWS Management Console ou en récupérant des informations d'identification temporaires pour accéder aux AWS services par programmation.

Pour ouvrir AWS Management Console ou récupérer des informations d'identification temporaires afin d'y accéder AWS par programmation, les utilisateurs effectuent les étapes suivantes :

1. Les utilisateurs ouvrent une fenêtre de navigateur et utilisent l'URL de connexion que vous fournissez pour accéder au portail AWS d'accès.
2. À l'aide de leurs identifiants d'annuaire, ils se connectent au portail AWS d'accès.
3. Après authentification, sur la page du portail d' AWS accès, ils choisissent l'onglet Comptes pour afficher la liste des comptes Comptes AWS auxquels ils ont accès.
4. Les utilisateurs choisissent ensuite Compte AWS celui qu'ils souhaitent utiliser.
5. Sous le nom du Compte AWS, tous les ensembles d'autorisations auxquels les utilisateurs sont affectés apparaissent sous forme de rôles disponibles. Par exemple, si vous avez attribué un utilisateur `john_stiles` à l'ensemble d'PowerUser autorisations, le rôle s'affiche dans le portail AWS d'accès sous la forme `PowerUser/john_stiles`. Les utilisateurs qui bénéficient de plusieurs jeux d'autorisations choisissent le rôle à utiliser. Les utilisateurs peuvent choisir leur rôle pour accéder au AWS Management Console.
6. Outre le rôle, les utilisateurs du portail AWS d'accès peuvent récupérer des informations d'identification temporaires pour l'accès par ligne de commande ou par programmation en choisissant les clés d'accès.

Pour step-by-step obtenir des conseils que vous pouvez fournir aux utilisateurs de votre personnel, consultez [Configuration et utilisation du portail AWS d'accès](#) et [Obtenir les informations d'identification utilisateur d'IAM Identity Center pour le ou AWS CLI AWS SDKs](#).

Renforcer et limiter l'accès

Lorsque vous activez IAM Identity Center, IAM Identity Center crée un rôle lié à un service. Vous pouvez également utiliser les politiques de contrôle des services (SCPs).

Délégation et renforcement de l'accès

Un rôle lié à un service est un type de rôle IAM directement lié à un service. AWS Une fois que vous avez activé IAM Identity Center, IAM Identity Center peut créer un rôle lié à un service dans chacun Compte AWS des membres de votre organisation. Ce rôle fournit des autorisations prédéfinies qui permettent à IAM Identity Center de déléguer et d'appliquer les utilisateurs disposant d'un accès par authentification unique à des utilisateurs spécifiques de votre organisation Comptes AWS dans. AWS Organizations Pour utiliser ce rôle, vous devez attribuer à un ou plusieurs utilisateurs l'accès à un compte. Pour plus d'informations, consultez [Comprendre les rôles liés aux services dans IAM Identity Center](#) et [Utilisation de rôles liés à un service pour IAM Identity Center](#).

Limiter l'accès à la banque d'identités depuis les comptes des membres

Pour le service de banque d'identité utilisé par IAM Identity Center, les utilisateurs ayant accès à un compte membre peuvent utiliser des actions d'API qui nécessitent des autorisations de lecture. Les comptes membres ont accès aux actions Read sur les espaces de noms sso-directory et identitystore. Pour plus d'informations, consultez [les sections Actions, ressources et clés de condition pour le AWS IAM Identity Center répertoire](#) et [Actions, ressources et clés de condition pour AWS Identity Store](#) dans la référence d'autorisation de service.

Pour empêcher les utilisateurs des comptes membres d'utiliser les opérations d'API dans le magasin d'identités, vous pouvez [joindre une politique de contrôle des services \(SCP\)](#). Un SCP est un type de politique d'organisation que vous pouvez utiliser pour gérer les autorisations au sein de votre organisation. L'exemple de SCP suivant empêche les utilisateurs des comptes membres d'accéder à toute opération d'API dans le magasin d'identités.

```
{
  "Sid": "ExplicitlyBlockIdentityStoreAccess",
  "Effect": "Deny",
  "Action": ["identitystore:*", "sso-directory:*"],
  "Resource": "*"
}
```

Note

Pour garantir le bon fonctionnement de vos applications AWS gérées avec votre IAM Identity Center, vous devez éviter d'appliquer ce SCP à l' Comptes AWS endroit où vous avez déployé ces applications. De plus, si vous utilisez l'administration déléguée, vous devez éviter

d'appliquer ce SCP au compte d'administration déléguée. Pour de plus amples informations, veuillez consulter [Bonnes pratiques](#).

Pour plus d'informations, voir [Politiques de contrôle des services \(SCPs\)](#) dans le guide de AWS Organizations l'utilisateur.

Administration déléguée

L'administration déléguée permet aux utilisateurs assignés à un compte membre enregistré d'effectuer facilement la plupart des tâches administratives d'IAM Identity Center. Lorsque vous activez IAM Identity Center, votre instance IAM Identity Center est créée AWS Organizations par défaut dans le compte de gestion. Cela a été initialement conçu de cette façon afin qu'IAM Identity Center puisse fournir, déprovisionner et mettre à jour les rôles sur tous les comptes membres de votre organisation. Même si votre instance IAM Identity Center doit toujours résider dans le compte de gestion, vous pouvez choisir de déléguer l'administration d'IAM Identity Center à un compte membre AWS Organizations, étendant ainsi la capacité de gérer IAM Identity Center depuis l'extérieur du compte de gestion.

L'activation de l'administration déléguée offre les avantages suivants :

- Minimise le nombre de personnes ayant besoin d'accéder au compte de gestion pour atténuer les problèmes de sécurité
- Permet à certains administrateurs d'attribuer des utilisateurs et des groupes aux applications et aux comptes des membres de votre organisation

Pour plus d'informations sur le fonctionnement d'IAM Identity Center AWS Organizations, consultez [Configurer l'accès à Comptes AWS](#). Pour plus d'informations et pour consulter un exemple de scénario d'entreprise montrant comment configurer l'administration déléguée, consultez [Getting started with IAM Identity Center Delegated Administration](#) dans le blog AWS de sécurité.

Rubriques

- [Bonnes pratiques](#)
- [Conditions préalables](#)
- [Enregistrez un compte membre](#)
- [Annuler l'enregistrement d'un compte membre](#)

- [Afficher quel compte de membre a été enregistré en tant qu'administrateur délégué](#)

Bonnes pratiques

Voici quelques bonnes pratiques à prendre en compte avant de configurer l'administration déléguée :

- Accorder le moindre privilège au compte de gestion — Sachant que le compte de gestion est un compte hautement privilégié et pour respecter le principe du moindre privilège, nous vous recommandons vivement de restreindre l'accès au compte de gestion au moins de personnes possible. La fonctionnalité d'administrateur délégué vise à minimiser le nombre de personnes ayant besoin d'accéder au compte de gestion. Vous pouvez également envisager d'utiliser [un accès élevé temporaire](#) pour n'accorder cet accès qu'en cas de besoin.
- Ensembles d'autorisations dédiés pour le compte de gestion : utilisez des ensembles d'autorisations dédiés pour le compte de gestion. Pour des raisons de sécurité, un ensemble d'autorisations utilisé pour accéder au compte de gestion ne peut être modifié que par un administrateur IAM Identity Center à partir du compte de gestion. L'administrateur délégué ne peut pas modifier les ensembles d'autorisations fournis dans le compte de gestion.
- Affecter uniquement des utilisateurs (et non des groupes) aux ensembles d'autorisations du compte de gestion : le compte de gestion disposant de privilèges spéciaux, vous devez faire preuve de prudence lorsque vous attribuez l'accès à ce compte dans la console ou AWS Command Line Interface (CLI). Si vous assignez des groupes à des ensembles d'autorisations ayant accès au compte de gestion, toute personne autorisée à modifier les adhésions à ces groupes add/remove peut to/from utiliser ces groupes, et ainsi déterminer qui a accès au compte de gestion. Il s'agit de tout administrateur de groupe contrôlant votre source d'identité, y compris l'administrateur de votre fournisseur d'identité (IdP), l'administrateur du service de domaine Microsoft Active Directory (AD DS) ou l'administrateur du centre d'identité IAM. Par conséquent, vous devez affecter les utilisateurs directement aux ensembles d'autorisations qui accordent l'accès au compte de gestion et éviter les groupes. Si vous utilisez des groupes pour gérer l'accès au compte de gestion, assurez-vous que les contrôles appropriés sont en place dans l'IdP afin de limiter les personnes autorisées à modifier ces groupes, et assurez-vous que les modifications apportées à ces groupes (ou les modifications des informations d'identification des utilisateurs du compte de gestion) sont enregistrées et examinées si nécessaire.
- Tenez compte de votre emplacement Active Directory : si vous prévoyez d'utiliser Active Directory comme source d'identité IAM Identity Center, localisez le répertoire dans le compte membre sur lequel vous avez activé la fonctionnalité d'administrateur délégué d'IAM Identity Center. Si vous décidez de remplacer la source d'identité IAM Identity Center d'une autre source par Active

Directory, ou de la remplacer par une autre source, le répertoire doit résider dans le compte membre administrateur délégué d'IAM Identity Center. Si vous souhaitez que votre Active Directory figure dans le compte de gestion, vous devez effectuer la configuration dans le compte de gestion, car l'administrateur délégué n'aura pas les autorisations nécessaires pour l'effectuer.

Limiter les actions de la banque d'identités IAM Identity Center dans le compte d'administration déléguée avec des sources d'identité externes

Si vous utilisez une source d'identité externe telle qu'un IdP Directory Service, vous devez mettre en œuvre des politiques qui limitent les actions du magasin d'identités qu'un administrateur du IAM Identity Center peut effectuer depuis le compte d'administration déléguée. Les opérations d'écriture et de suppression doivent être soigneusement étudiées. En général, la source d'identité externe est la source de vérité pour les utilisateurs et leurs attributs, ainsi que pour les appartenances aux groupes. Si vous les modifiez à l'aide du magasin d'identités APIs ou de la console, vos modifications seront remplacées au cours des cycles de synchronisation normaux. Il est préférable de confier ces opérations au contrôle exclusif de votre identité, source de vérité. Cela empêche également un administrateur du centre d'identité IAM de modifier les appartenances à un groupe pour accorder l'accès à un ensemble d'autorisations ou à une application attribué au groupe, plutôt que de laisser le contrôle de l'appartenance au groupe à votre administrateur IdP. Vous devez également vérifier qui peut créer des jetons porteurs SCIM à partir du compte d'administration déléguée, car ceux-ci pourraient permettre à un administrateur du compte membre de modifier des groupes et des utilisateurs via un client SCIM.

Il peut arriver que des opérations d'écriture ou de suppression soient appropriées à partir du compte administrateur délégué. Par exemple, vous pouvez créer un groupe sans ajouter de membres, puis attribuer un ensemble d'autorisations sans avoir à attendre que l'administrateur de l'IdP crée le groupe. Personne n'aura accès à cette attribution tant que l'administrateur de l'IdP n'aura pas approvisionné le groupe et que le processus de synchronisation de l'IdP n'aura pas établi les membres du groupe. Il peut également être approprié de supprimer un utilisateur ou un groupe pour empêcher la connexion ou l'autorisation lorsque vous ne pouvez pas attendre le processus de synchronisation de l'IdP pour supprimer l'accès à l'utilisateur ou au groupe. Cependant, l'utilisation abusive de cette autorisation peut perturber les utilisateurs. Vous devez utiliser le principe du moindre privilège lorsque vous attribuez des autorisations au magasin d'identités. Vous pouvez contrôler les actions du magasin d'identités autorisées par les administrateurs de votre compte d'administration déléguée à l'aide d'une politique de contrôle des services (SCP).

L'exemple de SCP ci-dessous empêche d'affecter des utilisateurs à des groupes via l'API Identity Store et le AWS Management Console, ce qui est recommandé lorsque votre source d'identité est externe. Cela n'affecte pas la synchronisation des utilisateurs depuis Directory Service ou depuis un IdP externe (via SCIM).

Note

Bien que vous utilisiez une source d'identité externe, il est possible que votre organisation s'appuie, en tout ou en partie, sur l'Identity Store APIs pour le provisionnement des utilisateurs et des groupes. Par conséquent, avant d'activer ce SCP, vous devez vérifier que votre processus de provisionnement utilisateur n'utilise pas cette opération d'API Identity Store. Reportez-vous également à la section suivante pour savoir comment limiter la gestion des adhésions à des groupes à des groupes spécifiques.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ "*" ] }
  ]
}
```

Si vous souhaitez empêcher l'ajout d'utilisateurs uniquement aux groupes qui accordent l'accès au compte de gestion, vous pouvez référencer ces groupes spécifiques à l'aide de l'ARN du groupe au format suivant :`arn:${Partition}:identitystore:::group/${GroupId}`. Ce type de ressource, ainsi que les autres types de ressources disponibles dans l'Identity Store, sont documentés dans la [section Types de ressources définis par AWS Identity Store](#) dans la référence d'autorisation de service. Vous pouvez également envisager d'inclure un magasin d'identité supplémentaire APIs dans le SCP. Pour plus d'informations, consultez la section [Actions](#) de la référence d'API Identity Store.

En ajoutant la déclaration de politique suivante à votre SCP, vous pouvez empêcher la création de jetons porteurs SCIM par l'administrateur délégué. Vous pouvez l'appliquer aux deux sources d'identité externes.

 Note

Si votre administrateur délégué doit configurer le provisionnement des utilisateurs avec SCIM ou effectuer la rotation périodique du jeton porteur SCIM, vous devrez autoriser temporairement l'accès à cette API pour permettre à l'administrateur délégué d'effectuer ces tâches.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

Limiter les actions de la banque d'identités IAM Identity Center dans le compte d'administration déléguée pour les utilisateurs gérés localement

Si vous créez vos utilisateurs et vos groupes directement dans IAM Identity Center, plutôt que d'utiliser un IdP externe, vous devez prendre Directory Service des précautions pour savoir qui peut créer des utilisateurs, réinitialiser les mots de passe et contrôler l'appartenance aux groupes. Ces actions confèrent à l'administrateur de grands pouvoirs pour déterminer qui peut se connecter et qui peut y accéder par le biais de l'adhésion à des groupes. Il est préférable de mettre en œuvre ces politiques sous forme de politiques intégrées dans les ensembles d'autorisations que vous utilisez pour les administrateurs de votre IAM Identity Center, plutôt que sous forme de politiques en ligne. SCPs L'exemple de politique en ligne suivant a deux objectifs. Tout d'abord, cela empêche d'ajouter des utilisateurs à des groupes spécifiques. Vous pouvez l'utiliser pour empêcher les administrateurs délégués d'ajouter des utilisateurs aux groupes qui accordent l'accès au compte de gestion. Deuxièmement, il empêche l'émission de jetons porteurs SCIM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ arn:${Partition}:identitystore::group/${GroupId1},
                    arn:${Partition}:identitystore::group/${GroupId2}
                  ]
    }
  ]
}
```

```
],  
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ] }  
]  
}
```

Séparez la gestion de la configuration d'IAM Identity Center de la gestion PermissionSet

Séparez les tâches administratives, notamment la modification de la source d'identité externe, la gestion des jetons SCIM, la configuration du délai d'expiration des sessions, des tâches de création, de modification et d'attribution d'ensembles d'autorisations en créant des ensembles d'autorisations d'administration distincts à partir de votre compte de gestion.

Limiter l'émission de jetons au porteur SCIM

Les jetons porteurs SCIM permettent à une source d'identité externe de fournir des informations aux utilisateurs, aux groupes et aux appartenances à des groupes via le protocole SCIM lorsque la source d'identité de votre centre d'identité IAM est un IdP externe tel qu'Okta ou Entra ID. Vous pouvez configurer le SCP suivant pour empêcher la création de jetons porteurs SCIM par les administrateurs délégués. Si votre administrateur délégué doit configurer le provisionnement des utilisateurs avec SCIM ou effectuer la rotation périodique du jeton porteur SCIM, vous devrez autoriser temporairement l'accès à cette API pour permettre à l'administrateur délégué d'effectuer ces tâches.

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

Utilisez des balises d'ensembles d'autorisations et des listes de comptes pour déléguer l'administration de comptes spécifiques

Vous pouvez créer des ensembles d'autorisations que vous attribuez à vos administrateurs IAM Identity Center afin de déléguer qui peut créer des ensembles d'autorisations et qui peut attribuer quels ensembles d'autorisations à quels comptes. Cela se fait en balisant les ensembles

d'autorisations et en utilisant des conditions de politique dans les ensembles d'autorisations que vous attribuez à vos administrateurs. Par exemple, vous pouvez créer des ensembles d'autorisations qui permettent à un utilisateur de créer des ensembles d'autorisations à condition qu'ils soient balisés d'une certaine manière. Vous pouvez également créer des politiques qui permettent à un administrateur d'attribuer des ensembles d'autorisations dotés d'une étiquette spécifique dans des comptes spécifiques. Cela peut vous aider à déléguer la gestion des comptes sans donner à un administrateur les privilèges nécessaires pour modifier son accès et ses privilèges sur le compte d'administration déléguée. Par exemple, en balisant les ensembles d'autorisations que vous utilisez uniquement dans le compte d'administration déléguée, vous pouvez définir une politique qui autorise uniquement certaines personnes à modifier les ensembles d'autorisations et les attributions qui affectent le compte d'administration déléguée. Vous pouvez également autoriser d'autres personnes à gérer une liste de comptes en dehors du compte d'administration déléguée. Pour en savoir plus, consultez la section [Délégation de la gestion des ensembles d'autorisations et de l'attribution de comptes AWS IAM Identity Center dans le blog sur la AWS sécurité](#).

Conditions préalables

Avant de pouvoir enregistrer un compte en tant qu'administrateur délégué, vous devez d'abord déployer l'environnement suivant :

- AWS Organizations doit être activé et configuré avec au moins un compte membre en plus de votre compte de gestion par défaut.
- Si votre source d'identité est définie sur Active Directory, la [Synchronisation AD configurable par IAM Identity Center](#) fonctionnalité doit être activée.

Enregistrez un compte membre

Pour configurer l'administration déléguée, vous devez d'abord enregistrer un compte membre dans votre organisation en tant qu'administrateur délégué. Les utilisateurs de ce compte membre disposant d'autorisations suffisantes auront un accès administratif à IAM Identity Center. Une fois qu'un compte membre est correctement enregistré pour l'administration déléguée, il est appelé compte d'administrateur délégué. Pour en savoir plus sur les tâches que le compte administrateur délégué peut effectuer, consultez [Compte AWS types](#).

IAM Identity Center prend en charge l'enregistrement d'un seul compte membre en tant qu'administrateur délégué à la fois. Vous ne pouvez créer un compte membre que lorsque vous êtes connecté avec les informations d'identification du compte de gestion.

Utilisez la procédure suivante pour accorder un accès administratif à IAM Identity Center en enregistrant un compte de membre spécifique dans votre AWS organisation en tant qu'administrateur délégué.

 Important

Cette opération délègue l'accès administratif d'IAM Identity Center aux utilisateurs administrateurs de ce compte membre. Tous les utilisateurs disposant d'autorisations suffisantes pour ce compte d'administrateur délégué peuvent effectuer toutes les tâches administratives d'IAM Identity Center à partir de ce compte, à l'exception de :

- Activation du centre d'identité IAM
- Suppression des configurations du centre d'identité IAM
- Gestion des ensembles d'autorisations fournis dans le compte de gestion
- Enregistrer ou désenregistrer d'autres comptes membres en tant qu'administrateurs délégués
- Activation ou désactivation de l'accès utilisateur dans le compte de gestion

L'administrateur délégué peut modifier l'appartenance au groupe.

Pour créer un compte membre

1. Connectez-vous à l' AWS Management Console aide des informations d'identification de votre compte de gestion dans AWS Organizations. Les informations d'identification du compte de gestion sont requises pour exécuter l'[RegisterDelegatedAdministrator](#) API.
2. Sélectionnez la région dans laquelle IAM Identity Center est activé, puis ouvrez la console [IAM Identity Center](#).
3. Choisissez Paramètres, puis sélectionnez l'onglet Gestion.
4. Dans la section Administrateur délégué, choisissez Enregistrer un compte.
5. Sur la page Enregistrer un administrateur délégué, sélectionnez celui que Compte AWS vous souhaitez enregistrer, puis choisissez Enregistrer un compte.

Annuler l'enregistrement d'un compte membre

Vous ne pouvez annuler l'enregistrement d'un compte membre que lorsque vous êtes connecté avec les informations d'identification du compte de gestion.

Utilisez la procédure suivante pour supprimer l'accès administratif à IAM Identity Center en annulant l'enregistrement d'un compte de membre de votre AWS organisation qui avait été précédemment désigné comme administrateur délégué.

Important

Lorsque vous désenregistrez un compte, vous empêchez effectivement tous les utilisateurs administrateurs de gérer IAM Identity Center à partir de ce compte. Par conséquent, ils ne peuvent plus administrer les identités IAM Identity Center, la gestion des accès, l'authentification ou l'accès aux applications à partir de ce compte. Cette opération n'affectera aucune autorisation ou attribution configurée dans IAM Identity Center et n'aura donc aucun impact sur vos utilisateurs finaux, car ils continueront d'avoir accès à leurs applications et Comptes AWS depuis le portail AWS d'accès.

Pour annuler l'enregistrement d'un compte de membre

1. Connectez-vous à l' AWS Management Console aide des informations d'identification de votre compte de gestion dans AWS Organizations. Les informations d'identification du compte de gestion sont requises pour exécuter l'[DeregisterDelegatedAdministratorAPI](#).
2. Sélectionnez la région dans laquelle IAM Identity Center est activé, puis ouvrez la console [IAM Identity Center](#).
3. Choisissez Paramètres, puis sélectionnez l'onglet Gestion.
4. Dans la section Administrateur délégué, choisissez Désenregistrer le compte.
5. Dans la boîte de dialogue Désenregistrer le compte, examinez les implications en matière de sécurité, puis entrez le nom du compte membre pour confirmer que vous avez bien compris.
6. Choisissez Désenregistrer le compte.

Afficher quel compte de membre a été enregistré en tant qu'administrateur délégué

Suivez la procédure ci-dessous pour savoir quel compte de membre AWS Organizations a été configuré en tant qu'administrateur délégué pour IAM Identity Center.

Pour consulter votre compte de membre enregistré

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Dans la section Détails, recherchez le nom du compte enregistré sous Administrateur délégué. Vous pouvez également trouver ces informations en sélectionnant l'onglet Gestion et en les consultant dans la section Administrateur délégué.

Accès surélevé temporaire pour Comptes AWS

Tout accès au votre Compte AWS implique un certain niveau de privilège. Les opérations sensibles, telles que la modification de la configuration d'un environnement de production, nécessitent un traitement spécial en raison de leur portée et de leur impact potentiel. L'accès élevé temporaire (également appelé just-in-time accès) est un moyen de demander, d'approuver et de suivre l'utilisation d'une autorisation pour effectuer une tâche spécifique pendant une période spécifiée. L'accès élevé temporaire complète d'autres formes de contrôle d'accès, telles que les ensembles d'autorisations et l'authentification multifactorielle.

Note

Pour garantir la continuité des activités, nous vous recommandons de [configurer un accès d'urgence au AWS Management Console](#).

Pour répondre aux besoins de nombreux clients, AWS IAM Identity Center s'intègre aux solutions des partenaires AWS Security Competency. AWS confirme que ces solutions répondent à un ensemble commun d'exigences en matière d'accès élevé temporaire. Nous vous recommandons d'examiner attentivement la solution de chaque partenaire afin de choisir celle qui correspond le mieux à vos besoins et préférences, notamment à votre activité, à l'architecture de votre environnement cloud et à votre budget.

Les solutions validées incluent la [plateforme de gestion des accès Apono](#), [CyberArk Secure Cloud Access](#), [Okta Access Requests](#) et [Tenable](#) (anciennement Ermetic).

Les partenaires peuvent proposer des solutions à l'aide de l'application AWS Security Competency dans Partner Center. Pour plus d'informations, consultez la section [Partenaires AWS de compétences en matière de sécurité](#).

Note

Si vous utilisez Amazon Elastic AWS Key Management Service Kubernetes Service basé sur les ressources [ou consultez Référencer les ensembles d'autorisations dans les politiques de ressources, les cartes de AWS KMS configuration du cluster Amazon EKS et les politiques](#) clés avant de choisir votre solution. just-in-time

Accès par authentification unique à Comptes AWS

Vous pouvez attribuer aux utilisateurs de votre annuaire connecté des autorisations d'accès au compte de gestion ou aux comptes de membres de votre organisation en AWS Organizations fonction des [fonctions professionnelles courantes](#). Vous pouvez également utiliser des autorisations personnalisées pour répondre à vos spécifications de sécurité spécifiques. Par exemple, vous pouvez accorder aux administrateurs de base de données des autorisations étendues sur Amazon RDS dans les comptes de développement, mais limiter leurs autorisations dans les comptes de production. IAM Identity Center configure automatiquement toutes les autorisations utilisateur nécessaires dans votre Comptes AWS système.

Note

Vous devrez peut-être accorder à des utilisateurs ou à des groupes des autorisations pour opérer dans le compte AWS Organizations de gestion. Comme il s'agit d'un compte hautement privilégié, des restrictions de sécurité supplémentaires nécessitent que vous disposiez de la politique [IAMFullD'accès](#) ou d'autorisations équivalentes avant de pouvoir le configurer. Ces restrictions de sécurité supplémentaires ne sont requises pour aucun des comptes membres de votre AWS organisation.

Rubriques

- [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#)

- [Supprimer l'accès des utilisateurs et des groupes à un Compte AWS](#)
- [Révoquer les sessions de rôle IAM actives créées par des ensembles d'autorisations](#)
- [Déléguer les personnes habilitées à attribuer un accès d'authentification unique aux utilisateurs et aux groupes du compte de gestion](#)

Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS

Utilisez la procédure suivante pour attribuer un accès par authentification unique aux utilisateurs et aux groupes de votre annuaire connecté et utiliser des ensembles d'autorisations pour déterminer leur niveau d'accès.

Pour vérifier l'accès des utilisateurs et des groupes existants, voir [Afficher et modifier un ensemble d'autorisations](#).

Note

Pour simplifier l'administration des autorisations d'accès, nous vous recommandons d'attribuer l'accès directement aux groupes et non pas aux différents utilisateurs. Avec les groupes, vous pouvez accorder ou refuser des autorisations à des groupes d'utilisateurs au lieu d'avoir à les appliquer individuellement à chaque utilisateur. Si un utilisateur change d'organisation, il vous suffit de le déplacer dans un autre groupe et il reçoit automatiquement les autorisations nécessaires pour la nouvelle organisation.

Pour attribuer un accès à un utilisateur ou à un groupe à Comptes AWS

1. Ouvrez la [console IAM Identity Center](#).

Note

Assurez-vous que la console IAM Identity Center utilise la région dans laquelle se trouve votre AWS Managed Microsoft AD répertoire avant de passer à l'étape suivante.

2. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Sur la Comptes AWS page, une liste arborescente de votre organisation s'affiche. Cochez la case à côté de Compte AWS laquelle vous souhaitez attribuer l'accès. Si vous configurez l'accès administratif pour IAM Identity Center, cochez la case à côté du compte de gestion.

 Note

Vous pouvez en sélectionner jusqu'à 10 Comptes AWS à la fois par ensemble d'autorisations lorsque vous attribuez un accès par authentification unique à des utilisateurs et à des groupes. Pour en attribuer plus de 10 Comptes AWS au même ensemble d'utilisateurs et de groupes, répétez cette procédure selon les besoins pour les comptes supplémentaires. Lorsque vous y êtes invité, sélectionnez les mêmes utilisateurs, groupes et ensembles d'autorisations.

4. Choisissez Attribuer des utilisateurs ou des groupes.
5. Pour l'étape 1 : sélectionner les utilisateurs et les groupes, sur la page Attribuer des utilisateurs et des groupes à **AWS-account-name** « », procédez comme suit :
 1. Dans l'onglet Utilisateurs, sélectionnez un ou plusieurs utilisateurs auxquels vous souhaitez accorder l'accès par authentification unique.

Pour filtrer les résultats, commencez à saisir le nom de l'utilisateur souhaité dans le champ de recherche.
 2. Dans l'onglet Groupes, sélectionnez un ou plusieurs groupes auxquels vous souhaitez accorder un accès par authentification unique.

Pour filtrer les résultats, commencez à taper le nom du groupe souhaité dans le champ de recherche.
 3. Pour afficher les utilisateurs et les groupes que vous avez sélectionnés, choisissez le triangle latéral à côté de Utilisateurs et groupes sélectionnés.
 4. Après avoir confirmé que les utilisateurs et les groupes sélectionnés sont corrects, choisissez Next.
6. Pour l'étape 2 : sélectionner des ensembles d'autorisations, sur la page Attribuer des ensembles d'autorisations à **AWS-account-name** « », procédez comme suit :
 1. Sélectionnez un ou plusieurs ensembles d'autorisations. Si nécessaire, vous pouvez créer et sélectionner de nouveaux ensembles d'autorisations.
 - Pour sélectionner un ou plusieurs ensembles d'autorisations existants, sous Ensembles d'autorisations, sélectionnez les ensembles d'autorisations que vous souhaitez appliquer aux utilisateurs et aux groupes que vous avez sélectionnés à l'étape précédente.

- Pour créer un ou plusieurs nouveaux ensembles d'autorisations, choisissez Créer un ensemble d'autorisations et suivez les étapes décrites dans [Crée un jeu d'autorisations](#). Après avoir créé les ensembles d'autorisations que vous souhaitez appliquer, dans la console IAM Identity Center, revenez Comptes AWS et suivez les instructions jusqu'à ce que vous atteigniez l'étape 2 : Sélectionnez les ensembles d'autorisations. Lorsque vous atteignez cette étape, sélectionnez les nouveaux ensembles d'autorisations que vous avez créés et passez à l'étape suivante de cette procédure.
2. Après avoir confirmé que les ensembles d'autorisations appropriés sont sélectionnés, choisissez Next.
7. Pour l'étape 3 : Réviser et envoyer, sur la page Réviser et envoyer les devoirs à **AWS-account-name** « », procédez comme suit :
1. Passez en revue les utilisateurs, les groupes et les ensembles d'autorisations sélectionnés.
 2. Après avoir confirmé que les utilisateurs, groupes et ensembles d'autorisations appropriés sont sélectionnés, choisissez Soumettre.

Considérations

- Le processus d'attribution des utilisateurs et des groupes peut prendre quelques minutes. Laissez cette page ouverte jusqu'à ce que le processus soit terminé avec succès.

Note

Vous devrez peut-être accorder à des utilisateurs ou à des groupes des autorisations pour opérer dans le compte AWS Organizations de gestion. Comme il s'agit d'un compte hautement privilégié, des restrictions de sécurité supplémentaires nécessitent que vous disposiez de la politique [IAMFullId'accès](#) ou d'autorisations équivalentes avant de pouvoir le configurer. Ces restrictions de sécurité supplémentaires ne sont requises pour aucun des comptes membres de votre AWS organisation.

8. Si l'une des conditions suivantes s'applique, suivez les étapes décrites [Inviter les utilisateurs à utiliser le MFA](#) pour activer le MFA pour IAM Identity Center :
- Vous utilisez le répertoire Identity Center par défaut comme source d'identité.
 - Vous utilisez un AWS Managed Microsoft AD annuaire ou un répertoire autogéré dans Active Directory comme source d'identité et vous n'utilisez pas RADIUS AWS Directory Service MFA avec.

 Note

Si vous utilisez un fournisseur d'identité externe, notez que c'est l'IdP externe, et non IAM Identity Center, qui gère les paramètres MFA. L'authentification MFA dans IAM Identity Center n'est pas prise en charge pour une utilisation par des tiers. IdPs

Lorsque vous configurez l'accès au compte pour l'utilisateur administratif, IAM Identity Center crée un rôle IAM correspondant. Ce rôle, qui est contrôlé par IAM Identity Center, est créé dans le répertoire approprié Compte AWS, et les politiques spécifiées dans le jeu d'autorisations sont associées au rôle.

Vous pouvez également utiliser [AWS CloudFormation](#) pour créer et attribuer des ensembles d'autorisations et affecter des utilisateurs à ces ensembles d'autorisations. Les utilisateurs peuvent ensuite se [connecter au portail AWS d'accès](#) ou utiliser les commandes [AWS Command Line Interface \(AWS CLI\)](#).

Supprimer l'accès des utilisateurs et des groupes à un Compte AWS

Utilisez cette procédure pour supprimer l'accès par authentification unique Compte AWS à un ou plusieurs utilisateurs et groupes de votre annuaire connecté. Vous pouvez également utiliser le kit [delete-account-assignment](#) AWS CLI.

 Note

Lorsque vous devez déprovisionner des utilisateurs ou des groupes IAM Identity Center, vous devez d'abord [supprimer toute attribution d'ensembles d'autorisations](#) à vos utilisateurs et groupes avant de supprimer les utilisateurs et les groupes.

Pour supprimer l'accès des utilisateurs et des groupes à un Compte AWS

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le volet de navigation, sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Sur la Comptes AWS page, une liste arborescente de votre organisation apparaît. Sélectionnez le nom Compte AWS qui contient les utilisateurs et les groupes pour lesquels vous souhaitez supprimer l'accès par authentification unique.

4. Sur la page d'aperçu de Compte AWS, sous Utilisateurs et groupes assignés, sélectionnez le nom d'un ou de plusieurs utilisateurs ou groupes, puis choisissez Supprimer l'accès.
5. Dans la boîte de dialogue Supprimer l'accès, vérifiez que les noms des utilisateurs ou des groupes sont corrects, puis choisissez Supprimer l'accès.

Révoquer les sessions de rôle IAM actives créées par des ensembles d'autorisations

La procédure générale suivante permet de révoquer une session d'ensemble d'autorisations active pour un utilisateur d'IAM Identity Center. La procédure part du principe que vous souhaitez supprimer tout accès à un utilisateur dont les informations d'identification ont été compromises ou à un acteur malveillant présent dans le système. La condition préalable est d'avoir suivi les directives en [Préparez-vous à révoquer une session de rôle IAM active créée par un ensemble d'autorisations](#). Nous supposons que la politique de refus de tout est présente dans une politique de contrôle des services (SCP).

Note

AWS vous recommande de créer une automatisation pour gérer toutes les étapes, à l'exception des opérations relatives à la console uniquement.

1. Obtenez le nom d'utilisateur de la personne dont vous devez révoquer l'accès. Vous pouvez utiliser le magasin d'identité APIs pour trouver l'utilisateur à l'aide de son nom d'utilisateur.
2. Mettez à jour la politique de refus pour ajouter l'ID utilisateur de l'étape 1 dans votre politique de contrôle des services (SCP). Une fois cette étape terminée, l'utilisateur cible perd son accès et n'est plus en mesure d'effectuer des actions avec les rôles concernés par la politique.
3. Supprimez tous les ensembles d'autorisations attribués à l'utilisateur. Si l'accès est attribué par le biais d'appartenances à des groupes, supprimez l'utilisateur de tous les groupes et de toutes les attributions directes d'ensembles d'autorisations. Cette étape empêche l'utilisateur d'assumer des rôles IAM supplémentaires. Si un utilisateur possède une session active sur le portail d'AWS accès et que vous le désactivez, il peut continuer à assumer de nouveaux rôles jusqu'à ce que vous supprimiez son accès.
4. Si vous utilisez un fournisseur d'identité (IdP) ou Microsoft Active Directory comme source d'identité, désactivez l'utilisateur dans la source d'identité. La désactivation de l'utilisateur

empêche la création de sessions supplémentaires sur le portail AWS d'accès. Utilisez la documentation de votre IdP ou de l'API Microsoft Active Directory pour savoir comment automatiser cette étape. Si vous utilisez le répertoire IAM Identity Center comme source d'identité, ne désactivez pas encore l'accès des utilisateurs. Vous allez désactiver l'accès des utilisateurs à l'étape 6.

5. Dans la console IAM Identity Center, recherchez l'utilisateur et supprimez sa session active.
 - a. Choisissez Utilisateurs.
 - b. Choisissez l'utilisateur dont vous souhaitez supprimer la session active.
 - c. Sur la page détaillée de l'utilisateur, choisissez l'onglet Sessions actives.
 - d. Cochez les cases à côté des sessions que vous souhaitez supprimer et choisissez Supprimer la session.

Après avoir supprimé une session utilisateur, l'utilisateur perd immédiatement l'accès au portail AWS d'accès. En savoir plus sur [la durée des sessions](#).

6. Dans la console IAM Identity Center, désactivez l'accès des utilisateurs.
 - a. Choisissez Utilisateurs.
 - b. Choisissez l'utilisateur dont vous souhaitez désactiver l'accès.
 - c. Sur la page détaillée de l'utilisateur, développez Informations générales et cliquez sur le bouton Désactiver l'accès utilisateur pour empêcher toute nouvelle connexion de l'utilisateur.
7. Laissez la politique de refus en place pendant au moins 12 heures. Dans le cas contraire, l'utilisateur disposant d'une session de rôle IAM active aura restauré les actions avec le rôle IAM. Si vous attendez 12 heures, les sessions actives expirent et l'utilisateur ne pourra plus accéder au rôle IAM.

Important

Si vous désactivez l'accès d'un utilisateur avant d'arrêter la session utilisateur (vous avez effectué l'étape 6 sans terminer l'étape 5), vous ne pouvez plus arrêter la session utilisateur via la console IAM Identity Center. Si vous désactivez par inadvertance l'accès utilisateur avant d'arrêter la session utilisateur, vous pouvez réactiver l'utilisateur, arrêter sa session, puis désactiver à nouveau son accès.

Vous pouvez désormais modifier les informations d'identification de l'utilisateur si son mot de passe a été compromis et [rétablir ses attributions](#).

Déléguer les personnes habilitées à attribuer un accès d'authentification unique aux utilisateurs et aux groupes du compte de gestion

L'attribution d'un accès d'authentification unique au compte de gestion à l'aide de la console IAM Identity Center est une action privilégiée. Par défaut, seul un Utilisateur racine d'un compte AWS ou un utilisateur auquel `AWSSSOMasterAccountAdministrator` les politiques `IAMFullAccess AWS` gérées sont associées peut attribuer un accès par authentification unique au compte de gestion. Les `IAMFullAccess` politiques `AWSSSOMasterAccountAdministrator` et gèrent l'accès par authentification unique au compte de gestion au sein d'une AWS Organizations organisation.

Vous pouvez également l'utiliser AWS CLI pour créer, associer des politiques et attribuer des ensembles d'autorisations. Voici la liste des commandes pour chaque étape :

- Pour créer un ensemble d'autorisations : [create-permission-set](#)
- Pour attacher AWS Managed Policy à un ensemble d'autorisations : [attach-managed-policy-to-permission-set](#)
- Pour associer une politique gérée par le client à un ensemble d'autorisations : [attach-customer-managed-policy-to-permission-set](#)
- Pour attribuer un ensemble d'autorisations à un directeur : [create-account-assignment](#)

Suivez les étapes ci-dessous pour déléguer des autorisations afin de gérer l'accès par authentification unique aux utilisateurs et aux groupes de votre annuaire.

Pour accorder des autorisations permettant de gérer l'accès par authentification unique aux utilisateurs et aux groupes de votre annuaire

1. Connectez-vous à la console IAM Identity Center en tant qu'utilisateur root du compte de gestion ou avec un autre utilisateur disposant d'autorisations d'administrateur sur le compte de gestion.
2. Suivez les étapes décrites [Crée un jeu d'autorisations](#) pour créer un ensemble d'autorisations, puis procédez comme suit :
 1. Sur la page Créer un nouvel ensemble d'autorisations, cochez la case Créer un ensemble d'autorisations personnalisé, puis choisissez Suivant : Détails.

2. Sur la page Créer un nouvel ensemble d'autorisations, spécifiez un nom pour le jeu d'autorisations personnalisé et éventuellement une description. Si nécessaire, modifiez la durée de la session et spécifiez l'URL de l'état du relais.

 Note

Pour l'URL de l'état du relais, vous devez spécifier une URL qui se trouve dans le AWS Management Console. Par exemple :

`https://console.aws.amazon.com/ec2/`

Pour de plus amples informations, veuillez consulter [Réglez l'état du relais pour un accès rapide au AWS Management Console](#).

3. Sous Quelles politiques souhaitez-vous inclure dans votre ensemble d'autorisations ? , cochez la case Joindre les politiques AWS gérées.
 4. Dans la liste des politiques IAM, sélectionnez à la fois les politiques AWSSSOMasterAccountAdministratore et les politiques IAMFullAccess AWS gérées. Ces politiques accordent des autorisations à tous les utilisateurs et groupes auxquels l'accès à cet ensemble d'autorisations sera attribué à l'avenir.
 5. Choisissez Suivant : Balises.
 6. Sous Ajouter des balises (facultatif), spécifiez les valeurs de clé et de valeur (facultatif), puis choisissez Suivant : Révision. Pour en savoir plus sur les identifications, consultez [Ressources de balisage AWS IAM Identity Center](#).
 7. Passez en revue les sélections que vous avez effectuées, puis choisissez Créer.
3. Suivez les étapes décrites [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#) pour attribuer les utilisateurs et les groupes appropriés à l'ensemble d'autorisations que vous venez de créer.
 4. Communiquez ce qui suit aux utilisateurs assignés : Lorsqu'ils se connectent au portail AWS d'accès et choisissent l'onglet Comptes, ils doivent choisir le nom de rôle approprié pour être authentifiés avec les autorisations que vous venez de déléguer.

Gérer Comptes AWS avec des ensembles d'autorisations

Un ensemble d'autorisations est un modèle que vous créez et gérez qui définit un ensemble d'une ou plusieurs [politiques IAM](#). Les ensembles d'autorisations simplifient l'attribution des Compte AWS accès aux utilisateurs et aux groupes de votre organisation. Par exemple, vous

pouvez créer un ensemble d'autorisations d'administrateur de base de données qui inclut des politiques d'administration des services AWS RDS, DynamoDB et Aurora, et utiliser cet ensemble d'autorisations unique pour accorder l'accès à une liste de cibles [AWS au sein](#) de votre organisation à vos administrateurs Comptes AWS de base de données.

IAM Identity Center attribue l'accès à un utilisateur ou à un groupe dans un ou plusieurs ensembles Comptes AWS d'autorisations. Lorsque vous attribuez un ensemble d'autorisations, IAM Identity Center crée les rôles IAM contrôlés par IAM Identity Center correspondants dans chaque compte et associe les politiques spécifiées dans le jeu d'autorisations à ces rôles. IAM Identity Center gère le rôle et permet aux utilisateurs autorisés que vous avez définis d'assumer ce rôle à l'aide du portail utilisateur ou de la CLI AWS d'IAM Identity Center. Lorsque vous modifiez l'ensemble d'autorisations, IAM Identity Center veille à ce que les politiques et rôles IAM correspondants soient mis à jour en conséquence.

Vous pouvez ajouter des [politiques AWS gérées](#), des [politiques gérées par le client](#), [des politiques intégrées](#) et des [politiques AWS gérées pour les fonctions professionnelles](#) à vos ensembles d'autorisations. Vous pouvez également attribuer une politique AWS gérée ou une politique gérée par le client comme [limite d'autorisation](#).

Pour créer un ensemble d'autorisations, voir [Création, gestion et suppression des jeux d'autorisations](#).

Créez un ensemble d'autorisations qui applique les autorisations du moindre privilège

Pour suivre la meilleure pratique consistant à appliquer des autorisations de moindre privilège, après avoir créé un ensemble d'autorisations administratives, vous créez un ensemble d'autorisations plus restrictif et vous l'attribuez à un ou plusieurs utilisateurs. Les ensembles d'autorisations créés lors de la procédure précédente constituent un point de départ pour évaluer le niveau d'accès aux ressources dont vos utilisateurs ont besoin. Pour passer aux autorisations du moindre privilège, vous pouvez exécuter IAM Access Analyzer pour surveiller les principaux à l'aide AWS de politiques gérées. Lorsque vous savez quelles autorisations ils utilisent, vous pouvez écrire une politique personnalisée ou générer une politique avec uniquement les autorisations requises pour votre équipe.

Avec IAM Identity Center, vous pouvez attribuer plusieurs ensembles d'autorisations au même utilisateur. Votre utilisateur administratif doit également se voir attribuer des ensembles d'autorisations supplémentaires, plus restrictifs. De cette façon, ils peuvent accéder à vous uniquement Compte AWS avec les autorisations requises, au lieu de toujours utiliser leurs autorisations administratives.

Par exemple, si vous êtes développeur, après avoir créé votre utilisateur administratif dans IAM Identity Center, vous pouvez créer un nouvel ensemble d'autorisations qui octroie des `PowerUserAccess` autorisations, puis vous attribuer cet ensemble d'autorisations. Contrairement à l'ensemble d'autorisations administratives, qui utilise des `AdministratorAccess` autorisations, le jeu `PowerUserAccess` d'autorisations ne permet pas la gestion des utilisateurs et des groupes IAM. Lorsque vous vous connectez au portail AWS d'accès pour accéder à votre AWS compte, vous pouvez choisir d'effectuer des tâches de développement dans le compte `PowerUserAccess` plutôt que de le `AdministratorAccess` faire.

Gardez les considérations suivantes à l'esprit :

- Pour commencer rapidement à créer un ensemble d'autorisations plus restrictif, utilisez un ensemble d'autorisations prédéfini plutôt qu'un ensemble d'autorisations personnalisé.

Avec un ensemble d'autorisations prédéfini, qui utilise [des autorisations prédéfinies](#), vous choisissez une seule politique AWS gérée parmi la liste des politiques disponibles. Chaque politique accorde un niveau spécifique d'accès aux AWS services et aux ressources ou des autorisations pour une fonction professionnelle commune. Pour plus d'informations sur chacune de ces politiques, consultez la section [Politiques AWS gérées pour les fonctions de travail](#).

- Vous pouvez configurer la durée de session pour un ensemble d'autorisations afin de contrôler la durée pendant laquelle un utilisateur est connecté à un Compte AWS.

Lorsque les utilisateurs se fédèrent dans leur Compte AWS et utilisent la console de AWS gestion ou l'interface de ligne de AWS commande (AWS CLI), IAM Identity Center utilise le paramètre de durée de session indiqué dans le jeu d'autorisations pour contrôler la durée de la session. Par défaut, la valeur de la durée de session, qui détermine la durée pendant laquelle un utilisateur peut être connecté au Compte AWS avant AWS de le déconnecter de la session, est définie sur une heure. Vous pouvez spécifier une valeur maximale de 12 heures. Pour de plus amples informations, veuillez consulter [Définissez la durée de session pour Comptes AWS](#).

- Vous pouvez également configurer la durée de session du portail d' AWS accès pour contrôler la durée pendant laquelle un utilisateur du personnel est connecté au portail.

Par défaut, la valeur de la durée maximale de session, qui détermine la durée pendant laquelle un utilisateur du personnel peut se connecter au portail d' AWS accès avant de devoir s'authentifier à nouveau, est de huit heures. Vous pouvez spécifier une valeur maximale de 90 jours. Pour de plus amples informations, veuillez consulter [Configuration de la durée de session dans IAM Identity Center](#).

- Lorsque vous vous connectez au portail AWS d'accès, choisissez le rôle qui fournit les autorisations les moins privilégiées.

Chaque ensemble d'autorisations que vous créez et attribuez à votre utilisateur apparaît comme un rôle disponible dans le portail AWS d'accès. Lorsque vous vous connectez au portail en tant qu'utilisateur, choisissez le rôle qui correspond à l'ensemble d'autorisations le plus restrictif que vous pouvez utiliser pour effectuer des tâches dans le compte, plutôt que `AdministratorAccess`.

- Vous pouvez ajouter d'autres utilisateurs à IAM Identity Center et leur attribuer des ensembles d'autorisations existants ou nouveaux.

Pour plus d'informations, voir, [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).

Rubriques

- [Autorisations prédéfinies pour les politiques AWS gérées](#)
- [Autorisations personnalisées pour les politiques AWS gérées et gérées par le client](#)
- [Création, gestion et suppression des jeux d'autorisations](#)
- [Configurer les propriétés des ensembles d'autorisations](#)

Autorisations prédéfinies pour les politiques AWS gérées

Vous pouvez créer un ensemble d'autorisations prédéfini avec des politiques AWS gérées.

Lorsque vous créez un ensemble d'autorisations avec des autorisations prédéfinies, vous choisissez une politique dans une liste de politiques AWS gérées. Parmi les politiques disponibles, vous pouvez choisir entre les politiques d'autorisation communes et les politiques relatives aux fonctions Job.

Politiques d'autorisation communes

Choisissez parmi une liste de politiques AWS gérées qui vous permettent d'accéder aux ressources dans votre intégralité Compte AWS. Vous pouvez ajouter l'une des politiques suivantes :

- `AdministratorAccess`
- `PowerUserAccess`
- `ReadOnlyAccess`

- ViewOnlyAccess

Politiques relatives aux fonctions professionnelles

Choisissez parmi une liste de politiques AWS gérées qui permettent d'accéder aux ressources de votre organisation Compte AWS susceptibles d'être pertinentes pour un poste au sein de votre organisation. Vous pouvez ajouter l'une des politiques suivantes :

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Pour une description détaillée des politiques d'autorisation communes et des politiques relatives aux fonctions professionnelles disponibles, voir [les politiques AWS gérées pour les fonctions professionnelles](#) dans le guide de Gestion des identités et des accès AWS l'utilisateur.

Pour obtenir des instructions sur la création d'un ensemble d'autorisations, consultez [Création, gestion et suppression des jeux d'autorisations](#).

Autorisations personnalisées pour les politiques AWS gérées et gérées par le client

Vous pouvez créer un ensemble d'autorisations avec des autorisations personnalisées, en combinant toutes les politiques AWS gérées et gérées par le client que vous avez dans Gestion des identités et des accès AWS (IAM) avec des politiques intégrées. Vous pouvez également inclure une limite d'autorisations, en définissant le maximum d'autorisations que les autres politiques peuvent accorder aux utilisateurs de votre ensemble d'autorisations.

Pour obtenir des instructions sur la création d'un ensemble d'autorisations, consultez [Création, gestion et suppression des jeux d'autorisations](#).

Types de politiques que vous pouvez associer à votre ensemble d'autorisations

Rubriques

- [Politiques en ligne](#)
- [AWS politiques gérées](#)
- [Politiques gérées par le client](#)
- [Limites d'autorisations](#)

Politiques en ligne

Vous pouvez associer une politique intégrée à un ensemble d'autorisations. Une politique intégrée est un bloc de texte formaté comme une politique IAM que vous ajoutez directement à votre ensemble d'autorisations. Vous pouvez coller une politique ou en générer une nouvelle à l'aide de l'outil de création de politiques de la console IAM Identity Center lorsque vous créez un nouvel ensemble d'autorisations. Vous pouvez également créer des politiques IAM à l'aide du [générateur AWS de politiques](#).

Lorsque vous déployez un ensemble d'autorisations avec une politique intégrée, IAM Identity Center crée une stratégie IAM à l'endroit où vous attribuez votre ensemble d'autorisations. IAM Identity Center crée la politique lorsque vous attribuez l'ensemble d'autorisations au compte. La politique est ensuite attachée au rôle IAM Compte AWS que votre utilisateur assume dans votre entreprise.

Lorsque vous créez une politique intégrée et que vous attribuez votre ensemble d'autorisations, IAM Identity Center configure les politiques qui s'y trouvent pour vos Comptes AWS. Lorsque vous créez votre ensemble d'autorisations avec [Politiques gérées par le client](#), vous devez créer Comptes AWS vous-même les politiques avant d'attribuer l'ensemble d'autorisations.

AWS politiques gérées

Vous pouvez associer des politiques AWS gérées à votre ensemble d'autorisations. AWS les politiques gérées sont des politiques IAM qui AWS maintiennent. En revanche, [Politiques gérées par le client](#) les politiques IAM de votre compte sont-elles créées et mises à jour ? AWS les politiques gérées répondent aux cas courants d'utilisation du moindre privilège dans votre Compte AWS. Vous pouvez attribuer une politique AWS gérée en tant qu'autorisations pour le rôle créé par IAM Identity Center ou en tant que [limite d'autorisations](#).

AWS maintient des [politiques AWS gérées pour les fonctions professionnelles](#) qui attribuent des autorisations d'accès spécifiques à la tâche à vos AWS ressources. Vous pouvez ajouter une politique de fonction professionnelle lorsque vous choisissez d'utiliser des autorisations prédéfinies

avec votre ensemble d'autorisations. Lorsque vous choisissez Autorisations personnalisées, vous pouvez ajouter plusieurs règles relatives aux fonctions professionnelles.

Vous contient Compte AWS également un grand nombre de politiques IAM AWS gérées pour des raisons spécifiques Services AWS et combinées de Services AWS. Lorsque vous créez un ensemble d'autorisations avec des autorisations personnalisées, vous pouvez choisir parmi de nombreuses politiques AWS gérées supplémentaires à attribuer à votre ensemble d'autorisations.

AWS remplit chacun d'entre eux Compte AWS avec des politiques AWS gérées. Pour déployer un ensemble d'autorisations avec des politiques AWS gérées, il n'est pas nécessaire de créer au préalable une politique dans votre Comptes AWS. Lorsque vous créez votre ensemble d'autorisations avec [Politiques gérées par le client](#), vous devez créer Comptes AWS vous-même les politiques avant d'attribuer l'ensemble d'autorisations.

Pour plus d'informations sur les politiques AWS gérées, voir les [politiques AWS gérées](#) dans le guide de l'utilisateur IAM.

Politiques gérées par le client

Vous pouvez associer des politiques gérées par le client à votre ensemble d'autorisations. Les politiques gérées par le client sont des politiques IAM de votre compte que vous créez et gérez. En revanche, [AWS politiques gérées](#) les politiques IAM de votre compte sont-elles AWS maintenues ? Vous pouvez attribuer une politique gérée par le client en tant qu'autorisations pour le rôle créé par IAM Identity Center ou en tant que [limite d'autorisations](#).

Lorsque vous créez un ensemble d'autorisations avec une politique gérée par le client, vous devez créer une stratégie IAM portant le même nom et le même chemin dans chaque Compte AWS cas où IAM Identity Center attribue votre ensemble d'autorisations. Si vous spécifiez un chemin personnalisé, assurez-vous de spécifier le même chemin pour chacun d'entre eux Compte AWS. Pour plus d'informations, consultez [Noms conviviaux et chemins](#) dans le Guide de l'utilisateur IAM. IAM Identity Center attache la politique IAM au rôle IAM qu'il crée dans votre. Compte AWS Il est recommandé d'appliquer les mêmes autorisations à la politique dans chaque compte auquel vous attribuez l'ensemble d'autorisations. Pour de plus amples informations, veuillez consulter [Utiliser les politiques IAM dans les ensembles d'autorisations](#).

Note

Lorsqu'une politique gérée par le client est associée à un ensemble d'autorisations, le nom de la politique ne distingue pas les majuscules et minuscules.

Pour plus d'informations, consultez la section [Politiques gérées par le client](#) dans le guide de l'utilisateur IAM.

Limites d'autorisations

Vous pouvez associer une limite d'autorisations à votre ensemble d'autorisations. Une limite d'autorisations est une politique IAM AWS gérée ou gérée par le client qui définit le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à un principal IAM. Lorsque vous appliquez une limite d'autorisations [Politiques en ligne](#)[Politiques gérées par le client](#), vous [AWS politiques gérées](#) ne pouvez pas accorder d'autorisations dépassant les autorisations accordées par votre limite d'autorisations. Une limite d'autorisations n'accorde aucune autorisation, mais fait en sorte qu'IAM ignore toutes les autorisations au-delà de cette limite.

Lorsque vous créez un ensemble d'autorisations avec une politique gérée par le client comme limite d'autorisations, vous devez créer une politique IAM portant le même nom dans chaque Compte AWS cas où IAM Identity Center attribue votre ensemble d'autorisations. IAM Identity Center associe la politique IAM en tant que limite d'autorisation au rôle IAM qu'il crée dans votre. Compte AWS

Pour plus d'informations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.

Création, gestion et suppression des jeux d'autorisations

Les ensembles d'autorisations définissent le niveau d'accès des utilisateurs et des groupes à un Compte AWS. Les ensembles d'autorisations sont stockés dans IAM Identity Center et peuvent être fournis à une ou plusieurs personnes. Comptes AWS Vous pouvez attribuer plus d'un jeu d'autorisations à un utilisateur. Pour plus d'informations sur les ensembles d'autorisations et leur utilisation dans IAM Identity Center, consultez [Gérer Comptes AWS avec des ensembles d'autorisations](#).

Note

Vous pouvez rechercher et trier les ensembles d'autorisations par nom dans la console IAM Identity Center.

Tenez compte des considérations suivantes lors de la création d'ensembles d'autorisations :

- Instance d'organisation

Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

- Commencez avec un ensemble d'autorisations prédéfini

Avec un ensemble d'autorisations prédéfini, qui utilise [des autorisations prédéfinies](#), vous choisissez une seule politique AWS gérée parmi la liste des politiques disponibles. Chaque politique accorde un niveau spécifique d'accès aux AWS services et aux ressources ou des autorisations pour une fonction professionnelle commune. Pour plus d'informations sur chacune de ces politiques, consultez la section [Politiques AWS gérées pour les fonctions de travail](#). Après avoir collecté les données d'utilisation, vous pouvez affiner l'ensemble d'autorisations pour le rendre plus restrictif.

- Limiter la durée des sessions de gestion à des périodes de travail raisonnables

Lorsque les utilisateurs se fédèrent dans leur interface de ligne de commande (CLI) Compte AWS et utilisent l' AWS Management Console interface de ligne de commande (AWS CLI), IAM Identity Center utilise le paramètre de durée de session indiqué dans le jeu d'autorisations pour contrôler la durée de la session. Lorsque la session utilisateur atteint sa durée de session, il est déconnecté de la console et invité à se reconnecter. Comme bonne pratique de sécurité, nous vous recommandons de ne pas définir une durée de la session plus longue que ce qui est nécessaire pour exécuter le rôle. Par défaut, la valeur de la durée de session est d'une heure. Vous pouvez spécifier une valeur maximale de 12 heures. Pour de plus amples informations, veuillez consulter [Définissez la durée de session pour Comptes AWS](#).

- Limiter la durée de session du portail utilisateur du personnel

Les utilisateurs du personnel utilisent les sessions du portail pour choisir les rôles et accéder aux applications. Par défaut, la valeur de la durée maximale de session, qui détermine la durée pendant laquelle un utilisateur du personnel peut se connecter au portail d' AWS accès avant de devoir s'authentifier à nouveau, est de huit heures. Vous pouvez spécifier une valeur maximale de 90 jours. Pour de plus amples informations, veuillez consulter [Configuration de la durée de session dans IAM Identity Center](#).

- Utiliser le rôle qui fournit les autorisations de moindre privilège

Chaque ensemble d'autorisations que vous créez et attribuez à votre utilisateur apparaît comme un rôle disponible dans le portail AWS d'accès. Lorsque vous vous connectez au portail en tant qu'utilisateur, choisissez le rôle qui correspond à l'ensemble d'autorisations

le plus restrictif que vous pouvez utiliser pour effectuer des tâches dans le compte, plutôt que `AdministratorAccess`. Testez vos ensembles d'autorisations pour vérifier qu'ils fournissent l'accès nécessaire avant d'envoyer l'invitation à l'utilisateur.

Note

Vous pouvez également l'utiliser [AWS CloudFormation](#) pour créer et attribuer des ensembles d'autorisations et attribuer des utilisateurs à ces ensembles d'autorisations.

Rubriques

- [Crée un jeu d'autorisations](#)
- [Afficher et modifier un ensemble d'autorisations](#)
- [Déléguer l'administration des ensembles d'autorisations](#)
- [Utiliser les politiques IAM dans les ensembles d'autorisations](#)
- [Supprimer des ensembles d'autorisations dans IAM Identity Center](#)
- [Supprimer des ensembles d'autorisations dans IAM Identity Center](#)

Crée un jeu d'autorisations

Utilisez cette procédure pour créer un ensemble d'autorisations prédéfini qui utilise une seule politique AWS gérée, ou un ensemble d'autorisations personnalisé qui utilise jusqu'à 10 politiques AWS gérées ou gérées par le client et une politique intégrée. Vous pouvez demander un ajustement du nombre maximum de 10 politiques dans la [console Service Quotas](#) pour IAM. Vous pouvez créer un ensemble d'autorisations dans la console IAM Identity Center.

Note

Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Pour créer un jeu d'autorisations

1. Ouvrez la [console IAM Identity Center](#).

2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez Create permission set (Créer un jeu d'autorisations).
4. Sur la page Sélectionner le type d'ensemble d'autorisations, sous Type d'ensemble d'autorisations, sélectionnez un type d'ensemble d'autorisations.
5. Choisissez une ou plusieurs politiques que vous souhaitez utiliser pour l'ensemble d'autorisations, en fonction du type d'ensemble d'autorisations :
 - Ensemble d'autorisations prédéfini
 1. Sous Politique pour un ensemble d'autorisations prédéfini, sélectionnez l'une des politiques de fonction IAM Job ou des politiques d'autorisation communes dans la liste, puis choisissez Next. Pour plus d'informations, consultez les [politiques AWS gérées pour les fonctions de travail](#) et [les politiques AWS gérées](#) dans le Guide de Gestion des identités et des accès AWS l'utilisateur.
 2. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.
 - Ensemble d'autorisations personnalisé
 1. Choisissez Suivant.
 2. Sur la page Spécifier les politiques et les limites d'autorisation, choisissez les types de politiques IAM que vous souhaitez appliquer à votre nouvel ensemble d'autorisations. Par défaut, vous pouvez ajouter n'importe quelle combinaison d'un maximum de 10 politiques AWS gérées et de politiques gérées par le client à votre ensemble d'autorisations. Ce quota est défini par IAM. Pour l'augmenter, demandez une augmentation du quota IAM. Les politiques gérées associées à un rôle IAM sont associées à un rôle IAM dans la console Service Quotas dans chaque instance à Compte AWS laquelle vous souhaitez attribuer l'ensemble d'autorisations.
 - Développez les politiques AWS gérées pour ajouter des politiques issues d'IAM qui AWS créent et gèrent. Pour de plus amples informations, veuillez consulter [AWS politiques gérées](#).
 - a. Recherchez et choisissez les politiques AWS gérées que vous souhaitez appliquer à vos utilisateurs dans l'ensemble d'autorisations.
 - b. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

- Développez les politiques gérées par le client pour ajouter des politiques IAM que vous créez et gérez. Pour de plus amples informations, veuillez consulter [Politiques gérées par le client](#).
 - a. Choisissez Joindre des politiques et entrez le nom de la politique que vous souhaitez ajouter à votre ensemble d'autorisations. Dans chaque compte auquel vous souhaitez attribuer l'ensemble d'autorisations, créez une politique portant le nom que vous avez saisi. Il est recommandé d'attribuer les mêmes autorisations à la politique dans chaque compte.
 - b. Choisissez Attacher plus pour ajouter une autre politique.
 - c. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.
- Développez la politique intégrée pour ajouter un texte de politique personnalisé au format JSON. Les politiques intégrées ne correspondent pas aux ressources IAM existantes. Pour créer une politique intégrée, entrez un langage de politique personnalisé dans le formulaire fourni. IAM Identity Center ajoute la politique aux ressources IAM qu'il crée dans vos comptes de membres. Pour de plus amples informations, veuillez consulter [Politiques en ligne](#).
 - a. Ajoutez les actions et les ressources souhaitées dans l'éditeur interactif à votre politique intégrée. Des déclarations supplémentaires peuvent être ajoutées à l'aide de l'option Ajouter une nouvelle déclaration.
 - b. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.
- Élargissez la limite des autorisations pour ajouter une politique IAM AWS gérée ou gérée par le client en tant qu'autorisations maximales que vos autres politiques de l'ensemble d'autorisations peuvent attribuer. Pour de plus amples informations, veuillez consulter [Limites d'autorisations](#).
 - a. Choisissez Utiliser une limite d'autorisations pour contrôler le maximum d'autorisations.
 - b. Choisissez une politique AWS gérée pour définir une politique d'IAM qui AWS crée et gère comme limite d'autorisations. Choisissez les politiques gérées par le client

pour définir une politique à partir d'IAM que vous créez et gérez comme limite d'autorisations.

- c. Si vous souhaitez ajouter un autre type de politique, choisissez son conteneur et effectuez votre sélection. Choisissez Next lorsque vous avez sélectionné toutes les politiques que vous souhaitez appliquer. Passez à l'étape 6 pour terminer la page de détails de l'ensemble d'autorisations.

6. Sur la page Spécifier les détails de l'ensemble d'autorisations, procédez comme suit :

1. Sous Nom de l'ensemble d'autorisations, tapez un nom pour identifier cet ensemble d'autorisations dans IAM Identity Center. Le nom que vous spécifiez pour cet ensemble d'autorisations apparaît dans le portail AWS d'accès en tant que rôle disponible. Les utilisateurs se connectent AWS au portail d'accès Compte AWS, choisissent un, puis le rôle.

 Note

Les noms des ensembles d'autorisations doivent être uniques au sein de votre instance IAM Identity Center.

2. (Facultatif) Vous pouvez également saisir une description. La description apparaît uniquement dans la console IAM Identity Center, et non dans le portail AWS d'accès.
3. (Facultatif) Spécifiez la valeur de la durée de la session. Cette valeur détermine la durée pendant laquelle un utilisateur peut être connecté avant que la console ne le déconnecte de sa session. Pour de plus amples informations, veuillez consulter [Définissez la durée de session pour Comptes AWS](#).
4. (Facultatif) Spécifiez la valeur de l'état du relais. Cette valeur est utilisée dans le processus de fédération pour rediriger les utilisateurs au sein du compte. Pour de plus amples informations, veuillez consulter [Réglez l'état du relais pour un accès rapide au AWS Management Console](#).

 Note

L'URL de l'état du relais doit se trouver dans le AWS Management Console. Par exemple :

`https://console.aws.amazon.com/ec2/`

5. Développez les balises (facultatif), choisissez Ajouter une balise, puis spécifiez les valeurs de clé et de valeur (facultatif).

Pour plus d'informations sur les balises, consultez [Ressources de balisage AWS IAM Identity Center](#).

6. Choisissez Suivant.
7. Sur la page Réviser et créer, passez en revue les sélections que vous avez effectuées, puis choisissez Créer.
8. Par défaut, lorsque vous créez un ensemble d'autorisations, celui-ci n'est pas provisionné (utilisé dans aucun d'entre eux Comptes AWS). Pour attribuer un ensemble d'autorisations dans un Compte AWS, vous devez attribuer l'accès à IAM Identity Center aux utilisateurs et aux groupes du compte, puis appliquer l'ensemble d'autorisations à ces utilisateurs et groupes. Pour de plus amples informations, veuillez consulter [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).

Afficher et modifier un ensemble d'autorisations

Vous pouvez utiliser des ensembles d'autorisations pour accorder aux utilisateurs l'accès à Comptes AWS. Vous pouvez consulter et modifier un ensemble d'autorisations à l'aide de la AWS IAM Identity Center console. Vous pouvez rechercher et trier les ensembles d'autorisations par nom dans la console IAM Identity Center. Pour plus d'informations sur les ensembles d'autorisations et leur utilisation dans IAM Identity Center, consultez [the section called “Ensembles d'autorisations”](#).

Les ensembles d'autorisations ne sont pas nécessaires pour gérer l'accès des utilisateurs aux applications.

Note

Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Afficher les attributions des ensembles d'autorisations

Utilisez cette procédure pour afficher l'ensemble d'autorisations appliqué dans la AWS IAM Identity Center console.

All Comptes AWS where a permission set is provisioned

Pour afficher toutes les attributions d'un ensemble d'autorisations, procédez comme suit :

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Sur la page Ensembles d'autorisations, sélectionnez l'ensemble d'autorisations que vous souhaitez consulter.
4. Une fois sur la page des ensembles d'autorisations sélectionnés, sous l'onglet Comptes, vous pouvez voir les comptes sur lesquels l'ensemble d'autorisations est utilisé. Vous pouvez sélectionner le compte pour voir comment l'ensemble d'autorisations est fourni au sein du compte. Vous pouvez [supprimer](#), modifier et associer des politiques à l'ensemble d'autorisations.

All permission sets for an Compte AWS

Pour afficher toutes les attributions d'un ensemble d'autorisations, procédez comme suit :

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Sous Autorisations multi-comptes, sélectionnez Comptes AWS. Sélectionnez le compte pour lequel vous souhaitez consulter les ensembles d'autorisations fournis.
3. Une fois sur la Compte AWS page sélectionnée, sous l'onglet Ensembles d'autorisations, vous pouvez consulter les différents ensembles d'autorisations attribués à la personne sélectionnée Compte AWS. Vous pouvez sélectionner le lien hypertexte de l'ensemble d'autorisations pour en savoir plus sur l'ensemble d'autorisations.

All applied permission sets to users and groups

Pour afficher tous les ensembles d'autorisations attribués aux utilisateurs ou aux groupes, procédez comme suit :

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Sélectionnez Utilisateurs ou Groupes sous Tableau de bord pour afficher les utilisateurs ou les groupes d'IAM Identity Center.
 - a. Une fois sur la page Utilisateurs, sélectionnez l'utilisateur pour lequel vous souhaitez voir les ensembles d'autorisations appliqués. Ensuite, sélectionnez l'Comptes AWSonglet et

Compte AWS sous la section d'accès au AWS compte. Vous pourrez voir les ensembles d'autorisations appliqués et Compte AWS pour l'utilisateur sélectionné.

- b. Une fois sur la page Groupes, sélectionnez le groupe auquel vous souhaitez voir les ensembles d'autorisations appliqués. Ensuite, sélectionnez l'Comptes AWSonglet et Compte AWS sous la section Compte AWS d'accès. Vous pourrez voir les ensembles d'autorisations appliqués et Compte AWS pour le groupe sélectionné.

Modifier un ensemble d'autorisations

Utilisez cette procédure pour modifier un [ensemble d'autorisations](#) à l'aide de la console IAM Identity Center. Vous pouvez ajouter ou supprimer des ensembles d'autorisations pour des utilisateurs ou des groupes.

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Sous Autorisations multi-comptes, sélectionnez Comptes AWS.
3. Sur la Compte AWSpage, une liste arborescente de votre organisation apparaît. Sélectionnez le nom du groupe d'autorisations Compte AWS à partir duquel vous souhaitez modifier l'ensemble d'autorisations.
4. Sur la page d'aperçu du Compte AWS, sous Utilisateurs et groupes assignés, sélectionnez le nom d'utilisateur ou le nom de groupe de l'ensemble d'autorisations que vous souhaitez modifier. Choisissez ensuite Modifier les ensembles d'autorisations.
5. Apportez les modifications souhaitées à l'ensemble d'autorisations, puis choisissez Enregistrer les modifications.
6. Accédez à l'onglet Ensembles d'autorisations, sélectionnez l'ensemble d'autorisations récemment modifié, puis choisissez Mettre à jour.
7. Sur la page Autorisations de mise à jour, choisissez Mettre à jour.

Déléguer l'administration des ensembles d'autorisations

IAM Identity Center vous permet de déléguer la gestion des ensembles d'autorisations et des attributions dans les comptes en créant des [politiques IAM qui font](#) référence aux [Amazon Resource Names \(ARNs\)](#) des ressources IAM Identity Center. Par exemple, vous pouvez créer des politiques qui permettent à différents administrateurs de gérer les attributions dans des comptes spécifiques pour des ensembles d'autorisations dotés de balises spécifiques.

 Note

Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

Vous pouvez utiliser l'une des méthodes suivantes pour créer ces types de politiques.

- (Recommandé) Créez des [ensembles d'autorisations](#) dans IAM Identity Center, chacun avec une politique différente, et attribuez les ensembles d'autorisations à différents utilisateurs ou groupes. Cela vous permet de gérer les autorisations administratives pour les utilisateurs qui se connectent à l'aide de la [source d'identité IAM Identity Center](#) que vous avez choisie.
- Créez des politiques personnalisées dans IAM, puis associez-les aux rôles IAM assumés par vos administrateurs. Pour plus d'informations sur les rôles, consultez la section [Rôles IAM](#) pour obtenir les autorisations administratives IAM Identity Center qui leur ont été attribuées.

 Important

Les ressources du IAM Identity Center distinguent ARNs les majuscules et minuscules.

Ce qui suit montre le cas approprié pour faire référence à l'ensemble d'autorisations IAM Identity Center et aux types de ressources du compte.

Types de ressources	ARN	Clés de contexte
PermissionSet	arn:\${Partition}:sso::permissionSet/\${InstanceId}/\${PermissionSetId}	aws:ResourceTag/\${TagKey}
Compte	arn:\${Partition}:sso::account/\${AccountId}	Non applicable

Utiliser les politiques IAM dans les ensembles d'autorisations

Dans [Crée un jeu d'autorisations](#), vous avez appris à ajouter des politiques, notamment des politiques gérées par le client et des limites d'autorisations, à un ensemble d'autorisations. Lorsque vous ajoutez des politiques et des autorisations gérées par le client à un ensemble d'autorisations, IAM Identity Center ne crée aucune Comptes AWS politique. Vous devez plutôt créer ces politiques à l'avance dans chaque compte auquel vous souhaitez attribuer votre ensemble d'autorisations, et les faire correspondre au nom et aux spécifications de chemin de votre ensemble d'autorisations. Lorsque vous attribuez un ensemble d'autorisations Compte AWS à un membre de votre organisation, IAM Identity Center crée un [rôle Gestion des identités et des accès AWS \(IAM\)](#) et associe vos [politiques IAM](#) à ce rôle.

Considérations

- Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).
- Avant d'attribuer votre ensemble d'autorisations aux politiques IAM, vous devez préparer votre compte de membre. Le nom d'une politique IAM dans votre compte membre doit correspondre au nom de la politique dans votre compte de gestion. IAM Identity Center ne parvient pas à attribuer l'ensemble d'autorisations si la politique n'existe pas dans votre compte de membre.

Note

Lorsqu'une politique gérée par le client est associée à un ensemble d'autorisations, le nom de la politique ne distingue pas les majuscules et minuscules.

- Les autorisations accordées par la politique ne doivent pas nécessairement correspondre exactement aux différents comptes.

Attribuer une politique IAM à un ensemble d'autorisations

1. Créez une politique IAM dans chacun des Comptes AWS endroits où vous souhaitez attribuer l'ensemble d'autorisations.
2. Attribuez des autorisations à la politique IAM. Vous pouvez attribuer différentes autorisations à différents comptes. Pour une expérience cohérente, configurez et maintenez des autorisations identiques dans chaque politique. Vous pouvez utiliser des ressources d'automatisation telles que AWS CloudFormation StackSets la création de copies d'une politique IAM portant le

même nom et les mêmes autorisations dans chaque compte membre. Pour plus d'informations CloudFormation StackSets, consultez la section [Travailler avec AWS CloudFormation StackSets](#) dans le guide de AWS CloudFormation l'utilisateur.

3. Créez un ensemble d'autorisations dans votre compte de gestion et ajoutez votre politique IAM sous Politiques gérées par le client ou Limite des autorisations. Pour plus de détails sur la création d'un ensemble d'autorisations, voir [Crée un jeu d'autorisations](#).
4. Ajoutez les politiques intégrées, les politiques AWS gérées ou les politiques IAM supplémentaires que vous avez préparées.
5. Créez et attribuez votre ensemble d'autorisations.

Supprimer des ensembles d'autorisations dans IAM Identity Center

Vous pouvez supprimer un ensemble d'autorisations pour les utilisateurs et les groupes IAM Identity Center dans la console IAM Identity Center. Vous pouvez également supprimer un ensemble d'autorisations d'un Compte AWS. Pour plus d'informations sur les ensembles d'autorisations et leur utilisation dans IAM Identity Center, consultez [Gérer Comptes AWS avec des ensembles d'autorisations](#).

Note

Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).

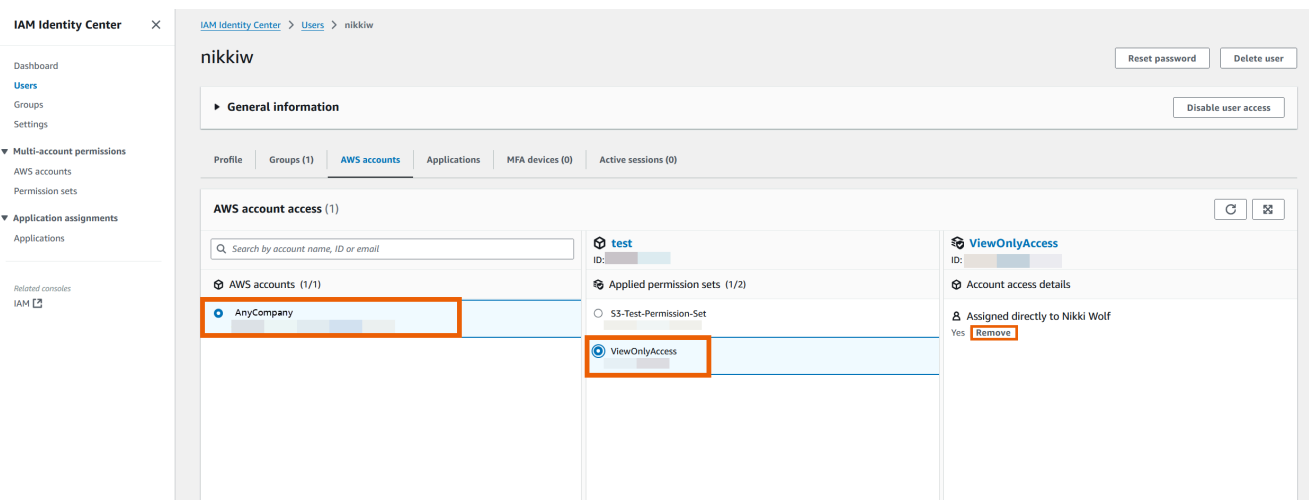
Remove permission set from a user

Supprimer un ensemble d'autorisations attribué à un utilisateur

Utilisez cette procédure pour supprimer un ensemble d'autorisations d'un utilisateur à l'aide de la console IAM Identity Center.

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Sous IAM Identity Center, sélectionnez Utilisateurs.
3. Sélectionnez le nom d'utilisateur de l'utilisateur dont vous souhaitez supprimer un ensemble d'autorisations.

- Sur la page des détails de l'utilisateur, sélectionnez l'onglet Comptes AWS. Sous Compte AWS Accès, sélectionnez votre Compte AWS.
- Dans le volet droit, les autorisations appliquées à l'utilisateur sélectionné apparaissent. Sélectionnez l'ensemble d'autorisations que vous souhaitez supprimer. Sous Détails d'accès au compte, sélectionnez Supprimer.
- Une boîte de dialogue s'affiche pour vous demander si vous souhaitez supprimer cet ensemble d'autorisations. Sélectionnez Remove (Retirer).

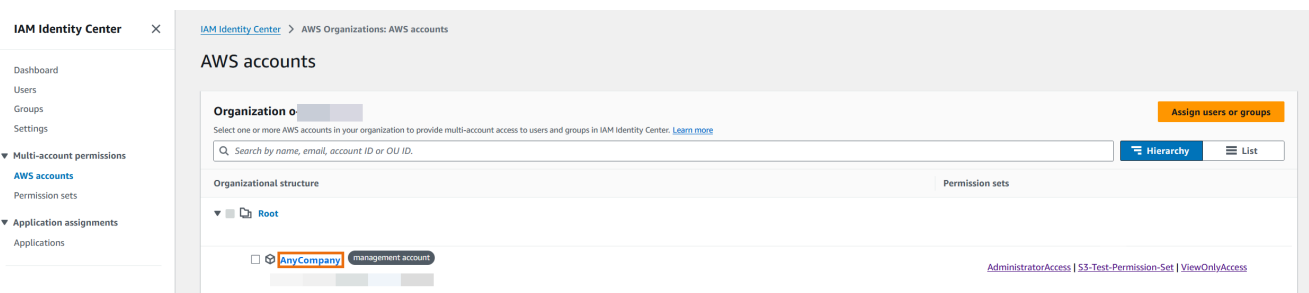


Remove permission set from a group

Supprimer un ensemble d'autorisations d'un groupe

Utilisez cette procédure pour supprimer un ensemble d'autorisations d'un groupe à l'aide de la console IAM Identity Center.

- Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
- Sous Autorisations multi-comptes, sélectionnez Comptes AWS. Sélectionnez le lien vers votre compte de gestion.



3. Sous l'onglet Utilisateurs et groupes assignés, sélectionnez le groupe dont vous souhaitez supprimer l'ensemble d'autorisations, puis sélectionnez Modifier le jeu d'autorisations.
4. Sur la page Modifier les ensembles d'autorisations, effacez le jeu d'autorisations que vous souhaitez supprimer, puis sélectionnez Enregistrer les modifications.

Remove permission set from an Compte AWS

Utilisez cette procédure pour supprimer un ensemble d'autorisations de la Compte AWS console IAM Identity Center.

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Sous Autorisations multi-comptes, sélectionnez Comptes AWS. Sélectionnez le nom du groupe Compte AWS d'autorisations dont vous souhaitez supprimer l'ensemble d'autorisations.
3. Sur la page Vue d'ensemble du Compte AWS, choisissez l'onglet Ensembles d'autorisations. Sélectionnez l'ensemble d'autorisations que vous souhaitez supprimer. Sélectionnez ensuite Supprimer.
4. Dans la boîte de dialogue Supprimer l'ensemble d'autorisations, vérifiez que le bon ensemble d'autorisations est sélectionné, tapez **Delete** pour confirmer la suppression, puis choisissez Supprimer l'accès.

Supprimer des ensembles d'autorisations dans IAM Identity Center

Avant de pouvoir supprimer un ensemble d'autorisations d'IAM Identity Center, vous devez le [supprimer](#) de tous Comptes AWS ceux qui l'utilisent. Pour vérifier l'accès des utilisateurs et des groupes existants, voir [Afficher et modifier un ensemble d'autorisations](#).

Considérations

- Pour utiliser des ensembles d'autorisations, vous devez utiliser une instance d'organisation d'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Instances d'organisation et de compte d'IAM Identity Center](#).
- Si vous souhaitez révoquer une session d'ensemble d'autorisations active, consultez [the section called "Mettre fin aux sessions actives pour les utilisateurs du personnel"](#).

- Vous devez supprimer les ensembles d'autorisations et les attributions d'applications des utilisateurs ou des groupes que vous souhaitez supprimer avant de les supprimer. Sinon, vous aurez des ensembles d'autorisations et des applications non attribués et non utilisés dans IAM Identity Center.

Suivez la procédure ci-dessous pour supprimer un ou plusieurs ensembles d'autorisations afin qu'aucun membre de l'organisation ne puisse plus Compte AWS les utiliser.

Important

Tous les utilisateurs et groupes auxquels cet ensemble d'autorisations a été attribué, quel que Compte AWS soit l'utilisateur qui l'utilise, ne pourront plus se connecter. Pour vérifier l'accès des utilisateurs et des groupes existants, voir [Afficher et modifier un ensemble d'autorisations](#).

Pour supprimer un ensemble d'autorisations d'un Compte AWS

1. Ouvrez la [console IAM Identity Center](#).
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Sélectionnez l'ensemble d'autorisations que vous souhaitez supprimer, puis choisissez Supprimer.
4. Dans la boîte de dialogue Supprimer l'ensemble d'autorisations, tapez le nom du jeu d'autorisations pour confirmer la suppression, puis choisissez Supprimer. Le nom est sensible à la casse.

Configurer les propriétés des ensembles d'autorisations

Dans IAM Identity Center, les administrateurs peuvent effectuer les tâches de configuration et de gestion suivantes pour contrôler l'accès des utilisateurs et la durée des sessions.

Sous-tâche	En savoir plus
Les administrateurs peuvent définir la durée maximale des sessions utilisateur lors de	Définissez la durée de session pour Comptes AWS

Sous-tâche	En savoir plus
l'accès aux AWS ressources via IAM Identity Center.	
Les administrateurs peuvent personnaliser la page de destination que les utilisateurs voient après s'être authentifiés avec succès via IAM Identity Center.	Réglez l'état du relais pour un accès rapide au AWS Management Console
Assurez-vous que les utilisateurs n'ont plus accès aux AWS ressources lorsque leurs autorisations sont révoquées.	Utiliser une politique de refus pour révoquer les autorisations des utilisateurs actifs

Définissez la durée de session pour Comptes AWS

Pour chaque [ensemble d'autorisations](#), vous pouvez spécifier une durée de session afin de contrôler la durée pendant laquelle un utilisateur peut être connecté à un Compte AWS. Lorsque la durée spécifiée est écoulée, AWS déconnecte l'utilisateur de la session.

Lorsque vous créez un nouvel ensemble d'autorisations, la durée de la session est fixée à 1 heure (en secondes) par défaut. La durée minimale de la session est d'une heure et peut être fixée à un maximum de 12 heures. IAM Identity Center crée automatiquement des rôles IAM dans chaque compte attribué pour chaque ensemble d'autorisations, et configure ces rôles avec une durée de session maximale de 12 heures.

Lorsque les utilisateurs se fédèrent dans leur Compte AWS console ou lorsque le AWS Command Line Interface (AWS CLI) est utilisé, IAM Identity Center utilise le paramètre de durée de session figurant sur le jeu d'autorisations pour contrôler la durée de la session. Par défaut, les rôles IAM générés par IAM Identity Center pour les ensembles d'autorisations ne peuvent être assumés que par les utilisateurs d'IAM Identity Center, ce qui garantit que la durée de session spécifiée dans le jeu d'autorisations IAM Identity Center est appliquée.

Important

Comme bonne pratique de sécurité, nous vous recommandons de ne pas définir une durée de la session plus longue que ce qui est nécessaire pour exécuter le rôle.

Après avoir créé un ensemble d'autorisations, vous pouvez le mettre à jour pour appliquer une nouvelle durée de session. Utilisez la procédure suivante pour modifier la durée de session d'un ensemble d'autorisations.

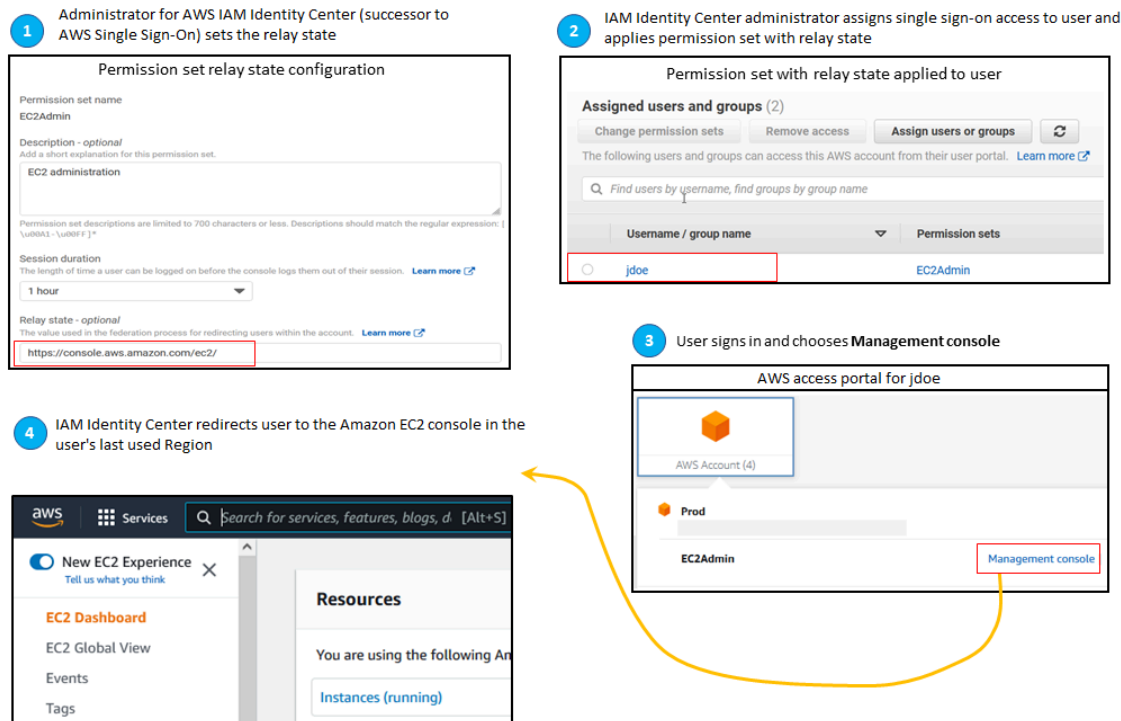
Pour définir la durée de session

1. Ouvrez la [console IAM Identity Center](#).
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez le nom de l'ensemble d'autorisations dont vous souhaitez modifier la durée de session.
4. Sur la page de détails de l'ensemble d'autorisations, à droite de l'en-tête de la section Paramètres généraux, choisissez Modifier.
5. Sur la page Modifier les paramètres généraux de l'ensemble d'autorisations, choisissez une nouvelle valeur pour la durée de la session.
6. Si l'ensemble d'autorisations est provisionné dans l'un d'entre Comptes AWS eux, les noms des comptes apparaissent sous Comptes AWS pour être réapprovisionnés automatiquement. Une fois que la valeur de durée de session pour l'ensemble d'autorisations est mise à jour, tous Comptes AWS ceux qui utilisent l'ensemble d'autorisations sont reprovisionnés. Cela signifie que la nouvelle valeur de ce paramètre est appliquée à tous ceux Comptes AWS qui utilisent l'ensemble d'autorisations.
7. Sélectionnez Enregistrer les modifications.
8. En haut de la Comptes AWSpage, une notification apparaît.
 - Si l'ensemble d'autorisations est fourni dans un ou plusieurs comptes Comptes AWS, la notification confirme qu' Comptes AWS ils ont été reprovisionnés avec succès et que le jeu d'autorisations mis à jour a été appliqué aux comptes.
 - Si l'ensemble d'autorisations n'est pas fourni dans un Compte AWS, la notification confirme que les paramètres du jeu d'autorisations ont été mis à jour.

Réglez l'état du relais pour un accès rapide au AWS Management Console

Par défaut, lorsqu'un utilisateur se connecte au portail d' AWS accès, choisit un compte, puis choisit le rôle AWS créé à partir de l'ensemble d'autorisations attribué, IAM Identity Center redirige le navigateur de l'utilisateur vers le. AWS Management Console Vous pouvez modifier ce comportement en définissant l'état du relais sur une autre URL de console.

La définition de l'état du relais vous permet de fournir à l'utilisateur un accès rapide à la console la mieux adaptée à son rôle. Par exemple, vous pouvez définir l'état du relais sur l'URL de la console Amazon EC2 (<https://console.aws.amazon.com/ec2/>) pour rediriger l'utilisateur vers cette console lorsqu'il choisit le rôle d'administrateur Amazon EC2. Lors de la redirection vers l'URL par défaut ou vers l'URL de l'état du relais, IAM Identity Center achemine le navigateur de l'utilisateur vers le point de terminaison de la console Région AWS utilisé pour la dernière fois par l'utilisateur. Par exemple, si un utilisateur a mis fin à sa dernière session de console dans la région Europe (Stockholm) (eu-north-1), il est redirigé vers la console Amazon EC2 de cette région.



Pour configurer IAM Identity Center afin de rediriger l'utilisateur vers une console dans un environnement spécifique Région AWS, incluez la spécification de région dans l'URL. Par exemple, pour rediriger l'utilisateur vers la console Amazon EC2 dans la région USA Est (Ohio) (us-east-2), spécifiez l'URL de la console Amazon EC2 dans cette région (). **<https://us-east-2.console.aws.amazon.com/ec2/>** Si vous avez activé le centre d'identité IAM dans la région USA Ouest (Oregon) (us-west-2) et que vous souhaitez rediriger l'utilisateur vers cette région, spécifiez-le. **<https://us-west-2.console.aws.amazon.com/>**

Configuration de l'état du relais

Utilisez la procédure suivante pour configurer l'URL de l'état du relais pour un ensemble d'autorisations.

1. Ouvrez la [console IAM Identity Center](#).
2. Sous Autorisations multi-comptes, choisissez Ensembles d'autorisations.
3. Choisissez le nom de l'ensemble d'autorisations pour lequel vous souhaitez définir la nouvelle URL de l'état du relais.
4. Sur la page de détails de l'ensemble d'autorisations, à droite de l'en-tête de la section Paramètres généraux, choisissez Modifier.
5. Sur la page Modifier les paramètres généraux de l'ensemble d'autorisations, sous État du relais, tapez une URL de console pour l'un des AWS services. Par exemple :

`https://console.aws.amazon.com/ec2/`

Note

L'URL de l'état du relais doit se trouver dans le AWS Management Console.

6. Si l'ensemble d'autorisations est provisionné dans l'un d'entre Comptes AWS eux, les noms des comptes apparaissent sous Comptes AWS pour être réapprovisionnés automatiquement. Une fois que l'URL de l'état du relais pour l'ensemble d'autorisations est mise à jour, tous Comptes AWS ceux qui utilisent l'ensemble d'autorisations sont reprovisionnés. Cela signifie que la nouvelle valeur de ce paramètre est appliquée à tous ceux Comptes AWS qui utilisent l'ensemble d'autorisations.
7. Sélectionnez Enregistrer les modifications.
8. En haut de la page AWS Organisation, une notification apparaît.
 - Si l'ensemble d'autorisations est fourni dans un ou plusieurs comptes Comptes AWS, la notification confirme qu' Comptes AWS ils ont été reprovisionnés avec succès et que le jeu d'autorisations mis à jour a été appliqué aux comptes.
 - Si l'ensemble d'autorisations n'est pas fourni dans un Compte AWS, la notification confirme que les paramètres du jeu d'autorisations ont été mis à jour.

 Note

Vous pouvez automatiser ce processus à l'aide de l' AWS API, d'un AWS SDK ou du AWS Command Line Interface(AWS CLI). Pour en savoir plus, consultez :

- Les UpdatePermissionSet actions CreatePermissionSet ou contenues dans le guide de référence de l'[API IAM Identity Center](#)
- Les update-permission-set commandes create-permission-set ou dans la [sso-admin](#) section de la référence des AWS CLI commandes.

Utiliser une politique de refus pour révoquer les autorisations des utilisateurs actifs

Il se peut que vous deviez révoquer l'accès d'un utilisateur à IAM Identity Center Comptes AWS alors que celui-ci utilise activement un ensemble d'autorisations. Vous pouvez les empêcher d'utiliser leurs sessions de rôle IAM actives en implémentant à l'avance une politique de refus pour un utilisateur non spécifié, puis si nécessaire, vous pouvez mettre à jour la politique de refus pour spécifier l'utilisateur dont vous souhaitez bloquer l'accès. Cette rubrique explique comment créer une politique de refus et explique comment déployer la politique.

Préparez-vous à révoquer une session de rôle IAM active créée par un ensemble d'autorisations

Vous pouvez empêcher l'utilisateur de prendre des mesures avec un rôle IAM qu'il utilise activement en appliquant une politique de refus de tout à un utilisateur spécifique par le biais d'une politique de contrôle des services. Vous pouvez également empêcher un utilisateur d'utiliser un ensemble d'autorisations tant que vous n'avez pas modifié son mot de passe, ce qui permet de supprimer un mauvais acteur utilisant activement des informations d'identification volées à mauvais escient. Si vous devez refuser l'accès de manière générale et empêcher un utilisateur de saisir à nouveau un ensemble d'autorisations ou d'accéder à d'autres ensembles d'autorisations, vous pouvez également supprimer tous les accès des utilisateurs, arrêter la session active du portail d' AWS accès et désactiver la connexion de l'utilisateur. Consultez [the section called “Mettre fin aux sessions actives pour les utilisateurs du personnel”](#) pour savoir comment utiliser la politique de refus en conjonction avec des actions supplémentaires pour une révocation d'accès plus large.

Politique de refus

Vous pouvez utiliser une politique de refus assortie d'une condition correspondant à celle UserID de l'utilisateur figurant dans la banque d'identités IAM Identity Center afin d'empêcher d'autres actions d'un rôle IAM que l'utilisateur utilise activement. L'utilisation de cette politique permet d'éviter

tout impact sur les autres utilisateurs susceptibles d'utiliser le même ensemble d'autorisations lorsque vous déployez la politique de refus. Cette politique utilise l'identifiant utilisateur fictif. Pour "identitystore:userId" cela *Add user ID here*, vous allez le mettre à jour avec le nom d'utilisateur pour lequel vous souhaitez révoquer l'accès.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:userId": "Add user ID here"
        }
      }
    }
  ]
}
```

Bien que vous puissiez utiliser une autre clé de condition "aws:userId", telle que, elle "identitystore:userId" est certaine, car il s'agit d'une valeur unique au monde associée à une personne. L'utilisation "aws:userId" dans cette condition peut être affectée par la façon dont les attributs utilisateur sont synchronisés à partir de votre source d'identités et peut changer si le nom d'utilisateur ou l'adresse e-mail de l'utilisateur changent.

Dans la console IAM Identity Center, vous pouvez trouver celui d'un utilisateur identitystore:userId en accédant à Utilisateurs, en recherchant l'utilisateur par son nom, en développant la section Informations générales et en copiant l'ID utilisateur. Il est également pratique d'arrêter la session du portail d' AWS accès d'un utilisateur et de désactiver son accès de connexion dans la même section lors de la recherche de son nom d'utilisateur. Vous pouvez automatiser le processus de création d'une politique de refus en obtenant l'ID utilisateur de l'utilisateur en interrogeant le magasin APIs d'identités.

Déploiement de la politique de refus

Vous pouvez utiliser un identifiant utilisateur fictif qui n'est pas valide, par exemple pour déployer la politique de refus à l'avance à l'aide d'une politique de contrôle des services (SCP) que vous attachez aux Comptes AWS utilisateurs susceptibles d'avoir accès. *Add user ID here* C'est l'approche recommandée pour sa facilité et sa rapidité d'impact. Lorsque vous révoquez l'accès d'un utilisateur à l'aide de la politique de refus, vous modifiez la politique pour remplacer l'ID utilisateur fictif par l'ID utilisateur de la personne dont vous souhaitez révoquer l'accès. Cela empêche l'utilisateur d'effectuer des actions avec les autorisations définies dans chaque compte auquel vous associez le SCP. Il bloque les actions de l'utilisateur même s'il utilise sa session de portail AWS d'accès active pour accéder à différents comptes et assumer différents rôles. L'accès de l'utilisateur étant totalement bloqué par le SCP, vous pouvez alors désactiver sa capacité à se connecter, révoquer ses attributions et arrêter sa session sur le portail AWS d'accès si nécessaire.

Au lieu de l'utiliser SCPs, vous pouvez également inclure la politique de refus dans la politique intégrée des ensembles d'autorisations et dans les politiques gérées par le client qui sont utilisées par les ensembles d'autorisations auxquels l'utilisateur peut accéder.

Si vous devez révoquer l'accès à plusieurs personnes, vous pouvez utiliser une liste de valeurs dans le bloc de conditions, telles que :

```
"Condition": {
  "StringEquals": {
    "identitystore:userId": [" user1 userId", "user2 userId"...]
  }
}
```

Important

Quelle que soit la ou les méthodes que vous utilisez, vous devez prendre toute autre mesure corrective et conserver le nom d'utilisateur de l'utilisateur dans la politique pendant au moins 12 heures. Passé ce délai, tous les rôles assumés par l'utilisateur expirent et vous pouvez alors supprimer son ID utilisateur de la politique de refus.

Référencement des ensembles d'autorisations dans les politiques de ressources, les cartes de configuration du cluster Amazon EKS et les politiques AWS KMS clés

Lorsque vous attribuez un ensemble d'autorisations à un AWS compte, IAM Identity Center crée un rôle dont le nom commence AWSReservedSSO_ par.

Le nom complet et le nom Amazon Resource Name (ARN) du rôle utilisent le format suivant :

Nom	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Si votre source d'identité dans IAM Identity Center est hébergée dans us-east-1, il n'en existe aucune dans l'ARN. *aws-region* Le nom complet et l'ARN du rôle utilisent le format suivant :

Nom	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Par exemple, si vous créez un ensemble d'autorisations qui accorde l'accès au AWS compte aux administrateurs de base de données, un rôle correspondant est créé avec le nom et l'ARN suivants :

Nom	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/

Nom	ARN
	eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

Si vous supprimez toutes les attributions associées à cet ensemble d'autorisations dans le AWS compte, le rôle correspondant créé par IAM Identity Center est également supprimé. Si vous attribuez ultérieurement une nouvelle attribution au même ensemble d'autorisations, IAM Identity Center crée un nouveau rôle pour le jeu d'autorisations. Le nom et l'ARN du nouveau rôle incluent un suffixe différent et unique. Dans cet exemple, le suffixe unique est abcdef0123456789.

Nom	ARN
AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789

La modification du suffixe du nouveau nom et du nouveau ARN du rôle entraînera la création de toutes les politiques faisant référence au nom et à l'ARN d'origine out-of-date, ce qui perturbera l'accès des personnes utilisant l'ensemble d'autorisations correspondant. Par exemple, une modification de l'ARN du rôle perturbera l'accès des utilisateurs à l'ensemble d'autorisations si l'ARN d'origine est référencé dans les configurations suivantes :

- Dans le `aws-auth ConfigMap` fichier relatif aux clusters Amazon Elastic Kubernetes Service (Amazon EKS) lorsque vous `aws-auth ConfigMap` utilisez le pour accéder au cluster.
- Dans une politique basée sur les ressources pour une clé AWS Key Management Service (AWS KMS). Cette politique est également appelée politique clé.

Note

Nous vous recommandons d'utiliser les [entrées d'accès Amazon EKS](#) pour gérer l'accès à vos clusters Amazon EKS. Cela vous permet d'utiliser les autorisations IAM pour gérer les

principaux ayant accès à un cluster Amazon EKS. En utilisant les entrées d'accès Amazon EKS, vous pouvez utiliser un principal IAM disposant des autorisations Amazon EKS pour accéder de nouveau à un cluster sans le contacter Support.

Bien que vous puissiez mettre à jour les politiques basées sur les ressources pour la plupart AWS des services afin de faire référence à un nouvel ARN pour un rôle correspondant à un ensemble d'autorisations, vous devez avoir un rôle de sauvegarde que vous devez créer dans IAM pour Amazon EKS et si AWS KMS l'ARN change. Pour Amazon EKS, le rôle IAM de sauvegarde doit exister dans le `aws-auth ConfigMap`. Car AWS KMS elle doit figurer dans vos politiques clés. Si vous ne disposez pas d'un rôle IAM de secours autorisé à mettre à jour la politique `aws-auth ConfigMap` ou la politique AWS KMS clé, contactez-nous Support pour retrouver l'accès à ces ressources.

Recommandations pour éviter les interruptions d'accès

Pour éviter les interruptions d'accès dues à des modifications de l'ARN d'un rôle correspondant à un ensemble d'autorisations, nous vous recommandons de procéder comme suit.

- Conservez au moins une attribution d'ensemble d'autorisations.

Conservez cette attribution dans les AWS comptes qui contiennent les rôles auxquels vous faites référence dans le `aws-auth ConfigMap` cas d'Amazon EKS, les politiques clés dans AWS KMS Amazon EKS ou les politiques basées sur les ressources pour les autres. Services AWS

Par exemple, si vous créez un ensemble d'`EKSAccessauthorisations` et que vous référencez l'ARN du rôle correspondant à partir du AWS compte `111122223333`, attribuez définitivement un groupe administratif au jeu d'autorisations de ce compte. L'attribution étant permanente, IAM Identity Center ne supprimera pas le rôle correspondant, ce qui élimine le risque de changement de nom. Le groupe administratif y aura toujours accès sans risque d'augmentation de privilèges.

- Pour les clusters Amazon EKS qui utilisent **aws-auth ConfigMap** et AWS KMS : incluez un rôle créé dans IAM.

Si vous faites référence à un rôle ARNs pour des ensembles d'autorisations dans un `aws-auth ConfigMap` cluster Amazon EKS ou dans des politiques AWS KMS clés relatives aux clés, nous vous recommandons d'inclure également au moins un rôle que vous créez dans IAM. Le rôle doit vous permettre d'accéder au cluster Amazon EKS ou de gérer la politique AWS KMS clé. L'ensemble d'autorisations doit être en mesure d'assumer ce rôle. Ainsi, si l'ARN du rôle d'un

ensemble d'autorisations change, vous pouvez mettre à jour la référence à l'ARN dans la politique AWS KMS clé `aws-auth ConfigMap` or. La section suivante fournit un exemple de la manière dont vous pouvez créer une politique de confiance pour un rôle créé dans IAM. Le rôle ne peut être assumé que par un ensemble d'AdministratorAccess autorisations.

Exemple de politique de confiance personnalisée

Voici un exemple de politique de confiance personnalisée qui fournit un ensemble d'AdministratorAccess autorisations permettant d'accéder à un rôle créé dans IAM. Les principaux éléments de cette politique sont les suivants :

- L'élément principal de cette politique de confiance spécifie un principal de AWS compte. Dans cette politique, les principaux du AWS compte 111122223333 disposant d'`sts:AssumeRole` autorisations peuvent assumer le rôle créé dans IAM.
- Cette politique `Condition` élément de confiance définit des exigences supplémentaires pour les principaux qui peuvent assumer le rôle créé dans IAM. Dans cette politique, l'ensemble d'autorisations avec le rôle ARN suivant peut assumer le rôle.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/  
AWSReservedSSO_AdministratorAccess_*
```

Note

L'`Condition` élément inclut l'opérateur de `ArnLike` condition et utilise un caractère générique à la fin de l'ARN du rôle défini d'autorisations, plutôt qu'un suffixe unique. Cela signifie que la politique permet à l'ensemble d'autorisations d'assumer le rôle créé dans IAM même si l'ARN du rôle pour l'ensemble d'autorisations change.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {
```

```
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
    }
  }
}
```

L'inclusion d'un rôle que vous créez dans IAM dans une telle politique vous fournira un accès d'urgence à vos clusters Amazon EKS ou à d'autres AWS ressources si un ensemble d'autorisations ou toutes les attributions à l'ensemble d'autorisations sont accidentellement supprimés et recréés. AWS KMS keys

Contrôle d'accès basé sur les attributs

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Vous pouvez utiliser IAM Identity Center pour gérer l'accès à vos AWS ressources sur plusieurs sites à Comptes AWS l'aide d'attributs utilisateur provenant de n'importe quelle source d'identité IAM Identity Center. Dans AWS, ces attributs sont appelés balises. L'utilisation des attributs utilisateur sous forme de balises vous AWS permet de simplifier le processus de création d'autorisations précises AWS et de garantir que votre personnel n'a accès qu'aux AWS ressources associées aux balises correspondantes.

Par exemple, vous pouvez attribuer aux développeurs Bob et Sally, issus de deux équipes différentes, le même ensemble d'autorisations dans IAM Identity Center, puis sélectionner l'attribut du nom de l'équipe pour le contrôle d'accès. Lorsque Bob et Sally se connectent à leur Comptes AWS, IAM Identity Center envoie leur attribut de nom d'équipe dans la AWS session afin que Bob et Sally puissent accéder aux ressources AWS du projet uniquement si leur attribut de nom d'équipe correspond au tag de nom d'équipe figurant sur la ressource du projet. Si Bob rejoint l'équipe de Sally à l'avenir, vous pouvez modifier son accès en mettant simplement à jour son attribut de nom d'équipe dans le répertoire de l'entreprise. La prochaine fois que Bob se connectera, il aura automatiquement accès aux ressources de projet de sa nouvelle équipe sans avoir à mettre à jour les autorisations AWS.

Cette approche permet également de réduire le nombre d'autorisations distinctes que vous devez créer et gérer dans IAM Identity Center, car les utilisateurs associés aux mêmes ensembles d'autorisations peuvent désormais disposer d'autorisations uniques en fonction de leurs attributs. Vous pouvez utiliser ces attributs utilisateur dans les ensembles d'autorisations et les politiques basées sur les ressources d'IAM Identity Center pour implémenter ABAC dans les AWS ressources et simplifier la gestion des autorisations à grande échelle.

Avantages

Les avantages supplémentaires de l'utilisation d'ABAC dans IAM Identity Center sont les suivants.

- ABAC nécessite moins d'ensembles d'autorisations : comme vous n'avez pas à créer de politiques différentes pour les différentes fonctions, vous créez moins d'ensembles d'autorisations. Cela réduit la complexité de la gestion des autorisations.
- Grâce à ABAC, les équipes peuvent évoluer et se développer rapidement : les autorisations pour les nouvelles ressources sont automatiquement accordées en fonction des attributs lorsque les ressources sont correctement étiquetées lors de leur création.
- Utilisez les attributs des employés de votre annuaire d'entreprise avec ABAC : vous pouvez utiliser les attributs des employés existants provenant de n'importe quelle source d'identité configurée dans IAM Identity Center pour prendre des décisions de contrôle d'accès dans AWS.
- Suivez qui accède aux ressources — Les administrateurs de sécurité peuvent facilement déterminer l'identité d'une session en examinant les attributs de l'utilisateur AWS CloudTrail pour suivre l'activité des utilisateurs AWS.

Pour plus d'informations sur la configuration d'ABAC à l'aide de la console IAM Identity Center, consultez [Attributs pour le contrôle d'accès](#). Pour plus d'informations sur l'activation et la configuration d'ABAC à l'aide de l'IAM Identity Center APIs, consultez le Guide de [CreateInstanceAccessControlAttributeConfiguration](#) référence de l'API IAM Identity Center.

Rubriques

- [Liste de contrôle : Configuration d'ABAC à AWS l'aide d'IAM Identity Center](#)
- [Attributs pour le contrôle d'accès](#)

Liste de contrôle : Configuration d'ABAC à AWS l'aide d'IAM Identity Center

Cette liste de contrôle inclut les tâches de configuration nécessaires pour préparer vos AWS ressources et configurer IAM Identity Center pour l'accès ABAC. Effectuez les tâches de cette liste de contrôle dans l'ordre. Lorsqu'un lien de référence vous amène à un sujet, revenez à ce sujet afin de pouvoir effectuer les tâches restantes de cette liste de contrôle.

Step (Étape)	Sous-tâche	Référence
1	Découvrez comment ajouter des balises à toutes vos AWS ressources. Pour implémenter ABAC dans IAM Identity Center, vous devez d'abord ajouter des balises à toutes les AWS ressources pour lesquelles vous souhaitez implémenter ABAC.	• Ressources de balisage AWS
2	Découvrez comment configurer votre source d'identité dans IAM Identity Center avec les identités utilisateur et les attributs associés dans votre magasin d'identités. IAM Identity Center vous permet d'utiliser les attributs utilisateur de n'importe quelle source d'identité IAM Identity Center prise en charge pour ABAC in. AWS	• Gérez votre source d'identité
3	Sur la base des critères suivants, déterminez les attributs que vous souhaitez utiliser pour prendre des décisions en matière de contrôle d'accès AWS et envoyez-les à IAM Identity Center. • Si vous utilisez un fournisseur d'identité (IdP) externe, décidez si vous souhaitez utiliser les attributs transmis par l'IdP ou sélectionner des attributs depuis IAM Identity Center. • Si vous choisissez que votre IdP envoie des attributs, configurez votre IdP pour transmettre les attributs dans des assertions SAML. Consultez les <code>Optional</code> sections du didacticiel correspondant à votre IdP spécifique.	• Prise en main • Choix des attributs lors de l'utilisation d'un fournisseur d'identité externe comme source d'identité • Tutoriels sur les sources d'identité IAM Identity Center

Step (Étape)	Sous-tâche	Référence
	• Si vous utilisez un IdP comme source d'identité et que vous choisissez de sélectionner des attributs dans IAM Identity Center, étudiez comment configurer le SCIM afin que les valeurs des attributs proviennent de votre IdP. Si vous ne pouvez pas utiliser SCIM avec votre IdP, ajoutez les utilisateurs et leurs attributs à l'aide de la page utilisateur de la console IAM Identity Center.	• Provisionner des utilisateurs et des groupes à partir d'un fournisseur d'identité externe à l'aide de SCIM • Attributs du fournisseur d'identité externe pris en charge
	• Si vous utilisez Active Directory ou IAM Identity Center comme source d'identité, ou si vous utilisez un IdP et choisissez de sélectionner des attributs dans IAM Identity Center, passez en revue les attributs disponibles que vous pouvez configurer. Passez ensuite immédiatement à l'étape 4 pour commencer à configurer vos attributs ABAC à l'aide de la console IAM Identity Center.	• Choix des attributs lors de l'utilisation d'IAM Identity Center comme source d'identité • Choix des attributs lorsque vous AWS Managed Microsoft AD les utilisez comme source d'identité • Mappages par défaut entre IAM Identity Center et Microsoft AD
4	Sélectionnez les attributs à utiliser pour ABAC à l'aide de la page Attributs pour le contrôle d'accès de la console IAM Identity Center. Sur cette page, vous pouvez sélectionner des attributs pour le contrôle d'accès à partir de la source d'identité que vous avez configurée à l'étape 2. Une fois que vos identités et leurs attributs se trouvent dans IAM Identity Center, vous devez créer des paires clé-valeur (mappages) qui vous seront transmises Comptes AWS pour être utilisées dans les décisions de contrôle d'accès.	• Activer et configurer les attributs pour le contrôle d'accès

Step (Étape)	Sous-tâche	Référence
5	Créez des politiques d'autorisation personnalisées au sein de votre ensemble d'autorisations et utilisez les attributs de contrôle d'accès pour créer des règles ABAC afin que les utilisateurs puissent uniquement accéder aux ressources dont les balises correspondent. Les attributs utilisateur que vous avez configurés à l'étape 4 sont utilisés comme balises AWS pour les décisions de contrôle d'accès. Vous pouvez faire référence aux attributs de contrôle d'accès dans la politique d'autorisation à l'aide de la <code>aws:PrincipalTag/key</code> condition.	• Création de politiques d'autorisation pour ABAC dans IAM Identity Center
6	Dans vos différents Comptes AWS, assignez des utilisateurs aux ensembles d'autorisations que vous avez créés à l'étape 5. Cela garantit que lorsqu'ils se fédèrent dans leurs comptes et accèdent aux AWS ressources, ils n'y accèdent qu'en fonction des balises correspondantes.	• Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS

Une fois ces étapes terminées, les utilisateurs qui se fédèrent pour Compte AWS utiliser l'authentification unique auront accès à leurs AWS ressources en fonction des attributs correspondants.

Attributs pour le contrôle d'accès

Attributs pour le contrôle d'accès est le nom de la page de la console IAM Identity Center où vous sélectionnez les attributs utilisateur que vous souhaitez utiliser dans les politiques pour contrôler l'accès aux ressources. Vous pouvez affecter des utilisateurs à des charges de travail en AWS fonction des attributs existants dans la source d'identité des utilisateurs.

Supposons, par exemple, que vous souhaitiez attribuer l'accès aux compartiments S3 en fonction des noms des départements. Sur la page Attributs pour le contrôle d'accès, vous sélectionnez l'attribut utilisateur du département à utiliser avec le contrôle d'accès basé sur les attributs (ABAC). Dans l'ensemble d'autorisations IAM Identity Center, vous rédigez ensuite une politique qui accorde l'accès

aux utilisateurs uniquement lorsque l'attribut Department correspond à la balise de département que vous avez attribuée à vos compartiments S3. IAM Identity Center transmet l'attribut de département de l'utilisateur au compte auquel il accède. L'attribut est ensuite utilisé pour déterminer l'accès en fonction de la politique. Pour plus d'informations sur ABAC, consultez [Contrôle d'accès basé sur les attributs](#).

Prise en main

La manière dont vous commencez à configurer les attributs pour le contrôle d'accès dépend de la source d'identité que vous utilisez. Quelle que soit la source d'identité que vous choisissiez, après avoir sélectionné vos attributs, vous devez créer ou modifier les politiques relatives aux ensembles d'autorisations. Ces politiques doivent accorder aux identités des utilisateurs l'accès aux AWS ressources.

Choix des attributs lors de l'utilisation d'IAM Identity Center comme source d'identité

Lorsque vous configurez IAM Identity Center comme source d'identité, vous devez d'abord ajouter des utilisateurs et configurer leurs attributs. Accédez ensuite à la page Attributs pour le contrôle d'accès et sélectionnez les attributs que vous souhaitez utiliser dans les politiques. Enfin, accédez à la Comptes AWSpage pour créer ou modifier des ensembles d'autorisations afin d'utiliser les attributs d'ABAC.

Choix des attributs lorsque vous AWS Managed Microsoft AD les utilisez comme source d'identité

Lorsque vous configurez IAM Identity Center AWS Managed Microsoft AD comme source d'identité, vous mappez d'abord un ensemble d'attributs d'Active Directory aux attributs utilisateur d'IAM Identity Center. Accédez ensuite à la page Attributs pour le contrôle d'accès. Choisissez ensuite les attributs à utiliser dans votre configuration ABAC en fonction de l'ensemble existant d'attributs SSO mappés à partir d'Active Directory. Enfin, créez des règles ABAC en utilisant les attributs de contrôle d'accès dans les ensembles d'autorisations pour accorder aux identités des utilisateurs l'accès aux AWS ressources. Pour obtenir la liste des mappages par défaut des attributs utilisateur dans IAM Identity Center avec les attributs utilisateur de votre AWS Managed Microsoft AD annuaire, consultez.

[Mappages par défaut entre IAM Identity Center et Microsoft AD](#)

Choix des attributs lors de l'utilisation d'un fournisseur d'identité externe comme source d'identité

Lorsque vous configurez IAM Identity Center avec un fournisseur d'identité externe (IdP) comme source d'identité, il existe deux manières d'utiliser les attributs pour ABAC.

- Vous pouvez configurer votre IdP pour envoyer les attributs via des assertions SAML. Dans ce cas, IAM Identity Center transmet le nom et la valeur de l'attribut de l'IdP à des fins d'évaluation des politiques.

 Note

Les attributs des assertions SAML ne seront pas visibles sur la page Attributs pour le contrôle d'accès. Vous devez connaître ces attributs à l'avance et les ajouter aux règles de contrôle d'accès lorsque vous créez des politiques. Si vous décidez de faire confiance à votre externe IdPs pour les attributs, ces attributs seront toujours transmis lorsque les utilisateurs se fédéreront dans Comptes AWS. Dans les scénarios où les mêmes attributs arrivent à IAM Identity Center via SAML et SCIM, la valeur des attributs SCIM a priorité dans les décisions de contrôle d'accès.

- Vous pouvez configurer les attributs que vous utilisez depuis la page Attributs pour le contrôle d'accès de la console IAM Identity Center. Les valeurs d'attributs que vous choisissez ici remplacent les valeurs de tous les attributs correspondants provenant d'un IdP via une assertion. Selon que vous utilisez ou non le SCIM, tenez compte des points suivants :
- Si vous utilisez SCIM, l'IdP synchronise automatiquement les valeurs des attributs dans IAM Identity Center. Les attributs supplémentaires requis pour le contrôle d'accès peuvent ne pas figurer dans la liste des attributs SCIM. Dans ce cas, envisagez de collaborer avec l'administrateur informatique de votre IdP pour envoyer ces attributs à IAM Identity Center via des assertions SAML en utilisant le préfixe requis. `https://aws.amazon.com/SAML/Attributes/AccessControl` : Pour plus d'informations sur la façon de configurer les attributs utilisateur pour le contrôle d'accès dans votre IdP à envoyer via des assertions SAML, consultez le [Tutoriels sur les sources d'identité IAM Identity Center](#)
- Si vous n'utilisez pas le SCIM, vous devez ajouter manuellement les utilisateurs et définir leurs attributs comme si vous utilisiez IAM Identity Center comme source d'identité. Accédez ensuite à la page Attributs pour le contrôle d'accès et choisissez les attributs que vous souhaitez utiliser dans les politiques.

Pour une liste complète des attributs pris en charge pour les attributs utilisateur dans IAM Identity Center et les attributs utilisateur dans votre environnement externe IdPs, consultez [Attributs du fournisseur d'identité externe pris en charge](#).

Pour commencer à utiliser ABAC dans IAM Identity Center, consultez les rubriques suivantes.

Rubriques

- [Activer et configurer les attributs pour le contrôle d'accès](#)
- [Création de politiques d'autorisation pour ABAC dans IAM Identity Center](#)

Activer et configurer les attributs pour le contrôle d'accès

[Pour utiliser le contrôle d'accès basé sur les attributs \(ABAC\), vous devez d'abord l'activer dans la page Paramètres de la console IAM Identity Center ou dans l'API IAM Identity Center.](#) Quelle que soit la source d'identité, vous pouvez toujours configurer les attributs utilisateur à partir de l'Identity Store pour les utiliser dans ABAC. Dans la console, vous pouvez le faire en accédant à l'onglet Attributs pour le contrôle d'accès sur la page Paramètres. Si vous utilisez un fournisseur d'identité externe (IdP) comme source d'identité, vous avez également la possibilité de recevoir des attributs de l'IdP externe dans des assertions SAML. Dans ce cas, vous devez configurer l'IdP externe pour envoyer les attributs souhaités. Si un attribut issu d'une assertion SAML est également défini comme un attribut ABAC dans IAM Identity Center, IAM Identity Center enverra la valeur depuis son magasin d'identités sous forme de [balise de session lors](#) de la connexion à un. Compte AWS

Note

Vous ne pouvez pas afficher les attributs configurés et envoyés par un IdP externe depuis la page Attributs pour le contrôle d'accès de la console IAM Identity Center. Si vous transmettez des attributs de contrôle d'accès dans les assertions SAML à partir de votre IdP externe, ces attributs sont directement envoyés au Compte AWS moment de la fédération des utilisateurs. Les attributs ne seront pas disponibles dans IAM Identity Center pour le mappage.

Rubriques

- [Activer les attributs pour le contrôle d'accès](#)
- [Sélectionnez vos attributs pour le contrôle d'accès](#)
- [Désactiver des attributs pour le contrôle d'accès](#)

Activer les attributs pour le contrôle d'accès

Utilisez la procédure suivante pour activer la fonctionnalité de contrôle des attributs d'accès (ABAC) à l'aide de la console IAM Identity Center.

 Note

Si vous disposez d'ensembles d'autorisations existants et que vous prévoyez d'activer ABAC dans votre instance IAM Identity Center, des restrictions de sécurité supplémentaires nécessitent que vous disposiez d'abord de la `iam:UpdateAssumeRolePolicy` politique. Ces restrictions de sécurité supplémentaires ne sont pas requises si aucun ensemble d'autorisations n'a été créé dans votre compte.

Si votre instance IAM Identity Center a été créée avant décembre 2020 et que vous prévoyez d'y activer ABAC, vous devez disposer de la `iam:UpdateAssumeRolePolicy` politique associée au rôle administratif IAM Identity Center, que vous ayez ou non créé des ensembles d'autorisations dans votre compte.

Pour activer les attributs pour le contrôle d'accès

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez les paramètres
3. Sur la page Paramètres, recherchez la zone Attributs pour les informations de contrôle d'accès, puis choisissez Activer. Passez à la procédure suivante pour le configurer.

Sélectionnez vos attributs pour le contrôle d'accès

Utilisez la procédure suivante pour configurer les attributs de votre configuration ABAC.

Pour sélectionner vos attributs à l'aide de la console IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez les paramètres
3. Sur la page Paramètres, choisissez l'onglet Attributs pour le contrôle d'accès, puis sélectionnez Gérer les attributs.
4. Sur la page Attributs pour le contrôle d'accès, choisissez Ajouter un attribut et entrez les détails de la clé et de la valeur. C'est ici que vous allez mapper l'attribut provenant de votre source d'identité à un attribut transmis par IAM Identity Center en tant que balise de session.

Key ⓘ	Value (optional) ⓘ	Remove
Department	<code>\${path:enterprise.department}</code>	✕
CostCenter	<code>\${path:enterprise.costCenter}</code>	✕
Add new key	Add new value	

La clé représente le nom que vous donnez à l'attribut à utiliser dans les politiques. Il peut s'agir de n'importe quel nom arbitraire, mais vous devez le spécifier exactement dans les politiques que vous créez pour le contrôle d'accès. Supposons, par exemple, que vous utilisiez Okta (un IdP externe) comme source d'identité et que vous deviez transmettre les données du centre de coûts de votre organisation sous forme de balises de session. Dans Key, vous devez saisir un nom correspondant de la même manière, CostCenter comme votre nom de clé. Il est important de noter que quel que soit le nom que vous choisissiez ici, il doit également porter exactement le même nom dans votre nom [Clé de condition aws:PrincipalTag](#) (c'est-à-dire, "ec2:ResourceTag/CostCenter": "\${aws:PrincipalTag/CostCenter}").

ⓘ Note

Utilisez un attribut à valeur unique pour votre clé, par exemple, **Manager**. IAM Identity Center ne prend pas en charge les attributs à valeurs multiples pour ABAC, par exemple. **Manager, IT Systems**

La valeur représente le contenu de l'attribut provenant de votre source d'identité configurée. Vous pouvez saisir ici n'importe quelle valeur de la table des sources d'identité appropriée répertoriée dans [Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes](#). Par exemple, en utilisant le contexte fourni dans l'exemple mentionné ci-dessus, vous examineriez la liste des attributs IdP pris en charge et détermineriez que la correspondance la plus proche d'un attribut pris en charge serait, **`${path:enterprise.costCenter}`** puis vous la saisissez dans le champ Valeur. Voir la capture d'écran ci-dessus pour référence. Notez que vous ne pouvez pas utiliser de valeurs d'attributs IdP externes en dehors de cette liste pour ABAC, sauf si vous utilisez l'option de transmission d'attributs via l'assertion SAML.

5. Sélectionnez Enregistrer les modifications.

Maintenant que vous avez configuré le mappage de vos attributs de contrôle d'accès, vous devez terminer le processus de configuration ABAC. Pour ce faire, créez vos règles ABAC et ajoutez-les aux politiques basées sur les and/or ressources de vos ensembles d'autorisations. Cela est nécessaire pour que vous puissiez accorder aux identités des utilisateurs l'accès aux AWS ressources. Pour de plus amples informations, veuillez consulter [Création de politiques d'autorisation pour ABAC dans IAM Identity Center](#).

Désactiver des attributs pour le contrôle d'accès

Utilisez la procédure suivante pour désactiver la fonctionnalité ABAC et supprimer tous les mappages d'attributs qui ont été configurés.

Pour désactiver les attributs pour le contrôle d'accès

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Attributs pour le contrôle d'accès, puis sélectionnez Gérer les attributs.
4. Sur la page Gérer les attributs pour le contrôle d'accès, choisissez Désactiver.
5. Dans la fenêtre de dialogue Désactiver les attributs pour le contrôle d'accès, passez en revue les informations et, lorsque vous êtes prêt **DÉSACTIVER**, saisissez-les, puis choisissez Confirmer.

Important

Cette étape supprime tous les attributs et arrête leur utilisation pour le contrôle d'accès lors de la fédération, Comptes AWS que des attributs soient présents ou non dans les assertions SAML d'un fournisseur de source d'identité externe.

Création de politiques d'autorisation pour ABAC dans IAM Identity Center

Vous pouvez créer des politiques d'autorisation qui déterminent qui peut accéder à vos AWS ressources en fonction de la valeur d'attribut configurée. Lorsque vous activez ABAC et que vous spécifiez des attributs, IAM Identity Center transmet la valeur d'attribut de l'utilisateur authentifié à IAM afin de l'utiliser dans le cadre de l'évaluation des politiques.

Clé de condition aws:PrincipalTag

Vous pouvez utiliser des attributs de contrôle d'accès dans vos ensembles d'autorisations à l'aide de la clé de `aws:PrincipalTag` condition pour créer des règles de contrôle d'accès. Par exemple, dans la politique suivante, vous pouvez étiqueter toutes les ressources de votre organisation avec leurs centres de coûts respectifs. Vous pouvez également utiliser un ensemble d'autorisations unique qui accorde aux développeurs l'accès aux ressources de leur centre de coûts. Désormais, chaque fois que les développeurs se fédèrent dans le compte à l'aide de l'authentification unique et de leur attribut de centre de coûts, ils n'ont accès qu'aux ressources de leurs centres de coûts respectifs. Au fur et à mesure que l'équipe ajoute des développeurs et des ressources à son projet, il vous suffit de baliser les ressources avec le centre de coûts approprié. Vous transmettez ensuite les informations du centre de coûts lors de la AWS session dans laquelle les développeurs se Comptes AWS fédèrent. Ainsi, à mesure que l'organisation ajoute de nouvelles ressources et de nouveaux développeurs au centre de coûts, les développeurs peuvent gérer les ressources alignées sur leurs centres de coûts sans avoir besoin de mettre à jour les autorisations.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/
CostCenter}"
        }
      }
    }
  ]
}
```

```
}  
  ]  
}
```

Pour plus d'informations, consultez [aws:PrincipalTaget EC2 : Démarrer ou arrêter des instances en fonction de la correspondance des balises principale et ressource](#) dans le guide de l'utilisateur IAM.

Si les politiques contiennent des attributs non valides dans leurs conditions, la condition de politique échouera et l'accès sera refusé. Pour de plus amples informations, veuillez consulter [Erreur « Une erreur inattendue s'est produite » lorsqu'un utilisateur tente de se connecter à l'aide d'un fournisseur d'identité externe](#).

Comprendre les rôles liés aux services dans IAM Identity Center

Les [rôles liés à un service sont des](#) autorisations IAM prédéfinies qui permettent à IAM Identity Center de déléguer et d'appliquer les utilisateurs disposant d'un accès par authentification unique à des utilisateurs spécifiques Comptes AWS de votre organisation dans AWS Organizations. Le service active cette fonctionnalité en attribuant un rôle lié au service Compte AWS dans chaque élément de son organisation. Le service permet ensuite à d'autres AWS services tels que IAM Identity Center de tirer parti de ces rôles pour effectuer des tâches liées au service. Pour plus d'informations, voir [AWS Organizations et rôles liés à un service](#).

Lorsque vous activez IAM Identity Center, IAM Identity Center crée un rôle lié à un service dans tous les comptes de l'organisation dans AWS Organizations. IAM Identity Center crée également le même rôle lié au service dans chaque compte ajouté ultérieurement à votre organisation. Ce rôle permet à IAM Identity Center d'accéder aux ressources de chaque compte en votre nom. Pour de plus amples informations, veuillez consulter [Configurer l'accès à Comptes AWS](#).

Les rôles liés à un service créés dans chacun d'eux Compte AWS sont nommés.

`AWSServiceRoleForSSO` Pour de plus amples informations, veuillez consulter [Utilisation de rôles liés à un service pour IAM Identity Center](#).

Remarques

- Si vous êtes connecté au compte de AWS Organizations gestion, celui-ci utilise votre rôle actuellement connecté et non le rôle lié au service. Cela empêche l'escalade des privilèges.

- Lorsque IAM Identity Center effectue des opérations IAM dans le compte de AWS Organizations gestion, toutes les opérations sont effectuées à l'aide des informations d'identification du principal IAM. Cela permet aux connexions de CloudTrail savoir qui a effectué tous les changements de privilèges dans le compte de gestion.

Configuration et utilisation du portail AWS d'accès

Le portail AWS d'accès connecte votre personnel Comptes AWS aux applications cloud via IAM Identity Center. Les administrateurs configurent le portail et gèrent l'accès des utilisateurs, tandis que les utilisateurs finaux se connectent une seule fois pour accéder facilement à toutes leurs ressources autorisées.

Le portail AWS d'accès fournit un accès par authentification unique pour :

- Comptes AWS au sein de votre organisation.
- AWS applications gérées telles qu'Amazon Quick et Kiro.
- Des applications cloud comme Office 365, Concur, Salesforce, etc.

Lorsque les utilisateurs se connectent au portail, ils trouvent les applications Comptes AWS et les applications auxquelles ils sont autorisés à accéder sans connexion supplémentaire.

Commencer à utiliser le portail AWS d'accès

Pour les administrateurs :

Vous avez besoin d'un accès administratif à [l'instance de votre organisation](#) ou à [l'instance de compte](#) d'IAM Identity Center pour configurer le portail AWS d'accès et gérer l'accès des utilisateurs.

1. Personnalisez éventuellement l'URL du portail AWS d'accès.
2. Attribuez l'accès des utilisateurs aux applications Comptes AWS et aux applications. Les AWS ressources attribuées s'affichent dans le portail.

Pour les utilisateurs finaux :

Votre administrateur doit avoir terminé la configuration du portail AWS d'accès et vous avoir fourni l'URL de votre portail et vos informations de connexion.

1. Obtenez l'URL de votre portail auprès de votre administrateur (généralement `https://your-company.awsapps.com/start`).
2. Connectez-vous à l'aide des informations d'identification fournies par votre administrateur.
3. Accédez à vos ressources sur votre portail.

Configuration du portail AWS d'accès

En tant qu'administrateur, vous pouvez personnaliser le portail AWS d'accès pour répondre aux besoins de votre organisation et garantir que les utilisateurs peuvent accéder facilement à leurs ressources autorisées.

Ce que vous pouvez configurer

AWS activation du portail d'accès : configurez l'accès utilisateur initial au portail d' AWS accès, y compris l'activation des informations d'identification utilisateur et les processus de première connexion.

URL du portail AWS d'accès personnalisé (facultatif) : personnalisez l'URL du portail AWS d'accès de votre organisation en passant du format par défaut (d-xxxxxxxxxx.awsapps.com/start) à un sous-domaine plus reconnaissable (your-company.awsapps.com/start).

Avant de commencer

Assurez-vous de disposer d'un accès administratif à IAM Identity Center, vérifiez qu'IAM Identity Center est configuré en tant qu'instance d'[organisation ou en tant qu'instance](#) de [compte](#), et planifiez votre nom de sous-domaine personnalisé (il s'agit d'une configuration unique qui ne peut pas être modifiée ultérieurement).

Une fois configuré, les utilisateurs peuvent accéder au portail AWS d'accès à l'aide de l'URL personnalisée et suivre le processus d'activation que vous avez défini pour votre organisation.

Rubriques

- [Activation du portail AWS d'accès pour les nouveaux utilisateurs d'IAM Identity Center](#)
- [Personnalisation de l'URL du portail AWS d'accès](#)
- [Confirmez que les utilisateurs peuvent se connecter au portail AWS d'accès](#)

Activation du portail AWS d'accès pour les nouveaux utilisateurs d'IAM Identity Center

Si c'est la première fois que vous essayez de vous connecter au portail d' AWS accès, consultez vos e-mails pour obtenir des instructions sur la façon d'activer vos informations d'identification d'utilisateur.

Pour activer vos informations d'identification d'utilisateur

1. En fonction de l'e-mail que vous avez reçu de votre entreprise, choisissez l'une des méthodes suivantes pour activer vos informations d'identification utilisateur afin de pouvoir commencer à utiliser le portail AWS d'accès.
 - a. Si vous avez reçu un e-mail avec pour objet Invitation à rejoindre AWS IAM Identity Center, ouvrez-le et choisissez Accepter l'invitation. Sur la page d'inscription d'un nouvel utilisateur, entrez et confirmez un mot de passe, puis choisissez Définir un nouveau mot de passe. Vous utiliserez ce mot de passe chaque fois que vous vous connecterez au portail.
 - b. Si le support informatique ou l'administrateur informatique de votre entreprise vous ont envoyé un e-mail, suivez les instructions fournies pour activer vos informations d'identification utilisateur.
2. Une fois que vous avez activé vos informations d'identification d'utilisateur en fournissant un nouveau mot de passe, le portail d' AWS accès vous connecte automatiquement. Si ce n'est pas le cas, vous pouvez vous connecter manuellement au portail AWS d'accès en suivant les instructions fournies dans [Connexion au portail d' AWS accès](#).

Personnalisation de l'URL du portail AWS d'accès

Par défaut, vous pouvez accéder au portail AWS d'accès en utilisant une URL au format suivant :d-**xxxxxxxxxx**.awsapps.com/start. Vous pouvez personnaliser l'URL comme suit :**your_subdomain**.awsapps.com/start.

Important

Si vous modifiez l'URL du portail AWS d'accès, vous ne pourrez pas la modifier ultérieurement.

Pour personnaliser votre URL

1. Ouvrez la AWS IAM Identity Center console à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Dans la console IAM Identity Center, choisissez Dashboard dans le volet de navigation et recherchez la section récapitulative des paramètres.
3. Cliquez sur le bouton Personnaliser situé sous l'URL de votre portail AWS d'accès.

 Note

Si le bouton Personnaliser ne s'affiche pas, cela signifie que le portail AWS d'accès a déjà été personnalisé. La personnalisation de l'URL du portail d' AWS accès est une opération unique qui ne peut pas être annulée.

4. Entrez le nom de sous-domaine souhaité et choisissez Enregistrer.

Vous pouvez désormais vous connecter à la AWS console via votre portail AWS d'accès à l'aide de votre URL personnalisée.

Confirmez que les utilisateurs peuvent se connecter au portail AWS d'accès

Les étapes suivantes permettent à l'administrateur d'IAM Identity Center de confirmer que l'utilisateur d'IAM Identity Center peut se connecter au portail AWS d'accès et accéder au. Compte AWS

Connectez-vous au portail d' AWS accès

1. Procédez de l'une des manières suivantes pour vous connecter au AWS Management Console.
 - Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
 - Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous avec vos informations d'identification IAM et sélectionnez un rôle d'administrateur.
2. Ouvrez la [console IAM Identity Center](#).
3. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
4. Sur la page Tableau de bord, sous Résumé des paramètres, choisissez l'URL du portail AWS d'accès.
5. Connectez-vous en utilisant l'une des méthodes suivantes :
 - Si vous utilisez Active Directory ou un fournisseur d'identité externe (IdP) comme source d'identité, connectez-vous à l'aide des informations d'identification de l'utilisateur Active Directory ou IdP.

- Si vous utilisez le répertoire Identity Center par défaut comme source d'identité, connectez-vous en utilisant le nom d'utilisateur que vous avez spécifié lors de la création de l'utilisateur et le nouveau mot de passe que vous avez spécifié pour l'utilisateur.
6. Dans l'onglet Comptes, localisez-le Compte AWS et développez-le.
 7. Les rôles mis à votre disposition s'affichent. Par exemple, si l'ensemble d'autorisations et les AdministratorAccessensembles d'autorisations de facturation vous sont attribués, ces rôles sont affichés dans le portail AWS d'accès. Choisissez le nom du rôle IAM que vous souhaitez utiliser pour la session.
 8. Si vous êtes redirigé vers la console AWS de gestion, vous avez correctement configuré l'accès au Compte AWS.

 Note

Si aucune autorisation n'est Comptes AWSrépertoriée, il est probable que l'utilisateur n'ait pas encore reçu d'ensemble d'autorisations pour ce compte. Pour obtenir des instructions sur l'attribution d'utilisateurs à un ensemble d'autorisations, consultez [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).

Maintenant que vous avez confirmé que vous pouvez vous connecter à l'aide des informations d'identification IAM Identity Center, passez au navigateur que vous avez utilisé pour vous connecter AWS Management Console et déconnectez-vous à partir de vos informations d'identification d'utilisateur root ou d'utilisateur IAM.

 Important

Nous vous recommandons vivement d'utiliser les informations d'identification de l'utilisateur administratif d'IAM Identity Center lorsque vous vous connectez au portail d' AWS accès pour effectuer des tâches administratives au lieu d'utiliser les informations d'identification de l'utilisateur IAM ou de l'utilisateur root. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour permettre à d'autres utilisateurs d'accéder à vos comptes et applications, et pour administrer IAM Identity Center, créez et attribuez des ensembles d'autorisations uniquement via IAM Identity Center.

Utiliser le portail AWS d'accès

Vous pouvez lancer plusieurs applications en choisissant l'onglet Compte AWS ou application dans le portail. La présence d'icônes d'applications dans votre portail AWS d'accès signifie qu'un administrateur de votre entreprise vous a accordé l'accès à ces applications Comptes AWS ou à ces applications. Cela signifie également que vous pouvez accéder à tous ces comptes ou applications depuis le portail AWS d'accès sans demander de connexion supplémentaire.

Comment utiliser le portail AWS d'accès

Pour utiliser le portail AWS d'accès :

1. Obtenez l'URL de votre portail auprès de votre administrateur (cela ressemble généralement à `https://your-company.awsapps.com/start`).
2. Connectez-vous à l'aide des informations d'identification fournies par votre administrateur.
3. Choisissez les comptes et les applications de votre portail auxquels vous souhaitez accéder.

Votre administrateur contrôle ce que vous voyez sur le portail en fonction de votre rôle et de vos autorisations. Contactez votre administrateur pour demander un accès supplémentaire dans les situations suivantes :

- Aucune application à laquelle vous devez accéder ne s'affiche. Compte AWS
- L'accès que vous avez à un compte ou à une application donné n'est pas celui que vous attendiez.

Rubriques

- [Connexion au portail d' AWS accès](#)
- [Réinitialisation du mot de passe utilisateur de votre portail d' AWS accès](#)
- [Obtenir les informations d'identification utilisateur d'IAM Identity Center pour le ou AWS CLI AWS SDKs](#)
- [Création de liens de raccourci vers des AWS Management Console destinations](#)
- [Enregistrement de votre appareil à la MFA](#)
- [Afficher et terminer votre session active](#)

Connexion au portail d' AWS accès

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à toutes les applications Comptes AWS et applications qui leur sont assignées via un portail Web. Ce qui suit décrit comment vous connecter au portail AWS d'accès, des conseils pour vous connecter et comment vous déconnecter du portail d' AWS accès.

Conditions préalables

IAM Identity Center doit être activé pour utiliser le portail AWS d'accès. Pour de plus amples informations, veuillez consulter [Activer IAM Identity Center](#).

Note

Une fois connecté, la durée par défaut de votre session AWS au portail d'accès est de 8 heures. Sachez qu'un administrateur peut [modifier la durée](#) de cette session.

Connectez-vous au portail d' AWS accès

Pour vous connecter au portail AWS d'accès

1. Dans la fenêtre de votre navigateur, collez l'URL de connexion qui vous a été fournie et choisissez Enter. L'URL ressemble à `d-xxxxxxxxx.awsapps.com/start` ou `your_subdomain.awsapps.com/start`. Nous vous recommandons de placer un signet sur ce lien pour pouvoir le réutiliser facilement.
2. Connectez-vous à l'aide des identifiants de connexion standard de votre entreprise.

Note

Si votre administrateur vous a envoyé un mot de passe à usage unique (OTP) par e-mail et que c'est la première fois que vous vous connectez, saisissez-le. Une fois connecté, vous devez créer un nouveau mot de passe pour les connexions futures.

Si un code de vérification vous est demandé, consultez vos e-mails, puis copiez-collez le code sur la page de connexion.

 Note

Les codes de vérification sont généralement envoyés par e-mail, mais le mode de livraison peut varier. Consultez votre administrateur pour plus de détails.

3. Une fois connecté, vous pouvez accéder à toutes les applications AWS qui s'affichent sur le portail.

Appareils approuvés

Lorsque vous choisissez l'option *Ceci est un appareil fiable* sur la page de connexion, IAM Identity Center considère toutes les futures connexions à partir de cet appareil comme autorisées. Cela signifie qu'IAM Identity Center ne proposera pas d'option permettant de saisir un code MFA tant que vous utiliserez cet appareil fiable. Il existe toutefois certaines exceptions, notamment la connexion à partir d'un nouveau navigateur ou l'attribution d'une adresse IP inconnue à votre appareil.

Conseils de connexion pour le portail AWS d'accès

Voici quelques conseils pour vous aider à gérer l'expérience de votre portail d'accès AWS.

- Il peut arriver que vous deviez vous déconnecter puis vous reconnecter au portail AWS d'accès. Cela peut être nécessaire pour accéder aux nouvelles applications que votre administrateur vous a récemment attribuées. Ce n'est toutefois pas obligatoire, car toutes les nouvelles applications sont actualisées toutes les heures.
- Lorsque vous vous connectez au portail AWS d'accès, vous pouvez ouvrir n'importe laquelle des applications répertoriées dans le portail en choisissant l'icône de l'application. Une fois que vous avez terminé d'utiliser l'application, vous pouvez fermer l'application ou vous déconnecter du portail AWS d'accès. Si vous vous contentez de fermer l'application, vous n'êtes pas déconnecté du portail utilisateur. Toutes les autres applications que vous avez ouvertes depuis le portail AWS d'accès restent ouvertes et en cours d'exécution.
- Avant de pouvoir vous connecter en tant qu'utilisateur différent, vous devez d'abord vous déconnecter du portail AWS d'accès. Lorsque vous vous déconnectez du portail utilisateur, toutes vos informations d'identification sont supprimées de la session du navigateur.
- Une fois connecté au portail AWS d'accès, vous pouvez passer à un rôle. Le changement de rôle met temporairement de côté vos autorisations d'utilisateur d'origine et vous donne à la place

les autorisations attribuées au rôle. Pour plus d'informations, consultez [Changement de rôles \(console\)](#).

Déconnexion du portail AWS d'accès

Lorsque vous vous déconnectez du portail utilisateur, vos informations d'identification sont entièrement supprimées de la session du navigateur. Pour plus d'informations, voir [Déconnexion du portail AWS d'accès](#) dans le Connexion à AWSguide.

Pour vous déconnecter du portail AWS d'accès

- Dans le portail AWS d'accès, choisissez Se déconnecter dans la barre de navigation.

Note

Si vous souhaitez vous connecter en tant qu'utilisateur différent, vous devez d'abord vous déconnecter du portail AWS d'accès.

Réinitialisation du mot de passe utilisateur de votre portail d' AWS accès

Le portail AWS d'accès fournit aux utilisateurs d'[IAM Identity Center](#) un accès par authentification unique à tous les AWS comptes et applications cloud qui leur sont attribués via un portail Web. Le portail AWS d'accès est différent du [AWS Management Console](#), qui est un ensemble de consoles de service permettant de gérer les AWS ressources.

Utilisez cette procédure pour réinitialiser votre mot de passe utilisateur IAM Identity Center pour le portail AWS d'accès. Pour en savoir plus sur les [types d'utilisateurs](#), consultez le guide de Connexion à AWS l'utilisateur.

Considérations

La fonctionnalité de réinitialisation de votre mot de passe pour votre portail d' AWS accès n'est disponible que pour les utilisateurs des instances d'Identity Center qui utilisent le répertoire Identity Center ou [AWS Managed Microsoft AD](#) comme source d'identité. Si votre utilisateur est connecté à un fournisseur d'identité externe ou à un [AD Connector](#), les réinitialisations du mot de passe utilisateur doivent être effectuées depuis le fournisseur d'identité externe ou être connectéActive Directory.

- Si votre source d'identité est un annuaire IAM Identity Center, consultez [Exigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center](#).
- Si votre source d'identité est une AWS Managed Microsoft AD, consultez la section [Exigences relatives au mot de passe lors de la réinitialisation d'un mot de passe](#). AWS Managed Microsoft AD

Pour réinitialiser votre mot de passe pour AWS accéder au portail d'accès

1. Ouvrez un navigateur Web et accédez à la page de connexion de votre portail AWS d'accès.

Si vous n'avez pas l'URL de votre portail d' AWS accès, vérifiez vos e-mails. Vous devriez avoir reçu par e-mail une invitation à rejoindre AWS IAM Identity Center qui inclut une URL de connexion spécifique au portail d'accès. AWS Il se peut également que votre administrateur vous ait directement fourni un mot de passe à usage unique et l'URL du portail AWS d'accès. Si vous ne trouvez pas ces informations, demandez à votre administrateur de vous les envoyer.

Pour plus d'informations sur la connexion au portail AWS d'accès, voir [Se connecter au portail AWS d'accès](#) dans le guide de Connexion à AWS l'utilisateur.

2. Entrez votre nom d'utilisateur, puis choisissez Next.
3. Sous Mot de passe, choisissez Mot de passe oublié.

Vérifiez votre nom d'utilisateur et entrez les caractères de l'image fournie pour confirmer que vous n'êtes pas un robot. Ensuite, sélectionnez Suivant. Vous devrez peut-être désactiver le logiciel de blocage des publicités si vous ne pouvez pas saisir de caractères.

4. Un message s'affiche pour confirmer qu'un e-mail de réinitialisation du mot de passe a été envoyé. Sélectionnez Continuer.
5. Vous recevrez un e-mail de la part du destinataire `no-reply@signin.aws` avec le sujet Réinitialisation du mot de passe demandée. Dans votre e-mail, choisissez Réinitialiser le mot de passe.
6. Sur la page Réinitialiser le mot de passe, vérifiez votre nom d'utilisateur, spécifiez un nouveau mot de passe pour le portail AWS d'accès, puis choisissez Définir un nouveau mot de passe.
7. Vous recevrez un e-mail de la part de celui-ci `no-reply@signin.aws` dont l'objet sera « Mot de passe mis à jour ».

 Note

Un administrateur peut réinitialiser votre mot de passe soit en vous envoyant un e-mail contenant des instructions pour réinitialiser votre mot de passe, soit en générant un mot de passe à usage unique et en le partageant avec vous. Si vous êtes administrateur, veuillez consulter [Réinitialisation du mot de passe utilisateur IAM Identity Center pour un utilisateur final](#).

Obtenir les informations d'identification utilisateur d'IAM Identity Center pour le ou AWS CLI AWS SDKs

Vous pouvez accéder aux AWS services par programmation en utilisant le AWS Command Line Interface ou les kits de développement AWS logiciel (SDKs) avec les informations d'identification utilisateur d'IAM Identity Center. Cette rubrique décrit comment obtenir des informations d'identification temporaires pour un utilisateur dans IAM Identity Center.

Le portail AWS d'accès fournit aux utilisateurs d'IAM Identity Center un accès par authentification unique à leurs applications Comptes AWS et à celles du cloud. Une fois connecté au portail d'AWS accès en tant qu'utilisateur d'IAM Identity Center, vous pouvez obtenir des informations d'identification temporaires. Vous pouvez ensuite utiliser les informations d'identification, également appelées informations d'identification utilisateur IAM Identity Center, dans le AWS CLI ou AWS SDKs pour accéder aux ressources d'un Compte AWS.

Si vous utilisez le AWS CLI pour accéder aux AWS services par programmation, vous pouvez utiliser les procédures décrites dans cette rubrique pour initier l'accès au. AWS CLI Pour plus d'informations à ce sujet AWS CLI, consultez le [guide de AWS Command Line Interface l'utilisateur](#).

Si vous utilisez le AWS SDKs pour accéder aux AWS services par programmation, le respect des procédures décrites dans cette rubrique permet également d'établir directement l'authentification pour le. AWS SDKs Pour plus d'informations sur le AWS SDKs, consultez le [guide de référence sur les outils AWS SDKs et](#).

 Note

Les utilisateurs d'IAM Identity Center sont différents des utilisateurs d'[IAM](#). Les utilisateurs IAM reçoivent des informations d'identification à long terme pour les AWS ressources. Les utilisateurs d'IAM Identity Center reçoivent des informations d'identification temporaires. Nous

vous recommandons d'utiliser des informations d'identification temporaires comme meilleure pratique de sécurité pour accéder à votre compte, Comptes AWS car ces informations d'identification sont générées à chaque fois que vous vous connectez.

Conditions préalables

Pour obtenir des informations d'identification temporaires pour votre utilisateur IAM Identity Center, vous aurez besoin des éléments suivants :

- Un utilisateur du IAM Identity Center : vous allez vous connecter au portail AWS d'accès en tant qu'utilisateur. Vous ou votre administrateur pouvez créer cet utilisateur. Pour plus d'informations sur la façon d'activer IAM Identity Center et de créer un utilisateur IAM Identity Center, consultez [Commencer à utiliser IAM Identity Center](#)
- Accès utilisateur à un Compte AWS — Pour accorder à un utilisateur IAM Identity Center l'autorisation de récupérer ses informations d'identification temporaires, vous ou un administrateur devez attribuer à l'utilisateur IAM Identity Center un ensemble d'[autorisations](#). Les ensembles d'autorisations sont stockés dans IAM Identity Center et définissent le niveau d'accès d'un utilisateur d'IAM Identity Center à un. Compte AWS Si votre administrateur a créé l'utilisateur IAM Identity Center pour vous, demandez-lui d'ajouter cet accès pour vous. Pour de plus amples informations, veuillez consulter [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).
- AWS CLI installé — Pour utiliser les informations d'identification temporaires, vous devez installer le AWS CLI. Pour obtenir des instructions, consultez [Installation ou mise à jour de la dernière version de l' AWS CLI](#) dans le Guide de l'utilisateur de l'AWS CLI .

Considérations

Avant de terminer les étapes permettant d'obtenir des informations d'identification temporaires pour votre utilisateur IAM Identity Center, tenez compte des points suivants :

- IAM Identity Center crée des rôles IAM : lorsque vous assignez un utilisateur dans IAM Identity Center à un ensemble d'autorisations, IAM Identity Center crée un rôle IAM correspondant à partir du jeu d'autorisations. Les rôles IAM créés par des ensembles d'autorisations diffèrent des rôles IAM créés de la Gestion des identités et des accès AWS manière suivante :
 - IAM Identity Center possède et sécurise les rôles créés par les ensembles d'autorisations. Seul IAM Identity Center peut modifier ces rôles.

- Seuls les utilisateurs d'IAM Identity Center peuvent assumer les rôles correspondant aux ensembles d'autorisations qui leur ont été attribués. Vous ne pouvez pas attribuer d'accès aux ensembles d'autorisations aux utilisateurs IAM, aux utilisateurs fédérés IAM ou aux comptes de service.
- Vous ne pouvez pas modifier une politique de confiance relative à ces rôles pour autoriser l'accès aux [principaux en dehors d'IAM Identity Center](#).

Pour plus d'informations sur la façon d'obtenir des informations d'identification temporaires pour un rôle que vous créez dans IAM, consultez la section [Utilisation des informations d'identification de sécurité temporaires AWS CLI dans le](#) guide de l'Gestion des identités et des accès AWS utilisateur.

- Vous pouvez définir la durée de session pour les ensembles d'autorisations : une fois que vous vous êtes connecté au portail d' AWS accès, le jeu d'autorisations auquel votre utilisateur IAM Identity Center est attribué apparaît comme un rôle disponible. IAM Identity Center crée une session distincte pour ce rôle. Cette session peut durer de une à 12 heures, selon la durée de session configurée pour l'ensemble d'autorisations. La durée de session par défaut est d'une heure. Pour de plus amples informations, veuillez consulter [Définissez la durée de session pour Comptes AWS](#).

Obtenir et actualiser les informations d'identification temporaires

Vous pouvez obtenir et actualiser les informations d'identification temporaires de votre utilisateur IAM Identity Center automatiquement ou manuellement.

Rubriques

- [Actualisation automatique des informations d'identification \(recommandée\)](#)
- [Actualisation manuelle des informations d'identification](#)

Actualisation automatique des informations d'identification (recommandée)

L'actualisation automatique des informations d'identification utilise la norme Open ID Connect (OIDC) Device Code Authorization. Avec cette méthode, vous initiez l'accès directement à l'aide de la `aws configure sso` commande du AWS CLI. Vous pouvez utiliser cette commande pour accéder automatiquement à tout rôle associé à un ensemble d'autorisations qui vous est attribué pour n'importe quel rôle Compte AWS.

Pour accéder au rôle créé pour votre utilisateur IAM Identity Center, exécutez la `aws configure sso` commande, puis autorisez-la AWS CLI depuis une fenêtre de navigateur. Tant que vous avez une session active sur le portail AWS d'accès, il récupère AWS CLI automatiquement les informations d'identification temporaires et les actualise automatiquement.

Pour plus d'informations, consultez la section [Configurer votre profil avec le `aws configure sso` wizard](#) dans le guide de AWS Command Line Interface l'utilisateur.

Pour obtenir des informations d'identification temporaires qui s'actualisent automatiquement

1. Connectez-vous au portail AWS d'accès en utilisant l'URL de connexion spécifique fournie par votre administrateur. Si vous avez créé l'utilisateur IAM Identity Center, vous avez AWS envoyé une invitation par e-mail contenant votre URL de connexion. Pour plus d'informations, voir [Se connecter au portail AWS d'accès](#) dans le Guide de l'utilisateur de AWS connexion.
2. Dans l'onglet Comptes, recherchez les informations d'identification Compte AWS à partir desquelles vous souhaitez récupérer les informations d'identification. Lorsque vous choisissez le compte, le nom du compte, l'identifiant du compte et l'adresse e-mail associés au compte apparaissent.

 Note

Si aucune autorisation n'est Comptes AWS répertoriée, il est probable qu'aucun ensemble d'autorisations ne vous ait encore été attribué pour ce compte. Dans ce cas, contactez votre administrateur et demandez-lui d'ajouter cet accès pour vous. Pour de plus amples informations, veuillez consulter [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).

3. Sous le nom du compte, le jeu d'autorisations auquel votre utilisateur IAM Identity Center est attribué apparaît sous la forme d'un rôle disponible. Par exemple, si l'utilisateur de votre IAM Identity Center est affecté à l'ensemble d'PowerUserAccess autorisations pour le compte, le rôle apparaît dans le portail AWS d'accès sous PowerUserAccess la forme.
4. En fonction de l'option que vous avez choisie à côté du nom du rôle, choisissez les touches d'accès ou l'accès par ligne de commande ou par programmation.
5. Dans la boîte de dialogue Obtenir les informations d'identification, choisissez macOS et Linux, Windows ou PowerShell, selon le système d'exploitation sur lequel vous avez installé le AWS CLI.

6. Sous les informations d'identification du centre d'identité AWS IAM (recommandé), vos SSO Start URL identifiants SSO Region sont affichés. Ces valeurs sont requises pour configurer à la fois un profil activé par IAM Identity Center et sso-session pour votre AWS CLI. Pour terminer cette configuration, suivez les instructions de la section [Configurer votre profil aws configure sso wizard à l'aide du](#) guide de l'AWS Command Line Interface utilisateur.

Continuez à utiliser le AWS CLI selon vos besoins Compte AWS jusqu'à ce que les informations d'identification aient expiré.

Actualisation manuelle des informations d'identification

Vous pouvez utiliser la méthode d'actualisation manuelle des informations d'identification pour obtenir des informations d'identification temporaires pour un rôle associé à un ensemble d'autorisations spécifique dans un domaine spécifique Compte AWS. Pour ce faire, vous devez copier et coller les commandes requises pour les informations d'identification temporaires. Avec cette méthode, vous devez actualiser les informations d'identification temporaires manuellement.

Vous pouvez exécuter des AWS CLI commandes jusqu'à ce que vos informations d'identification temporaires expirent.

Pour obtenir des informations d'identification que vous actualisez manuellement

1. Connectez-vous au portail AWS d'accès en utilisant l'URL de connexion spécifique fournie par votre administrateur. Si vous avez créé l'utilisateur IAM Identity Center, vous avez AWS envoyé une invitation par e-mail contenant votre URL de connexion. Pour plus d'informations, voir [Se connecter au portail AWS d'accès](#) dans le Guide de l'utilisateur de AWS connexion.
2. Dans l'onglet Comptes, recherchez le nom du rôle IAM à Compte AWS partir duquel vous souhaitez récupérer les informations d'accès et développez-le pour afficher le nom du rôle IAM (par exemple Administrateur). En fonction de votre option à côté du nom du rôle IAM, choisissez les touches d'accès ou choisissez l'accès par ligne de commande ou par programmation.

Note

Si aucune autorisation n'est Comptes AWS répertoriée, il est probable qu'aucun ensemble d'autorisations ne vous ait encore été attribué pour ce compte. Dans ce cas, contactez votre administrateur et demandez-lui d'ajouter cet accès pour vous. Pour de plus amples informations, veuillez consulter [Attribuer l'accès d'un utilisateur ou d'un groupe à Comptes AWS](#).

3. Dans la boîte de dialogue Obtenir les informations d'identification, choisissez macOS et Linux, Windows ou PowerShell, selon le système d'exploitation sur lequel vous avez installé le AWS CLI.
4. Choisissez l'une des options suivantes :

- Option 1 : définir les variables d' AWS environnement

Choisissez cette option pour annuler tous les paramètres d'identification, y compris les paramètres des `credentials` fichiers et `config` des fichiers. Pour plus d'informations, consultez la section [Variables d'environnement pour les configurer AWS CLI](#) dans le Guide de AWS CLI l'utilisateur.

Pour utiliser cette option, copiez les commandes dans votre presse-papiers, collez-les dans la fenêtre de votre AWS CLI terminal, puis appuyez sur Entrée pour définir les variables d'environnement requises.

- Option 2 : ajouter un profil à votre fichier AWS d'informations d'identification

Choisissez cette option pour exécuter des commandes avec différents ensembles d'informations d'identification.

Pour utiliser cette option, copiez les commandes dans votre presse-papiers, puis collez-les dans votre AWS `credentials` fichier partagé pour configurer un nouveau profil nommé. Pour plus d'informations, consultez la section [Fichiers de configuration et d'informations d'identification partagés](#) dans le Guide de référence AWS SDKs et Tools. Pour utiliser ces informations d'identification, spécifiez l'`--profile` option dans votre AWS CLI commande. Cela concerne tous les environnements qui utilisent le même fichier d'informations d'identification.

- Option 3 : utilisez des valeurs individuelles dans votre AWS service client

Choisissez cette option pour accéder aux AWS ressources d'un client AWS de service. Pour de plus amples informations, veuillez consulter [Outils pour créer sur AWS](#).

Pour utiliser cette option, copiez les valeurs dans votre presse-papiers, collez-les dans votre code et attribuez-les aux variables appropriées pour votre SDK. Pour plus d'informations, consultez la documentation de l'API de votre SDK spécifique.

Création de liens de raccourci vers des AWS Management Console destinations

Les liens de raccourci créés dans le portail AWS d'accès dirigent les utilisateurs d'IAM Identity Center vers une destination spécifique dans le AWS Management Console, avec un ensemble d'autorisations spécifique, et dans un autre. Compte AWS

Les liens de raccourci vous font gagner du temps, à vous et à vos collaborateurs. Au lieu de naviguer vers l'URL de destination souhaitée AWS Management Console (par exemple, une page d'instance de compartiment Amazon S3) via plusieurs pages, y compris le portail AWS d'accès, vous pouvez utiliser un lien de raccourci pour accéder automatiquement à la même destination.

Options de destination des liens de raccourci

Les liens de raccourci comportent trois options de destination, répertoriées ici par ordre de priorité :

- (Facultatif) Toute URL de destination AWS Management Console spécifiée dans le lien de raccourci. Par exemple, la page relative à l'instance du compartiment Amazon S3.
- (Facultatif) URL de l'état du relais configurée par l'administrateur pour l'ensemble d'autorisations en question. Pour plus d'informations sur le réglage de l'état du relais, consultez [Réglez l'état du relais pour un accès rapide au AWS Management Console](#).
- AWS Management Console maison. Destination par défaut si vous n'en spécifiez aucune.

Note

La navigation automatique vers une destination n'est réussie que lorsque vous êtes authentifié auprès d'IAM Identity Center et que les autorisations nécessaires sont attribuées pour le AWS compte et l'URL de destination.

Le portail AWS d'accès inclut un bouton Créer un raccourci qui vous permet de créer un lien de raccourci partageable. Si vous prévoyez de spécifier une URL de destination (première option de la liste précédente), vous pouvez copier l'URL dans un presse-papiers pour la partager.

Création d'un lien de raccourci dans le portail AWS d'accès

1. Lorsque vous êtes connecté au portail AWS d'accès, cliquez sur l'onglet Comptes, puis sur le bouton Créer un raccourci.

2. Dans la boîte de dialogue :

- a. Choisissez un Compte AWS en utilisant l'identifiant ou le nom du compte. Au fur et à mesure que vous tapez, un menu déroulant affiche le compte correspondant IDs et les noms auxquels vous pouvez accéder. Vous ne pouvez choisir qu'un compte auquel vous avez accès.
- b. Choisissez éventuellement un rôle IAM dans la liste déroulante. Il s'agit des ensembles d'autorisations qui vous sont attribués pour le compte sélectionné. Si vous omettez de sélectionner le rôle, les utilisateurs sont invités à en sélectionner un qui leur est attribué pour le compte choisi lorsqu'ils utilisent le lien de raccourci.

Note

Vous ne pouvez pas accorder de nouveaux accès à l'aide de liens de raccourci. Les liens de raccourci fonctionnent uniquement avec les ensembles d'autorisations déjà attribués à l'utilisateur. Si l'utilisateur ne dispose pas des ensembles d'autorisations nécessaires pour le compte et l'URL de destination, l'accès lui est refusé.

- c. Entrez éventuellement l'URL de destination du portail d' AWS accès. Si vous omettez de saisir une URL, la destination est automatiquement déterminée lors de l'utilisation du lien de raccourci, en fonction des options de destination du lien de raccourci mentionnées précédemment.
- d. Votre lien de raccourci est généré en bas de la boîte de dialogue, en fonction de vos entrées. Cliquez sur le bouton Copier l'URL. Vous pouvez désormais créer un signet avec le lien de raccourci copié ou le partager avec vos collaborateurs qui ont accès au même compte avec le même ensemble d'autorisations ou un autre ensemble d'autorisations suffisant.

Création de liens de AWS Management Console raccourci sécurisés avec encodage d'URL

Toutes les valeurs des paramètres de l'URL, y compris l'ID du compte, le nom de l'ensemble d'autorisations et l'URL de destination, doivent être codées en URL.

Les liens de raccourci étendent l'URL du portail d' AWS accès avec le chemin suivant :

`/#/console?`

`account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]`

L'URL complète de la AWS partition classique suit le modèle suivant :

IPv4 point de terminaison :

```
https://[your_subdomain].awsapps.com/start/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Point de terminaison à double pile

```
https://[identity_center_instance_id].portal.[region].app.aws/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Voici un exemple de lien de raccourci qui permet à un utilisateur de se connecter à un compte 123456789012 avec l'ensemble d'S3FullAccess autorisations et d'accéder à la page d'accueil de la console S3 :

- IPv4 point de terminaison : `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- Point de terminaison à double pile : `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) IPv4 point de terminaison : `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) Point de terminaison à double pile : `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Enregistrement de votre appareil à la MFA

Pour les utilisateurs de l'annuaire Identity Center, suivez la procédure suivante dans le portail AWS d'accès pour enregistrer votre nouvel appareil pour l'authentification multifactorielle (MFA).

 Important

Le MFA dans IAM Identity Center n'est actuellement pas pris en charge pour les fournisseurs d'identité [externes](#).

Avant de commencer

Nous vous recommandons de télécharger d'abord l'application Authenticator appropriée sur votre appareil avant de commencer les étapes de cette procédure. Pour obtenir la liste des applications que vous pouvez utiliser pour les appareils MFA, consultez. [Applications d'authentification virtuelle](#)

Enregistrez votre appareil

Pour enregistrer votre appareil afin de l'utiliser avec le MFA

1. Connectez-vous à votre portail AWS d'accès. Pour de plus amples informations, veuillez consulter [Connexion au portail d' AWS accès](#).
2. En haut à droite de la page, sélectionnez les appareils MFA.
3. Sur la page des appareils d'authentification multifactorielle (MFA), choisissez Enregistrer un appareil.

 Note

Si l'option Enregistrer un appareil MFA est grisée, contactez votre administrateur pour obtenir de l'aide pour enregistrer votre appareil.

4. Sur la page Enregistrer un appareil MFA, sélectionnez l'un des types de périphériques MFA suivants et suivez les instructions :

- Application Authenticator

1. Sur la page Configurer l'application d'authentification, vous remarquerez peut-être des informations de configuration pour le nouveau dispositif MFA, notamment un code QR graphique. Le graphique est une représentation de la clé secrète qui peut être saisie manuellement sur les appareils qui ne prennent pas en charge les codes QR.
2. À l'aide du périphérique MFA physique, procédez comme suit :
 - a. Ouvrez une application d'authentification MFA compatible. Pour obtenir la liste des applications testées que vous pouvez utiliser avec les appareils MFA, consultez.

[Applications d'authentification virtuelle](#) Si l'application MFA prend en charge plusieurs comptes (plusieurs appareils MFA), choisissez l'option permettant de créer un nouveau compte (un nouvel appareil MFA).

- b. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des opérations suivantes sur la page Configurer l'application d'authentification :
 - i. Choisissez Afficher le code QR, puis utilisez l'application pour scanner le code QR. Par exemple, vous pouvez choisir l'icône de l'appareil photo ou une option similaire à Scanner le code. Utilisez ensuite l'appareil photo de l'appareil pour scanner le code.
 - ii. Choisissez Afficher la clé secrète, puis entrez cette clé secrète dans votre application MFA.

 Important

Lorsque vous configurez un dispositif MFA pour IAM Identity Center, nous vous recommandons d'enregistrer une copie du code QR ou de la clé secrète dans un endroit sûr. Cela peut être utile si vous perdez le téléphone ou si vous devez réinstaller l'application d'authentification MFA. Si l'une de ces situations se produit, vous pouvez rapidement reconfigurer l'application pour qu'elle utilise la même configuration MFA.

3. Sur la page Configurer l'application d'authentification, sous Code d'authentification, entrez le mot de passe à usage unique qui apparaît actuellement sur le dispositif MFA physique.

 Important

Envoyez votre demande immédiatement après avoir généré le code. Si vous générez le code puis attendez trop longtemps pour soumettre la demande, le dispositif MFA est correctement associé à votre utilisateur, mais le dispositif MFA n'est pas synchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez synchroniser à nouveau l'appareil.

4. Choisissez Assign MFA (Affecter le MFA). Le dispositif MFA peut désormais commencer à générer des mots de passe à usage unique et est maintenant prêt à être utilisé avec. AWS

- Clé de sécurité ou authentificateur intégré

1. Sur la page Enregistrer la clé de sécurité de votre utilisateur, suivez les instructions fournies par votre navigateur ou votre plateforme.

 Note

L'expérience varie en fonction du navigateur ou de la plateforme. Une fois votre appareil enregistré avec succès, vous pouvez associer un nom d'affichage convivial à votre appareil nouvellement inscrit. Pour modifier le nom, choisissez Renommer, entrez le nouveau nom, puis cliquez sur Enregistrer.

Afficher et terminer votre session active

Vous pouvez utiliser votre portail AWS d'accès pour consulter la liste de vos sessions actives et, si nécessaire, mettre fin à une ou plusieurs sessions.

Terminez votre session active à l'aide de votre portail AWS d'accès

1. Connectez-vous à votre portail AWS d'accès. Pour de plus amples informations, veuillez consulter [Connexion au portail d' AWS accès](#).
2. Dans le coin supérieur droit de la page, sélectionnez Sécurité.
3. Sur la page Sécurité, le nombre entre parenthèses à côté de Sessions actives indique le nombre de sessions actives dont vous disposez. Cochez la case à côté de chaque session à laquelle vous souhaitez mettre fin, puis choisissez Terminer les sessions.

 Tip

Pour les sessions d'arrière-plan de l'utilisateur, vous pouvez rechercher des sessions par le nom de ressource Amazon (ARN) de la tâche qui utilise la session. Dans la liste Type de session, choisissez Sessions d'arrière-plan utilisateur, puis entrez l'ARN de la tâche dans le champ de recherche.

Vous ne pouvez mettre fin qu'aux sessions actives qui sont chargées. Si vous avez de nombreuses sessions, choisissez Charger plus de sessions actives pour afficher des sessions supplémentaires.

4. Cochez la case à côté de chaque session à laquelle vous souhaitez mettre fin, puis choisissez Terminer les sessions.
5. Une boîte de dialogue apparaît pour confirmer que vous mettez fin aux sessions actives. Passez en revue les informations, et si vous souhaitez continuer, tapez `confirm`, puis choisissez Terminer les sessions.
6. Vous revenez à votre liste de sessions actives. Un message de notification vert apparaît pour indiquer que les sessions sélectionnées se sont terminées avec succès.

Utilisation d'IAM Identity Center sur plusieurs Régions AWS

Cette rubrique explique comment l'utiliser AWS IAM Identity Center sur plusieurs appareils Régions AWS. Découvrez comment répliquer votre instance dans d'autres régions, gérer l'accès du personnel et les sessions, déployer des applications et maintenir l'accès aux comptes en cas d'interruption de service.

Lorsque vous activez une instance d'organisation d'IAM Identity Center, vous en choisissez une seule Région AWS (région principale). Vous pouvez répliquer cette instance vers une instance supplémentaire Régions AWS si elle répond à certaines conditions préalables. IAM Identity Center réplique automatiquement les identités du personnel, les ensembles d'autorisations, les affectations d'utilisateurs et de groupes, les sessions et les autres métadonnées de la région principale vers les régions supplémentaires choisies.

Avantages du support multirégional

La réplication d'IAM Identity Center vers Régions AWS un autre offre deux avantages essentiels :

- Résilience d' Compte AWS accès améliorée : votre personnel peut accéder à ses Compte AWS données même si l'instance IAM Identity Center subit une interruption de service dans sa région principale. Cela s'applique à l'accès avec des autorisations accordées avant l'interruption.
- Flexibilité accrue dans le choix des régions de déploiement pour les applications AWS gérées : vous pouvez déployer des applications AWS gérées dans vos régions préférées afin de répondre aux exigences de résidence des données des applications et d'améliorer les performances grâce à la proximité des utilisateurs. Les applications déployées dans d'autres régions accèdent aux identités du personnel répliquées localement pour des performances et une fiabilité optimales.

Prérequis et considérations

Avant de répliquer votre instance IAM Identity Center, assurez-vous que les exigences suivantes sont respectées :

- Type d'instance : votre instance IAM Identity Center doit être une [instance d'organisation](#). Le support multirégional n'est pas disponible dans les [instances de compte](#).

- Source d'identité : votre instance IAM Identity Center doit être connectée à un fournisseur d'identité externe (IdP), tel que [Okta](#). La prise en charge multirégionale n'est pas disponible pour les instances qui utilisent [Active Directory](#) ou le [répertoire Identity Center](#) comme source d'identité.
- AWS Régions - Le support multirégional est disponible dans [les régions commerciales activées par défaut](#) dans votre Compte AWS. Les régions optionnelles ne sont actuellement pas prises en charge.
- Type de clé KMS pour le chiffrement au repos : votre instance IAM Identity Center doit être configurée avec une clé [KMS gérée par le client](#) dans plusieurs régions. La clé KMS doit se trouver dans le même AWS compte qu'IAM Identity Center. Pour de plus amples informations, veuillez consulter [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#).
- AWS compatibilité des applications gérées : consultez le tableau des applications [the section called “Applications que vous pouvez utiliser avec IAM Identity Center”](#) pour vérifier les deux exigences suivantes :
 - Toutes les applications AWS gérées utilisées par votre organisation doivent prendre en charge le centre d'identité IAM configuré avec une clé KMS gérée par le client.
 - Les applications AWS gérées que vous souhaitez déployer dans des régions supplémentaires doivent prendre en charge ce type de déploiement.
- Compatibilité avec l'IdP externe : pour tirer pleinement parti de la prise en charge multirégionale, l'IdP externe doit prendre en charge le service ACS (Multiple Assertion Consumer Service). URLs Il s'agit d'une fonctionnalité SAML prise en charge par Okta, Microsoft Entra ID, PingFederate, PingOne, et JumpCloud.

Si vous utilisez un IdP qui ne prend pas en charge plusieurs ACS URLs, par exemple Google Workspace, nous vous recommandons de contacter votre fournisseur d'IdP pour activer cette fonctionnalité. Pour les options disponibles sans plusieurs ACS URLs, voir [the section called “Utilisation d'applications AWS gérées sans plusieurs ACS URLs”](#) et [the section called “Compte AWS résilience des accès sans plusieurs ACS URLs”](#).

Choix d'une région supplémentaire

Lorsque vous choisissez une région supplémentaire parmi les régions commerciales activées par défaut, tenez compte des facteurs suivants :

- Exigences de conformité : si vous devez exécuter des applications AWS gérées qui accèdent à des ensembles de données limités à une région spécifique pour des raisons de conformité, choisissez la région dans laquelle se trouvent les ensembles de données.

- Optimisation des performances : si la résidence des données n'est pas un facteur, sélectionnez la région la plus proche des utilisateurs de votre application afin d'optimiser leur expérience.
- Assistance aux applications — Vérifiez que les AWS applications requises sont disponibles dans la région que vous avez choisie.
- Compte AWS résilience de l'accès : pour garantir la continuité de l'accès à Compte AWS s, choisissez une région géographiquement éloignée de la région principale de votre instance IAM Identity Center.

 Note

IAM Identity Center dispose d'un quota sur le nombre de Régions AWS. Pour de plus amples informations, veuillez consulter [the section called “Quotas supplémentaires”](#).

Répliquer le centre d'identité IAM dans une région supplémentaire

Si votre environnement répond aux [conditions requises](#), telles que la configuration d'IAM Identity Center à l'aide d'une clé KMS multirégionale gérée par le client, effectuez les étapes suivantes pour répliquer votre instance IAM Identity Center dans une région supplémentaire. Votre région principale continue de fonctionner normalement pendant et après ces étapes.

Étape 1 : créer une réplique de clé dans la région supplémentaire

Avant de répliquer IAM Identity Center vers une région, vous devez d'abord créer une clé de réplique de votre clé KMS gérée par le client dans cette région et configurer la clé de réplique avec les autorisations requises pour le fonctionnement d'IAM Identity Center. Pour obtenir des instructions sur la création de clés de réplification multirégionales, consultez la section [Création de clés de réplification multirégionales](#).

L'approche recommandée pour les autorisations relatives aux clés KMS consiste à copier la politique clé à partir de la clé primaire, qui accorde les mêmes autorisations déjà établies pour le centre d'identité IAM dans la région principale. Vous pouvez également définir des politiques clés spécifiques à une région, bien que cette approche complique la gestion des autorisations entre les régions et puisse nécessiter une coordination supplémentaire lors de la mise à jour des politiques à l'avenir.

 Note

AWS KMS ne synchronise pas votre politique de clé KMS entre les régions de votre clé KMS multirégionale. Pour que la politique des clés KMS reste synchronisée dans les régions clés KMS, vous devez appliquer les modifications dans chaque région individuellement.

Étape 2 : ajouter la région dans le centre d'identité IAM

L'ajout d'une région dans le centre d'identité IAM déclenche la réplication automatique des données du centre d'identité IAM dans cette région. La réplication est asynchrone avec une cohérence éventuelle. Les onglets suivants fournissent des instructions pour effectuer cette opération dans AWS Management Console et AWS CLI.

Console

Pour ajouter une région

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez l'onglet Gestion.
4. Dans la section Régions pour le centre d'identité IAM, sélectionnez Ajouter une région.
5. Dans la section Régions AWS Disponible pour la réplication, sélectionnez votre option préférée Région AWS. Si la région n'apparaît pas dans la liste, elle n'est pas disponible pour la réplication car la clé KMS n'y a pas été répliquée. Pour de plus amples informations, veuillez consulter [the section called "Mise en œuvre de clés KMS gérées par le client"](#).
6. Choisissez Ajouter une région.
7. Dans la section Régions pour le centre d'identité IAM, surveillez le statut de la région. Utilisez le bouton Actualiser (flèche circulaire) pour vérifier le dernier état de la région selon les besoins. Une fois la réplication terminée, passez à l'étape 2.

AWS CLI

Pour ajouter une région

```
aws sso-admin add-region \  
--instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
```



```
--region-name eu-west-1
```

Pour vérifier le statut actuel de la région

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Lorsque le statut de la région est ACTIF, vous pouvez passer à l'étape 2.

La durée de la répliquation initiale vers une région supplémentaire dépend de la quantité de données contenue dans votre instance IAM Identity Center. Les modifications incrémentielles ultérieures sont répliquées en quelques secondes dans la plupart des cas.

Étape 3 : Mettre à jour la configuration de l'IdP externe

Suivez le didacticiel correspondant à votre IdP externe [Tutoriels d'identification des sources](#) pour suivre les étapes suivantes :

Étape 3.a : Ajoutez l'Assertion Consumer Service (ACS) URLs à votre IdP externe

Cette étape permet la connexion directe à chaque région supplémentaire et est requise pour permettre la connexion aux applications AWS gérées déployées dans ces régions et pour accéder à Compte AWS s via ces régions. Pour savoir où se trouve l'ACS URLs, voir [Points de terminaison ACS dans le primaire et dans le module supplémentaire Régions AWS](#).

Étape 3.b (facultatif) : Rendre le Portail d'accès AWS disponible sur le portail IdP externe

Rendez la Portail d'accès AWS région supplémentaire disponible sous forme d'application de favoris sur le portail IdP externe. Les applications de favoris contiennent uniquement un lien (URL) vers la destination souhaitée et sont similaires à un signet de navigateur. Vous pouvez les trouver Portail d'accès AWS URLs dans la console en choisissant Afficher tout Portail d'accès AWS URLs dans la section Régions pour le centre d'identité IAM. Pour de plus amples informations, veuillez consulter [the section called “AWS accéder aux points de terminaison du portail dans le système principal et dans le système supplémentaire Régions AWS”](#).

IAM Identity Center prend en charge le SSO SAML initié par l'IdP dans chaque région supplémentaire, mais les applications externes le prennent IdPs généralement en charge avec une seule URL ACS. Pour des raisons de continuité, nous vous recommandons de continuer à utiliser

l'URL ACS de la région principale pour l'authentification unique SAML initiée par l'IdP et de vous fier aux applications de favoris et aux signets du navigateur pour accéder à des régions supplémentaires.

Étape 4 : Confirmer les listes d'autorisation du pare-feu et de la passerelle

[Passez en revue vos listes d'autorisation de domaines dans les pare-feux ou les passerelles, et mettez-les à jour en fonction des listes d'autorisation documentées.](#)

Étape 5 : Fournissez des informations à vos utilisateurs

Fournissez à vos utilisateurs des informations sur la nouvelle configuration, notamment l' Portail d'accès AWS URL de la région supplémentaire et la manière d'utiliser les régions supplémentaires. Consultez les sections suivantes pour obtenir des informations pertinentes :

- [the section called “Accès à la main-d'œuvre par le biais d'une région supplémentaire”](#)
- [the section called “Basculement vers une région supplémentaire pour y accéder Compte AWS ”](#)
- [the section called “Déploiement et gestion d'applications sur plusieurs Régions AWS”](#)

Changements de région au-delà de l'ajout de la première région

Vous pouvez ajouter et supprimer des régions supplémentaires. La région principale ne peut pas être supprimée autrement qu'en supprimant l'intégralité de l'instance IAM Identity Center. Pour plus d'informations sur la suppression d'une région, consultez [the section called “Supprimer une région du centre d'identité IAM”](#).

Vous ne pouvez pas promouvoir une région supplémentaire en tant que région principale ou rétrograder la région principale pour en faire une région supplémentaire.

Quelles données sont répliquées ?

IAM Identity Center réplique les données suivantes :

Données	Source et cible de réplication
Identités du personnel (utilisateurs, groupes, appartenances à des groupes)	De la région principale aux régions supplémentaires

Données	Source et cible de réplication
Ensembles d'autorisations et leur attribution aux utilisateurs et aux groupes	De la région principale aux régions supplémentaires
Configuration (tels que les paramètres SAML de l'IdP externe)	De la région principale aux régions supplémentaires
Métadonnées des applications et attributions d'applications aux utilisateurs et aux groupes	De la région IAM Identity Center connectée à une application vers les autres régions activées
Émetteurs de jetons fiables	De la région principale aux régions supplémentaires
Séances	De la région d'origine de la session aux autres régions activées

 Note

IAM Identity Center ne réplique pas les données stockées dans les applications AWS gérées. En outre, cela ne modifie pas l'empreinte régionale du déploiement d'une application. Par exemple, si votre instance IAM Identity Center se trouve dans l'est des États-Unis (Virginie du Nord) et qu'Amazon Redshift est déployé dans la même région, la réplication d'IAM Identity Center vers l'ouest des États-Unis (Oregon) n'a aucune incidence sur la région de déploiement d'Amazon Redshift ni sur les données qu'elle stocke.

Considérations :

- Identifiants de ressources globaux dans les régions activées : les utilisateurs, les groupes, les ensembles d'autorisations et les autres ressources ont les mêmes identifiants dans les régions activées.
- La réplication n'affecte pas les rôles IAM provisionnés - Les rôles IAM existants fournis à partir d'attributions d'ensembles d'autorisations sont utilisés lors de la connexion au compte depuis n'importe quelle région activée.

Accès à la main-d'œuvre par le biais d'une région supplémentaire

Cette section explique comment votre personnel peut accéder aux Portail d'accès AWS, Compte AWS et aux applications lorsque vous avez activé IAM Identity Center dans plusieurs régions.

Le Portail d'accès AWS menu dans une région supplémentaire affiche Compte AWS les applications et les applications auxquelles votre personnel a accès de la même manière que dans la région principale. Votre personnel peut se connecter Portail d'accès AWS à une région supplémentaire via un lien direct vers le point de terminaison du portail régional (par exemple, <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>) ou via une [application de favoris](#) que vous avez configurée dans l'IdP externe.

Vous pouvez utiliser le Portail d'accès AWS point de terminaison dans une région supplémentaire AWS CLI pour autoriser l'accès APIs en tant qu'utilisateur du IAM Identity Center. Cette fonctionnalité fonctionne de la même manière que dans la région principale. Toutefois, les autorisations CLI ne sont pas répliquées entre les régions activées. Par conséquent, vous devez autoriser la CLI dans chaque région individuellement.

Sessions utilisateur sur plusieurs Régions AWS

IAM Identity Center réplique les sessions utilisateur de la région d'origine vers les autres régions activées. La révocation de session et la déconnexion dans une région sont également reproduites dans les autres régions.

Révocation de session par les administrateurs d'IAM Identity Center

Les administrateurs d'IAM Identity Center peuvent révoquer les sessions utilisateur dans des régions supplémentaires. Lorsque les sessions sont répliquées entre les régions, dans des conditions normales, il suffit de révoquer une session dans une seule région et de laisser IAM Identity Center répliquer la modification dans les autres régions activées. En cas d'interruption de la région principale d'IAM Identity Center, les administrateurs peuvent effectuer cette opération dans d'autres régions.

Portail d'accès AWS points de terminaison dans le primaire et dans le module supplémentaire Régions AWS

Si vous devez rechercher le portail AWS d'accès URLs pour les régions activées, procédez comme suit :

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez l'onglet Gestion.
4. Dans la section Régions pour le centre d'identité IAM, choisissez Afficher tout le portail AWS URLs d'accès.

Le tableau suivant indique les Portail d'accès AWS points de terminaison dans les régions principale et supplémentaire d'une instance IAM Identity Center.

Portail d'accès AWS point de terminaison	Région principale	Région supplémentaire	Modèle d'URL et exemple
Classique IPv4 uniquement ¹	Oui	Non	Modèle : <code>https://[Identity Store ID].awsapps.com/start</code> Exemple : <code>https://d-12345678.awsapps.com/start</code>
Alias personnalisé IPv4 uniquement ¹	Oui (facultatif)	Non	Modèle : <code>https://[custom alias].awsapps.com/start</code> Exemple : <code>https://mycompany.awsapps.com/start</code>
Alternative IPv4 uniquement ²	Oui	Oui	Modèle : <code>https://[Identity Center instance ID].[Region].portal.amazonaws.com</code> Exemple : <code>https://soins-111111h2222j33pp.eu-west-1.portal.amazonaws.com</code>

Portail d'accès AWS point de terminaison	Région principale	Région supplémentaire	Modèle d'URL et exemple
Double pile 2	Oui	Oui	Modèle : <code>https://[Identity Center instance ID].portal.[Region].app.aws</code> Exemple : <code>https://soins-111111h2222j33pp.portal.eu-west-1.app.aws</code>

¹ Dans d'autres régions, l'alias personnalisé n'est pas pris en charge et le domaine `awsapps.com` parent n'est pas disponible.

² IPv4 Seule alternative, et les points de terminaison du portail à double pile n'ont pas de queue / start dans l'URL.

Points de terminaison Assertion Consumer Service (ACS) du serveur principal et du terminal supplémentaire Régions AWS

Si vous devez consulter l'ACS URLs ou le télécharger dans le cadre des métadonnées SAML, procédez comme suit :

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez l'onglet Source d'identité.
4. Dans le menu déroulant Actions, choisissez Gérer l'authentification.
5. La section des métadonnées du fournisseur de services affiche Portail d'accès AWS l'URL ACS pour chaque région activée. IPv4-only et dual-stack URLs sont affichés dans des onglets séparés. Si votre IdP prend en charge le téléchargement d'un fichier de métadonnées SAML, vous pouvez choisir Télécharger le fichier de métadonnées pour télécharger le fichier de métadonnées SAML avec tous les ACS. URLs Si votre IdP ne prend pas en charge le téléchargement d'un fichier de métadonnées, ou si vous préférez ajouter ACS URLs individuellement, vous pouvez copier un fichier URLs à partir du tableau de la console, ou

choisir Afficher ACS URLs puis Copier tout. URLs Conservez l'URL ACS déjà configurée pour la région principale afin de garantir que l'authentification unique SAML initiée par le fournisseur de services depuis la région principale reste fonctionnelle.

Le tableau suivant indique les points de terminaison du SAML Assertion Consumer Service (ACS) dans les régions principales et supplémentaires d'une instance IAM Identity Center :

Point final ACS	Région principale	Région supplémentaire	Modèle d'URL et exemple
IPv4 uniquement	Oui	Oui	Modèle : <code>https://[Region].signin.aws/platform/saml/acs/ [Tenant ID]</code> Exemple : <code>https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code>
Alternative IPv4 seulement*	Oui	Non	Modèle : <code>https://[Region].signin.aws.amazon.com/platform/saml/acs/ [Tenant ID]</code> Exemple : <code>https://us-west-2.signin.aws.amazon.com/platform/saml/acs/111111111111111111-aaee-ffff-dddd-111111111111</code>
Double pile	Oui	Oui	Modèle : <code>https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID]</code> Exemple : <code>https://us-west-2.sso.signin.aws/platform/sam</code>

Point final ACS	Région principale	Région supplémentaire	Modèle d'URL et exemple
			l/acs/1111111111111111-aaee -ffff-dddd-1111111111

* Pour les instances activées avant février 2026, conservez ce point de terminaison car l'authentification unique SAML initiée par le fournisseur de services dans la région principale l'exige. IAM Identity Center n'utilise pas ce point de terminaison pour les instances activées en février 2026 ou ultérieurement.

Utilisation d'applications AWS gérées sans plusieurs ACS URLs

Certains fournisseurs d'identité externes (IdPs) ne prennent pas en charge le service client à assertions multiples (ACS) URLs dans leur application IAM Identity Center. URLs Les ACS multiples sont une fonctionnalité SAML requise pour la connexion directe à une région spécifique dans un centre d'identité IAM multirégional.

Par exemple, si vous lancez une application AWS gérée via un lien d'application, le système déclenche la connexion via la région du centre d'identité IAM connectée à l'application. Toutefois, si l'URL ACS pour cette région n'est pas configurée dans l'IdP externe, la connexion échoue.

Pour résoudre ce problème, contactez votre fournisseur d'IdP pour activer la prise en charge de plusieurs ACS. URLs Dans l'intervalle, vous pouvez toujours utiliser les applications AWS gérées dans d'autres régions. Connectez-vous d'abord à la région dont l'URL ACS est configurée dans l'IdP externe (la région principale par défaut). Une fois que vous avez une session active dans IAM Identity Center, vous pouvez lancer l'application depuis le portail AWS d'accès de n'importe quelle région activée ou via un lien vers l'application.

Basculement vers une région supplémentaire pour y accéder Compte AWS

Le sujet de l' Compte AWS accès via IAM Identity Center est traité en détail dans [Compte AWS accès](#). Cette section fournit des informations supplémentaires relatives au maintien de l' Compte AWS accès sur plusieurs réseaux Régions AWS en cas d'interruption de service dans la région principale.

Si votre instance IAM Identity Center subit une interruption dans la région principale (par exemple, le portail d' AWS accès de la région principale n'est pas disponible), votre personnel peut passer à une autre région pour continuer à accéder à des Compte AWS applications non concernées. Pour de plus amples informations, veuillez consulter [the section called “Accès à la main-d'œuvre par le biais d'une région supplémentaire”](#).

Nous vous recommandons de communiquer les Portail d'accès AWS points de terminaison des régions supplémentaires et la configuration de l'IdP externe (par exemple, les applications de favoris pour les régions supplémentaires) à votre personnel dès que vous avez terminé la configuration dans. [the section called “Répliquer le centre d'identité IAM dans une région supplémentaire”](#) Cela leur permettra d'être prêts à basculer vers une région supplémentaire si nécessaire.

De même, nous recommandons AWS CLI aux utilisateurs de créer [AWS CLI des profils](#) pour des régions supplémentaires pour chacun des profils qu'ils possèdent pour la région principale. Ils peuvent ensuite passer à ce profil en cas d'interruption de service dans la région principale.

Note

La continuité de l'accès à Compte AWS s dépend également de l'état de santé de votre IdP externe et des autorisations, telles que les attributions d'ensembles d'autorisations et les appartenances à des groupes, fournies et répliquées avant une interruption de service. Nous recommandons également à votre entreprise de configurer un [accès AWS sans](#) faille afin de maintenir l' AWS accès à un petit groupe d'utilisateurs privilégiés en cas d'interruption de service de l'IdP externe. [L'accès d'urgence](#) est une option similaire qui évite d'utiliser des utilisateurs IAM, mais elle dépend également de l'IdP externe.

Compte AWS résilience des accès sans plusieurs ACS URLs

Certains fournisseurs d'identité externes (IdPs) ne prennent pas en charge le service client à assertions multiples (ACS) URLs dans leur application IAM Identity Center. URLs Les ACS multiples sont une fonctionnalité SAML requise pour la connexion directe à une région spécifique dans un centre d'identité IAM multirégional.

Pour permettre à vos utilisateurs d'y accéder Comptes AWS via plusieurs régions du centre d'identité IAM, vous devez configurer l'ACS régional correspondant URLs dans l'IdP externe. Toutefois, si l'IdP externe ne prend en charge qu'une seule URL ACS dans son application IAM Identity Center, les utilisateurs peuvent se connecter directement à une seule région du centre d'identité IAM.

Pour résoudre ce problème, contactez votre fournisseur d'IdP pour activer la prise en charge de plusieurs ACS. URLs En attendant, vous pouvez utiliser des régions supplémentaires comme sauvegarde pour accéder à Comptes AWS.

Si une interruption du service IAM Identity Center survient dans la région principale, vous devez mettre à jour l'URL ACS dans l'IdP externe avec l'URL ACS d'une région supplémentaire. Après cette mise à jour, vos utilisateurs peuvent accéder au portail AWS d'accès de la région supplémentaire à l'aide de l'application IAM Identity Center existante sur le portail IdP externe, ou via un lien direct que vous partagez avec eux.

Nous vous recommandons de tester régulièrement cette configuration pour vous assurer qu'elle fonctionne en cas de besoin et de communiquer ce processus de basculement à votre organisation.

Note

Lorsque vous utilisez une région supplémentaire pour y accéder Comptes AWS dans cette configuration, vos utilisateurs peuvent ne pas être en mesure d'accéder aux applications AWS gérées connectées à la région principale. Par conséquent, nous recommandons cette mesure uniquement comme mesure temporaire pour maintenir l'accès à Comptes AWS.

Déploiement et gestion d'applications dans plusieurs AWS régions

Le sujet de l'accès aux applications via IAM Identity Center est traité en détail dans [Accès aux applications](#). Cette section fournit des informations supplémentaires relatives au déploiement et à la gestion d'applications multiples Régions AWS.

Déploiement et gestion d'applications AWS gérées sur plusieurs Régions AWS

Avec une instance IAM Identity Center à région unique, vous pouvez déployer des applications AWS gérées dans la même région que votre instance. Certaines applications telles qu'Amazon Q Business prennent en charge une connexion interrégionale à IAM Identity Center, ce qui permet leur déploiement en dehors de la région du IAM Identity Center si l'application qui vous intéresse y est disponible. Cependant, les appels interrégionaux peuvent ralentir les performances des applications, et la plupart des applications AWS gérées ne prennent pas en charge ce type de connexion.

Une instance de centre d'identité IAM multirégion vous permet de déployer des applications AWS gérées dans n'importe quelle région activée avec une connexion au centre d'identité IAM de la

même région (« connexion régionale locale »). Le déploiement dans la région principale est pris en charge par toutes les applications AWS gérées intégrées. Pour savoir quelles applications AWS gérées prennent en charge le déploiement dans des régions supplémentaires d'IAM Identity Center, consultez le tableau des applications dans [the section called “Applications que vous pouvez utiliser avec IAM Identity Center”](#). Dans tous les cas, l'application AWS gérée doit être disponible dans la région où vous souhaitez la déployer.

Grâce à une connexion régionale locale à IAM Identity Center, les applications AWS gérées accèdent aux identités du personnel de la même région pour des performances et une fiabilité optimales. Nous vous recommandons de choisir une connexion régionale locale lors du déploiement d'une application AWS gérée lorsque les [conditions préalables sont remplies](#).

Pour déployer une application AWS gérée dans une région supplémentaire d'IAM Identity Center, lancez le déploiement dans cette région via la console ou l'API de l'application de la même manière que vous déployez dans la région principale.

Considérations :

- Si vous n'avez pas encore répliqué votre IAM Identity Center dans cette région, nous vous recommandons de le faire d'abord afin que le déploiement de l'application puisse être terminé immédiatement.
- AWS dans de nombreux cas, les applications gérées établiront automatiquement une connexion régionale si vous avez déjà répliqué IAM Identity Center dans la région.
- [Si une application AWS gérée propose une connexion interrégionale à IAM Identity Center, nous vous recommandons de choisir une connexion régionale locale à condition que les conditions requises soient remplies.](#)
- Si l'application ne prend pas en charge le déploiement dans des régions supplémentaires, vous pouvez la déployer dans la région principale à condition que l'application y soit disponible.

Important

Si votre instance IAM Identity Center est multirégionale, toutes les applications AWS gérées utilisées par votre organisation doivent prendre en charge IAM Identity Center configuré avec une clé KMS gérée par le client, quelle que soit la région de déploiement de l'application. Vérifiez cela avant de déployer une application et [the section called “Applications que vous pouvez utiliser avec IAM Identity Center”](#) avant de configurer une clé KMS gérée par le client dans votre IAM Identity Center.

Région de gestion d'une application

Après avoir déployé une application AWS gérée dans une région supplémentaire d'IAM Identity Center à l'aide d'une connexion régionale locale, vous gérez l'application et ses attributions aux utilisateurs et aux groupes de la même région. IAM Identity Center réplique les métadonnées de l'application, y compris les affectations aux utilisateurs et aux groupes, vers d'autres régions activées afin que votre personnel puisse lancer des applications depuis n'importe quelle région activée.

Si votre application AWS gérée utilise une connexion interrégionale à IAM Identity Center, vous pouvez gérer les détails de l'application tels que le nom et la description, ainsi que les attributions des applications aux utilisateurs et aux groupes via la console et l'API IAM Identity Center dans la région connectée. Quel que soit le type de connexion, vous pouvez gérer l'application via sa console dans sa région de déploiement.

Propagation d'identité de confiance

Vous pouvez utiliser la propagation d'identité fiable avec des applications AWS gérées qui la prennent en charge dans n'importe quelle région activée de votre instance IAM Identity Center.

Toutes les applications qui se propagent le contexte d'identité doivent se trouver dans la même région.

Dépendance d'une application par rapport à sa région IAM Identity Center connectée

Chaque application AWS gérée se connecte à une région spécifique du centre d'identité IAM lors du déploiement. L'application dépend alors de cette région pour la connexion des utilisateurs, même si votre centre d'identité IAM est activé dans plusieurs régions. Si votre centre d'identité IAM est perturbé dans cette région, les utilisateurs ne pourront peut-être pas accéder aux applications AWS gérées connectées à la région.

Déploiement et gestion d'applications gérées par le client sur plusieurs Régions AWS

IAM Identity Center prend en charge le SAML et les applications [gérées par OAuth2 le client](#).

Vous pouvez choisir de les créer dans n'importe quelle région activée de votre instance IAM Identity Center. Une fois que vous en avez créé une, vous gérez l'application et ses attributions aux utilisateurs et aux groupes de la même région.

Supprimer une région du centre d'identité IAM

Pour supprimer une région supplémentaire de votre instance IAM Identity Center, procédez comme suit :

Étape 1 : Mettre à jour la configuration de l'IdP externe

Vous pouvez choisir de supprimer l'URL ACS de cette région de votre IdP externe ou de la conserver au cas où vous souhaiteriez ajouter à nouveau cette région ultérieurement. Nous vous recommandons de supprimer ou de masquer l'application de favoris que vous avez peut-être créée pour cette Portail d'accès AWS région.

Étape 2 : supprimer la région

Console

Pour ajouter une région

1. Ouvrez la [console IAM Identity Center](#).
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez l'onglet Gestion.
4. Dans la section Régions pour le centre d'identité IAM, choisissez la région supplémentaire que vous souhaitez supprimer.
5. Cliquez sur Supprimer.
6. Avant de confirmer la suppression en choisissant Supprimer la région, prêtez attention à l'avertissement concernant la perte potentielle d'accès aux applications créées dans cette région du centre d'identité IAM. Si vous n'êtes pas sûr de disposer de telles applications, sélectionnez Applications dans le volet de navigation et confirmez la région connectée dans la colonne Créée à partir de pour chaque application AWS gérée et gérée par le client.

Note

Vous pouvez continuer à payer des frais pour les déploiements d'applications AWS gérées qui sont toujours connectées à la région supprimée, même si vous perdez l'accès à ces applications. Pour éviter cela, vous devez supprimer ces déploiements d'applications AWS gérées via la console d'application ou l'API avant de supprimer la région dans IAM Identity Center. Si vous avez déjà supprimé la région du centre

d'identité IAM, vous pouvez rétablir l'accès aux applications en ajoutant de nouveau la région.

7. Dans la section Régions pour le centre d'identité IAM, surveillez le statut de la région. Utilisez le bouton Actualiser (flèche circulaire) pour voir le dernier état de la région selon vos besoins. Une fois la région supprimée, elle n'apparaît plus dans la liste des régions.

AWS CLI

Pour supprimer une région

```
aws sso-admin remove-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Pour vérifier le statut actuel de la région

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Lorsque la région est supprimée, passez à l'étape 2.

Étape 3 : supprimer la clé de réplique

Vous pouvez choisir de supprimer la clé de réplique de cette région pour éviter d'encourir des frais de stockage KMS. Pour plus d'informations, consultez [la section Suppression d'une AWS KMS clé](#).

Important

Assurez-vous de supprimer uniquement la clé de réplique dans cette région spécifique. Les autres régions du centre d'identité IAM continuent de s'appuyer sur la clé KMS dans les autres régions activées pour leurs opérations normales.

Service IAM Identity Center APIs pris en charge dans d'autres régions AWS

API	Fonctionnalité dans d'autres régions
API Identity Center	Pris en charge : • read/write Opérations de gestion des applications • Opérations de lecture des instances Non pris en charge : • Toutes les opérations d'écriture autres que celles liées à l'application • Opérations de lecture relatives aux ensembles d'autorisations et aux attributions de comptes
API Identity Store	Opérations de lecture
API OIDC	Toutes les opérations sont prises en charge
API du portail d'accès	Toutes les opérations sont prises en charge
API SCIM	Aucune opération n'est prise en charge

AWS CloudTrail événements du centre d'identité IAM dans la région principale et dans la région supplémentaire

Dans AWS CloudTrail, vous pouvez auditer les actions effectuées par les utilisateurs et les administrateurs d'IAM Identity Center sur toutes les instances activées Régions AWS de votre instance IAM Identity Center. Les AWS CloudTrail événements sont émis et enregistrés dans la région où l'action a lieu. Pour de plus amples informations, veuillez consulter [the section called "Journalisation et surveillance"](#).

Disponibilité des cas d'utilisation d'IAM Identity Center dans la région principale et dans les régions supplémentaires

Fonctionnalité	Disponibilité par région
Annuaire des effectifs avec portail utilisateur	
Accès utilisateur à la connexion Portail d'accès AWS au portail et aux sessions globales (connexion unique pour toutes les régions)	Toutes les régions activées
Affichage de tous les comptes attribués	Toutes les régions activées
Affichage de toutes les applications assignées (quel que soit l'endroit où elles ont été créées)	Toutes les régions activées
Accès en lecture aux utilisateurs, aux groupes et aux adhésions dans la AWS console ou via Identity Store APIs	Toutes les régions activées
Révoquer les sessions utilisateur	Toutes les régions activées
Synchronisation automatique des utilisateurs et des groupes à partir d'une source d'identité externe telle qu'un IdP externe via l'API SCIM ou l'API Identity Store	Région principale uniquement
Configurer le provisionnement automatique des identités avec SCIM	Région principale uniquement
Configurer le SSO SAML avec un IdP externe	Région principale uniquement : accès en lecture via la console dans toutes les régions activées
Create/update/deleteopérations sur les utilisateurs, les groupes et les appartenances à des groupes via la console ou Identity Store APIs.	Région principale : disponible via l'API Identity Store mais bloquée dans la console IAM Identity Center lorsque l'API SCIM est utilisée pour le provisionnement (à l'exception de disable/enable

Fonctionnalité	Disponibilité par région
	l'accès utilisateur et de la suppression d'un utilisateur, qui sont toujours disponibles). Régions supplémentaires : non disponible
Accès à plusieurs comptes	
Accédez aux comptes attribués via les liens Portail d'accès AWS AWS CLI, et de raccourci	Toutes les régions activées
Gérez les ensembles d'autorisations multi-comptes et leurs attributions dans la console et APIs (y compris l'accès élevé temporaire)	Région principale uniquement
Accès aux applications et AWS aux services	
Déployez des applications AWS gérées via la console d'applications et APIs	Toutes les régions activées, sous réserve de la disponibilité régionale des applications et de la prise en charge du déploiement dans d'autres régions
Créez des applications gérées par le client via la console Identity Center et APIs	Toutes les régions activées
Gérez les métadonnées et les attributions des applications dans la console et APIs	Région du centre d'identité IAM connectée à l'application
Lancez des applications depuis Portail d'accès AWS ou directement via un lien d'application ou un signet	Toutes les régions activées
SSO vers les instances Amazon EC2	Toutes les régions activées
Propagation d'identité fiable	
Création d'un émetteur de jetons approuvé	Région principale uniquement

Fonctionnalité	Disponibilité par région
Propagation d'identité fiable avec des applications AWS gérées	Toutes les régions activées : les applications qui se propagent le contexte d'identité doivent se trouver dans la même région
Autres fonctionnalités administratives	
Toutes les autres fonctionnalités administratives telles que la gestion des régions, la gestion des clés KMS, la gestion des instances et la gestion des sessions (à l'exception de la révocation de session)	Région principale uniquement : accès en lecture disponible dans toutes les régions activées pour certaines données (les attributions d'ensembles d'autorisations sont exclues)

Conception de la résilience et comportement régional

Le service IAM Identity Center est entièrement géré et utilise des AWS services hautement disponibles et durables, tels qu'Amazon S3 et Amazon EC2. Pour garantir la disponibilité en cas d'interruption de la zone de disponibilité, IAM Identity Center fonctionne dans plusieurs zones de disponibilité. Vous pouvez répliquer votre instance IAM Identity Center vers des régions supplémentaires afin de conserver l'accès au compte avec les autorisations déjà accordées en cas de perturbation régionale. Pour de plus amples informations, veuillez consulter [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

Vous activez IAM Identity Center dans votre compte AWS Organizations de gestion. Cela est nécessaire pour qu'IAM Identity Center puisse provisionner, déprovisionner et mettre à jour les rôles dans tous vos domaines. Comptes AWS Lorsque vous activez IAM Identity Center, il est déployé dans la Région AWS région actuellement sélectionnée, appelée « région principale ». Si vous souhaitez effectuer un déploiement vers une région spécifique Région AWS, modifiez la sélection de région avant d'activer IAM Identity Center, car la région principale ne peut pas être modifiée une fois IAM Identity Center activé.

IAM Identity Center prend en charge la plupart des fonctions administratives uniquement à partir de la région principale. Cela inclut la connexion à un fournisseur d'identité externe, la synchronisation des utilisateurs et des groupes, ainsi que la création et l'attribution d'ensembles d'autorisations aux utilisateurs et aux groupes. En revanche, la gestion des applications et de leurs attributions doit avoir lieu dans la région du centre d'identité IAM où l'application a été créée.

Note

Même si votre IAM Identity Center est répliqué dans d'autres régions, nous vous recommandons de configurer un accès sans faille [AWS](#). Cela vous permet de conserver AWS l'accès d'un petit groupe d'utilisateurs privilégiés lors d'événements tels qu'une interruption de service dans l'IdP externe. [L'accès d'urgence](#) est une autre option qui utilise les identités d'un IdP externe plutôt que celles des utilisateurs IAM ; toutefois, il ne protège pas contre une interruption de l'IdP externe.

Bien qu'IAM Identity Center détermine l'accès depuis la région dans laquelle vous activez le service, Comptes AWS ils sont mondiaux. Cela signifie qu'une fois que les utilisateurs se sont connectés à IAM Identity Center, ils peuvent opérer dans n'importe quelle région lorsqu'ils y accèdent

Comptes AWS via IAM Identity Center. La plupart des applications AWS gérées telles qu'Amazon SageMaker AI doivent toutefois être installées dans une région de votre instance IAM Identity Center pour que les utilisateurs puissent s'authentifier et attribuer l'accès à ces applications. Pour plus d'informations sur les contraintes régionales lors de l'utilisation d'une application avec IAM Identity Center, consultez la documentation de l'application et [the section called “Déploiement et gestion d'applications AWS gérées sur plusieurs Régions AWS”](#).

Vous pouvez également utiliser IAM Identity Center pour authentifier et autoriser l'accès aux applications SAML gérées par le client accessibles via une URL publique, indépendamment de la plateforme ou du cloud sur lequel l'application est construite.

Nous vous déconseillons de les utiliser [Instances de compte d'IAM Identity Center](#) comme moyen de mise en œuvre de la résilience, car ils ne prennent pas en charge l'accès aux AWS comptes et créent un deuxième point de contrôle isolé qui n'est pas connecté à l'instance de votre organisation.

Conçu pour la disponibilité

Le tableau suivant indique la disponibilité pour laquelle IAM Identity Center est conçu dans une seule AWS région. Ces valeurs ne constituent pas un accord de niveau de service ou une garantie, mais fournissent plutôt un aperçu des objectifs de conception. Les pourcentages de disponibilité font référence à l'accès aux données ou aux fonctions, et non à la durabilité (par exemple, conservation à long terme des données).

Composant de service	Objectif de la conception de la disponibilité
Plan de données (connexion incluse)	99.95%
Plan de contrôle	99.90%

Configurez un accès d'urgence au AWS Management Console

IAM Identity Center est construit à partir d'une AWS infrastructure à haute disponibilité et utilise une architecture de zone de disponibilité pour éliminer les points de défaillance uniques. Pour une couche de protection supplémentaire dans le cas peu probable d'un IAM Identity Center ou d'une Région AWS interruption, nous vous recommandons de configurer une configuration que vous pouvez utiliser pour fournir un accès temporaire au AWS Management Console.

AWS vous permet de :

- [Connectez votre IdP tiers à IAM Identity Center.](#)
- Connectez votre IdP tiers à un individu en Comptes AWS utilisant la fédération basée sur [SAML 2.0](#).

Si vous utilisez IAM Identity Center, vous pouvez utiliser ces fonctionnalités pour créer la configuration d'accès d'urgence décrite dans les sections suivantes. Cette configuration vous permet d'utiliser IAM Identity Center comme mécanisme d' Compte AWS accès. Si le centre d'identité IAM est perturbé, les utilisateurs de vos opérations d'urgence peuvent se connecter à la fédération par le AWS Management Console biais de la fédération directe, en utilisant les mêmes informations d'identification que celles qu'ils utilisent pour accéder à leurs comptes. Cette configuration fonctionne lorsque le centre d'identité IAM n'est pas disponible, mais que le plan de données IAM et votre fournisseur d'identité externe (IdP) sont disponibles. [Si vous préférez ne pas dépendre de l'IdP externe, pensez à configurer un accès brise-vitre AWS](#)

Important

Nous vous recommandons de déployer cette configuration avant qu'une interruption ne survienne, car vous ne pouvez pas créer la configuration si votre accès pour créer les rôles IAM requis est également perturbé. Testez également cette configuration régulièrement pour vous assurer que votre équipe comprend ce qu'elle doit faire en cas d'interruption d'IAM Identity Center.

Rubriques

- [Résumé de la configuration des accès d'urgence](#)
- [Comment concevoir vos rôles opérationnels critiques](#)
- [Comment planifier votre modèle d'accès](#)
- [Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence](#)
- [Comment créer votre configuration d'accès d'urgence](#)
- [Tâches de préparation aux urgences](#)
- [Processus de basculement d'urgence](#)
- [Retour aux activités normales](#)
- [Configuration unique d'une application de fédération IAM directe dans Okta](#)
- [Configuration unique d'une application de fédération IAM directe avec ADFS](#)

Résumé de la configuration des accès d'urgence

Pour configurer l'accès d'urgence, vous devez effectuer les tâches suivantes :

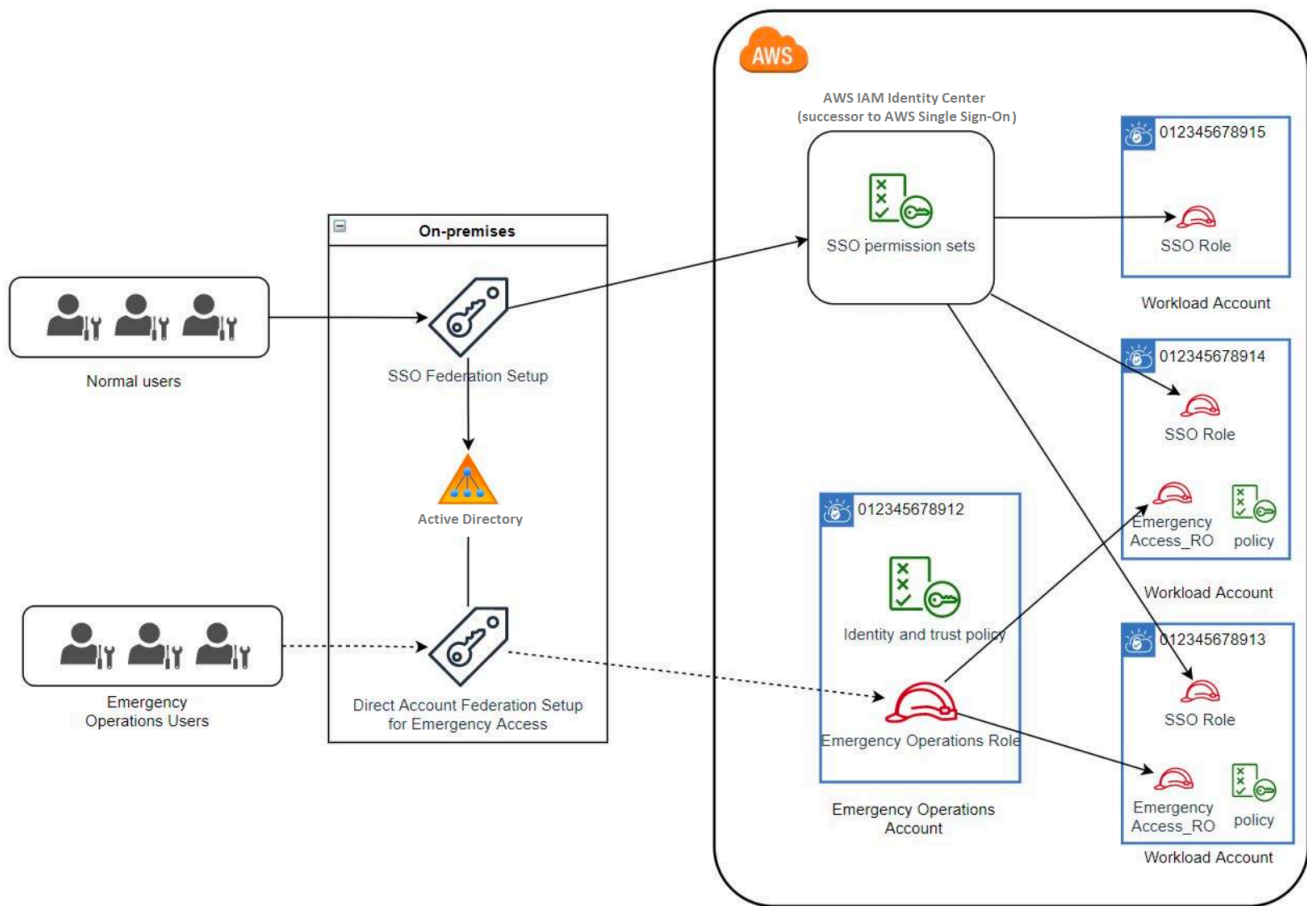
1. [Créez un compte des opérations d'urgence dans votre organisation dans AWS Organizations](#). Ce compte deviendra votre compte des opérations d'urgence.
2. Connectez votre IdP au compte des opérations d'urgence à l'aide de la fédération basée sur [SAML 2.0](#).
3. Dans le compte des opérations d'urgence, [créez un rôle pour la fédération des fournisseurs d'identité tiers](#). Créez également un rôle d'opérations d'urgence dans chacun de vos comptes de charge de travail, avec les autorisations requises.
4. [Déléguez l'accès à vos comptes de charge de travail pour le rôle IAM](#) que vous avez créé dans le compte des opérations d'urgence. Pour autoriser l'accès à votre compte d'opérations d'urgence, créez un groupe d'opérations d'urgence dans votre IdP, sans aucun membre.
5. Permettez au groupe des opérations d'urgence de votre IdP d'utiliser le rôle des opérations d'urgence en créant une règle dans votre IdP qui [autorise l'accès fédéré SAML 2.0](#) au. AWS Management Console

Pendant les opérations normales, personne n'a accès au compte des opérations d'urgence car le groupe des opérations d'urgence de votre IdP ne compte aucun membre. En cas d'interruption du centre d'identité IAM, utilisez votre IdP pour ajouter des utilisateurs de confiance au groupe des opérations d'urgence de votre IdP. Ces utilisateurs peuvent ensuite se connecter à votre IdP, accéder au et assumer le AWS Management Console rôle des opérations d'urgence dans le compte des opérations d'urgence. À partir de là, ces utilisateurs peuvent [passer au rôle](#) d'accès d'urgence dans vos comptes de charge de travail où ils doivent effectuer des opérations.

Comment concevoir vos rôles opérationnels critiques

Avec cette conception, vous configurez un système unique Compte AWS dans lequel vous fédérez via IAM, afin que les utilisateurs puissent assumer des rôles opérationnels critiques. Les rôles liés aux opérations critiques sont régis par une politique de confiance qui permet aux utilisateurs d'assumer un rôle correspondant dans vos comptes de charge de travail. Les rôles des comptes de charge de travail fournissent les autorisations dont les utilisateurs ont besoin pour effectuer des tâches essentielles.

Le schéma suivant fournit une vue d'ensemble de la conception.



Comment planifier votre modèle d'accès

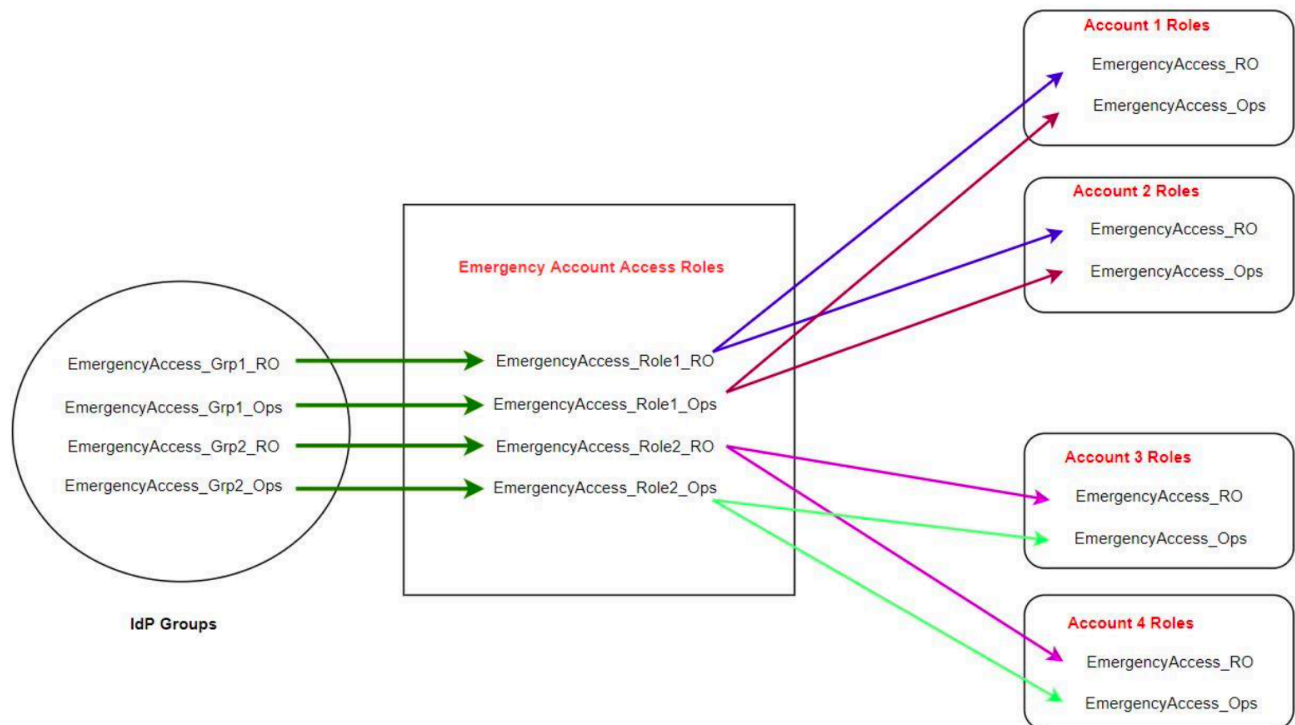
Avant de configurer l'accès d'urgence, créez un plan de fonctionnement du modèle d'accès. Utilisez le processus suivant pour créer ce plan.

1. Identifiez les Comptes AWS endroits où l'accès des opérateurs d'urgence est essentiel lors d'une interruption du IAM Identity Center. Par exemple, vos comptes de production sont probablement essentiels, mais vos comptes de développement et de test ne le sont peut-être pas.
2. Pour cette collection de comptes, identifiez les rôles critiques spécifiques dont vous avez besoin dans vos comptes. Sur l'ensemble de ces comptes, définissez de manière cohérente ce que les rôles peuvent faire. Cela simplifie le travail dans votre compte d'accès d'urgence où vous pouvez créer des rôles entre comptes. Nous vous recommandons de commencer par deux rôles distincts dans ces comptes : Read Only (RO) et Operations (Ops). Si nécessaire, vous pouvez créer d'autres rôles et les associer à un groupe plus distinct d'utilisateurs d'accès d'urgence dans votre configuration.

3. Identifiez et créez des groupes d'accès d'urgence dans votre IdP. Les membres du groupe sont les utilisateurs auxquels vous déléguez l'accès aux rôles d'accès d'urgence.
4. Définissez les rôles que ces groupes peuvent assumer dans le compte d'accès d'urgence. Pour ce faire, définissez des règles dans votre IdP qui génèrent des revendications répertoriant les rôles auxquels le groupe peut accéder. Ces groupes peuvent ensuite assumer vos rôles de lecture seule ou d'opérations dans le compte d'accès d'urgence. À partir de ces rôles, ils peuvent assumer les rôles correspondants dans vos comptes de charge de travail.

Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence

Le schéma suivant montre comment mapper vos groupes d'accès d'urgence aux rôles de votre compte d'accès d'urgence. Le diagramme montre également les relations de confiance entre comptes qui permettent aux rôles d'accès d'urgence d'accéder aux rôles correspondants dans vos comptes de charge de travail. Nous recommandons que la conception de votre plan d'urgence utilise ces mappages comme point de départ.



Comment créer votre configuration d'accès d'urgence

Utilisez le tableau de mappage suivant pour créer votre configuration d'accès d'urgence. Ce tableau reflète un plan qui inclut deux rôles dans les comptes de charge de travail : Read Only (RO) et Operations (Ops), avec les politiques de confiance et les politiques d'autorisation correspondantes. Les politiques de confiance permettent aux rôles des comptes d'accès d'urgence d'accéder aux rôles des comptes de charge de travail individuels. Les rôles individuels du compte de charge de travail sont également soumis à des politiques d'autorisation concernant ce que le rôle peut faire dans le compte. Les politiques d'autorisation peuvent être des [politiques AWS gérées ou des politiques gérées par le client](#).

Compte	Rôles à créer	Politique d'approbation	Politique d'autorisations
Compte 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Compte 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Compte 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Compte 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Compte d'accès d'urgence	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO	IdP	AssumeRole pour le rôle, la ressource dans le compte

Compte	Rôles à créer	Politique d'approbation	Politique d'autorisations
	Emergency Access_Role2_Ops		

Dans ce plan de mappage, le compte d'accès d'urgence contient deux rôles en lecture seule et deux rôles opérationnels. Ces rôles font confiance à votre IdP pour authentifier et autoriser les groupes que vous avez sélectionnés à accéder aux rôles en transmettant les noms des rôles dans des assertions. Il existe des rôles de lecture seule et d'exploitation correspondants dans le compte de charge de travail 1 et le compte 2. Pour le compte de charge de travail 1, le EmergencyAccess_R0 rôle fait confiance au EmergencyAccess_Role1_R0 rôle qui réside dans le compte d'accès d'urgence. Le tableau indique des modèles de confiance similaires entre les rôles de lecture seule et d'exploitation du compte de charge de travail et les rôles d'accès d'urgence correspondants.

Tâches de préparation aux urgences

Pour préparer la configuration de votre accès d'urgence, nous vous recommandons d'effectuer les tâches suivantes avant qu'une urgence ne se produise.

1. Configurez une application de fédération IAM directe dans votre IdP. Si vous utilisez Okta ou une autre source externe IdPs comme source d'identité, consultez [Configuration unique d'une application de fédération IAM directe dans Okta](#). Si vous utilisez Active Directory comme source d'identité, consultez [Configuration unique d'une application de fédération IAM directe avec ADFS](#).
2. Créez une connexion IdP dans le compte d'accès d'urgence accessible pendant l'événement.
3. Créez des rôles d'accès d'urgence dans les comptes d'accès d'urgence, comme décrit dans le tableau de mappage ci-dessus.
4. Créez des rôles opérationnels temporaires avec des politiques de confiance et d'autorisation dans chacun des comptes de charge de travail.
5. Créez des groupes d'opérations temporaires dans votre IdP. Les noms des groupes dépendront des noms des rôles des opérations temporaires.
6. Testez la fédération IAM directe.
7. Désactivez l'application de fédération IdP dans votre IdP pour empêcher une utilisation régulière.

Processus de basculement d'urgence

Lorsqu'une instance IAM Identity Center n'est pas disponible et que vous déterminez que vous devez fournir un accès d'urgence à la console AWS de gestion, nous recommandons le processus de basculement suivant.

1. L'administrateur de l'IdP active l'application de fédération IAM directe dans votre IdP.
2. Les utilisateurs demandent l'accès au groupe des opérations temporaires par le biais de votre mécanisme existant, tel qu'une demande par e-mail, un canal Slack ou une autre forme de communication.
3. Les utilisateurs que vous ajoutez à vos groupes d'accès d'urgence se connectent à l'IdP, sélectionnent le compte d'accès d'urgence, puis les utilisateurs choisissent un rôle à utiliser dans le compte d'accès d'urgence. À partir de ces rôles, ils peuvent assumer des rôles dans les comptes de charge de travail correspondants bénéficiant d'une confiance croisée avec le rôle de compte d'urgence.

Retour aux activités normales

Consultez le [AWS Health Dashboard](#) pour confirmer le moment où l'état du service IAM Identity Center est rétabli. Pour revenir à un fonctionnement normal, effectuez les opérations suivantes.

1. Une fois que l'icône d'état du service IAM Identity Center indique que le service est en bon état, connectez-vous à IAM Identity Center.
2. Si vous parvenez à vous connecter à IAM Identity Center, informez les utilisateurs d'accès d'urgence qu'IAM Identity Center est disponible. Demandez à ces utilisateurs de se déconnecter et d'utiliser le portail AWS d'accès pour se reconnecter à IAM Identity Center.
3. Une fois que tous les utilisateurs d'accès d'urgence se sont déconnectés, dans l'IdP, désactivez l'application de fédération IdP. Nous vous recommandons d'effectuer cette tâche en dehors des heures de travail.
4. Supprimez tous les utilisateurs du groupe d'accès d'urgence dans l'IdP.

Votre infrastructure de rôles d'accès d'urgence reste en place en tant que plan d'accès de secours, mais elle est désormais désactivée.

Configuration unique d'une application de fédération IAM directe dans Okta

1. Connectez-vous à votre Okta compte en tant qu'utilisateur disposant d'autorisations administratives.
2. Dans la Okta console d'administration, sous Applications, sélectionnez Applications.
3. Choisissez Parcourir le catalogue d'applications. Recherchez et choisissez AWS Account Federation. Choisissez ensuite Ajouter une intégration.
4. Configurez la fédération IAM directe avec AWS en suivant les étapes décrites dans [Comment configurer SAML 2.0 pour la fédération de AWS comptes](#). Pour gérer les scénarios de défaillance régionaux, lorsque vous configurez le point de terminaison de connexion, nous vous recommandons d'activer à la fois le point de terminaison non régional et plusieurs points de terminaison régionaux pour toutes les régions dans lesquelles vous opérez afin d'améliorer la résilience de la fédération. Lorsque vous configurez l'URL ACS pour cet accès d'urgence, nous vous recommandons d'utiliser le point de terminaison régional d'une région différente de celle dans laquelle votre centre d'identité IAM est déployé. Reportez-vous à la section [Points de terminaison de connexion](#) dans le manuel de référence AWS général pour obtenir la liste des points de terminaison régionaux.
5. Dans l'onglet Options de connexion, sélectionnez SAML 2.0 et entrez les paramètres du filtre de groupe et du modèle de valeur des rôles. Le nom du groupe pour l'annuaire des utilisateurs dépend du filtre que vous configurez.

Group Filter

```
^aws\#\S+\#(?{{role}}[w\-.]+\)\#(?{{accountid}}\d+)\$
```

Role Value Pattern

```
arn:aws:iam::{{accountid}}:saml-provider/Okta,arn:aws:iam::{{accountid}}:role/{{role}}
```

Dans la figure ci-dessus, la `role` variable concerne le rôle des opérations d'urgence dans votre compte d'accès d'urgence. Par exemple, si vous créez le `EmergencyAccess_Role1_R0` rôle (comme décrit dans le tableau de mappage) dans Compte AWS 123456789012, et si votre paramètre de filtre de groupe est configuré comme indiqué dans la figure ci-dessus, le nom de votre groupe doit être `aws#EmergencyAccess_Role1_R0#123456789012`.

6. Dans votre répertoire (par exemple, votre répertoire dans Active Directory), créez le groupe d'accès d'urgence et attribuez un nom au répertoire (par exemple, `aws#EmergencyAccess_Role1_R0#123456789012`). Affectez vos utilisateurs à ce groupe en utilisant votre mécanisme de provisionnement existant.

7. Dans le compte d'accès d'urgence, [configurez une politique de confiance personnalisée](#) qui fournit les autorisations requises pour que le rôle d'accès d'urgence soit assumé lors d'une interruption. Vous trouverez ci-dessous un exemple de déclaration pour une politique de confiance personnalisée attachée au EmergencyAccess_Role1_R0 rôle. Pour une illustration, voir le compte d'urgence dans le schéma ci-dessous [Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence](#). Remplacez l'exemple d'ARN du fournisseur SAML par le bon ARN que vous avez créé dans le compte d'accès d'urgence. Remplacez les points de terminaison régionaux dans l'exemple par les régions de votre choix.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML PROVIDER NAME]"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:aud": [
            "https://signin.aws.amazon.com/saml",
            "https://us-west-2.signin.aws.amazon.com/saml",
            "https://us-west-1.signin.aws.amazon.com/saml",
            "https://us-east-2.signin.aws.amazon.com/saml"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
      },
      "Action": "sts:SetSourceIdentity"
    }
  ]
}
```

```

    }
  ]
}

```

8. Voici un exemple de déclaration pour une politique d'autorisation attachée au EmergencyAccess_Role1_R0 rôle. Pour une illustration, voir le compte d'urgence dans le schéma ci-dessous [Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
        "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
      ]
    }
  ]
}

```

9. Sur les comptes de charge de travail, configurez une politique de confiance personnalisée. Vous trouverez ci-dessous un exemple de déclaration pour une politique de confiance attachée au EmergencyAccess_R0 rôle. Dans cet exemple, le compte 123456789012 est le compte d'accès d'urgence. Pour une illustration, voir le compte de charge de travail dans le schéma ci-dessous [Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",

```

```
"Principal":{
  "AWS":"arn:aws:iam::123456789012:root"
},
"Action":"sts:AssumeRole"
}
]
```

Note

La plupart des IdPs permettent de désactiver l'intégration d'une application jusqu'à ce que vous en ayez besoin. Nous vous recommandons de laisser l'application de fédération IAM directe désactivée dans votre IdP jusqu'à ce qu'elle soit requise pour un accès d'urgence.

Configuration unique d'une application de fédération IAM directe avec ADFS

Ce guide décrit le processus de configuration unique permettant de configurer la fédération IAM directe afin que ADFS permette un accès d'urgence aux Comptes AWS lorsque IAM Identity Center n'est pas disponible.

Conditions préalables

Si vous envisagez de configurer ADFS avec AWS Managed Microsoft AD, nous vous recommandons de [configurer d'abord la réplique multirégionale](#) et de poursuivre les étapes suivantes dans la région supplémentaire et non dans la région principale pour des raisons de résilience.

Planifiez votre convention de dénomination des groupes Active Directory

Créez des groupes AD à l'aide d'un modèle de dénomination spécifique qui permet une correspondance automatique entre les noms de groupes et les rôles AWS IAM.

Format de dénomination des groupes : AWS- <AccountNumber> - <RoleName>

Pour une illustration, voir le compte d'urgence dans le schéma ci-dessous [Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence](#). Lorsqu'un utilisateur est affecté à ce groupe, il a accès au EmergencyAccess_Role1_R0 rôle dans le compte 123456789012. Si un

utilisateur est associé à plusieurs groupes, il voit la liste des rôles disponibles Compte AWS et peut choisir le rôle à assumer.

AWS configuration

La configuration complète inclut les configurations d'un compte d'accès d'urgence et des comptes de charge de travail. Pour une illustration de la configuration globale, voir [Comment concevoir un mappage des rôles, des comptes et des groupes en cas d'urgence](#).

1. [Création d'un fournisseur d'identité SAML](#)
2. [Création de rôles d'accès d'urgence](#)
3. [Configurer les rôles des comptes de charge de travail](#)

Création d'un fournisseur d'identité SAML

Dans le compte d'accès d'urgence, créez un fournisseur d'identité SAML dans IAM en suivant les étapes décrites dans [Créer un fournisseur d'identité SAML](#) dans IAM. Téléchargez les métadonnées requises depuis votre ADFS serveur :

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/  
FederationMetadata.xml
```

Création de rôles d'accès d'urgence

[Créez des rôles d'accès d'urgence](#) dans le compte d'urgence en utilisant la fédération SAML 2.0 comme type d'entité de confiance. Sélectionnez le fournisseur SAML 2.0 que vous avez créé à l'étape précédente.

Considérations :

- Incluez toutes les régions dans lesquelles vous exercez vos activités : sélectionnez toutes les régions dans lesquelles vous avez des charges de travail actives pour vous assurer que la fédération reste disponible en cas de perturbation régionale.
- Configurez au moins un point de terminaison régional supplémentaire, même si vous opérez dans une seule région. Par exemple, si vous n'opérez que dans us-east-1, ajoutez-le en us-west-2 tant que point de terminaison secondaire. Vous pouvez transférer votre IdP vers le point de terminaison de connexion us-west-2 SAML tout en continuant à accéder à vos us-east-1 ressources, même sans aucune charge de travail. us-west-2

- Activez à la fois le point de terminaison non régional et le point de terminaison régional : bien que le point de terminaison non régional (<https://signin.aws.amazon.com/saml>) soit hautement disponible, il est hébergé dans un seul terminal Région AWSus-east-1, tandis que les points de terminaison régionaux (<https://<region>.signin.aws.amazon.com/saml>) améliorent la résilience en réduisant la dépendance à l'égard d'un seul point de terminaison mondial.

Configuration de la politique de confiance

Reportez-vous à un [Configuration unique d'une application de fédération IAM directe dans Okta](#) exemple de politique de confiance avec plusieurs points de terminaison régionaux de connexion. Remplacez les points de terminaison régionaux et le fournisseur ARNs SAML de l'échantillon par les vôtres.

Configuration des politiques d'autorisation

Reportez-vous à un [Configuration unique d'une application de fédération IAM directe dans Okta](#) exemple de politique d'autorisation que vous associez aux rôles d'accès d'urgence.

Configurer les rôles des comptes de charge de travail

Pour les rôles du compte de charge de travail, configurez une politique de confiance personnalisée qui permet aux rôles d'accès d'urgence du compte d'accès d'urgence de les assumer. Reportez-vous à un [Configuration unique d'une application de fédération IAM directe dans Okta](#) exemple de politique de confiance, où le compte 123456789012 est le compte d'accès d'urgence.

Configuration d'Active Directory

Les étapes suivantes décrivent comment configurer Active Directory et ADFS pour l'accès d'urgence.

1. [Création de groupes](#)
2. [Créez un groupe de confiance](#)
3. [Créez des règles de réclamation](#)

Création de groupes

Créez des groupes d'urgence dans Active Directory conformément à la convention de dénomination décrite précédemment (par exemple, AWS-123456789012-EmergencyAccess_Role1_R0). Affectez des utilisateurs à ces groupes par le biais de vos mécanismes de provisionnement existants.

Créez un groupe de confiance

ADFS la fédération nécessite une configuration de parties dépendantes. La partie utilisatrice est AWS Security Token Service (AWS STS), qui sous-traite l'authentification en ADFS tant que fournisseur d'identité.

1. Dans la console ADFS de gestion, utilisez le menu Action et sélectionnez Ajouter la confiance d'une partie fiable. Sélectionnez Claims aware lorsque vous ajoutez une partie de confiance.
2. Pour les métadonnées de fédération, entrez l'URL des métadonnées figurant dans les informations de métadonnées du fournisseur d'identité sur la console IAM. Par exemple :

`https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml`
3. Définissez le nom d'affichage de la partie utilisatrice (par exemple, AWS Account Access), puis choisissez Next.
4. Sélectionnez les personnes auxquelles vous souhaitez autoriser l'accès AWS. Vous pouvez sélectionner des groupes spécifiques et définir des exigences telles que le MFA.
5. Choisissez Fermer sur la page Terminer pour terminer l'assistant d'ajout de confiance à une partie fiable. AWS est désormais configuré en tant que partie utilisatrice.

Créez des règles de réclamation

ADFS utilise le langage des règles relatives aux réclamations pour émettre et transformer les réclamations entre les fournisseurs de réclamations et les parties utilisatrices. Vous devez créer quatre règles de réclamation : NameId, RoleSessionName, Get AD Groups et Roles for AWS Access.

Cliquez avec le bouton droit sur la partie utilisatrice, puis choisissez Modifier la politique d'émission des demandes. Choisissez Ajouter une règle pour ajouter des règles.

1NameId.

- a. Sélectionnez Transformer une réclamation entrante, puis cliquez sur Suivant.
- b. Utilisez les paramètres suivants :
 - Nom de la règle de réclamation : NameId
 - Type de réclamation entrante : Windows Account Name
 - Type de demande sortante : Name ID
 - Format du nom et de l'identifiant sortant : Persistent Identifier

- Passez en revue toutes les valeurs des réclamations : coché

c. Choisissez OK.

2. RoleSessionName

a. Choisissez Add Rule (Ajouter une règle).

b. Dans la liste des modèles de règles de réclamation, sélectionnez Envoyer les attributs LDAP sous forme de revendications.

c. Utilisez les paramètres suivants :

- Nom de la règle de réclamation : RoleSessionName
- Boutique d'attributs : Active Directory
- Attribut LDAP : E-Mail-Addresses
- Type de réclamation sortante : `https://aws.amazon.com/SAML/Attributes/RoleSessionName`

d. Choisissez OK.

3. Obtenir des groupes AD

a. Choisissez Add Rule (Ajouter une règle).

b. Dans la liste des modèles de règles de réclamation, sélectionnez Envoyer les réclamations à l'aide d'une règle personnalisée, puis cliquez sur Suivant.

c. Dans Nom de la règle de réclamationGet AD Groups, entrez, puis dans Règle personnalisée, entrez ce qui suit :

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

Cette règle personnalisée utilise un script dans le langage des règles de réclamation qui récupère tous les groupes dont l'utilisateur authentifié est membre et les place dans une réclamation temporaire nommée. `http://temp/variable`

 Note

Assurez-vous qu'il n'y a pas d'espace blanc à la fin pour éviter des résultats inattendus.

4. Attributs du rôle

- a. Choisissez Add Rule (Ajouter une règle).
- b. Dans la liste des modèles de règles de réclamation, sélectionnez Envoyer les réclamations à l'aide d'une règle personnalisée, puis cliquez sur Suivant.
- c. Dans Nom de la règle de réclamationRoles, entrez, puis dans Règle personnalisée, entrez ce qui suit :

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]  
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/  
<ADFS>,arn:aws:iam::$1:role/"));
```

Cette règle personnalisée utilise des expressions régulières pour transformer chacune des appartenances de groupe du formulaire AWS-**<Account Number>**-**<Role Name>** en ARN du rôle IAM et en formulaire ARN du fournisseur de fédération IAM attendu. AWS

 Note

Dans l'exemple de langage de règles ci-dessus, ADFS représente le nom logique donné au fournisseur d'identité SAML dans la configuration du fournisseur AWS d'identité. Modifiez-le en fonction du nom logique que vous avez choisi dans la console IAM pour votre fournisseur d'identité.

Tester la configuration

Vérifiez que la solution fonctionne en vous authentifiant auprès `https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx` de. Sélectionnez le nom de la partie utilisatrice que vous avez créée dans la liste déroulante des sites.

Mettre à jour le point de terminaison d'assertion SAML par défaut dans ADFS

Important

Lors de la configuration de la confiance des parties ADFS dépendantes, le point de terminaison d'assertion SAML utilise par défaut celui `https://signin.aws.amazon.com/` qui n'est pas un point de terminaison global et se trouve dans `us-east-1`. Nous vous recommandons de remplacer le point de terminaison par défaut par un point de terminaison régional différent de celui où votre centre d'identité IAM est configuré pour la résilience. Par exemple, si votre centre d'identité IAM est déployé `us-east-1` et que vous y opérez également `us-west-2`, remplacez le point de terminaison client par défaut de l'assertion SAML par `https://us-west-2.signin.aws.amazon.com/saml`.

1. Choisissez Propriétés en fonction de la confiance de la partie fiable et accédez à l'onglet Surveillance. Décochez la case Mettre automatiquement à jour la partie utilisatrice.
2. Accédez à l'onglet Points de terminaison, sélectionnez votre point de terminaison de connexion préféré, puis choisissez Modifier.
3. Cochez la case Définir l'URL sécurisée par défaut. Cliquez sur OK et sur Appliquer pour que le réglage prenne effet.

Note

La plupart des IdPs permettent de désactiver l'intégration d'une application jusqu'à ce que vous en ayez besoin. Nous vous recommandons de laisser l'application de fédération IAM directe désactivée dans votre IdP jusqu'à ce qu'elle soit requise pour un accès d'urgence.

Sécurité dans AWS IAM Identity Center

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des [programmes de conformité AWS](#). Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS IAM Identity Center, consultez la section [AWS Services concernés par programme de conformité](#).
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'IAM Identity Center. Les rubriques suivantes expliquent comment configurer IAM Identity Center pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre IAM Identity Center.

Rubriques

- [Gestion des identités et des accès pour IAM Identity Center](#)
- [Autorisation de la console et de l'API IAM Identity Center](#)
- [AWS STS clés contextuelles de condition pour IAM Identity Center](#)
- [Journalisation et surveillance dans IAM Identity Center](#)
- [Validation de conformité pour IAM Identity Center](#)
- [Résilience dans IAM Identity Center](#)
- [Sécurité de l'infrastructure dans IAM Identity Center](#)

Gestion des identités et des accès pour IAM Identity Center

L'accès à IAM Identity Center nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Ces informations d'identification doivent être autorisées à accéder aux AWS ressources, telles qu'une application AWS gérée.

L'authentification sur le portail AWS d'accès est contrôlée par le répertoire que vous avez connecté à IAM Identity Center. Cependant, l' Comptes AWS autorisation accordée aux utilisateurs depuis le portail AWS d'accès est déterminée par deux facteurs :

1. Qui a reçu l'accès à ceux de Comptes AWS la console IAM Identity Center. Pour de plus amples informations, veuillez consulter [Accès par authentification unique à Comptes AWS](#).
2. Quel niveau d'autorisations a été accordé aux utilisateurs dans la console IAM Identity Center pour leur permettre d'y accéder de manière appropriée ? Comptes AWS Pour de plus amples informations, veuillez consulter [Création, gestion et suppression des jeux d'autorisations](#).

Les sections suivantes expliquent comment, en tant qu'administrateur, vous pouvez contrôler l'accès à la console IAM Identity Center ou déléguer l'accès administratif aux day-to-day tâches depuis la console IAM Identity Center.

- [Authentification](#)
- [Contrôle d'accès](#)

Authentification

Découvrez comment accéder à l' AWS aide des [identités IAM](#).

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais vous ne pouvez pas créer de ressources IAM Identity Center ou y accéder sans autorisation. Par exemple, vous devez disposer des autorisations nécessaires pour créer un répertoire connecté à IAM Identity Center.

Note

Si votre instance IAM Identity Center est configurée avec une clé KMS gérée par le client, les administrateurs de votre IAM Identity Center et les autres acteurs ayant besoin d'accéder à la

clé KMS auront besoin d'autorisations supplémentaires. Reportez-vous à [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#).

Les sections suivantes décrivent comment gérer les autorisations pour IAM Identity Center. Nous vous recommandons de lire d'abord la présentation.

- [Vue d'ensemble de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center](#)
- [Exemples de politiques basées sur l'identité pour IAM Identity Center](#)
- [Exemple de politique basée sur les ressources pour IAM Identity Center IAM Identity Center](#)
- [Utilisation de rôles liés à un service pour IAM Identity Center](#)

Vue d'ensemble de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center

Chaque AWS ressource appartient à un Compte AWS, et les autorisations de création ou d'accès aux ressources sont régies par des politiques d'autorisation. Pour fournir un accès, un administrateur de compte peut ajouter des autorisations aux identités IAM (c'est-à-dire aux utilisateurs, aux groupes et aux rôles). Certains services (tels que AWS Lambda) prennent également en charge l'ajout d'autorisations aux ressources.

Note

Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté des privilèges d'administrateur. Pour plus d'informations, consultez [Bonnes pratiques IAM](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [Ressources et opérations de l'IAM Identity Center](#)
- [Présentation de la propriété des ressources](#)
- [Gestion de l'accès aux ressources](#)
- [Spécification des éléments de politique : actions, effets, ressources et principes](#)
- [Spécification de conditions dans une politique](#)

Ressources et opérations de l'IAM Identity Center

Dans IAM Identity Center, les ressources principales sont les instances d'applications, les profils et les ensembles d'autorisations.

Présentation de la propriété des ressources

Le propriétaire d'une ressource est celui Compte AWS qui a créé une ressource. En d'autres termes, le propriétaire Compte AWS de la ressource est l'entité principale (le compte, un utilisateur ou un rôle IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si le Utilisateur racine d'un compte AWS crée une ressource IAM Identity Center, telle qu'une instance d'application ou un ensemble d'autorisations, vous Compte AWS êtes le propriétaire de cette ressource.
- Si vous créez un utilisateur dans votre AWS compte et que vous lui accordez les autorisations nécessaires pour créer des ressources IAM Identity Center, l'utilisateur peut alors créer des ressources IAM Identity Center. Cependant, votre AWS compte, auquel appartient l'utilisateur, est propriétaire des ressources.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour créer des ressources IAM Identity Center, toute personne pouvant assumer ce rôle peut créer des ressources IAM Identity Center. Vous Compte AWS, à qui appartient le rôle, êtes propriétaire des ressources de l'IAM Identity Center.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

Note

Cette section décrit l'utilisation d'IAM dans le contexte d'IAM Identity Center. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, consultez la rubrique [Qu'est-ce que IAM ?](#) dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, consultez la [Référence des politiques AWS IAM](#) dans le Guide de l'utilisateur IAM.

Les politiques qui sont associées à une identité IAM sont appelées des politiques basées sur l'identité (politiques IAM). Les politiques qui sont attachées à une ressource sont appelées politiques basées sur la ressource. IAM Identity Center ne prend en charge que les politiques basées sur l'identité (politiques IAM).

Rubriques

- [Politiques basées sur une identité \(politiques IAM\)](#)
- [Politiques basées sur les ressources](#)

Politiques basées sur une identité (politiques IAM)

Vous pouvez ajouter des autorisations aux identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associez une politique d'autorisations à un utilisateur ou à un groupe de votre compte
Compte AWS : un administrateur de compte peut utiliser une politique d'autorisations associée à un utilisateur particulier pour autoriser cet utilisateur à ajouter une ressource IAM Identity Center, telle qu'une nouvelle application.
- Attacher une politique d'autorisations à un rôle (accorder des autorisations entre comptes) : vous pouvez attacher une politique d'autorisation basée sur une identité à un rôle IAM afin d'accorder des autorisations entre comptes.

Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, veuillez consulter la section [Access management](#) (français non garanti) dans le Guide de l'utilisateur IAM.

La politique d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `List`. Ces actions affichent des informations sur une ressource IAM Identity Center, telle qu'une instance d'application ou un ensemble d'autorisations. Notez que le caractère générique (*) dans l'`Resource` élément indique que les actions sont autorisées pour toutes les ressources IAM Identity Center détenues par le compte.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
    "Effect": "Allow",
    "Action": "sso:List*",
    "Resource": "*"
  }
]
```

Pour plus d'informations sur l'utilisation de politiques basées sur l'identité avec IAM Identity Center, consultez [Exemples de politiques basées sur l'identité pour IAM Identity Center](#). Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez [Identités \(utilisateurs, groupes et rôles\)](#) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez attacher une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. IAM Identity Center ne prend pas en charge les politiques basées sur les ressources.

Spécification des éléments de politique : actions, effets, ressources et principes

Pour chaque ressource IAM Identity Center (voir [Ressources et opérations de l'IAM Identity Center](#)), le service définit un ensemble d'opérations d'API. Pour accorder des autorisations pour ces opérations d'API, IAM Identity Center définit un ensemble d'actions que vous pouvez spécifier dans une politique. Notez que l'exécution d'une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments de base d'une politique :

- **Ressource** : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique.
- **Action** : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, l'`sso:DescribePermissionsPolicies` autorise l'utilisateur à effectuer l'`DescribePermissionsPolicies` opération IAM Identity Center.
- **Effet** – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être une autorisation ou un refus. Si vous n'octroyez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.

- **Principal** – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). IAM Identity Center ne prend pas en charge les politiques basées sur les ressources.

Pour en savoir plus sur la syntaxe et les descriptions des politiques IAM, consultez la [Référence des politiques AWS IAM](#) dans le Guide de l'utilisateur IAM.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage d'access policy pour spécifier les conditions qui doivent être remplies pour qu'une stratégie prenne effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de politique, consultez [Condition](#) dans le Guide de l'utilisateur IAM.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe aucune clé de condition spécifique à IAM Identity Center. Cependant, il existe des clés de AWS condition que vous pouvez utiliser selon les besoins. Pour obtenir la liste complète des AWS clés, consultez la section [Clés de condition globales disponibles](#) dans le guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour IAM Identity Center

Cette rubrique fournit des exemples de politiques IAM que vous pouvez créer pour accorder aux utilisateurs et aux rôles les autorisations nécessaires à l'administration d'IAM Identity Center.

Important

Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options disponibles pour gérer l'accès aux ressources de votre IAM Identity Center. Pour de plus amples informations, veuillez consulter [Vue d'ensemble de la gestion des autorisations d'accès aux ressources de votre IAM Identity Center](#).

Les sections de cette rubrique couvrent les sujets suivants :

- [Exemples de politiques personnalisées](#)

- [Autorisations requises pour utiliser la console IAM Identity Center](#)

Exemples de politiques personnalisées

Cette section fournit des exemples de cas d'utilisation courants qui nécessitent une politique IAM personnalisée. Ces exemples de politiques sont des politiques basées sur l'identité, qui ne spécifient pas l'élément principal. En effet, avec une politique basée sur l'identité, vous ne spécifiez pas le principal qui obtient l'autorisation. Au lieu de cela, vous attachez la politique au principal. Lorsque vous associez une politique d'autorisation basée sur l'identité à un rôle IAM, le principal identifié dans la politique de confiance du rôle obtient les autorisations. Vous pouvez créer des politiques basées sur l'identité dans IAM et les associer à des utilisateurs, des groupes et des rôles. and/or Vous pouvez également appliquer ces politiques aux utilisateurs d'IAM Identity Center lorsque vous créez un ensemble d'autorisations dans IAM Identity Center.

Note

Utilisez ces exemples lorsque vous créez des politiques pour votre environnement et assurez-vous de tester les cas positifs (« accès accordé ») et négatifs (« accès refusé ») avant de déployer ces politiques dans votre environnement de production. Pour plus d'informations sur le test des politiques IAM, consultez la section [Tester les politiques IAM avec le simulateur de politiques IAM dans le guide](#) de l'utilisateur IAM.

Rubriques

- [Exemple 1 : Autoriser un utilisateur à consulter le centre d'identité IAM](#)
- [Exemple 2 : Autoriser un utilisateur à gérer les autorisations Comptes AWS dans IAM Identity Center](#)
- [Exemple 3 : Autoriser un utilisateur à gérer des applications dans IAM Identity Center](#)
- [Exemple 4 : autoriser un utilisateur à gérer les utilisateurs et les groupes dans votre annuaire Identity Center](#)

Exemple 1 : Autoriser un utilisateur à consulter le centre d'identité IAM

La politique d'autorisation suivante accorde des autorisations en lecture seule à un utilisateur afin qu'il puisse consulter tous les paramètres et informations d'annuaire configurés dans IAM Identity Center.

 Note

Cette politique n'est fournie qu'à titre d'exemple. Dans un environnement de production, nous vous recommandons d'utiliser la politique ViewOnlyAccess AWS gérée pour IAM Identity Center.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListAccountAssignments",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListPermissionSets",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso-directory:DescribeDirectory",
        "sso-directory:SearchUsers",
        "sso-directory:SearchGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Exemple 2 : Autoriser un utilisateur à gérer les autorisations Comptes AWS dans IAM Identity Center

La politique d'autorisation suivante accorde des autorisations permettant à un utilisateur de créer, de gérer et de déployer des ensembles d'autorisations pour votre Comptes AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AttachManagedPolicyToPermissionSet",
        "sso:CreateAccountAssignment",
        "sso:CreatePermissionSet",
        "sso>DeleteAccountAssignment",
        "sso>DeleteInlinePolicyFromPermissionSet",
        "sso>DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:UpdatePermissionSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMListPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:ListPolicies"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AccessToSSOProvisionedRoles",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
```

```

        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:GetSAMLProvider"
    ],
    "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
  }
]
}

```

Note

Les autorisations supplémentaires répertoriées sous "Sid": "IAMListPermissions" les "Sid": "AccessToSSOProvisionedRoles" sections et sont requises uniquement pour permettre à l'utilisateur de créer des attributions dans le compte AWS Organizations de gestion. Dans certains cas, il se peut que vous deviez également ajouter des `iam:UpdateSAMLProvider` éléments à ces sections.

Exemple 3 : Autoriser un utilisateur à gérer des applications dans IAM Identity Center

La politique d'autorisation suivante accorde des autorisations permettant à un utilisateur de visualiser et de configurer des applications dans IAM Identity Center, y compris des applications SaaS préintégrées issues du catalogue IAM Identity Center.

 Note

L'`sso:AssociateProfile` opération utilisée dans l'exemple de politique suivant est requise pour la gestion des affectations d'utilisateurs et de groupes aux applications. Il permet également à un utilisateur d'attribuer des utilisateurs et des groupes à Comptes AWS l'aide des ensembles d'autorisations existants. Si un utilisateur doit gérer l' Compte AWS accès au sein d'IAM Identity Center et a besoin des autorisations nécessaires pour gérer les ensembles d'autorisations, consultez [Exemple 2 : Autoriser un utilisateur à gérer les autorisations Comptes AWS dans IAM Identity Center](#).

Depuis octobre 2020, bon nombre de ces opérations ne sont disponibles que via la AWS console. Cet exemple de politique inclut des actions de « lecture » telles que `list`, `get` et `search`, qui sont pertinentes pour le fonctionnement sans erreur de la console dans ce cas.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AssociateProfile",
        "sso:CreateApplicationInstance",
        "sso:ImportApplicationInstanceServiceProviderMetadata",
        "sso:DeleteApplicationInstance",
        "sso:DeleteProfile",
        "sso:DisassociateProfile",
        "sso:GetApplicationTemplate",
        "sso:UpdateApplicationInstanceServiceProviderConfiguration",
        "sso:UpdateApplicationInstanceDisplayData",
        "sso:DeleteManagedApplicationInstance",
        "sso:UpdateApplicationInstanceStatus",
        "sso:GetManagedApplicationInstance",
        "sso:UpdateManagedApplicationInstanceStatus",
        "sso:CreateManagedApplicationInstance",
        "sso:UpdateApplicationInstanceSecurityConfiguration",
        "sso:UpdateApplicationInstanceResponseConfiguration",
        "sso:GetApplicationInstance",

```

```

        "sso:CreateApplicationInstanceCertificate",
        "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
        "sso:UpdateApplicationInstanceActiveCertificate",
        "sso:DeleteApplicationInstanceCertificate",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationTemplates",
        "sso:ListApplications",
        "sso:ListApplicationInstances",
        "sso:ListDirectoryAssociations",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:ListInstances",
        "sso:GetProfile",
        "sso:GetSSOStatus",
        "sso:GetSsoConfiguration",
        "sso-directory:DescribeDirectory",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
    ],
    "Resource": "*"
}
]
}

```

Exemple 4 : autoriser un utilisateur à gérer les utilisateurs et les groupes dans votre annuaire Identity Center

La politique d'autorisation suivante accorde des autorisations permettant à un utilisateur de créer, d'afficher, de modifier et de supprimer des utilisateurs et des groupes dans IAM Identity Center.

Dans certains cas, les modifications directes apportées aux utilisateurs et aux groupes dans IAM Identity Center sont limitées. Par exemple, lorsqu'Active Directory ou un fournisseur d'identité externe avec le provisionnement automatique activé est sélectionné comme source d'identité.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [

```

```

    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:ListGroupForUser",
        "sso-directory:DisableUser",
        "sso-directory:EnableUser",
        "sso-directory:SearchGroups",
        "sso-directory>DeleteGroup",
        "sso-directory:AddMemberToGroup",
        "sso-directory:DescribeDirectory",
        "sso-directory:UpdateUser",
        "sso-directory:ListMembersInGroup",
        "sso-directory:CreateUser",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchUsers",
        "sso:ListDirectoryAssociations",
        "sso-directory:RemoveMemberFromGroup",
        "sso-directory>DeleteUser",
        "sso-directory:DescribeUsers",
        "sso-directory:UpdateGroup",
        "sso-directory:CreateGroup"
      ],
      "Resource": "*"
    }
  ]
}

```

Autorisations requises pour utiliser la console IAM Identity Center

Pour qu'un utilisateur puisse utiliser la console IAM Identity Center sans erreur, des autorisations supplémentaires sont nécessaires. Si une politique IAM plus restrictive que les autorisations minimales requises a été créée, la console ne fonctionnera pas comme prévu pour les utilisateurs dotés de cette politique. L'exemple suivant répertorie l'ensemble des autorisations qui peuvent être nécessaires pour garantir un fonctionnement sans erreur dans la console IAM Identity Center.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```
"Effect": "Allow",
"Action": [
    "sso:DescribeAccountAssignmentCreationStatus",
    "sso:DescribeAccountAssignmentDeletionStatus",
    "sso:DescribePermissionSet",
    "sso:DescribePermissionSetProvisioningStatus",
    "sso:DescribeRegisteredRegions",
    "sso:GetApplicationInstance",
    "sso:GetApplicationTemplate",
    "sso:GetInlinePolicyForPermissionSet",
    "sso:GetManagedApplicationInstance",
    "sso:GetMfaDeviceManagementForDirectory",
    "sso:GetPermissionSet",
    "sso:GetProfile",
    "sso:GetSharedSsoConfiguration",
    "sso:GetSsoConfiguration",
    "sso:GetSSOStatus",
    "sso:GetTrust",
    "sso:ListAccountAssignmentCreationStatus",
    "sso:ListAccountAssignmentDeletionStatus",
    "sso:ListAccountAssignments",
    "sso:ListAccountsForProvisionedPermissionSet",
    "sso:ListApplicationInstanceCertificates",
    "sso:ListApplicationInstances",
    "sso:ListApplications",
    "sso:ListApplicationTemplates",
    "sso:ListDirectoryAssociations",
    "sso:ListInstances",
    "sso:ListManagedPoliciesInPermissionSet",
    "sso:ListPermissionSetProvisioningStatus",
    "sso:ListPermissionSets",
    "sso:ListPermissionSetsProvisionedToAccount",
    "sso:ListProfileAssociations",
    "sso:ListProfiles",
    "sso:ListTagsForResource",
    "sso-directory:DescribeDirectory",
    "sso-directory:DescribeGroups",
    "sso-directory:DescribeUsers",
    "sso-directory:ListGroupsForUser",
    "sso-directory:ListMembersInGroup",
    "sso-directory:SearchGroups",
    "sso-directory:SearchUsers"
],
"Resource": "*"

```

```

    }
  ]
}
```

Exemple de politique basée sur les ressources pour IAM Identity Center

Chaque application qui fonctionne avec IAM Identity Center et utilise la [OAuth version 2.0](#) nécessite une politique basée sur les ressources. L'application peut être gérée par le client ou AWS gérée. La stratégie basée sur les ressources requise, appelée politique d'application (ou [ActorPolicy](#) dans le APIs), définit les [principaux IAM autorisés à appeler des actions d'API](#) de la méthode d'authentification IAM, telles que. [CreateTokenWithIAM](#) La méthode d'authentification IAM permet à un principal IAM, tel qu'un rôle ou un AWS service IAM, de s'authentifier auprès du service IAM Identity Center OIDC en présentant des informations d'identification IAM pour demander ou gérer des jetons d'accès sur le répertoire /token ? point de terminaison aws_iam=t.

La politique d'application régit les opérations d'émission de jetons (CreateTokenWithIAM). La politique régit également les actions avec autorisation uniquement utilisées par les applications AWS gérées pour valider les jetons (IntrospectTokenWithIAM) et révoquer les jetons (). RevokeTokenWithIAM Pour une application gérée par le client, vous configurez cette politique en spécifiant les principaux IAM autorisés à appeler. CreateTokenWithIAM Lorsqu'un principal autorisé appelle cette action d'API, il reçoit des jetons d'accès et d'actualisation pour l'application.

Si vous utilisez la console IAM Identity Center pour configurer une application gérée par le client pour une [propagation d'identité fiable](#), reportez-vous à l'étape 4 de la section [Configuration des applications OAuth 2.0 gérées par le client](#) pour savoir comment configurer la politique d'application. Pour un exemple de politique, voir [Exemple de politique : autoriser un rôle IAM à créer des jetons d'accès et à actualiser](#) plus loin dans cette rubrique.

Exigences des stratégies

La politique doit répondre aux exigences suivantes :

- La politique doit inclure un Version élément défini sur « 2012-10-17 ».
- La politique doit inclure au moins un Statement élément.
- Chaque politique Statement doit inclure les éléments suivants : EffectPrincipal, Action, et Resource.

Éléments de stratégie

La politique doit inclure les éléments suivants :

Version

Spécifie la version du document de politique. Définissez la version sur 2012-10-17 (la dernière version).

Instruction

Contient la politiqueStatements. La politique doit en contenir au moins unStatement.

Chaque politique Statement comprend les éléments suivants.

Effet

(Requis) Détermine s'il convient d'autoriser ou de rejeter les autorisations figurant dans l'instruction de politique. Les valeurs valides sont Allow ou Deny.

Principal

(Requis) Le [principal](#) est l'identité qui obtient les autorisations figurant dans l'instruction de politique. Vous pouvez spécifier les rôles IAM ou les principaux AWS de service.

Action

(Obligatoire) Les opérations d'API du service IAM Identity Center OIDC à autoriser ou à refuser. Les actions valides incluent :

- `sso-oauth:CreateTokenWithIAM`: Cette action, qui correspond à l'opération de l'[CreateTokenWithIAM](#) API, autorise la création et le renvoi de jetons d'accès et d'actualisation pour les applications clientes autorisées authentifiées à l'aide de n'importe quelle entité IAM, telle qu'un rôle de AWS service ou un utilisateur. Ces jetons peuvent contenir des étendues définies qui spécifient des autorisations telles que `read:profile` ou `write:data`.
- `sso-oauth:IntrospectTokenWithIAM` [autorisation uniquement] : accorde l'autorisation de valider et de récupérer des informations sur les jetons d'accès OAuth 2.0 actifs et 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.

Ressource

(Obligatoire) Dans cette politique, la valeur de l'élément `Resource` est `"*"`, ce qui signifie « cette application ».

Pour plus d'informations sur la syntaxe des AWS politiques, voir la [référence de stratégie AWS IAM](#) dans le guide de l'utilisateur IAM.

Exemple de politique : autoriser un rôle IAM à créer des jetons d'accès et à actualiser

La politique d'autorisation suivante accorde des autorisations à `ExampleAppClientRole` un rôle IAM assumé par une charge de travail pour créer et renvoyer des jetons d'accès et d'actualisation.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRoleToCreateTokens",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
      },
      "Action": "sso-oauth:CreateTokenWithIAM",
      "Resource": "*"
    }
  ]
}
```

AWS politiques gérées pour IAM Identity Center

La [création de politiques gérées par les clients IAM](#) qui fournissent à votre équipe uniquement les autorisations dont elle a besoin demande du temps et de l'expertise. Pour démarrer rapidement, vous pouvez utiliser des politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques gérées par AWS, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement

des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page [politiques gérées par AWS pour les fonctions de tâche](#) dans le Guide de l'utilisateur IAM.

De nouvelles actions vous permettant de répertorier et de supprimer des sessions utilisateur sont disponibles dans le nouvel espace de noms `identitystore-auth`. Toutes les autorisations supplémentaires pour les actions dans cet espace de noms seront mises à jour sur cette page. Lorsque vous créez vos politiques IAM personnalisées, évitez d'utiliser `*after,identitystore-auth` car cela s'applique à toutes les actions existant dans l'espace de noms aujourd'hui ou à l'avenir.

AWS politique gérée : `AWSSSOMasterAccountAdministrator`

La `AWSSSOMasterAccountAdministrator` politique fournit les mesures administratives requises aux directeurs d'école. La politique est destinée aux directeurs qui jouent le rôle d' AWS IAM Identity Center administrateur. Au fil du temps, la liste des actions fournies sera mise à jour pour correspondre aux fonctionnalités existantes d'IAM Identity Center et aux actions requises en tant qu'administrateur.

Vous pouvez associer la politique `AWSSSOMasterAccountAdministrator` à vos identités IAM. Lorsque vous associez la `AWSSSOMasterAccountAdministrator` politique à une identité, vous accordez AWS IAM Identity Center des autorisations administratives. Les principaux détenteurs de cette politique peuvent accéder à IAM Identity Center depuis le compte de AWS Organizations gestion et tous les comptes des membres. Ce principal peut gérer entièrement toutes les opérations du centre d'identité IAM, y compris la possibilité de créer une instance d'IAM Identity Center, des utilisateurs, des ensembles d'autorisations et des attributions. Le principal peut également instancier ces attributions dans les comptes des membres de l' AWS organisation et établir des connexions entre les annuaires AWS Directory Service gérés et IAM Identity Center. Au fur et à mesure que de nouvelles fonctionnalités administratives seront publiées, ces autorisations seront automatiquement accordées à l'administrateur du compte.

Cette politique inclut également AWS Key Management Service les autorisations requises pour les instances IAM Identity Center qui utilisent des clés gérées par le client pour le chiffrement.

Regroupements d'autorisations

Cette politique est groupée en instructions basées sur le jeu d'autorisations fourni.

- `AWSSSOMasterAccountAdministrator`— Permet à IAM Identity Center de [transmettre le rôle de service](#) nommé `AWSServiceRoleforSSO` à IAM Identity Center afin qu'il puisse ultérieurement assumer le rôle et effectuer des actions en son nom. Cela est nécessaire lorsque la personne ou l'application tente d'activer IAM Identity Center. Pour de plus amples informations, veuillez consulter [Configurer l'accès à Comptes AWS](#).
- `AWSSSOMemberAccountAdministrator`— Permet à IAM Identity Center d'effectuer des actions d'administrateur de compte dans un environnement multi-comptes AWS . Pour de plus amples informations, veuillez consulter [AWS politique gérée : AWSSSOMember AccountAdministrator](#).
- `AWSSSOManageDelegatedAdministrator`— Permet à IAM Identity Center d'enregistrer et de désenregistrer un administrateur délégué pour votre organisation.
- `AllowKMSKeyUseViaServiceet AllowKMSKeyDiscovery` — Autorise les AWS Key Management Service opérations relatives aux clés gérées par le client utilisées par les instances d'IAM Identity Center.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSSSOMasterAccountAdministrator](#) à la section AWS Managed Policy Reference.

Informations supplémentaires sur cette politique

Lorsque IAM Identity Center est activé pour la première fois, le service IAM Identity Center crée un [rôle lié au service](#) dans le compte de AWS Organizations gestion (ancien compte principal) afin que IAM Identity Center puisse gérer les ressources de votre compte. Les actions requises sont `iam:CreateServiceLinkedRole` et `iam:PassRole`.

AWS politique gérée : AWSSSOMember AccountAdministrator

La `AWSSSOMemberAccountAdministrator` politique fournit les mesures administratives requises aux directeurs d'école. La politique est destinée aux directeurs qui jouent le rôle d'administrateur du centre d'identité IAM. Au fil du temps, la liste des actions fournies sera mise à jour pour correspondre aux fonctionnalités existantes d'IAM Identity Center et aux actions requises en tant qu'administrateur.

Vous pouvez associer la politique `AWSSSOMemberAccountAdministrator` à vos identités IAM. Lorsque vous associez la `AWSSSOMemberAccountAdministrator` politique à une identité, vous accordez AWS IAM Identity Center des autorisations administratives. Les principaux détenteurs de cette politique peuvent accéder à IAM Identity Center depuis le compte de AWS Organizations gestion et tous les comptes des membres. Ce principal peut gérer entièrement toutes les opérations de l'IAM Identity Center, y compris la possibilité de créer des utilisateurs, des ensembles d'autorisations et des attributions. Le principal peut également instancier ces attributions dans les comptes des membres de l' AWS organisation et établir des connexions entre les annuaires AWS Directory Service gérés et IAM Identity Center. À mesure que de nouvelles fonctionnalités administratives sont publiées, ces autorisations sont automatiquement accordées à l'administrateur du compte.

Cette politique inclut également AWS Key Management Service les autorisations requises pour les instances IAM Identity Center qui utilisent des clés gérées par le client pour le chiffrement.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSSSOMemberAccountAdministrator](#) à la section AWS Managed Policy Reference.

Informations supplémentaires sur cette politique

Les administrateurs d'IAM Identity Center gèrent les utilisateurs, les groupes et les mots de passe dans leur répertoire Identity Center (répertoire SSO). Le rôle d'administrateur du compte inclut des autorisations pour les actions suivantes :

- `"sso:*"`
- `"sso-directory:*"`

Les administrateurs d'IAM Identity Center ont besoin d'autorisations limitées pour effectuer les Directory Service actions suivantes afin d'effectuer les tâches quotidiennes.

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `"ds>CreateAlias"`

Ces autorisations permettent aux administrateurs d'IAM Identity Center d'identifier les annuaires existants et de gérer les applications afin qu'elles puissent être configurées pour être utilisées avec IAM Identity Center. Pour plus d'informations sur chacune de ces actions, consultez la section [Autorisations d'Directory Service API : référence des actions, des ressources et des conditions](#).

IAM Identity Center utilise des politiques IAM pour accorder des autorisations aux utilisateurs d'IAM Identity Center. Les administrateurs d'IAM Identity Center créent des ensembles d'autorisations et y associent des politiques. L'administrateur du centre d'identité IAM doit être autorisé à répertorier les politiques existantes afin de pouvoir choisir les politiques à utiliser avec l'ensemble d'autorisations qu'il crée ou met à jour. Pour définir des autorisations sécurisées et fonctionnelles, l'administrateur du centre d'identité IAM doit disposer des autorisations nécessaires pour exécuter la validation de la politique d'IAM Access Analyzer.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

Les administrateurs d'IAM Identity Center ont besoin d'un accès limité aux AWS Organizations actions suivantes pour effectuer leurs tâches quotidiennes :

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

Ces autorisations permettent aux administrateurs d'IAM Identity Center de travailler avec les ressources de l'organisation (comptes) pour les tâches administratives de base d'IAM Identity Center, telles que les suivantes :

- Identifier le compte de gestion appartenant à l'organisation
- Identifier les comptes des membres appartenant à l'organisation
- Activation AWS de l'accès aux services pour les comptes
- Configuration et gestion d'un administrateur délégué

Pour plus d'informations sur l'utilisation d'un administrateur délégué avec IAM Identity Center, consultez [Administration déléguée](#). Pour plus d'informations sur la manière dont ces autorisations sont utilisées AWS Organizations, consultez la section [Utilisation AWS Organizations avec d'autres AWS services](#).

AWS politique gérée : AWSSSODirectory Administrateur

Vous pouvez associer la politique `AWSSSODirectoryAdministrator` à vos identités IAM.

Cette politique accorde des autorisations administratives aux utilisateurs et aux groupes d'IAM Identity Center. Les responsables auxquels cette politique est attachée peuvent apporter des mises à jour aux utilisateurs et aux groupes IAM Identity Center. Cette politique inclut également AWS Key Management Service les autorisations requises pour les instances IAM Identity Center qui utilisent des clés gérées par le client pour le chiffrement.

Cette politique inclut les autorisations suivantes :

- Répertoire du centre d'identité IAM : accès administratif complet aux opérations du répertoire d'IAM Identity Center.
- Identity Store : accès administratif complet aux opérations et à l'authentification du magasin d'identités.
- IAM Identity Center : autorisation de répertorier les associations d'annuaires.
- AWS Key Management Service- Autorisations permettant de déchiffrer, de décrire les clés et de générer des clés de données pour les clés gérées par le client utilisées par les instances d'IAM Identity Center.

Pour consulter les autorisations associées à cette politique, consultez la section [AWSSSODirectoryAdministrateur](#) dans AWS Managed Policy Reference.

AWS politique gérée : AWSSSORRead uniquement

Vous pouvez associer la politique AWSSS0Read0n1y à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations dans IAM Identity Center. Les principaux auxquels cette politique est attachée ne peuvent pas voir directement les utilisateurs ou les groupes de l'IAM Identity Center. Les principaux auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour dans IAM Identity Center. Par exemple, les principaux disposant de ces autorisations peuvent consulter les paramètres du centre d'identité IAM, mais ne peuvent modifier aucune des valeurs des paramètres.

Cette politique inclut également AWS Key Management Service les autorisations requises pour les instances IAM Identity Center qui utilisent des clés gérées par le client pour le chiffrement.

Pour consulter les autorisations associées à cette politique, reportez-vous à la section [AWSSS0ReadUniquement](#) dans la référence des politiques AWS gérées.

AWS politique gérée : AWSSSODirectory ReadOnly

Vous pouvez associer la politique AWSSS0DirectoryRead0n1y à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de visualiser les utilisateurs et les groupes dans IAM Identity Center. Les responsables auxquels cette politique est attachée ne peuvent pas consulter les attributions, les ensembles d'autorisations, les applications ou les paramètres d'IAM Identity Center. Les principaux auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour dans IAM Identity Center. Par exemple, les principaux disposant de ces autorisations peuvent voir les utilisateurs d'IAM Identity Center, mais ils ne peuvent modifier aucun attribut utilisateur ni attribuer de dispositifs MFA.

Cette politique inclut également AWS Key Management Service les autorisations requises pour les instances IAM Identity Center qui utilisent des clés gérées par le client pour le chiffrement.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSSS0DirectoryReadOnly](#) à la section AWS Managed Policy Reference.

AWS politique gérée : AWSIdentity SyncFullAccess

Vous pouvez associer la politique AWSIdentitySyncFullAccess à vos identités IAM.

Les principaux auxquels cette politique est attachée disposent d'autorisations d'accès complètes pour créer et supprimer des profils de synchronisation, associer ou mettre à jour un profil de

synchronisation à une cible de synchronisation, créer, répertorier et supprimer des filtres de synchronisation, et démarrer ou arrêter la synchronisation.

Détails de l'autorisation

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSIdentitySyncFullAccess](#) à la section AWS Managed Policy Reference.

AWS politique gérée : AWSIdentity SyncReadOnlyAccess

Vous pouvez associer la politique AWSIdentitySyncReadOnlyAccess à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations relatives au profil de synchronisation des identités, aux filtres et aux paramètres cibles. Les principaux auxquels cette politique est attachée ne peuvent pas mettre à jour les paramètres de synchronisation. Par exemple, les principaux disposant de ces autorisations peuvent consulter les paramètres de synchronisation des identités, mais ne peuvent modifier aucune des valeurs de profil ou de filtre.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSIdentitySyncReadOnlyAccess](#) à la section AWS Managed Policy Reference.

AWS politique gérée : AWSSSOService RolePolicy

Vous ne pouvez pas associer la AWSSSOServiceRolePolicy politique à vos identités IAM.

Cette politique est associée à un rôle lié à un service qui permet à IAM Identity Center de déléguer et d'appliquer les utilisateurs disposant d'un accès par authentification unique à un domaine spécifique. Comptes AWS AWS Organizations Lorsque vous activez IAM, un rôle lié à un service est créé Comptes AWS dans l'ensemble de votre organisation. IAM Identity Center crée également le même rôle lié au service dans chaque compte ajouté ultérieurement à votre organisation. Ce rôle permet à IAM Identity Center d'accéder aux ressources de chaque compte en votre nom. Les rôles liés à un service créés dans chacun d'eux Compte AWS sont nommés. AWSServiceRoleForSSO Pour de plus amples informations, veuillez consulter [Utilisation de rôles liés à un service pour IAM Identity Center](#).

AWS politique gérée : AWSIAMIdentity CenterAllowListForIdentityContext

Lorsque vous assumez un rôle dans le contexte d'identité de l'IAM Identity Center, AWS Security Token Service (AWS STS) attache automatiquement la AWSIAMIdentityCenterAllowListForIdentityContext politique au rôle.

Cette politique fournit la liste des actions autorisées lorsque vous utilisez la propagation d'identité sécurisée avec des rôles assumés dans le contexte d'identité IAM Identity Center. Toutes les autres actions appelées dans ce contexte sont bloquées. Le contexte d'identité est transmis en tant que `ProvidedContext`.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSIAMIdentityCenterAllowListForIdentityContext](#) à la section AWS Managed Policy Reference.

AWS politique gérée : AWSIdentityCenterExternalManagementPolicy

Vous pouvez associer la politique `AWSIdentityCenterExternalManagementPolicy` à vos identités IAM.

Cette politique permet de gérer les utilisateurs d'IAM Identity Center à partir d'un fournisseur externe.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSIdentityCenterExternalManagementPolicy](#) à la section AWS Managed Policy Reference.

Mises à jour des politiques AWS gérées par IAM Identity Center

Le tableau suivant décrit les mises à jour apportées aux politiques AWS gérées pour IAM Identity Center depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents d'IAM Identity Center.

Modifier	Description	Date
AWSIdentityCenterExternalManagementPolicy	Politique gérée mise à jour pour modifier l'ARN du locataire d'approvisionnement.	5 décembre 2025
AWSIdentityCenterExternalManagementPolicy	Cette politique permet de gérer les utilisateurs d'IAM Identity Center à partir d'un fournisseur externe.	21 novembre 2025
AWSSSOMasterAccountAdministrator , AWSSSOMemberAccountAdministrator , AWSSSORReadUniqueme	Politiques gérées mises à jour pour inclure AWS KMS les autorisations requises pour les instances IAM Identity Center	17 septembre 2025

Modifier	Description	Date
nt, AWSSSODirectoryAdministrateur, AWSSSODirectoryReadOnly	qui utilisent des clés gérées par le client pour le chiffrement.	
AWSSSOServiceRolePolicy	Cette politique inclut désormais les autorisations d'appelidentity-sync:DeleteSyncProfile .	11 février 2025
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les qapps:ExportQAppSessionData actions qapps:ListQAppSessionData et destinées à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	2 octobre 2024
AWSSSOMasterAccountAdministrator	IAM Identity Center a ajouté une nouvelle action pour accorder DeleteSyncProfile des autorisations afin de vous permettre d'utiliser cette politique pour supprimer des profils de synchronisation. Cette action est associée à DeleteInstance l'API.	26 septembre 2024

Modifier	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais l' <code>s3:ListCachedObjectAccessGrants</code> action visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	4 septembre 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les <code>aws:APIAccessAll</code> , <code>es:ESHttpHead</code> , <code>es:ESHttpPost</code> , <code>es:ESHttpGet</code> , <code>es:ESHttpPatch</code> , <code>es:ESHttpDelete</code> , et les <code>es:ESHttpPut</code> actions visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	12 juillet 2024

Modifier	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais lesqapps:PredictQApp ,,,qapps:ImportDocume nt ,,,qapps:AssociateLibraryItemReview , qapps:Dis associateLibraryItemReview qapps:Get QAppSession qapps:UpdateQAppSession qapps:GetQAppSessionMetadata qapps:UpdateQAppSessionMetadata , et les qapps:Tag Resource actions visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	27 juin 2024

Modifier	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais leselasticmapreduce:AddJobFlowSteps , elasticmapreduce:DescribeCluster elasticmapreduce:CancelSteps elasticmapreduce:DescribeStep , et les elasticmapreduce:ListSteps actions visant à soutenir la propagation d'identités fiables dans Amazon EMR.	17 mai 2024

Modifier	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les actions : <code>qapps:CreateQApp</code> <code>qapps:PredictProblemStatementFromConversation</code> <code>qapps:PredictQAppFromProblemStatement</code> <code>qapps:CopyQApp</code> <code>qapps:GetQApp</code> <code>qapps:ListQApps</code> <code>qapps:UpdateQApp</code> <code>qapps>DeleteQApp</code> <code>qapps:AssociateQAppWithUser</code> <code>qapps:DisassociateQAppFromUser</code> <code>qapps:ImportDocumentToQAppSession</code> <code>qapps:CreateLibraryItem</code> <code>qapps:GetLibraryItem</code> <code>qapps:UpdateLibraryItem</code> <code>qapps:CreateLibraryItemReview</code> <code>qapps:ListLibraryItems</code> <code>qapps:CreateSubscriptionToken</code> <code>qapps:StartQAppSession</code> <code>qapps:StopQAppSession</code> et les actions visant à prendre en charge les	30 avril 2024

Modifier	Description	Date
	sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	
AWSSSOMasterAccountAdministrator	Cette politique inclut désormais les <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> actions <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> et destinées à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024
AWSSSOMemberAccountAdministrator	Cette politique inclut désormais les <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> actions <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> et destinées à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024

Modifier	Description	Date
AWSSSOReadUniquement	Cette politique inclut désormais l' <code>signin:ListTrustedIdentityPropagationsForConsole</code> action visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais l' <code>qbusiness:PutFeedback</code> action visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	26 avril 2024

Modifier	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversation</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , et les <code>q:UpdateTroubleshootingCommandResult</code> actions visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	24 avril 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais l' <code>sts:SetContext</code> action visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	19 avril 2024

Modifier	Description	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> , <code>qbusiness:ListConversations</code> , <code>qbusiness:ListMessages</code> , et les <code>qbusiness:DeleteConversation</code> actions visant à prendre en charge les sessions de console à identité améliorée pour les applications AWS gérées qui prennent en charge ces sessions.	11 avril 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique inclut désormais les <code>s3:GetDataAccess</code> actions <code>s3:GetAccessGrants</code> <code>InstanceForPrefix</code> et.	26 novembre 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Cette politique fournit la liste des actions autorisées lorsque vous utilisez la propagation d'identité sécurisée avec des rôles assumés dans le contexte d'identité IAM Identity Center.	15 novembre 2023

Modifier	Description	Date
AWSSSODirectoryReadOnly	Cette politique inclut désormais le nouvel espace de noms <code>identitystore-auth</code> avec de nouvelles autorisations permettant aux utilisateurs de répertorier et d'obtenir des sessions.	21 février 2023
AWSSSOServiceRolePolicy	Cette politique permet désormais de UpdateSAMLProvider prendre des mesures sur le compte de gestion.	20 octobre 2022
AWSSSOMasterAccountAdministrator	Cette politique inclut désormais le nouvel espace de noms <code>identitystore-auth</code> avec de nouvelles autorisations permettant à l'administrateur de répertorier et de supprimer les sessions d'un utilisateur.	20 octobre 2022
AWSSSOMemberAccountAdministrator	Cette politique inclut désormais le nouvel espace de noms <code>identitystore-auth</code> avec de nouvelles autorisations permettant à l'administrateur de répertorier et de supprimer les sessions d'un utilisateur.	20 octobre 2022

Modifier	Description	Date
<u>AWSSSODirectoryAdministrator</u>	Cette politique inclut désormais le nouvel espace de noms <code>identitystore-auth</code> avec de nouvelles autorisations permettant à l'administrateur de répertorier et de supprimer les sessions d'un utilisateur.	20 octobre 2022
<u>AWSSSOMasterAccountAdministrator</u>	Cette politique inclut désormais de nouvelles autorisations <u>ListDelegatedAdministrators</u> d'appel AWS Organizations. Cette politique inclut également désormais un sous-ensemble d'autorisations <code>AWSSSOManageDelegatedAdministrator</code> qui inclut les autorisations d'appeler <u>RegisterDelegatedAdministrator</u> et <u>DeregisterDelegatedAdministrator</u> .	16 août 2022

Modifier	Description	Date
<u>AWSSSOMemberAccountAdministrator</u>	Cette politique inclut désormais de nouvelles autorisations <u>ListDelegatedAdministrators</u> d'appel AWS Organizations. Cette politique inclut également désormais un sous-ensemble d'autorisations <u>AWSSSOManageDelegatedAdministrator</u> qui inclut les autorisations d'appeler <u>RegisterDelegatedAdministrator</u> et <u>DeregisterDelegatedAdministrator</u> .	16 août 2022
<u>AWSSSOReadUniquement</u>	Cette politique inclut désormais de nouvelles autorisations <u>ListDelegatedAdministrators</u> d'appel AWS Organizations.	11 août 2022
<u>AWSSSOServiceRolePolicy</u>	Cette politique inclut désormais de nouvelles autorisations pour appeler <u>DeleteRolePermissionsBoundary</u> et <u>PutRolePermissionsBoundary</u> .	14 juillet 2022

Modifier	Description	Date
AWSSSOServiceRolePolicy	Cette politique inclut désormais de nouvelles autorisations qui autorisent les appels ListAWSServiceAccessForOrganization and ListDelegatedAdministrators entrants AWS Organizations.	11 mai 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSORReadUniquement	Ajoutez des autorisations IAM Access Analyzer qui permettent au principal d'utiliser les contrôles de politique à des fins de validation.	28 avril 2022
AWSSSOMasterAccountAdministrator	Cette politique autorise désormais toutes les actions du service IAM Identity Center Identity Store. Pour plus d'informations sur les actions disponibles dans le service IAM Identity Center Identity Store, consultez le document de référence de l'API IAM Identity Center Identity Store.	29 mars 2022
AWSSSOMemberAccountAdministrator	Cette politique autorise désormais toutes les actions du service IAM Identity Center Identity Store.	29 mars 2022

Modifier	Description	Date
AWSSSODirectoryAdministrateur	Cette politique autorise désormais toutes les actions du service IAM Identity Center Identity Store.	29 mars 2022
AWSSSODirectoryReadOnly	Cette politique donne désormais accès aux actions de lecture du service IAM Identity Center Identity Store. Cet accès est nécessaire pour récupérer les informations relatives aux utilisateurs et aux groupes à partir du service IAM Identity Center Identity Store.	29 mars 2022
AWSIdentitySyncFullAccess	Cette politique permet un accès complet aux autorisations de synchronisation des identités.	3 mars 2022
AWSIdentitySyncReadOnlyAccess	Cette politique accorde des autorisations en lecture seule qui permettent au principal de consulter les paramètres de synchronisation des identités.	3 mars 2022
AWSSSORReadUniquement	Cette politique accorde des autorisations en lecture seule qui permettent au principal de consulter les paramètres de configuration d'IAM Identity Center.	4 août 2021

Modifier	Description	Date
IAM Identity Center a commencé à suivre les modifications	IAM Identity Center a commencé à suivre les modifications apportées aux politiques AWS gérées.	4 août 2021

Utilisation de rôles liés à un service pour IAM Identity Center

AWS IAM Identity Center utilise des Gestion des identités et des accès AWS rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à IAM Identity Center. Il est prédéfini par IAM Identity Center et inclut toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom. Pour de plus amples informations, veuillez consulter [Comprendre les rôles liés aux services dans IAM Identity Center](#).

Un rôle lié à un service facilite la configuration d'IAM Identity Center, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. IAM Identity Center définit les autorisations associées à son rôle lié au service et, sauf indication contraire, seul IAM Identity Center peut assumer ce rôle. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, veuillez consulter [Services AWS qui fonctionnent avec IAM](#) et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour IAM Identity Center

IAM Identity Center utilise le rôle lié au service nommé AWSServiceRoleForSSO pour accorder à IAM Identity Center les autorisations nécessaires à la gestion des AWS ressources, notamment les rôles IAM, les politiques et l'IdP SAML en votre nom.

Le rôle lié au service AWSService RoleFor SSO fait confiance aux services suivants pour assumer le rôle :

- IAM Identity Center (préfixe de service :) sso

La politique d'autorisation des rôles `AWSSSOServiceRolePolicy` liés au service permet à IAM Identity Center d'effectuer les tâches suivantes concernant les rôles situés sur le chemin « `/aws-reserved/sso.amazonaws.com/` » et avec le préfixe de nom « `SSO_` » : `AWSReserved`

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePermissionsBoundary`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

La politique d'autorisation des rôles `AWSSSOServiceRolePolicy` liés au service permet à IAM Identity Center d'effectuer les opérations suivantes sur les fournisseurs SAML dont le préfixe de nom est « `_` » : `AWSSSO`

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam>DeleteSAMLProvider`

La politique d'autorisation des rôles `AWSSSOServiceRolePolicy` liés au service permet à IAM Identity Center d'effectuer les tâches suivantes pour toutes les organisations :

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

La politique d'autorisation des rôles AWSSSOService RolePolicy liés au service permet à IAM Identity Center d'effectuer les opérations suivantes pour tous les rôles IAM (*) :

- `iam:listRoles`

La politique d'autorisation des rôles AWSSSOService RolePolicy liés au service permet à IAM Identity Center d'effectuer les opérations suivantes sur « `arn:aws:iam : :* : » : role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO`

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

La politique d'autorisation des rôles AWSSSOService RolePolicy liés au service permet à IAM Identity Center d'effectuer les opérations suivantes sur « `arn:aws:identity-sync : *:*:profile/*` » :

- `identity-sync:DeleteSyncProfile`

Pour plus d'informations sur les mises à jour de la politique d'autorisation des rôles AWSSSOService RolePolicy liés à un service, consultez. [Mises à jour des politiques AWS gérées par IAM Identity Center](#)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMRoleProvisioningActions",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam>DeleteRolePermissionsBoundary",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy"
      ],
    },
  ],
}
```



```

    "Resource": [
      "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "IAMRoleReadActions",
    "Effect": "Allow",
    "Action": [
      "iam:GetRole",
      "iam:ListRoles"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "IAMRoleCleanupActions",
    "Effect": "Allow",
    "Action": [
      "iam:DeleteRole",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:ListRolePolicies",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource": [
      "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
    ]
  },
  {
    "Sid": "IAMSLRCleanupActions",
    "Effect": "Allow",
    "Action": [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus",
      "iam:DeleteRole",
      "iam:GetRole"
    ],
    "Resource": [

```

```

        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
    ],
    {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
            "iam:CreateSAMLProvider"
        ],
        "Resource": [
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
            }
        }
    },
    {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
            "iam:UpdateSAMLProvider"
        ],
        "Resource": [
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
    },
    {
        "Sid": "IAMSAMLProviderCleanupActions",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteSAMLProvider",
            "iam:GetSAMLProvider"
        ],
        "Resource": [
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "organizations:DescribeAccount",

```

```

        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowUnauthAppForDirectory",
    "Effect": "Allow",
    "Action": [
        "ds:UnauthorizeApplication"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDescribeForDirectory",
    "Effect": "Allow",
    "Action": [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDescribeAndListOperationsOnIdentitySource",
    "Effect": "Allow",
    "Action": [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
    ],
    "Resource": [
        "*"
    ]
},
{

```

```
    "Sid": "AllowDeleteSyncProfile",
    "Effect": "Allow",
    "Action": [
        "identity-sync:DeleteSyncProfile"
    ],
    "Resource": [
        "arn:aws:identity-sync:*:*:profile/*"
    ]
  }
]
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour IAM Identity Center

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Une fois activé, IAM Identity Center crée un rôle lié à un service dans tous les comptes de l'organisation dans Organizations. AWS IAM Identity Center crée également le même rôle lié au service dans chaque compte ajouté ultérieurement à votre organisation. Ce rôle permet à IAM Identity Center d'accéder aux ressources de chaque compte en votre nom.

Remarques

- Si vous êtes connecté au compte de AWS Organizations gestion, celui-ci utilise votre rôle actuellement connecté et non le rôle lié au service. Cela empêche l'escalade des privilèges.
- Lorsque IAM Identity Center effectue des opérations IAM dans le compte de AWS Organizations gestion, toutes les opérations sont effectuées à l'aide des informations d'identification du principal IAM. Cela permet aux connexions de CloudTrail savoir qui a effectué tous les changements de privilèges dans le compte de gestion.

 Important

Si vous utilisiez le service IAM Identity Center avant le 7 décembre 2017, date à laquelle il a commencé à prendre en charge les rôles liés au service, IAM Identity Center a créé le rôle `AWSService RoleFor SSO` dans votre compte. Pour plus d'informations, consultez [A New Role Appeared in My IAM Account](#) (Un nouveau rôle est apparu dans mon compte IAM).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour le recréer dans votre compte.

Modification d'un rôle lié à un service pour IAM Identity Center

IAM Identity Center ne vous permet pas de modifier le rôle lié au service `AWSService RoleFor SSO`. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour IAM Identity Center

Il n'est pas nécessaire de supprimer manuellement le rôle `AWSService RoleFor SSO`. Lorsqu'un Compte AWS est supprimé d'une AWS organisation, IAM Identity Center nettoie automatiquement les ressources et en supprime le rôle lié au service. Compte AWS

Vous pouvez également utiliser la console IAM, la CLI IAM ou l'API IAM pour supprimer manuellement le rôle lié à un service. Pour ce faire, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle manuellement.

 Note

Si le service IAM Identity Center utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources IAM Identity Center utilisées par le SSO `AWSService RoleFor`

1. [Supprimer l'accès des utilisateurs et des groupes à un Compte AWS](#) pour tous les utilisateurs et groupes ayant accès au Compte AWS.

2. [Supprimer des ensembles d'autorisations dans IAM Identity Center](#) que vous avez associé au Compte AWS.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, la CLI IAM ou l'API IAM pour supprimer le rôle lié au service AWS Service Role For SSO. Pour en savoir plus, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Autorisation de la console et de l'API IAM Identity Center

La console IAM Identity Center existante APIs prend en charge la double autorisation, ce qui vous permet de continuer à utiliser les opérations d'API existantes lorsque de nouvelles APIs sont disponibles. Si vous possédez des instances d'IAM Identity Center créées avant le 15 novembre 2023 et le 15 octobre 2020, vous pouvez utiliser les tableaux suivants pour déterminer quelles opérations d'API correspondent désormais aux opérations d'API plus récentes publiées après ces dates.

Rubriques

- [Actions relatives à l'API après novembre 2023](#)
- [Actions de l'API après octobre 2020](#)

Actions relatives à l'API après novembre 2023

Les instances d'IAM Identity Center créées avant le 15 novembre 2023 honorent à la fois les anciennes et les nouvelles actions d'API, à condition qu'aucune de ces actions ne soit explicitement refusée. Les instances créées après le 15 novembre 2023 utilisent des [actions d'API plus récentes](#) pour l'autorisation dans la console IAM Identity Center.

Nom du fonctionnement de la console utilisé avant le 15 novembre 2023	Action API utilisée après le 15 novembre 2023
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance CreateApplicationInstance	CreateApplication

Nom du fonctionnement de la console utilisé avant le 15 novembre 2023	Action API utilisée après le 15 novembre 2023
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData UpdateApplicationInstanceStatus UpdateManagedApplicationInstanceStatus	UpdateApplication

Actions de l'API après octobre 2020

Les instances d'IAM Identity Center créées avant le 15 octobre 2020 honorent à la fois les anciennes et les nouvelles actions d'API, à condition qu'aucune de ces actions ne soit explicitement refusée. Les instances créées après le 15 octobre 2020 utilisent des [actions d'API plus récentes](#) pour l'autorisation dans la console IAM Identity Center.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWSAccount	DeleteApplicationInstance DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAWSAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile CreateProfile UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust CreateTrust UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS clés contextuelles de condition pour IAM Identity Center

Lorsqu'un [principal](#) fait une [demande](#) à AWS, AWS rassemble les informations de la demande dans un contexte de demande, qui est utilisé pour évaluer et autoriser la demande. Vous pouvez utiliser l'élément Condition d'une politique JSON pour comparer des clés dans le contexte de demande avec les valeurs de clé spécifiées dans votre politique. Les informations relatives à la demande sont fournies par différentes sources, notamment le principal auteur de la demande, la ressource, la demande pour laquelle elle est faite et les métadonnées relatives à la demande elle-même. Les clés de condition spécifiques au service sont définies pour être utilisées avec un service individuel AWS .

IAM Identity Center inclut un fournisseur de AWS STS contexte qui permet aux applications AWS gérées et aux applications tierces d'ajouter des valeurs aux clés de condition définies par IAM

Identity Center. Ces clés sont incluses dans les [rôles IAM](#). Les valeurs clés sont définies lorsqu'une application transmet un jeton à AWS STS. L'application obtient le jeton auquel elle passe de AWS STS l'une des manières suivantes :

- Lors de l'authentification auprès d'IAM Identity Center.
- Après échange de jetons avec un [émetteur de jetons de confiance](#) pour une propagation d'identité fiable. Dans ce cas, l'application obtient un jeton auprès d'un émetteur de jetons fiable et échange ce jeton contre un jeton auprès d'IAM Identity Center.

Ces clés sont généralement utilisées par les applications qui s'intègrent à la propagation d'identité sécurisée. Dans certains cas, lorsque des valeurs clés sont présentes, vous pouvez utiliser ces clés dans les politiques IAM que vous créez pour autoriser ou refuser des autorisations.

Par exemple, vous souhaitez peut-être fournir un accès conditionnel à une ressource en fonction de la valeur de `UserId`. Cette valeur indique quel utilisateur IAM Identity Center utilise le rôle. L'exemple est similaire à l'utilisation de `SourceId`. Contrairement à `SourceId` ce qui se passe, la valeur pour `UserId` représente un utilisateur spécifique vérifié dans le magasin d'identités. Cette valeur est présente dans le jeton que l'application obtient puis transmet. AWS STS Il ne s'agit pas d'une chaîne à usage général qui peut contenir des valeurs arbitraires.

Rubriques

- [boutique d'identité : UserId](#)
- [boutique d'identité : IdentityStoreArn](#)
- [centre d'identité : ApplicationArn](#)
- [centre d'identité : CredentialId](#)
- [centre d'identité : InstanceArn](#)

boutique d'identité : UserId

Cette clé de contexte est celle `UserId` de l'utilisateur IAM Identity Center qui fait l'objet de l'assertion de contexte émise par IAM Identity Center. L'assertion de contexte est transmise à AWS STS. Vous pouvez utiliser cette clé pour comparer l'identifiant `UserId` de l'utilisateur IAM Identity Center au nom duquel la demande est faite avec l'identifiant de l'utilisateur que vous spécifiez dans la politique.

- Disponibilité : cette clé est incluse dans le contexte de la demande après la définition d'une assertion de contexte émise par IAM Identity Center, lorsqu'un rôle est assumé à l'aide d'une AWS

STS `assume-role` commande quelconque dans le cadre de l'opération AWS CLI ou de l' AWS STS `AssumeRoleAPI`.

- Types de données – [Chaîne](#)
- Type de valeur – À valeur unique

boutique d'identité : `IdentityStoreArn`

Cette clé de contexte est l'ARN de la banque d'identités attachée à l'instance d'IAM Identity Center qui a émis l'assertion de contexte. C'est également le magasin d'identité dans lequel vous pouvez rechercher des attributs `identitystore:UserID`. Vous pouvez utiliser cette clé dans les politiques pour déterminer si elle `identitystore:UserID` provient d'un ARN de magasin d'identités attendu.

- Disponibilité : cette clé est incluse dans le contexte de la demande après la définition d'une assertion de contexte émise par IAM Identity Center, lorsqu'un rôle est assumé à l'aide d'une AWS STS `assume-role` commande quelconque dans le cadre de l'opération AWS CLI ou de l' AWS STS `AssumeRoleAPI`.
- Type de données : [Arn](#), [String](#)
- Type de valeur – À valeur unique

centre d'identité : `ApplicationArn`

Cette clé de contexte est l'ARN de l'application à laquelle IAM Identity Center a émis une assertion de contexte. Vous pouvez utiliser cette clé dans les politiques pour déterminer si elle `identitycenter:ApplicationArn` provient d'une application attendue. L'utilisation de cette clé permet d'empêcher une application inattendue d'accéder à un rôle IAM.

- Disponibilité — Cette clé est incluse dans le contexte de demande d'une opération d' AWS STS `AssumeRoleAPI`. Le contexte de demande inclut une assertion de contexte émise par IAM Identity Center.
- Type de données : [Arn](#), [String](#)
- Type de valeur – À valeur unique

centre d'identité : CredentialId

Cette clé de contexte est un identifiant aléatoire pour les informations d'identification du rôle à identité améliorée et est utilisée uniquement pour la journalisation. Cette valeur clé étant imprévisible, nous vous recommandons de ne pas l'utiliser pour les assertions contextuelles dans les politiques.

- Disponibilité — Cette clé est incluse dans le contexte de demande d'une opération d' AWS STS AssumeRoleAPI. Le contexte de demande inclut une assertion de contexte émise par IAM Identity Center.
- Types de données – [Chaîne](#)
- Type de valeur – À valeur unique

centre d'identité : InstanceArn

Cette clé de contexte est l'ARN de l'instance d'IAM Identity Center qui a émis l'assertion de contexte pour. `identitystore:UserID` Vous pouvez utiliser cette clé pour déterminer si l'assertion de contexte `identitystore:UserID` et provient d'un ARN d'instance IAM Identity Center attendu.

- Disponibilité — Cette clé est incluse dans le contexte de demande d'une opération d' AWS STS AssumeRoleAPI. Le contexte de demande inclut une assertion de contexte émise par IAM Identity Center.
- Type de données : [Arn](#), [String](#)
- Type de valeur – À valeur unique

Journalisation et surveillance dans IAM Identity Center

Une bonne pratique consiste à surveiller votre organisation pour vous assurer que les modifications sont enregistrées. La surveillance vous permet de vous assurer que vous pouvez enquêter sur tout changement inattendu et annuler les modifications indésirables. IAM Identity Center prend actuellement en charge deux AWS services qui vous aident à surveiller votre organisation et les activités qui s'y déroulent : AWS CloudTrail et Amazon EventBridge.

Rubriques

- [Journalisation des appels d'API IAM Identity Center avec AWS CloudTrail](#)
- [Journalisation des appels d'API SCIM d'IAM Identity Center avec AWS CloudTrail](#)
- [Connect les composants de l'application à Amazon EventBridge](#)

- [Enregistrement des erreurs de synchronisation AD configurables](#)

Journalisation des appels d'API IAM Identity Center avec AWS CloudTrail

AWS IAM Identity Center est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans IAM Identity Center. CloudTrail capture les appels d'API pour IAM Identity Center sous forme d'événements. Les appels capturés incluent des appels provenant de la console IAM Identity Center et des appels de code vers les opérations de l'API IAM Identity Center. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour IAM Identity Center. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à IAM Identity Center, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Le tableau suivant récapitule les CloudTrail événements d'IAM Identity Center, leurs sources d' CloudTrail événements et leurs correspondances. APIs Reportez-vous aux [références de l'API IAM Identity Center](#) pour en savoir plus sur le APIs.

Note

Il existe un groupe supplémentaire d' CloudTrail événements, appelé Sign-in, qui est émis lorsque vous AWS vous connectez en AWS tant qu'utilisateur d'IAM Identity Center. Ces événements n'ont aucun public APIs correspondant et ne sont donc pas répertoriés dans les références d'API.

CloudTrail événement s	Publique APIs	Description	CloudTrail sources d'événements
IAM Identity Center	IAM Identity Center	L'IAM Identity Center APIs permet de gérer les ensembles d'autorisations, les	sso . amazo naws . com

CloudTrail événements	Publique APIs	Description	CloudTrail sources d'événements
		applications, les émetteurs de jetons fiables, les attributions de comptes et d'applications, les instances du IAM Identity Center et les balises.	
Boutique d'identités	Boutique d'identités	L'Identity Store APIs permet de gérer le cycle de vie des utilisateurs et des groupes de votre personnel, ainsi que les adhésions aux groupes d'utilisateurs. Ils prennent également en charge la gestion des appareils MFA des utilisateurs.	sso-directory.amazonaws.com, identitystore.amazonaws.com
OIDC	OIDC	L'OIDC APIs prend en charge la propagation fiable des identités et la connexion aux boîtes à AWS CLI outils IDE en tant qu'utilisateur IAM Identity Center déjà authentifié.	sso.amazonaws.com, sso-oauth.amazonaws.com

CloudTrail événements	Publique APIs	Description	CloudTrail sources d'événements
AWS portail d'accès	AWS portail d'accès	Le portail AWS d'accès APIs prend en charge les opérations du portail d' AWS accès et les utilisateurs obtiennent les informations d'identification de leur compte via le AWS CLI.	sso.amazonaws.com
SCIM	SCIM	Le SCIM APIs prend en charge le provisionnement des utilisateurs, des groupes et des adhésions à des groupes via le protocole SCIM. Pour plus d'informations, consultez Journalisation des appels d'API SCIM d'IAM Identity Center avec AWS CloudTrail .	identitystore-scim.amazonaws.com
Connexion à AWS	Aucune API publique	AWS émet des CloudTrail événements de connexion pour l'authentification des utilisateurs et les flux de fédération dans IAM Identity Center.	signin.amazonaws.com

Rubriques

- [CloudTrail cas d'utilisation d'IAM Identity Center](#)
- [Informations sur le centre d'identité IAM dans CloudTrail](#)

CloudTrail cas d'utilisation d'IAM Identity Center

Les CloudTrail événements émis par IAM Identity Center peuvent être utiles dans de nombreux cas d'utilisation. Organisations peuvent utiliser ces journaux d'événements pour surveiller et auditer l'accès et l'activité des utilisateurs dans leur AWS environnement. Cela peut faciliter les cas d'utilisation liés à la conformité, car les journaux enregistrent des informations sur qui accède à quelles ressources et à quel moment. Vous pouvez également utiliser les CloudTrail données pour enquêter sur les incidents, ce qui permet aux équipes d'analyser les actions des utilisateurs et de suivre les comportements suspects. En outre, l'historique des événements peut faciliter les efforts de dépannage, en fournissant une visibilité sur les modifications apportées aux autorisations et aux configurations des utilisateurs au fil du temps.

Les sections suivantes décrivent les principaux cas d'utilisation qui éclairent vos flux de travail, tels que l'audit, l'investigation des incidents et le dépannage.

Identification de l'utilisateur dans les événements initiés par CloudTrail l'utilisateur d'IAM Identity Center

IAM Identity Center émet deux CloudTrail champs qui vous permettent d'identifier l'utilisateur IAM Identity Center à l'origine des CloudTrail événements, tels que la connexion à IAM Identity Center ou l'utilisation du portail d' AWS accès AWS CLI, y compris la gestion des appareils MFA :

- `userId`— L'identifiant utilisateur unique et immuable issu de l'Identity Store d'une instance IAM Identity Center.
- `identityStoreArn`— Le nom de ressource Amazon (ARN) de l'Identity Store qui contient l'utilisateur.

Les `identityStoreArn` champs `userId` et s'affichent dans l'`onBehalfOf` élément imbriqué dans l'`userIdentity` élément, comme illustré dans l'exemple de journal des CloudTrail événements suivant. Ce journal des événements affiche ces deux champs sur un événement dont le `userIdentity` type est « `IdentityCenterUser` ». Vous pouvez également trouver ces champs sur les événements destinés aux utilisateurs authentifiés de l'IAM Identity Center dont le `userIdentity` type est « `Unknown` ». Vos flux de travail doivent accepter les deux valeurs de type.


```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

Tip

Nous vous recommandons d'utiliser `userId` et `identityStoreArn` pour identifier l'utilisateur à l'origine des CloudTrail événements IAM Identity Center. Les principaux champs `userName` et situés sous l'`userIdentity` élément ne sont plus disponibles. Si vos flux de travail, tels que l'audit ou la réponse aux incidents, dépendent de l'accès au `username`, deux options s'offrent à vous :

- Récupérez le nom d'utilisateur dans le répertoire IAM Identity Center comme expliqué dans [Nom d'utilisateur lors des événements de connexion CloudTrail](#).
- Obtenez le code `UserName` émis par IAM Identity Center sous l'`additionalEventData` élément dans Sign-in. Cette option ne nécessite pas d'accès au répertoire IAM Identity Center. Pour de plus amples informations, veuillez consulter [Nom d'utilisateur lors des événements de connexion CloudTrail](#).

Pour récupérer les informations d'un utilisateur, y compris le `username` champ, vous interrogez l'Identity Store avec l'ID utilisateur et l'Identity Store ID comme paramètres. Vous pouvez effectuer cette action par le biais de la demande d'[DescribeUser](#) API ou de la CLI. Voici un exemple de commande CLI. Vous pouvez omettre le `region` paramètre si votre instance IAM Identity Center se trouve dans la région par défaut de la CLI.

```
aws identitystore describe-user \
--identity-store-id d-1234567890 \
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

Pour déterminer la valeur Identity Store ID pour la commande CLI dans l'exemple précédent, vous pouvez extraire l'ID Identity Store de cette `identityStoreArn` valeur. Dans l'exemple d'`ARNarn:aws:identitystore::111122223333:identitystore/d-1234567890`, l'ID du magasin d'identités est `d-1234567890`. Vous pouvez également trouver l'identifiant Identity Store en accédant à l'onglet Identity Store dans la section Paramètres de la console IAM Identity Center.

Si vous automatisez la recherche d'utilisateurs dans le répertoire IAM Identity Center, nous vous recommandons d'estimer la fréquence des recherches d'utilisateurs et de prendre en compte la [limite de limitation du IAM Identity Center sur l'API Identity Store](#). La mise en cache des attributs utilisateur récupérés peut vous aider à rester dans les limites autorisées.

Corrélation des événements utilisateur au sein d'une même session utilisateur

Le `AuthWorkflowID` champ émis dans les événements de connexion permet de suivre tous les CloudTrail événements associés à une séquence de connexion avant le début d'une session utilisateur IAM Identity Center.

Pour les actions de l'utilisateur dans le portail d' AWS accès, la `credentialId` valeur est définie sur l'ID de la session de l'utilisateur IAM Identity Center utilisée pour demander l'action. Vous pouvez utiliser cette valeur pour identifier les CloudTrail événements initiés au cours de la même session utilisateur authentifiée IAM Identity Center sur le portail d' AWS accès.

Note

Vous ne pouvez pas l'utiliser `credentialId` pour corréler les événements de connexion aux événements suivants, tels que l'utilisation du portail d' AWS accès. La valeur du `credentialId` champ émis lors des événements de connexion est destinée à un usage interne, et nous vous recommandons de ne pas vous y fier. La valeur du `credentialId` champ émis pour les [événements du portail AWS d'accès](#) invoqués avec OIDC est égale à l'ID du jeton d'accès.

Identification des détails de la session d'arrière-plan de l'utilisateur dans les événements initiés par l'utilisateur CloudTrail d'IAM Identity Center

L' CloudTrail événement suivant capture le processus d'échange de jetons OAuth 2.0, au cours duquel un jeton d'accès existant (`accessToken`) qui représente la session interactive de l'utilisateur est échangé contre un jeton d'actualisation (`refreshToken`). Le jeton

d'actualisation permet aux tâches de longue durée initiées par un utilisateur de continuer à s'exécuter avec les autorisations de l'utilisateur, même après sa déconnexion.

Pour les [sessions d'arrière-plan des utilisateurs d'IAM Identity Center](#), l' CloudTrail événement inclut un élément supplémentaire appelé `resource` dans l'`requestParameters` élément. Le `resource` paramètre contient l'Amazon Resource Name (ARN) de la tâche exécutée en arrière-plan. Cet élément est présent uniquement dans les enregistrements d' CloudTrail événements et n'est pas inclus dans les réponses de l'API IAM ou du SDK [CreateTokenWithIAM](#) Identity Center.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

Corrélation des utilisateurs entre IAM Identity Center et les annuaires externes

IAM Identity Center fournit deux attributs utilisateur que vous pouvez utiliser pour corréler un utilisateur dans son annuaire avec le même utilisateur dans un annuaire externe (par exemple, Microsoft Active Directory et Okta Universal Directory).

- `externalId`— L'identifiant externe d'un utilisateur de l'IAM Identity Center. Nous vous recommandons de mapper cet identifiant à un identifiant utilisateur immuable dans le répertoire externe. Notez qu'IAM Identity Center n'émet pas cette valeur dans CloudTrail.
- `username`— Une valeur fournie par le client avec laquelle les utilisateurs se connectent généralement. La valeur peut changer (par exemple, lors d'une mise à jour du SCIM). Notez que lorsque la source d'identité est Directory Service, le nom d'utilisateur émis par IAM Identity Center CloudTrail correspond au nom d'utilisateur que vous entrez pour vous authentifier. Il n'est pas nécessaire que le nom d'utilisateur corresponde exactement au nom d'utilisateur figurant dans le répertoire IAM Identity Center.

Si vous avez accès aux CloudTrail événements mais pas au répertoire IAM Identity Center, vous pouvez utiliser le nom d'utilisateur émis sous l'`additionalEventData` élément lors de la

connexion. Pour plus de détails sur le nom d'utilisateur dans `additionalEventData`, reportez-vous à [Nom d'utilisateur lors des événements de connexion CloudTrail](#).

Le mappage de ces deux attributs utilisateur aux attributs utilisateur correspondants dans un annuaire externe est défini dans IAM Identity Center lorsque la source d'identité est le Directory Service. Pour plus d'informations, voir. [Mappages d'attributs entre le centre d'identité IAM et le répertoire des fournisseurs d'identité externes](#) Les utilisateurs externes IdPs qui fournissent du SCIM disposent de leur propre mappage. Même si vous utilisez le répertoire IAM Identity Center comme source d'identité, vous pouvez utiliser `externalId` attribut pour croiser les principes de sécurité avec votre répertoire externe.

La section suivante explique comment rechercher un utilisateur IAM Identity Center à partir de ses identifiants `username` et `externalId`.

Affichage d'un utilisateur IAM Identity Center par nom d'utilisateur et ID externe

Vous pouvez récupérer les attributs utilisateur d'un nom d'utilisateur connu dans le répertoire IAM Identity Center en demandant d'abord un correspondant à `userId` l'aide de la demande d'[GetUserId](#) API, puis en émettant une demande d'[DescribeUser](#) API, comme indiqué dans l'exemple précédent. L'exemple suivant montre comment vous pouvez récupérer un nom `userId` d'utilisateur spécifique dans l'Identity Store. Vous pouvez omettre le `region` paramètre si votre instance IAM Identity Center se trouve dans la région par défaut avec la CLI.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifiant '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

De même, vous pouvez utiliser le même mécanisme lorsque vous connaissez le `externalId`. Dans l'exemple précédent, mettez à jour le chemin de l'attribut avec la `externalId` valeur, et la valeur de l'attribut avec le nom spécifique `externalId` que vous recherchez.

Afficher l'identifiant sécurisé (SID) d'un utilisateur dans Microsoft Active Directory (AD) et ExternalID

Dans certains cas, IAM Identity Center émet le SID d'un utilisateur dans le `principalId` champ des CloudTrail événements, tels que ceux émis par le portail AWS d'accès et l'OIDC APIs. Ces cas sont progressivement supprimés. Nous recommandons à vos flux de travail d'utiliser l'attribut AD `objectguid` lorsque vous avez besoin d'un identifiant utilisateur unique de la part d'AD. Vous pouvez trouver cette valeur dans l'`externalId`attribut du répertoire IAM Identity Center. Toutefois, si vos flux de travail nécessitent l'utilisation du SID, récupérez la valeur auprès d'AD car elle n'est pas disponible via IAM Identity Center APIs.

[Corrélation des événements utilisateur au sein d'une même session utilisateur](#) décrit comment vous pouvez utiliser les `username` champs `externalId` et pour corréler un utilisateur IAM Identity Center à un utilisateur correspondant dans un annuaire externe. Par défaut, IAM Identity Center est mappé `externalId` à l'`objectguid`attribut dans AD, et ce mappage est corrigé. IAM Identity Center offre aux administrateurs la flexibilité de mapper `username` différemment de son mappage par défaut `userprincipalname` dans AD.

Vous pouvez consulter ces mappages dans la console IAM Identity Center. Accédez à l'onglet Source d'identité des paramètres, puis choisissez Gérer la synchronisation dans le menu Actions. Dans la section Gérer la synchronisation, cliquez sur le bouton Afficher les mappages d'attributs.

Bien que vous puissiez utiliser n'importe quel identifiant utilisateur AD unique disponible dans IAM Identity Center pour rechercher un utilisateur dans AD, nous vous recommandons de l'utiliser `objectguid` dans vos requêtes car il s'agit d'un identifiant immuable. L'exemple suivant montre comment interroger Microsoft AD avec Powershell pour récupérer un utilisateur à l'aide de la `objectguid` valeur utilisateur de `16809ecc-7225-4c20-ad98-30094aefdbca`. Une réponse réussie à cette requête inclut le SID de l'utilisateur.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell
```

```
Get-ADUser `
-Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
-Properties *
```

Informations sur le centre d'identité IAM dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans IAM Identity Center, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour

plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

 Note

Pour plus d'informations sur l'évolution de l'identification des utilisateurs et du suivi des actions des utilisateurs lors d' CloudTrail événements, reportez-vous à la section [Modifications importantes apportées aux CloudTrail événements pour IAM Identity Center](#) dans le blog sur la AWS sécurité.

Pour un enregistrement continu des événements survenus dans votre entreprise Compte AWS, y compris ceux relatifs à IAM Identity Center, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrail Guide de l'utilisateur :

- [Présentation de la création d'un journal d'activité](#)
- [CloudTrail services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Lorsque la CloudTrail journalisation est activée dans vos actions Compte AWS, les appels d'API effectués aux actions d'IAM Identity Center sont suivis dans des fichiers journaux. Les enregistrements IAM Identity Center sont écrits avec les autres enregistrements AWS de service dans un fichier journal. CloudTrail détermine à quel moment créer et écrire dans un nouveau fichier en fonction d'une période et de la taille du fichier.

CloudTrail événements pour le centre d'identité IAM pris en charge APIs

Les sections suivantes fournissent des informations sur les CloudTrail événements associés aux éléments suivants APIs pris en charge par IAM Identity Center :

- [API du centre d'identité IAM](#)
- [API Identity Store](#)
- [API OIDC](#)
- [AWS API du portail d'accès](#)
- [API SCIM](#)

CloudTrail événements liés aux opérations de l'API IAM Identity Center

La liste suivante contient les CloudTrail événements que les opérations publiques d'IAM Identity Center émettent avec la source `sso.amazonaws.com` d'événements. Pour plus d'informations sur les opérations de l'API IAM Identity Center publique, consultez le document de référence de l'[API IAM Identity Center](#).

Vous trouverez peut-être des événements supplémentaires dans CloudTrail les opérations d'API de la console IAM Identity Center sur lesquelles repose la console. Pour plus d'informations sur ces consoles APIs, consultez la [référence d'autorisation de service](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)

- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)
- [DeleteInlinePolicyFromPermissionSet](#)
- [DeleteInstance](#)
- [DeleteInstanceAccessControlAttributeConfiguration](#)
- [DeletePermissionsBoundaryFromPermissionSet](#)
- [DeletePermissionSet](#)
- [DeleteTrustedTokenIssuer](#)
- [DescribeAccountAssignmentCreationStatuss](#)
- [DescribeAccountAssignmentDeletionStatus](#)
- [DescribeApplication](#)
- [DescribeApplicationAssignment](#)
-

[DescribeApplicationProvider](#)

-

[DescribeInstance](#)

-

[DescribeInstanceAccessControlAttributeConfiguration](#)

-

[DescribePermissionSet](#)

-

[DescribePermissionSetProvisioningStatus](#)

-

[DescribeTrustedTokenIssuer](#)

-

[DetachCustomerManagedPolicyReferenceFromPermissionSet](#)

-

[DetachManagedPolicyFromPermissionSet](#)

-

[GetApplicationAccessScope](#)

-

[GetApplicationAssignmentConfiguration](#)

-

[GetApplicationAuthenticationMethod](#)

-

[GetApplicationGrant](#)

-

[GetInlinePolicyForPermissionSet](#)

-

[GetPermissionsBoundaryForPermissionSet](#)

-

[ListAccountAssignmentCreationStatus](#)

-

-

[ListAccountAssignmentDeletionStatus](#)

-

[ListAccountAssignments](#)

- [ListAccountAssignmentsForPrincipal](#)
- [ListAccountsForProvisionedPermissionSet](#)
- [ListApplicationAccessScopes](#)
- [ListApplicationAssignments](#)
- [ListApplicationAssignmentsForPrincipal](#)
- [ListApplicationAuthenticationMethods](#)
- [ListApplicationGrants](#)
- [ListApplicationProviders](#)
- [ListApplications](#)
- [ListCustomerManagedPolicyReferencesInPermissionSet](#)
- [ListInstances](#)
- [ListManagedPoliciesInPermissionSet](#)
- [ListPermissionSetProvisioningStatus](#)
- [ListPermissionSets](#)
-

[ListPermissionSetsProvisionedToAccount](#)

-

[ListTagsForResource](#)

-

[ListTrustedTokenIssuers](#)

-

[ProvisionPermissionSet](#)

-

[PutApplicationAccessScope](#)

-

[PutApplicationAssignmentConfiguration](#)

-

[PutApplicationAuthenticationMethod](#)

-

[PutApplicationGrant](#)

-

[PutInlinePolicyToPermissionSet](#)

-

[PutPermissionsBoundaryToPermissionSet](#)

-

[TagResource](#)

-

[UntagResource](#)

-

[UpdateApplication](#)

-

[UpdateInstance](#)

-

[UpdateInstanceAccessControlAttributeConfiguration](#)

-

[UpdatePermissionSet](#)

-

[UpdateTrustedTokenIssuer](#)

CloudTrail événements liés aux opérations de l'API Identity Store

La liste suivante contient les CloudTrail événements que les opérations publiques d'Identity Store émettent avec la source de `identitystore.amazonaws.com` événement. Pour plus d'informations sur les opérations de l'API publique Identity Store, consultez le manuel [Identity Store API Reference](#).

Vous trouverez peut-être des événements supplémentaires dans CloudTrail les opérations de l'API de la console Identity Store avec la source de `sso-directory.amazonaws.com` événement. Ils APIs prennent en charge la console et le portail AWS d'accès. Si vous devez détecter l'occurrence d'une opération particulière, telle que l'ajout d'un membre à un groupe, nous vous recommandons de prendre en compte les opérations d'API publiques et de console. Pour plus d'informations sur ces consoles APIs, consultez la [référence d'autorisation de service](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)

- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

CloudTrail événements liés aux opérations de l'API OIDC

La liste suivante contient les CloudTrail événements émis par les opérations publiques de l'OIDC. Pour plus d'informations sur les opérations de l'API OIDC publique, consultez le Guide de référence des [API OIDC](#).

- [CreateToken](#)(source de l'événementsso.amazonaws.com)
- [CreateTokenWithIAM](#)(source de l'événementsso-oauth.amazonaws.com)

CloudTrail événements liés aux opérations de AWS l'API du portail d'accès

La liste suivante contient les CloudTrail événements que les opérations de l'API du portail d' AWS accès émettent avec la source d'sso.amazonaws.comévénements. Les opérations d'API signalées comme étant indisponibles dans l'API publique prennent en charge les opérations du portail AWS d'accès. L'utilisation de AWS CLI peut entraîner l'émission d' CloudTrail événements liés à la fois aux opérations de l'API du portail d' AWS accès public et à celles qui ne sont pas disponibles dans l'API publique. Pour plus d'informations sur les opérations de l'API du portail AWS d'accès public, consultez le document de [référence de l'API du portail d'AWS accès](#).

- Authenticate(Non disponible dans l'API publique. Fournit un identifiant au portail AWS d'accès.)
- Federate(Non disponible dans l'API publique. Fournit une fédération dans les applications.)
- [ListAccountRoles](#)
- [ListAccounts](#)
- ListApplications(Non disponible dans l'API publique. Fournit les ressources assignées aux utilisateurs à afficher sur le portail AWS d'accès.)
- ListProfilesForApplication(Non disponible dans l'API publique. Fournit les métadonnées de l'application à afficher sur le portail AWS d'accès.)
- [GetRoleCredentials](#)
- [Logout](#)

CloudTrail événements liés aux opérations de l'API SCIM

Pour plus d'informations sur les opérations de l'API SCIM publique, consultez la [référence de l'API du portail d'AWS accès](#).

Informations d'identité dans les événements de l'IAM Identity Center CloudTrail

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou de l'utilisateur Gestion des identités et des accès AWS (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.
- Si la demande a été faite par un utilisateur de l'IAM Identity Center. Si tel est le cas, `identityStoreArn` les champs `userId` et sont disponibles dans les CloudTrail événements pour identifier l'utilisateur IAM Identity Center à l'origine de la demande. Pour de plus amples informations, veuillez consulter [Identification de l'utilisateur dans les événements initiés par CloudTrail l'utilisateur d'IAM Identity Center](#).

Pour de plus amples informations, veuillez consulter l'[élément userIdentity CloudTrail](#) .

Note

Actuellement, IAM Identity Center n'émet pas d' CloudTrail événements pour la connexion des utilisateurs à des applications Web AWS gérées (par exemple, Amazon SageMaker AI Studio) avec l'API [OIDC](#). Ces applications Web constituent un sous-ensemble d'un ensemble plus large [the section called "AWS applications gérées"](#), qui inclut également des applications non Web telles qu'Amazon Athena SQL et Amazon S3 Access Grants.

Comprendre CloudTrail les événements pour IAM Identity Center

Un journal de suivi est une configuration qui permet la transmission d'événements à un compartiment Amazon S3 que vous spécifiez. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les événements ne sont pas une trace ordonnée des

appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique. Pour en savoir plus sur le [contenu d'un CloudTrail enregistrement](#), consultez le guide de CloudTrail l'utilisateur.

Cet exemple illustre une entrée de CloudTrail journal capturant une `DescribePermissionsPolicies` action effectuée par un utilisateur IAM (samadams) interagissant avec IAM Identity Center :

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIIJM2K4example",
        "userName": "samadams"
      },
      "eventTime": "2017-11-29T22:39:43Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "DescribePermissionsPolicies",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "permissionSetId": "ps-79a0dde74b95ed05"
      },
      "responseElements": null,
      "requestID": "319ac6a1-d556-11e7-a34f-69a333106015",
      "eventID": "a93a952b-13dd-4ae5-a156-d3ad6220b071",
      "readOnly": true,
      "resources": [

    ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Cet exemple illustre une entrée de CloudTrail journal capturant une `ListApplications` action effectuée par un utilisateur d'IAM Identity Center sur le portail d' AWS accès :

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "eventTime": "2017-11-29T18:48:28Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "ListApplications",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
      "eventID": "e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Cet exemple illustre une entrée de CloudTrail journal capturant une `CreateToken` action effectuée par un utilisateur d'IAM Identity Center s'authentifiant auprès du service IAM Identity Center OIDC :

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
```



```

        "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
        "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
},
"eventTime": "2020-06-16T01:31:15Z",
"eventSource": "sso.amazonaws.com",
"eventName": "CreateToken",
"awsRegion": "us-east-1",
"sourceIPAddress": "203.0.113.0",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
"requestParameters": {
    "clientId": "clientid1234example",
    "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "grantType": "urn:ietf:params:oauth:grant-type:device_code",
    "deviceCode": "devicecode1234example"
},
"responseElements": {
    "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "tokenType": "Bearer",
    "expiresIn": 28800,
    "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
"readOnly": false,
"resources": [
    {
        "accountId": "111122223333",
        "type": "IdentityStoreId",
        "ARN": "d-1234567890"
    }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

Comprendre les événements de connexion à IAM Identity Center

AWS CloudTrail enregistre les événements de connexion réussis et infructueux pour toutes les sources d'identité IAM Identity Center. Les identités sourcées par IAM Identity Center et Active

Directory (AD Connector et AWS Managed Microsoft AD) incluent des événements de connexion supplémentaires qui sont capturés chaque fois qu'un utilisateur est invité à résoudre un problème ou un facteur d'identification spécifique, en plus du statut de cette demande de vérification d'identification en particulier. Ce n'est qu'une fois qu'un utilisateur a terminé tous les tests d'identification requis qu'il sera connecté, ce qui entraînera l'enregistrement d'un `UserAuthentication` événement.

Le tableau suivant présente les noms de chacun des CloudTrail événements de connexion à IAM Identity Center, leur objectif et leur applicabilité aux différentes sources d'identité.

Nom de l'événement	But de l'événement	Applicabilité de la source d'identité
<code>CredentialChallenge</code>	Utilisé pour indiquer qu'IAM Identity Center a demandé à l'utilisateur de résoudre un problème d'identification spécifique et indique <code>CredentialType</code> ce qui était requis (par exemple, <code>PASSWORD</code> ou <code>TOTP</code>).	Utilisateurs natifs d'IAM Identity Center, AD Connector et AWS Managed Microsoft AD
<code>CredentialVerification</code>	Utilisé pour indiquer que l'utilisateur a tenté de résoudre une <code>CredentialChallenge</code> demande spécifique et indique si cet identifiant a réussi ou échoué.	Utilisateurs natifs d'IAM Identity Center, AD Connector et AWS Managed Microsoft AD
<code>UserAuthentication</code>	Utilisé pour indiquer que toutes les exigences d'authentification auxquelles l'utilisateur a été confronté ont été satisfaites avec succès et que l'utilisateur s'est connecté avec succès. Si les utilisateurs ne parviennent pas à relever les défis d'identification requis, aucun <i>UserAuth</i>	Toutes les sources d'identité

Nom de l'événement	But de l'événement	Applicabilité de la source d'identité

ntication événement ne sera enregistré.

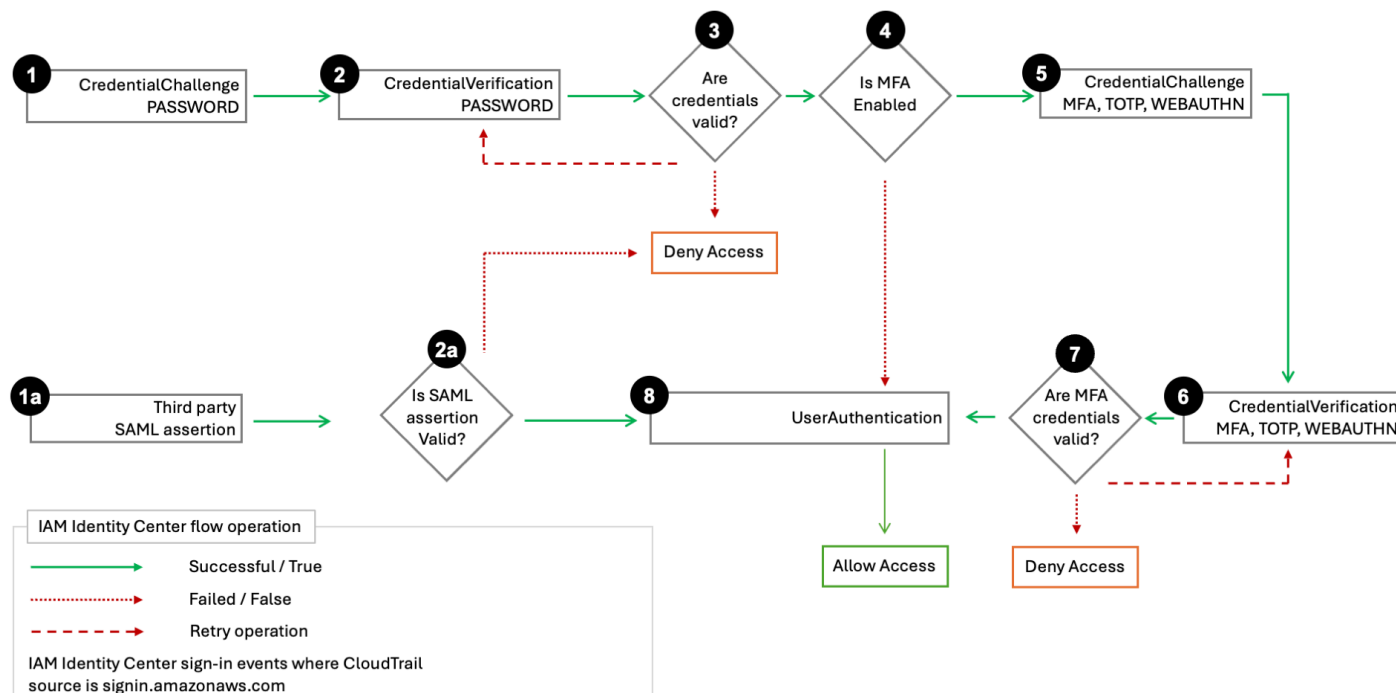
Le tableau suivant présente d'autres champs de données d'événements utiles contenus dans des CloudTrail événements de connexion spécifiques.

Champ	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
AuthWorkflowID	Utilisé pour corréler tous les événements émis sur l'ensemble d'une séquence de connexion. Pour chaque connexion utilisateur, plusieurs événements peuvent être émis par IAM Identity Center.	CredentialChallenge, CredentialVerification, UserAuthentication	« AuthWorkflowIdentifiant » : « 9de74b32-8362-4a01-a524-de21df59fd83 »
CredentialType	Utilisé pour spécifier l'identifiant ou le facteur contesté. UserAuthentication les événements incluront toutes les CredentialType valeurs qui ont été vérifiées avec succès tout au long de la séquence de	CredentialChallenge, CredentialVerification, UserAuthentication	CredentialType« : « PASSWORD » ou "CredentialType« : « PASSWORD, TOTP » (les valeurs possibles incluent : PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)

Champ	But de l'événement	Applicabilité dans un événement de connexion	Exemples de valeur
	connexion de l'utilisateur.		
DeviceEnrollmentRequired	Utilisé pour spécifier que l'utilisateur devait enregistrer un dispositif MFA lors de la connexion et qu'il a correctement répondu à cette demande.	UserAuthentication	DeviceEnrollmentRequired« : « vrai »
LoginTo	Utilisé pour spécifier l'emplacement de la redirection après une séquence de connexion réussie.	UserAuthentication	"LoginTo": "https://mydirectory.awsapps.com/start/....."

CloudTrail événements dans les flux de connexion à l'IAM Identity Center

Le schéma suivant décrit le flux de connexion et les CloudTrail événements émis par la connexion.



Le schéma montre un flux de connexion par mot de passe et un flux de connexion fédéré.

Le flux de connexion par mot de passe, qui comprend les étapes 1 à 8, illustre les étapes du processus de connexion par nom d'utilisateur et mot de passe. IAM Identity Center passe `userIdentity.additionalEventData.CredentialType` à `PASSWORD` « », et IAM Identity Center suit le cycle de question-réponse aux informations d'identification, en réessayant si nécessaire.

Le nombre d'étapes dépend du type de [connexion et de la présence de l'authentification multifactorielle \(MFA\)](#). Le processus initial entraîne trois ou cinq CloudTrail événements mettant `UserAuthentication` fin à la séquence pour une authentification réussie. Les tentatives infructueuses d'authentification par mot de passe entraînent CloudTrail des événements supplémentaires lorsque le IAM Identity Center réémet `CredentialChallenge` une authentification normale ou, si elle est activée, une authentification MFA.

Le flux de connexion par mot de passe couvre également le scénario dans lequel un utilisateur IAM Identity Center nouvellement créé grâce à un appel d'`CreateUserAPI` se connecte avec un mot de passe à usage unique (OTP). Le type d'identifiant dans ce scénario est « `EMAIL_OTP` ».

Le flux de connexion fédérée, composé des étapes 1a, 2a et 8, illustre les principales étapes du processus d'authentification fédérée au cours desquelles une [assertion SAML est fournie par un fournisseur d'identité, validée par](#) IAM Identity Center et, en cas de réussite, aboutit à. UserAuthentication IAM Identity Center n'invoque pas la séquence d'authentification MFA interne aux étapes 3 à 7, car un fournisseur d'identité fédéré externe est responsable de toutes les authentifications d'identification des utilisateurs.

Nom d'utilisateur lors des événements de connexion CloudTrail

IAM Identity Center émet le `UserName` champ situé sous l'`additionalEventData` élément une fois par connexion réussie d'un utilisateur d'IAM Identity Center. La liste suivante décrit les deux événements de connexion concernés et les conditions dans lesquelles ces événements se produisent. Une seule des conditions peut être vraie lorsqu'un utilisateur se connecte.

- `CredentialChallenge`
 - Quand `CredentialType` est « `PASSWORD` » — s'applique à l'authentification par mot de passe avec Directory Service ou Répertoire IAM Identity Center.
 - Quand `CredentialType` est « `EMAIL_OTP` » : s'applique uniquement Répertoire IAM Identity Center lorsqu'un utilisateur créé à l'aide d'un appel d'`CreateUserAPI` tente de se connecter pour la première fois et qu'il reçoit un mot de passe à usage unique pour se connecter une fois avec ce mot de passe.
- `UserAuthentication`
 - Quand `CredentialType` est « `EXTERNAL_IDP` » — s'applique à l'authentification avec un IdP externe.

La valeur de `UserName` pour les authentifications réussies est la suivante :

- Lorsque la source d'identité est un IdP externe, la valeur est égale à la valeur de l'`nameID` assertion SAML entrante. Cette valeur est égale au `UserName` champ du Répertoire IAM Identity Center.
- Lorsque la source d'identité est un Répertoire IAM Identity Center, la valeur émise est égale au `UserName` champ de ce répertoire.
- Lorsque la source d'identité est le Directory Service, la valeur émise est égale au nom d'utilisateur saisi par l'utilisateur lors de l'authentification. Par exemple, un utilisateur qui possède le nom d'utilisateur `anyuser@company.com` peut s'authentifier avec `anyuseranyuser@company.com`, `oucompany.com/anyuser`, et dans chaque cas, la valeur saisie est émise CloudTrail respectivement.

Masquage de sécurité en cas de tentatives de nom d'utilisateur incorrectes

Le `UserName` champ contient la chaîne `HIDDEN_DUE_TO_SECURITY_REASONS` lorsque l'événement enregistré est un échec de connexion à la console dû à une saisie incorrecte du nom d'utilisateur. CloudTrail n'enregistre pas le contenu dans ce cas car le texte peut contenir des informations sensibles, comme décrit dans les exemples suivants :

- Un utilisateur tape par erreur un mot de passe dans le champ de nom d'utilisateur.
- Un utilisateur tape accidentellement le nom d'un compte de messagerie personnelle, un identifiant de connexion bancaire ou un autre ID privé.

Tip

Nous vous recommandons d'utiliser `userId` et `identityStoreArn` pour identifier l'utilisateur à l'origine des CloudTrail événements IAM Identity Center. Si vous devez utiliser le `userName` champ, vous pouvez utiliser l'`additionalEventData` élément `userName` under `the` qui est émis une fois par connexion réussie.

Pour plus d'informations sur la façon dont vous pouvez utiliser le `UserName` champ, reportez-vous à [Corrélation des événements utilisateur au sein d'une même session utilisateur](#).

Exemples d'événements pour les scénarios de connexion à IAM Identity Center

Les exemples suivants illustrent les séquences d' CloudTrail événements typiques générées lors de différents scénarios de AWS connexion. Ces exemples servent de modèles de référence pour vous aider à interpréter les journaux d'authentification, à identifier les problèmes de sécurité et à vérifier que vos politiques d'authentification fonctionnent correctement.

Rubriques

- [Connexion réussie lors de l'authentification par mot de passe uniquement](#)
- [Connexion réussie lors de l'authentification auprès d'un fournisseur d'identité externe](#)
- [Connexion réussie lors de l'authentification à l'aide d'un mot de passe et d'une application d'authentification par mot de passe à usage unique basé sur le temps \(TOTP\)](#)
- [Une connexion réussie est requise lorsque vous vous authentifiez avec un mot de passe et que l'enregistrement MFA est obligatoire](#)
- [Échec de connexion en raison d'une authentification par mot de passe incorrecte](#)

Connexion réussie lors de l'authentification par mot de passe uniquement

La séquence d'événements suivante présente un exemple de connexion réussie uniquement par mot de passe.

CredentialChallenge (Mot de passe)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71",
  "eventTime": "2020-12-07T20:33:58Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "UserName": "bobsmith@example.com",
    "CredentialType": "PASSWORD"
  },
  "requestID": "5be44ffb-6946-4f47-acaf-1adebd4afead",
  "eventID": "27ea7725-c1fd-4355-bdba-d0e628e0e604",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```



```
}
```

Succès CredentialVerification (mot de passe)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-07T20:34:09Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "CredentialType": "PASSWORD"
  },
  "requestID": "f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
  "eventID": "c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialVerification": "Success"
  }
}
```

UserAuthentication Réussite (mot de passe uniquement)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-07T20:34:09Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "LoginTo": "https://d-1234567890.awsapps.com/start/?state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBsh1Ic50BAA6ftz73M6LsflWDlf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-east-1",
    "CredentialType": "PASSWORD"
  },
  "requestID": "f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
  "eventID": "e959a95a-2b33-478d-906c-4fe303e8a9f1",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "UserAuthentication": "Success"
  }
}
```

}

Connexion réussie lors de l'authentification auprès d'un fournisseur d'identité externe

La séquence d'événements suivante présente un exemple de connexion réussie lors d'une authentification via le protocole SAML à l'aide d'un fournisseur d'identité externe.

UserAuthentication Succès (fournisseur d'identité externe)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-07T20:34:09Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "LoginTo": "https://d-1234567890.awsapps.com/start/?state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIic50BAA6ftz73M6LsfLWD1f0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-east-1",
    "CredentialType": "EXTERNAL_IDP",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
}
```

```

    "eventID": "e959a95a-2b33-478d-906c-4fe303e8a9f1",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
      "UserAuthentication": "Success"
    }
  }
}

```

Connexion réussie lors de l'authentification à l'aide d'un mot de passe et d'une application d'authentification par mot de passe à usage unique basé sur le temps (TOTP)

La séquence d'événements suivante illustre un exemple où une authentification multifactorielle était requise lors de la connexion et où l'utilisateur s'est connecté avec succès à l'aide d'un mot de passe et d'une application d'authentification TOTP.

CredentialChallenge (Mot de passe)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-08T20:40:13Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
}

```

```

"additionalEventData":{
  "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
  "CredentialType":"PASSWORD",
  "UserName":"bobsmith@example.com"
},
"requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
"eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

Succès CredentialVerification (mot de passe)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:20Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{

```

```

    "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
    "CredentialType": "PASSWORD"
  },
  "requestID": "92c4ac90-0d9b-452d-95d5-728487612f5e",
  "eventID": "4533fd49-6669-4d0b-b272-a0b2139309a8",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialVerification": "Success"
  }
}

```

CredentialChallenge (TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
},
  "eventTime": "2020-12-08T20:40:20Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
    "CredentialType": "TOTP"
  }
}

```

```

},
"requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
"eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

Succès CredentialVerification (TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:27Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
    "CredentialType":"TOTP"
  },
  "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",

```

```

"eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialVerification":"Success"
}
}

```

UserAuthentication Réussi (mot de passe + TOTP)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-08T20:40:27Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
    "LoginTo": "https://d-1234567890.awsapps.com/start/?state\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS\u0026auth_code\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFf00108qc3RFSx-pjBXXG_jUcvBk_UILdGytV4o1u97h42B-
```



```
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNmlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
  "CredentialType": "PASSWORD, TOTP"
},
"requestID": "c40a691f-eeb1-4352-b286-5e909f96f318",
"eventID": "7a8c8725-db2f-488d-a43e-788dc6c73a4a",
"readOnly": false,
"eventType": "AwsServiceEvent",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333",
"serviceEventDetails": {
  "UserAuthentication": "Success"
}
}
```

Une connexion réussie est requise lorsque vous vous authentifiez avec un mot de passe et que l'enregistrement MFA est obligatoire

La séquence d'événements suivante illustre une authentification par mot de passe réussie où l'utilisateur devait s'enregistrer et réussir l'authentification multifactorielle (MFA) avant de finaliser son processus de connexion.

CredentialChallenge (Mot de passe)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-09T01:24:02Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",

```

```

"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
  "CredentialType":"PASSWORD",
  "UserName":"bobsmith@example.com"
},
"requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
"eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

Succès CredentialVerification (mot de passe)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-09T01:24:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",

```

```

    "sourceIPAddress":"203.0.113.0",
    "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters":null,
    "responseElements":null,
    "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
    },
    "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
    "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
      "CredentialVerification":"Success"
    }
  }
}

```

UserAuthentication Réussite (mot de passe et enregistrement MFA requis)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-09T01:24:14Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",

```

```

    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
        "LoginTo": "https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHyz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiQuYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbt175y8vAmwZhAqrggrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
        "CredentialType": "PASSWORD",
        "DeviceEnrollmentRequired": "true"
    },
    "requestID": "74d24604-a365-4237-8c4a-350795494b92",
    "eventID": "a15bf257-7f37-46c0-b67c-fea5fa6166be",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "UserAuthentication": "Success"
    }
}

```

Échec de connexion en raison d'une authentification par mot de passe incorrecte

La séquence d'événements suivante illustre une tentative d'authentification au cours de laquelle l'utilisateur a correctement saisi son nom d'utilisateur mais a échoué à l'étape de vérification du mot de passe, ce qui a entraîné un échec de connexion.

CredentialChallenge (Mot de passe)

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "arn": "",
        "accountId": "111122223333",

```

```

    "accessKeyId": "",
  },
  "eventTime": "2020-12-08T18:56:15Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "adbf67c4-8188-4e2b-8527-fe539e328fa7",
    "CredentialType": "PASSWORD",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
  "eventID": "d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}

```

Echec CredentialVerification (mot de passe)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
  },
  "eventTime": "2020-12-08T18:56:21Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",

```

```
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
  "CredentialType":"PASSWORD"
},
"requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
"eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialVerification":"Failure"
}
}
```

Journalisation des appels d'API SCIM d'IAM Identity Center avec AWS CloudTrail

[IAM Identity Center SCIM](#) est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un. Service AWS CloudTrail capture les appels d'API pour SCIM sous forme d'événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer les informations concernant l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Note

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Toutefois, vous devrez peut-être faire pivoter votre jeton d'accès pour voir les événements du SCIM, si votre jeton a été créé avant septembre 2024.

Pour de plus amples informations, veuillez consulter [Faire pivoter un jeton d'accès](#).

SCIM prend en charge la journalisation des opérations suivantes sous forme d'événements dans CloudTrail :

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroup](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

Exemples d' CloudTrail événements

Les exemples suivants illustrent les journaux d' CloudTrail événements typiques générés lors des opérations SCIM avec IAM Identity Center. Ces exemples présentent la structure et le contenu des événements nécessaires à la réussite des opérations ainsi que les scénarios d'erreur courants. Ils vous aident à comprendre comment interpréter les CloudTrail journaux lors de la résolution des problèmes de provisionnement SCIM.

CreateUserOpération réussie

Cet CloudTrail événement indique une `CreateUser` opération réussie réalisée via l'API SCIM. L'événement capture à la fois les paramètres de la demande (les informations sensibles étant masquées) et les éléments de réponse, y compris le nouvel identifiant de l'utilisateur. Ce type d'événement est généré lorsqu'un fournisseur d'identité fournit avec succès un nouvel utilisateur à IAM Identity Center à l'aide du protocole SCIM.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
```

```

    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "requestID": "xxxx",

```



```

"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Échec **PatchGroup** de l'opération : attribut de chemin requis manquant

Cet CloudTrail événement indique PatchGroup l'échec d'une opération qui a entraîné ValidationException un message d'erreur "Missing path in PATCH request". L'erreur s'est produite parce que l'PATCH opération nécessite un attribut de chemin pour spécifier l'attribut de groupe à modifier, mais cet attribut était absent de la demande.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ]
    },
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  }
}

```

```

    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Échec de **CreateGroup** l'opération : le nom du groupe existe déjà

Cet CloudTrail événement indique CreateGroup l'échec d'une opération qui a entraîné `ConflictException` un message d'erreur "Duplicate GroupDisplayName". Cette erreur se produit lors de la tentative de création d'un groupe dont le nom d'affichage existe déjà dans IAM Identity Center. Le fournisseur d'identité doit utiliser un nom de groupe unique ou mettre à jour le groupe existant au lieu d'en créer un nouveau.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {

```

```

    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Échec de **PatchUser** l'opération : plusieurs adresses e-mail ne sont pas prises en charge

Cet CloudTrail événement indique PatchUser l'échec d'une opération qui a entraîné ValidationException un message d'erreur "List attribute emails exceeds allowed limit of 1". Cette erreur se produit lorsque vous essayez d'attribuer plusieurs adresses e-mail à un utilisateur, car IAM Identity Center ne prend en charge qu'une seule adresse e-mail par utilisateur. Le fournisseur d'identité doit configurer le mappage SCIM pour n'envoyer qu'une seule adresse e-mail pour chaque utilisateur.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {

```

```

    "operations": [
      {
        "op": "REPLACE",
        "path": "emails",
        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Erreurs courantes de validation de l'API SCIM dans IAM Identity Center

Les messages d'erreur de validation suivants apparaissent généralement lors d' CloudTrail événements liés à l'utilisation de l'API SCIM avec IAM Identity Center. Ces erreurs de validation se produisent généralement lors des opérations de provisionnement des utilisateurs et des groupes.

[Pour obtenir des conseils détaillés sur la résolution de ces erreurs et la configuration correcte du provisionnement SCIM, consultez cet AWS re:Post article.](#)

- L'adresse e-mail associée à l'attribut de liste dépasse la limite autorisée de 1
- Limite autorisée de 1 pour les adresses attributaires de la liste
- 1 erreur de validation détectée : la valeur de « *Name.FamilyName* » n'a pas satisfait la contrainte : le membre doit satisfaire le modèle d'expression régulière : `[ \ p {L} \ \ p {M} \ \ p {S} \ \ p {N} \ \ p {P} \ \ t \ \ n \ \ r] +`

- 2 erreurs de validation détectées : la valeur de « Name.FamilyName » n'a pas satisfait la contrainte : la longueur du membre doit être supérieure ou égale à 1 ; la valeur de « Name.FamilyName » n'a pas satisfait la contrainte : le membre doit satisfaire le modèle d'expression régulière : `[\\ p {L} \\ \\ p {P} \\ t \\ n \\ r] +`
- 2 erreurs de validation détectées : la valeur dans 'urn:IETF:params:scim:schemas:Extension:Enterprise:2.0:User.Manager.value' n'a pas satisfait la contrainte : le membre doit avoir une longueur supérieure ou égale à 1 ; la valeur dans 'urn:IETF:params:SCIM:Schemas:Extension:Enterprise:2.0:User.Manager.Value' n'a pas satisfait la contrainte : le membre doit satisfaire le modèle d'expression régulière : `[\\ p {L} \\ \\ p {M} \\ \\ p {S} \\ \\ p {N} \\ \\ p {P} \\ t \\ n \\ r] +` »,
- JSON non valide provenant de RequestBody
- Format de filtre non valide

Connect les composants de l'application à Amazon EventBridge

Vous pouvez intégrer IAM Identity Center EventBridge à [Amazon](#) pour déclencher des événements qui déclenchent des notifications administratives ou invoquent des flux de travail automatisés en réponse à des actions spécifiques d'IAM Identity Center enregistrées lors CloudTrail d'événements.

Par exemple, vous pouvez configurer des [EventBridge règles](#) pour détecter lorsqu'un utilisateur supprime une application ou lorsqu'IAM Identity Center crée un nouveau groupe. [En fonction de votre cas d'utilisation, vous pouvez rediriger ces événements vers une rubrique Amazon SNS pour avertir les administrateurs ou invoquer une automatisation supplémentaire à l'aide AWS Lambda de Step Functions ou d'autres EventBridge services pris en charge.](#)

Enregistrement des erreurs de synchronisation AD configurables

Vous pouvez activer la journalisation sur vos configurations de synchronisation Active Directory (AD) configurables pour recevoir des journaux contenant des informations sur les erreurs susceptibles de se produire pendant le processus de synchronisation. Grâce à ces journaux, vous pouvez vérifier s'il existe un problème avec votre synchronisation AD configurable et prendre des mesures le cas échéant. Vous pouvez envoyer vos journaux vers un groupe de CloudWatch journaux Amazon Logs, un bucket Amazon Simple Storage Service (Amazon S3) ou un Amazon Data Firehose dont la livraison entre comptes est prise en charge pour les buckets Amazon S3 et Firehose.

Pour plus d'informations sur les limitations, les autorisations et les journaux vendus, consultez la section [Activation de la journalisation à partir de Services AWS](#).

 Note

La connexion vous est facturée. Pour plus d'informations, consultez [Vended Logs](#) sur la page de [CloudWatch tarification d'Amazon](#).

Pour activer les journaux d'erreurs configurables de synchronisation AD

1. Connectez-vous à la [console IAM Identity Center](#).
2. Cliquez sur Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer les journaux.
4. Choisissez Ajouter la livraison du journal et l'un des types de destination suivants.
 - a. Choisissez To Amazon CloudWatch Logs. Choisissez ou entrez ensuite le groupe de journaux de destination.
 - b. Choisissez To Amazon S3. Choisissez ou entrez ensuite le compartiment de destination.
 - c. Choisissez To Firehose. Choisissez ou entrez ensuite le flux de diffusion de destination.
5. Sélectionnez Soumettre.

Pour désactiver les journaux d'erreurs configurables de synchronisation AD

1. Connectez-vous à la [console IAM Identity Center](#).
2. Cliquez sur Paramètres.
3. Sur la page Paramètres, choisissez l'onglet Source d'identité, sélectionnez Actions, puis sélectionnez Gérer les journaux.
4. Choisissez Supprimer pour la destination que vous souhaitez supprimer.
5. Sélectionnez Soumettre.

Champs du journal des erreurs de synchronisation AD configurables

Consultez la liste suivante pour connaître les éventuels champs du journal des erreurs.

`sync_profile_name`

Nom du profil de synchronisation.

error_code

Le code d'erreur qui représente le type d'erreur qui s'est produit.

error_message

Message contenant des informations détaillées sur l'erreur survenue.

sync_source

La source de synchronisation est l'endroit à partir duquel les entités sont synchronisées. Pour IAM Identity Center, il s'agit d'un Active Directory (AD) géré par Directory Service. La source de synchronisation contient le domaine et l'ARN du répertoire concerné.

sync_target

La cible de synchronisation est la destination où les entités sont enregistrées. Pour IAM Identity Center, il s'agit d'un magasin d'identités. La cible de synchronisation contient l'ARN du magasin d'identités concerné.

source_entity_id

Identifiant unique de l'entité à l'origine de l'erreur. Pour IAM Identity Center, il s'agit du SID de l'entité.

source_entity_type

Type d'entité à l'origine de l'erreur. La valeur peut être USER ou GROUP.

eventTimestamp

Horodatage auquel l'erreur s'est produite.

Exemples de journaux d'erreurs configurables de synchronisation AD

Exemple 1 : journal des erreurs pour un mot de passe expiré pour un annuaire AD

```
{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "InvalidDirectoryCredentials",
    "error_message": "The password for your AD directory has expired. Please reset the password to allow Identity Sync to access the directory."
  }
}
```

```

    },
    "sync_source": {
      "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
      "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
  }
}

```

Exemple 2 : journal des erreurs pour un utilisateur dont le nom d'utilisateur n'est pas unique

```

{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "ConflictError",
    "error_message": "The source entity has a username conflict with the sync target. Please verify that the source identity has a unique username in the target."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "sync_target": {
    "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
  },
  "source_entity_id": "SID-1234",
  "source_entity_type": "USER",
  "eventTimestamp": "1683355579981"
}

```

Validation de conformité pour IAM Identity Center

Services AWS Des auditeurs tiers évaluent leur sécurité et leur conformité dans AWS IAM Identity Center le cadre de multiples programmes de AWS conformité.

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez [AWS la documentation de sécurité](#).

Normes de conformité prises en charge

IAM Identity Center a fait l'objet d'un audit selon les normes suivantes et peut être utilisé dans le cadre de solutions pour lesquelles vous devez obtenir une certification de conformité.



AWS a étendu son programme de conformité à la loi HIPAA (Health Insurance Portability and Accountability Act) pour inclure IAM Identity Center en tant que service éligible à la loi [HIPAA](#).

AWS propose un [livre blanc axé sur la loi HIPAA](#) aux clients qui souhaitent en savoir plus sur la manière dont ils peuvent traiter et stocker les informations Services AWS de santé. Pour plus d'informations, consultez [HIPAA compliance](#) (français non garanti).



Le programme d'évaluateurs enregistrés en matière de sécurité de l'information (IRAP) permet aux clients du gouvernement australien de s'assurer que des contrôles de conformité appropriés sont en place et de déterminer le modèle de responsabilité approprié pour répondre aux exigences du manuel de sécurité des informations (ISM) du gouvernement australien produit par le Centre australien de cybersécurité (ACSC). Pour plus d'informations, consultez les [ressources de l'IRAP](#).



IAM Identity Center dispose d'une attestation de conformité à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) version 3.2 au niveau 1 des fournisseurs de services.

Les clients qui utilisent AWS des produits et services pour stocker, traiter ou transmettre les données des titulaires

de cartes peuvent utiliser les sources d'identité suivantes dans IAM Identity Center pour gérer leur propre certification de conformité à la norme PCI DSS :

- Active Directory
- Fournisseur d'identité externe

La source d'identité IAM Identity Center n'est actuellement pas conforme à la norme PCI DSS.

Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section [PCI DSS niveau 1](#).



Les rapports de contrôle du système et de l'organisation (SOC) sont des rapports d'examen indépendants réalisés par des tiers qui montrent comment IAM Identity Center atteint les principaux contrôles et objectifs de conformité. Ces rapports vous aident, ainsi que vos auditeurs, à comprendre comment les contrôles soutiennent les opérations et la conformité. Il existe trois types de rapports SOC :

- AWS Rapport SOC 1 - [Télécharger avec AWS Artifacts](#)
- AWS SOC 2 : Rapport sur la sécurité, la disponibilité et la confidentialité - [Télécharger avec AWS Artifacts](#)
- [AWS SOC 3 : Rapport sur la sécurité, la disponibilité et la confidentialité](#)

IAM Identity Center est concerné par les rapports AWS SOC 1, SOC 2 et SOC 3. Pour plus d'informations, consultez [Conformité SOC](#).

Résilience dans IAM Identity Center

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Pour en savoir plus sur AWS IAM Identity Center la résilience, voir [Conception de la résilience et comportement régional](#).

Sécurité de l'infrastructure dans IAM Identity Center

En tant que service géré, AWS IAM Identity Center il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à IAM Identity Center via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Protection des données dans IAM Identity Center

Le [modèle de responsabilité AWS partagée](#) s'applique à la protection des données dans AWS IAM Identity Center. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale qui gère l'ensemble du AWS cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) relatives à la confidentialité des données](#). Pour plus d'informations sur la protection des données en Europe, consultez l'article intitulé [AWS Shared Responsibility Model and GDPR](#) sur le blog sur la sécurité .

Nous vous recommandons de sécuriser vos données de la manière suivante :

- Utilisez l'authentification multifactorielle (MFA) avec IAM Identity Center.
- Utilisez le protocole TLS pour communiquer avec les AWS ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libres tels que le champ Nom. Cela inclut lorsque vous travaillez avec ou avec AWS IAM Identity Center d'autres AWS services à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans les balises ou les champs de texte libre utilisés pour les noms peuvent être utilisées pour les journaux de diagnostic.

Chiffrement en transit

IAM Identity Center protège les données en transit, lorsqu'elles sont acheminées vers et depuis le service, en chiffrant automatiquement toutes les données interréseaux à l'aide du protocole de chiffrement TLS (Transport Layer Security) 1.2 ou TLS 1.3. Les demandes HTTPS directes

authentifiées par IAM et envoyées à l'IAM Identity Center APIs, à l'API Identity Store ou à l'API OIDC sont signées à l'aide de l'[algorithme AWS Signature Version 4](#) pour établir une connexion sécurisée.

Confidentialité des données

Avec IAM Identity Center, vous gardez le contrôle des données de votre entreprise. Vos identités d'utilisateur et de groupe stockées dans IAM Identity Center ne sont partagées avec d'autres AWS services tels que les [applications AWS gérées](#) que si vous les activez avec IAM Identity Center et si ces services en ont besoin.

Pour plus d'informations, consultez la [FAQ sur la confidentialité AWS des données](#).

Conservation des données

IAM Identity Center stocke vos données, telles que les identités des utilisateurs et des groupes, ainsi que les métadonnées, jusqu'à ce que vous les supprimiez du service. Lorsque vous supprimez une instance d'IAM Identity Center, les données qu'elle contient sont également supprimées.

Chiffrement au repos

IAM Identity Center fournit un chiffrement pour protéger les données clients inactives à l'aide des types de clés suivants :

- Clés détenues par AWS (type de clé par défaut) — IAM Identity Center utilise ces clés par défaut pour chiffrer automatiquement vos données. Vous ne pouvez pas consulter, gérer, auditer leur utilisation ou utiliser les clés AWS détenues à d'autres fins. IAM Identity Center gère entièrement la gestion des clés afin de garantir la sécurité de vos données, sans que vous ayez à prendre aucune mesure. Pour plus d'informations, consultez [Clés détenues par AWS](#) dans le [Guide du développeur AWS Key Management Service](#).
- Clés gérées par le client : dans les instances organisationnelles d'IAM Identity Center, vous pouvez choisir une clé symétrique gérée par le client pour le chiffrement du reste des données d'identité de votre personnel, telles que les attributs des utilisateurs et des groupes. Vous créez, détenez et gérez ces clés de chiffrement. Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :
 - Établir et maintenir des politiques clés pour restreindre l'accès à la clé aux seuls responsables IAM qui en ont besoin, tels que IAM Identity Center et [AWS applications gérées](#) ses administrateurs AWS Organizations.

- Établir et maintenir des politiques IAM pour l'accès à la clé, y compris l'accès entre comptes
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Audit de l'accès à vos données nécessitant un accès par clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Pour savoir comment implémenter une clé KMS gérée par le client dans IAM Identity Center, consultez [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#). Pour plus d'informations sur les clés gérées par le client, consultez la section [clé gérée par le client](#) dans le Guide du AWS Key Management Service développeur.

 Note

IAM Identity Center active automatiquement le chiffrement au repos à l'aide de clés KMS AWS détenues afin de protéger gratuitement les données des clients. Toutefois, AWS KMS des frais s'appliquent lors de l'utilisation d'une clé gérée par le client. Pour plus d'informations sur les tarifs, consultez les [AWS Key Management Service tarifs](#).

Considérations relatives à la mise en œuvre de clés gérées par le client :

- Clés dédiées : nous recommandons de créer une nouvelle clé KMS dédiée gérée par le client pour chaque instance d'IAM Identity Center plutôt que de réutiliser une clé existante. Cette approche permet une séparation plus claire des tâches, simplifie la gestion du contrôle d'accès et simplifie l'audit de sécurité. Le fait de disposer d'une clé dédiée réduit également les risques en limitant l'impact des modifications clés sur une seule instance IAM Identity Center.
- Utilisation d'IAM Identity Center sur plusieurs instances Régions AWS : si vous prévoyez de répliquer votre instance IAM Identity Center sur une instance supplémentaire Régions AWS, vous devrez utiliser une clé KMS gérée par le client pour le chiffrement au repos. Le type de clé KMS AWS détenue par défaut n'est pas pris en charge dans un centre d'identité IAM multirégional. Pour de plus amples informations, veuillez consulter [Utilisation d'IAM Identity Center sur plusieurs Régions AWS](#).

 Note

IAM Identity Center utilise le [chiffrement d'enveloppe](#) pour chiffrer les données d'identité de votre personnel. Votre clé KMS joue le rôle d'une clé d'encapsulation qui chiffre la clé de données réellement utilisée pour chiffrer les données.

Pour plus d'informations sur AWS KMS, voir [Qu'est-ce que le service de gestion des AWS clés ?](#)

Contexte de chiffrement IAM Identity Center

Un [contexte de chiffrement](#) est un ensemble facultatif de paires clé-valeur non secrètes qui contiennent des informations contextuelles supplémentaires sur les données. AWS KMS utilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande. Reportez-vous au [guide du AWS KMS développeur](#) pour plus d'informations sur le contexte de chiffrement.

IAM Identity Center utilise les clés de contexte de chiffrement suivantes : `aws:sso:instance-arn`, `aws:identitystore:identitystore-arn` et `tenant-key-id`. Par exemple, le contexte de chiffrement suivant peut apparaître dans les opérations d' AWS KMS API invoquées par l'[API IAM Identity Center](#).

```
"encryptionContext": {
  "tenant-key-id": "ssoins-1234567890abcdef",
  "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

Le contexte de chiffrement suivant peut apparaître dans les opérations AWS KMS d'API invoquées par l'[API Identity Store](#).

```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
    "arn:aws:identitystore:::123456789012:identitystore/d-1234567890"
}
```


Contrôle de l'accès à votre clé gérée par le client à l'aide du contexte de chiffrement

Vous pouvez utiliser le contexte de chiffrement dans les stratégies de clé et les politiques IAM en tant que conditions pour contrôler l'accès à votre clé symétrique gérée par le client. Certains des principaux modèles de politique [Déclarations de politique clés avancées de KMS](#) inclus incluent de telles conditions pour garantir que la clé est utilisée uniquement avec une instance IAM Identity Center spécifique.

Surveillance de vos clés de chiffrement pour IAM Identity Center

Lorsque vous utilisez une clé KMS gérée par le client avec votre instance IAM Identity Center, vous pouvez utiliser [AWS CloudTrailAmazon CloudWatch Logs](#) pour suivre les demandes auxquelles IAM Identity Center envoie. AWS KMS Les opérations d'API KMS appelées par IAM Identity Center sont répertoriées dans [Étape 2 : Préparation des déclarations de politique clés de KMS](#). CloudTrail les événements relatifs à ces opérations d'API contiennent le contexte de chiffrement, qui vous permet de surveiller les opérations d' AWS KMS API appelées par votre instance IAM Identity Center pour accéder aux données chiffrées par votre clé gérée par le client.

Exemple de contexte de chiffrement dans le CloudTrail cas d'une opération d' AWS KMS API :

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxxxx"
    }
  }
}
```

AWS stockage, chiffrement et suppression des attributs d'identité d'IAM Identity Center dans les applications gérées

Certaines applications AWS gérées que vous déployez AWS IAM Identity Center, telles que AWS Systems Manager et Amazon CodeCatalyst, stockent des attributs d'utilisateur et de groupe spécifiques provenant d'IAM Identity Center dans leur propre banque de données. Le chiffrement au repos avec une clé KMS gérée par le client dans IAM Identity Center ne s'étend pas aux attributs d'utilisateur et de groupe IAM Identity Center stockés dans les applications AWS gérées. AWS les

applications gérées prennent en charge différentes méthodes de chiffrement pour les données qu'elles stockent. Enfin, lorsque vous supprimez des attributs d'utilisateur et de groupe dans IAM Identity Center, ces applications AWS gérées peuvent continuer à stocker ces informations après leur suppression dans IAM Identity Center. Reportez-vous au guide de l'utilisateur de vos applications AWS gérées pour connaître le chiffrement et la sécurité des données stockées dans les applications.

Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center

Les clés gérées par le client sont AWS des clés du service de gestion des clés que vous créez, détenez et gérez. Pour implémenter une clé KMS gérée par le client pour le chiffement au repos dans AWS IAM Identity Center, procédez comme suit :

Important

Certaines applications AWS gérées ne peuvent pas être utilisées avec AWS IAM Identity Center configuré avec une clé KMS gérée par le client. Consultez [AWS applications gérées que vous pouvez utiliser avec IAM Identity Center](#).

1. [Étape 1 : Identifier les cas d'utilisation pour votre organisation](#)- Pour définir les autorisations correctes pour l'utilisation de la clé KMS, vous devez identifier les cas d'utilisation pertinents au sein de votre organisation. Les autorisations clés KMS comprennent des déclarations de politique clés KMS et des politiques basées sur l'identité qui fonctionnent ensemble pour permettre aux principaux IAM appropriés d'utiliser la clé KMS pour leurs cas d'utilisation spécifiques.
2. [Étape 2 : Préparation des déclarations de politique clés de KMS](#)- Choisissez des modèles de déclaration de politique clé KMS pertinents en fonction des cas d'utilisation identifiés à l'étape 1, et renseignez les identifiants requis et les noms principaux IAM. Commencez par les déclarations de politique clés KMS de base et, si vos politiques de sécurité l'exigent, affinez-les comme décrit dans la section Déclarations de politique clés KMS avancées.
3. [Étape 3 : Création d'une clé KMS gérée par le client](#)- Créez une clé KMS dans AWS KMS qui répond aux exigences du centre d'identité IAM, et ajoutez les déclarations de politique clé KMS préparées à l'étape 2 à la politique clé KMS.
4. [Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes](#)- Choisissez des modèles de déclaration de politique IAM pertinents en fonction des cas d'utilisation identifiés à l'étape 1, et préparez-les en vue de leur utilisation en remplissant le code ARN. Autorisez ensuite les responsables IAM pour chaque cas d'utilisation spécifique à utiliser la clé

KMS sur tous les comptes en ajoutant les déclarations de politique IAM préparées aux politiques IAM des principaux.

5. [Étape 5 : Configuration de la clé KMS dans IAM Identity Center](#)- Activez la clé KMS gérée par le client dans votre instance IAM Identity Center afin de l'utiliser pour le chiffrement au repos.

Étape 1 : Identifier les cas d'utilisation pour votre organisation

Avant de créer et de configurer votre clé KMS gérée par le client, identifiez vos cas d'utilisation et préparez les autorisations de clé KMS requises. Reportez-vous au [guide du développeur AWS KMS](#) pour plus d'informations sur la politique relative aux clés KMS.

Les principaux IAM qui appellent le service APIs IAM Identity Center ont besoin d'autorisations. Par exemple, un administrateur délégué peut être autorisé à les utiliser par le biais d'une politique d'ensemble d'autorisations. Lorsque IAM Identity Center est configuré avec une clé gérée par le client, les principaux IAM doivent également être autorisés à utiliser l'API KMS via le service IAM Identity Center. Vous définissez ces autorisations d'API KMS à deux endroits : dans la politique clé KMS et dans les politiques IAM associées aux principes IAM.

Les autorisations clés KMS sont les suivantes :

1. Déclarations de politique relatives aux clés KMS que vous spécifiez sur la clé KMS lors de sa création dans [Étape 3 : Création d'une clé KMS gérée par le client](#).
2. Déclarations de politique IAM pour les principes IAM que vous spécifiez [Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes](#) après avoir créé la clé KMS.

Le tableau suivant indique les cas d'utilisation pertinents et les principes IAM qui nécessitent des autorisations pour utiliser votre clé KMS.

Cas d'utilisation	Principaux IAM qui ont besoin d'autorisations pour utiliser la clé KMS	Obligatoire/facultatif
Utilisation d' AWS IAM Identity Center	- Administrateurs d' AWS IAM Identity Center - Service IAM Identity Center et service Identity Store associé	Obligatoire

Cas d'utilisation	Principaux IAM qui ont besoin d'autorisations pour utiliser la clé KMS	Obligatoire/facultatif
Utilisation d'applications AWS gérées avec IAM Identity Center	- Administrateurs d'applications AWS gérées - AWS applications gérées Rôles de service supposés appeler le service IAM Identity Center par les applications AWS gérées APIs	Facultatif
Utilisation de AWS Control Tower sur l'instance AWS IAM Identity Center qu'elle a activée	AWS Control Tower administrateurs	Facultatif
SSO vers les instances Amazon EC2 AWS avec IAM Identity Center	Principaux IAM autorisés à effectuer l'authentification unique sur les instances Amazon EC2	Facultatif
Tout autre cas d'utilisation faisant appel au service IAM Identity Center APIs avec des principes IAM, tels que des applications gérées par le client, des ensembles d'autorisations, des flux de travail de mise en service ou des fonctions AWS Lambda	Principaux IAM utilisés par ces flux de travail pour appeler le service IAM Identity Center APIs	Facultatif

Note

Plusieurs principaux IAM répertoriés dans le tableau nécessitent des autorisations d'API AWS KMS. Toutefois, pour protéger les données de vos utilisateurs et de vos groupes dans IAM Identity Center, seuls les services IAM Identity Center et Identity Store appellent directement l'API AWS KMS.

Étape 2 : Préparation des déclarations de politique clés de KMS

Après avoir identifié les cas d'utilisation pertinents pour votre organisation, vous pouvez préparer les déclarations de politique clés KMS correspondantes.

1. Choisissez les principales déclarations de politique KMS qui correspondent aux cas d'utilisation de votre organisation. Commencez par les modèles de politique de base. Si vous avez besoin de politiques plus spécifiques en fonction de vos exigences de sécurité, vous pouvez modifier les déclarations de politique à l'aide des exemples présentés dans [Déclarations de politique clés avancées de KMS](#). Pour obtenir des conseils sur cette décision, voir [Considérations relatives au choix des principales déclarations de politique KMS de référence par rapport aux déclarations de politique clés](#). En outre, chaque section de référence [Déclarations de base relatives aux clés KMS et à la politique IAM](#) inclut des considérations pertinentes.
2. Copiez les politiques pertinentes dans un éditeur et insérez les identifiants requis et les noms principaux IAM dans les déclarations de politique clés de KMS. Pour obtenir de l'aide pour trouver les valeurs des identifiants référencés, consultez [Où trouver les identifiants requis](#).

Vous trouverez ci-dessous des modèles de politique de base pour chaque cas d'utilisation. Seul le premier ensemble d'autorisations pour AWS IAM Identity Center est requis pour utiliser une clé KMS. Nous vous recommandons de consulter les sous-sections applicables pour obtenir des informations supplémentaires spécifiques aux cas d'utilisation.

- [Déclarations de politique clés de base de KMS pour l'utilisation d'IAM Identity Center \(obligatoire\)](#)
- [Déclarations de base relatives aux clés KMS et à la politique IAM pour l'utilisation des applications AWS gérées](#)
- [Déclaration clé de référence du KMS pour l'utilisation de AWS Control Tower](#)
- [Déclarations de base relatives à la clé KMS et à la politique IAM pour l'utilisation d'IAM Identity Center sur les instances Amazon EC2](#)
- [Déclarations de base relatives aux clés KMS et à la politique IAM pour l'utilisation de flux de travail personnalisés avec IAM Identity Center](#)

Important

Faites preuve de prudence lorsque vous modifiez les politiques relatives aux clés KMS pour les clés déjà utilisées par IAM Identity Center. Bien qu'IAM Identity Center valide les autorisations de chiffrement et de déchiffrement lors de la configuration initiale d'une clé KMS, il ne peut pas vérifier les modifications de politique ultérieures. La suppression par

inadvertance des autorisations nécessaires peut perturber le fonctionnement normal de votre IAM Identity Center. Pour obtenir des conseils sur la résolution des erreurs courantes liées aux clés gérées par le client dans IAM Identity Center, reportez-vous à [Résoudre les problèmes liés aux clés gérées par le client dans AWS IAM Identity Center](#).

Note

IAM Identity Center et son magasin d'identités associé nécessitent des autorisations de niveau de service pour utiliser votre clé KMS gérée par le client. Cette exigence s'étend aux applications AWS gérées qui appellent le service IAM Identity Center à l'APIs aide des informations d'identification du service. Pour les autres cas d'utilisation où le service APIs IAM Identity Center est appelé avec des [sessions d'accès direct](#), seul le principal IAM initiateur (tel qu'un administrateur) a besoin d'autorisations clés KMS. En particulier, les utilisateurs finaux utilisant le portail AWS d'accès et les applications AWS gérées n'ont pas besoin d'autorisations clés KMS directes, car elles sont accordées par le biais des services respectifs.

Étape 3 : Création d'une clé KMS gérée par le client

Vous pouvez créer une clé gérée par le client à l'aide de la console AWS de gestion ou du AWS KMS APIs. Lors de la création de la clé, ajoutez les déclarations de politique clé KMS que vous avez préparées à l'étape 2 dans la politique clé KMS. Pour obtenir des instructions détaillées, notamment des conseils sur la politique de clé KMS par défaut, consultez le [Guide du développeur du service de gestion des AWS clés](#).

La clé doit répondre aux exigences suivantes :

- La clé KMS doit se trouver dans la même AWS région que l'instance IAM Identity Center
- Vous pouvez choisir une clé multirégionale ou une clé mono-régionale. Toutefois, si vous prévoyez d'utiliser IAM Identity Center en plusieurs exemplaires, Régions AWS vous devez créer une clé KMS multirégionale. Vous ne pouvez pas convertir une clé KMS à région unique en clé KMS multirégionale. Nous vous recommandons donc de commencer par une clé KMS multirégionale, sauf si vous avez des exigences spécifiques concernant l'utilisation d'une clé KMS à région unique.
- La clé KMS doit être une clé symétrique configurée pour une utilisation « crypter et déchiffrer »
- La clé KMS doit se trouver dans le même compte AWS Organizations de gestion que l'instance organisationnelle d'IAM Identity Center

 Note

Si vous envisagez de répliquer cette clé KMS dans les régions dans lesquelles vous souhaitez répliquer votre centre d'identité IAM, nous vous recommandons de commencer par effectuer la configuration décrite dans cette section, puis de suivre les instructions de [the section called “Répliquer le centre d'identité IAM dans une région supplémentaire”](#)

Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes

Tout principal IAM qui utilise le service IAM Identity Center à APIs partir d'un autre AWS compte, tel que les administrateurs délégués d'IAM Identity Center, doit également disposer d'une déclaration de politique IAM autorisant l'utilisation de la clé KMS par le biais de ce compte. APIs

Pour chaque cas d'utilisation identifié à l'étape 1 :

1. Recherchez les modèles de déclaration de politique IAM pertinents dans les déclarations de politique IAM et de clé KMS de base.
2. Copiez les modèles dans un éditeur et renseignez l'ARN de la clé, qui est désormais disponible après la création de la clé KMS à l'étape 3. Pour obtenir de l'aide pour trouver la valeur de l'ARN clé, consultez [Où trouver les identifiants requis](#).
3. Dans le AWS Management Console, recherchez la politique IAM du principal IAM associée au cas d'utilisation. L'emplacement de cette politique varie en fonction du cas d'utilisation et de la manière dont l'accès est accordé.
 - Pour l'accès accordé directement dans IAM, vous pouvez localiser les principaux IAM, tels que les rôles IAM dans la console IAM.
 - Pour l'accès accordé via IAM Identity Center, vous pouvez trouver l'ensemble d'autorisations pertinent dans la console IAM Identity Center.
4. Ajoutez les déclarations de politique IAM spécifiques au cas d'utilisation au rôle IAM et enregistrez la modification.

 Note

Les politiques IAM décrites ici sont des politiques basées sur l'identité. Bien que ces politiques puissent être associées aux utilisateurs, aux groupes et aux rôles IAM, nous

recommandons d'utiliser des rôles IAM dans la mesure du possible. Consultez le guide de l'utilisateur IAM pour plus d'informations sur les rôles IAM par rapport aux utilisateurs IAM.

Configuration supplémentaire dans certaines applications AWS gérées

Certaines applications AWS gérées nécessitent que vous configuriez un rôle de service pour permettre aux applications d'utiliser le service APIs IAM Identity Center. Si votre organisation utilise des applications AWS gérées avec IAM Identity Center, procédez comme suit pour chaque application déployée :

1. Consultez le guide de l'utilisateur de l'application pour vérifier si les autorisations ont été mises à jour pour inclure les autorisations liées aux clés KMS pour l'utilisation de l'application avec IAM Identity Center.
2. Si tel est le cas, mettez à jour les autorisations conformément aux instructions du guide de l'utilisateur de l'application afin d'éviter toute interruption des opérations de l'application.

Note

Si vous ne savez pas si une application AWS gérée utilise ces autorisations, nous vous recommandons de consulter les guides d'utilisation de toutes les applications AWS gérées déployées. Vous ne devez effectuer cette configuration qu'une seule fois pour chaque application nécessitant cette configuration.

Étape 5 : Configuration de la clé KMS dans IAM Identity Center

Important

Avant de procéder à cette étape :

- Vérifiez que vos applications AWS gérées sont compatibles avec les clés KMS gérées par le client. Pour obtenir la liste des applications compatibles, consultez la section [Applications AWS gérées que vous pouvez utiliser avec IAM Identity Center](#). Si vous avez des applications incompatibles, ne poursuivez pas.
- Configurez les autorisations nécessaires pour utiliser la clé KMS. Sans autorisations appropriées, cette étape peut échouer ou perturber l'administration d'IAM Identity Center,

l'utilisation d'applications AWS gérées et d'autres cas d'utilisation nécessitant des autorisations clés KMS. Pour de plus amples informations, veuillez consulter [Étape 1 : Identifier les cas d'utilisation pour votre organisation](#).

- Assurez-vous que les autorisations pour les applications AWS gérées et les applications gérées par le client qui appellent le service IAM Identity Center APIs avec des rôles IAM autorisent également l'utilisation de la clé KMS via le service IAM Identity Center. APIs Certaines applications AWS gérées nécessitent que vous configuriez des autorisations, telles qu'un rôle de service, pour pouvoir les utiliser APIs. Reportez-vous au guide de l'utilisateur de chaque application AWS gérée déployée pour vérifier si vous devez ajouter des autorisations clés KMS spécifiques.

Spécifiez une clé KMS lors de l'activation d'une nouvelle instance organisationnelle d'IAM Identity Center

Lorsque vous activez une nouvelle instance d'organisation d'IAM Identity Center, vous pouvez spécifier une clé KMS gérée par le client lors de la configuration. Cela garantit que l'instance utilise votre clé pour le chiffrement au repos dès le début. Avant de commencer, reportez-vous à [Considérations relatives aux clés KMS gérées par le client et aux politiques avancées en matière de clés KMS](#).

1. Sur la page Activer le centre d'identité IAM, développez la section Chiffrement au repos.
2. Choisissez Gérer le chiffrement.
3. Choisissez Clé gérée par le client.
4. Pour la clé KMS, effectuez l'une des opérations suivantes :
 - a. Choisissez Sélectionner parmi vos clés KMS et sélectionnez la clé que vous avez créée dans la liste déroulante.
 - b. Choisissez Enter KMS key ARN et saisissez l'ARN complet de votre clé.
5. Choisissez Enregistrer.
6. Choisissez Activer pour terminer la configuration.

Pour plus d'informations, consultez la section [Activer le centre d'identité IAM](#).

Modifier la configuration clé d'une instance organisationnelle existante d'IAM Identity Center

Vous pouvez remplacer la clé KMS gérée par le client par une autre clé ou passer à une AWS clé que vous possédez à tout moment.

Console

Pour modifier la configuration de votre clé KMS

1. Ouvrez la console IAM Identity Center à <https://console.aws.amazon.com/singlesignon/> l'adresse.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez l'onglet Paramètres supplémentaires.
4. Choisissez Gérer le chiffrement.
5. Sélectionnez l'une des méthodes suivantes :
 - a. Clé gérée par le client : sélectionnez une autre clé gérée par le client dans la liste déroulante ou saisissez un nouvel ARN de clé.
 - b. AWS clé possédée : passez à l'option de chiffrement par défaut.
6. Choisissez Enregistrer.

AWS CLI

Pour modifier une instance organisationnelle existante d'IAM Identity Center afin d'utiliser la clé gérée par le client KMS

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Pour modifier une instance organisationnelle existante d'IAM Identity Center afin qu'elle utilise une clé AWS détenue

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration
```

```
--encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

Considérations clés gérées par le client

- La mise à jour de la configuration de la clé KMS pour le fonctionnement d'IAM Identity Center n'a aucun effet sur les sessions utilisateur actives dans votre IAM Identity Center. Vous pouvez continuer à utiliser le portail AWS d'accès, la console IAM Identity Center et le service IAM Identity Center APIs au cours de ce processus.
- Lors du passage à une nouvelle clé KMS, IAM Identity Center confirme qu'il peut utiliser la clé avec succès pour le chiffrement et le déchiffrement. Si vous avez commis une erreur lors de la configuration de la politique clé ou de la politique IAM, la console affichera un message d'erreur explicatif et la clé KMS précédente restera utilisée.
- La rotation annuelle des clés KMS par défaut aura lieu automatiquement. Vous pouvez consulter le [guide du AWS KMS développeur](#) pour obtenir des informations sur des sujets tels que la [rotation des clés](#), la [surveillance des AWS KMS clés](#) et le [contrôle de l'accès à la suppression des clés](#).

Important

Si la clé KMS gérée par le client et utilisée par votre instance IAM Identity Center est supprimée, désactivée ou inaccessible en raison d'une politique de clé KMS incorrecte, les utilisateurs de votre personnel et les administrateurs d'IAM Identity Center ne pourront pas utiliser IAM Identity Center. La perte d'accès peut être temporaire (une politique de clé peut être corrigée) ou permanente (une clé supprimée ne peut pas être restaurée) selon les circonstances. Nous vous recommandons de [restreindre l'accès aux](#) opérations critiques, telles que la suppression ou la désactivation de la clé KMS. Nous recommandons également à votre organisation de mettre en place des [procédures d'accès AWS rapides](#) afin de garantir l'accès de vos utilisateurs privilégiés AWS en cas d'inaccessibilité d'IAM Identity Center.

Où trouver les identifiants requis

Lorsque vous configurez les autorisations pour votre clé KMS gérée par le client, vous aurez besoin d'identifiants de AWS ressource spécifiques pour compléter les modèles de politique clé et de déclaration de politique IAM. Insérez les identifiants requis (par exemple, l'identifiant de l'organisation) et les noms principaux IAM dans les déclarations de politique clés de KMS.

Vous trouverez ci-dessous un guide pour localiser ces identifiants dans la console AWS de gestion.

Nom de ressource Amazon (ARN) du centre d'identité IAM et ARN du magasin d'identités

Une instance IAM Identity Center est une AWS ressource dotée de son propre ARN unique, tel que `arn:aws:sso::instance/ssoins-1234567890abcdef`. L'ARN suit le modèle décrit dans la section sur les types de ressources IAM Identity Center de la référence d'autorisation de service.

Chaque instance d'IAM Identity Center possède un magasin d'identités associé qui stocke les identités des utilisateurs et des groupes. Un magasin d'identité possède un identifiant unique appelé Identity Store ID (par exemple, `d-123456789a`). L'ARN suit le modèle décrit dans la section des types de ressources Identity Store de la [référence d'autorisation de service](#).

Vous trouverez les valeurs ARN et Identity Store ID sur la page Paramètres de votre IAM Identity Center. L'ID du magasin d'identités se trouve dans l'onglet Source d'identité.

AWS Organizations ID

Si vous souhaitez spécifier un identifiant d'organisation (par exemple, `o-exampleorg1`) dans votre politique clé, vous pouvez trouver sa valeur sur la page Paramètres de vos consoles IAM Identity Center et Organizations. L'ARN suit le modèle décrit dans la section « Organizations resource types » du Service Authorization Reference.

ARN de la clé KMS

Vous pouvez trouver l'ARN d'une clé KMS dans la AWS KMS console. Choisissez Clés gérées par le client sur la gauche, cliquez sur la clé dont vous souhaitez rechercher l'ARN, et vous la verrez dans la section Configuration générale. L'ARN suit le modèle décrit dans la section sur les types de AWS KMS ressources de la référence d'autorisation de service.

Consultez le guide du AWS Key Management Service développeur pour plus d'informations sur les politiques clés relatives aux AWS KMS autorisations AWS KMS et leur résolution des problèmes. Pour plus d'informations sur les politiques IAM et leur représentation JSON, consultez le guide de l'utilisateur IAM.

Déclarations de base relatives aux clés KMS et à la politique IAM

Les politiques de base basées sur les clés et les identités KMS fournies ici servent de base aux exigences communes. Nous vous recommandons également de passer en revue celles [Déclarations de politique clés avancées de KMS](#) qui fournissent des contrôles d'accès plus précis, par exemple en garantissant que la clé KMS n'est accessible qu'à une instance ou à une application AWS gérée IAM Identity Center spécifique. Avant d'utiliser les déclarations de politique clés avancées de KMS,

consultez le [Considérations relatives au choix des principales déclarations de politique KMS de référence par rapport aux déclarations de politique clés](#).

Les sections suivantes fournissent des déclarations de politique de base pour chaque cas d'utilisation. Développez les sections correspondant à vos cas d'utilisation et copiez les principales déclarations de politique de KMS. Ensuite, revenez à [Étape 2 : Préparation des déclarations de politique clés de KMS](#).

Déclarations de politique clés de base de KMS pour l'utilisation d'IAM Identity Center (obligatoire)

Utilisez le modèle de déclaration de politique de clé KMS suivant [Étape 2 : Préparation des déclarations de politique clés de KMS](#) pour permettre aux administrateurs d'IAM Identity Center, de son magasin d'identités associé et d'IAM Identity Center d'utiliser la clé KMS.

- Dans l'élément principal pour les déclarations de politique de l'administrateur, spécifiez les AWS principaux comptes des comptes d'administration de l'IAM Identity Center, à savoir le compte de gestion de l' AWS organisation et le compte d'administration déléguée, en utilisant le format « `arn:aws:iam::111122223333:root` ».
- Dans l' PrincipalArn élément, remplacez l'exemple par les rôles IAM ARNs des administrateurs de l'IAM Identity Center.

Vous pouvez spécifier soit :

- ARN du rôle IAM spécifique :

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_12345678"
```

- Modèle Wildcard (recommandé) :

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_*
```

L'utilisation du caractère générique (*) empêche la perte d'accès si l'ensemble d'autorisations est supprimé et recréé, car Identity Center génère de nouveaux identifiants uniques pour les ensembles d'autorisations recréés. Pour un exemple de mise en œuvre, voir [Exemple de politique de confiance personnalisée](#).

- Dans l' SourceAccount élément, spécifiez l'ID de compte IAM Identity Center.
- Identity Store possède son propre principal de service `identitystore.amazonaws.com`, qui doit être autorisé à utiliser la clé KMS.

- Ces déclarations de politique permettent à vos instances IAM Identity Center d'un AWS compte spécifique d'utiliser la clé KMS. Pour restreindre l'accès à une instance IAM Identity Center spécifique, consultez [Déclarations de politique clés avancées de KMS](#). Vous ne pouvez avoir qu'une seule instance IAM Identity Center pour chaque AWS compte.

Déclarations de politique clés de KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
          ]
        }
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  ],
  {
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
```

```

    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    },
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": "kms:DescribeKey",
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",

```

```

        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
    ]
}
},
{
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "sso.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:sso:instance-arn": "*"
        },
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        }
    }
},
{
    "Sid": "AllowIdentityStoreToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "identitystore.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
    }
}
}

```

```

    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "identitystore.amazonaws.com",
        "sso.amazonaws.com"
      ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  }
]
}

```

Utilisez le modèle de déclaration de politique IAM suivant [the section called “Étape 4 : Configuration des politiques IAM”](#) pour permettre aux administrateurs du IAM Identity Center d'utiliser la clé KMS.

- Remplacez l'exemple d'ARN de clé dans l'Resource élément par l'ARN de votre clé KMS réel. Pour obtenir de l'aide pour trouver les valeurs des identifiants référencés, consultez [Où trouver les identifiants requis](#).
- Ces déclarations de politique IAM accordent un accès par clé KMS au principal IAM mais ne limitent pas le AWS service autorisé à effectuer la demande. La politique des clés KMS prévoit généralement ces restrictions de service. Toutefois, vous pouvez ajouter un contexte de chiffrement à cette politique IAM pour limiter l'utilisation à une instance d'Identity Center spécifique. Pour plus d'informations, consultez [Déclarations de politique clés avancées de KMS](#).

Déclarations de politique IAM requises pour les administrateurs délégués d'IAM Identity Center

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToUseKMSkey",
    "Effect": "Allow",
    "Action": [

```



```
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  {
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToListKeyAliases",
    "Effect": "Allow",
    "Action": "kms:ListAliases",
    "Resource": "*"
  }
]
```

Déclarations de base relatives aux clés KMS et à la politique IAM pour l'utilisation des applications AWS gérées

 Note

Certaines applications AWS gérées ne peuvent pas être utilisées avec IAM Identity Center configuré avec une clé KMS gérée par le client. Pour plus d'informations, consultez la section [Applications AWS gérées qui fonctionnent avec IAM Identity Center](#).

Utilisez le modèle de déclaration de politique de clé KMS suivant [Étape 2 : Préparation des déclarations de politique clés de KMS](#) pour autoriser les applications AWS gérées et leurs administrateurs à utiliser la clé KMS.

- Insérez votre AWS Organizations identifiant dans l' PrincipalOrgidentifiant et SourceOrgId les conditions. Pour obtenir de l'aide pour trouver les valeurs des identifiants référencés, consultez [Où trouver les identifiants requis](#).
- Ces déclarations de politique permettent à toutes vos applications AWS gérées et à tous les principaux IAM (administrateurs d'applications) de l' AWS organisation d'utiliser kms: Decrypt à l'aide d'IAM Identity Center et d'Identity Store. Pour limiter ces déclarations de politique à des applications AWS gérées, à des comptes ou à des instances IAM Identity Center spécifiques, consultez [Déclarations de politique clés avancées de KMS](#).

Vous pouvez restreindre l'accès à des administrateurs d'applications spécifiques en les * remplaçant par des principes IAM spécifiques. Pour vous protéger contre les changements de nom de rôle IAM lorsque des ensembles d'autorisations sont recréés, utilisez l'approche décrite dans le [Exemple de politique de confiance personnalisée](#). Pour de plus amples informations, veuillez consulter [Considérations relatives au choix des principales déclarations de politique KMS de référence par rapport aux déclarations de politique clés](#).

Déclarations de politique clés de KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
]
}

```

Utilisez le modèle de déclaration de politique IAM suivant [Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes](#) pour permettre aux administrateurs d'applications AWS gérées d'utiliser la clé KMS d'un compte membre.

- Remplacez l'exemple d'ARN dans l'élément Resource par l'ARN de votre clé KMS réelle. Pour obtenir de l'aide pour trouver les valeurs des identifiants référencés, consultez [Où trouver les identifiants requis](#).
- Certaines applications AWS gérées nécessitent que vous configuriez des autorisations pour le service APIs IAM Identity Center. Avant de configurer une clé gérée par le client dans IAM Identity Center, vérifiez que ces autorisations autorisent également l'utilisation de la clé KMS. Pour connaître les exigences d'autorisation spécifiques relatives aux clés KMS, consultez la documentation de chaque application AWS gérée que vous avez déployée.

Déclarations de politique IAM requises pour les administrateurs d'applications AWS gérées :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid":
    "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Déclaration clé de référence du KMS pour l'utilisation de AWS Control Tower

Utilisez les modèles de déclaration de clé KMS suivants [Étape 2 : Préparation des déclarations de politique clés de KMS](#) pour permettre aux administrateurs de AWS Control Tower d'utiliser la clé KMS.

- Dans l'élément Principal, spécifiez les principaux IAM utilisés pour accéder au service IAM Identity Center. APIs Pour plus d'informations sur les principaux IAM, consultez la section [Spécification d'un principal](#) dans le Guide de l'utilisateur IAM.
- Ces déclarations de politique permettent aux administrateurs de AWS Control Tower d'utiliser la clé KMS via n'importe laquelle de vos instances IAM Identity Center. Cependant, AWS Control Tower restreint l'accès à l'instance organisationnelle d'IAM Identity Center au sein de la même AWS organisation. En raison de cette restriction, il n'y a aucun avantage pratique à restreindre davantage la clé KMS à une instance IAM Identity Center spécifique, comme décrit dans [Déclarations de politique clés avancées de KMS](#).
- Pour vous protéger contre les changements de nom de rôle IAM lorsque des ensembles d'autorisations sont recréés, utilisez l'approche décrite dans le [Exemple de politique de confiance personnalisée](#)

Déclaration de politique de clé KMS :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
```

```

    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

AWS Control Tower ne prend pas en charge l'administration déléguée et, par conséquent, il n'est pas nécessaire de configurer une politique IAM pour ses administrateurs.

Important

La déclaration de politique précédente couvre les opérations AWS Control Tower gérées par les services, telles que l'inscription automatique des comptes, où AWS Control Tower assume le `AWSControlTowerAdmin` rôle. Toutefois, pour les opérations initiées par le client, telles que l'approvisionnement de comptes via Account Factory ou les appels AWS Control Tower APIs directs, AWS Control Tower utilise des [sessions d'accès direct \(FAS\) et fonctionne sous le propre rôle](#) IAM du client. Cela signifie que le rôle IAM que vous utilisez pour lancer ces opérations nécessite également des `kms:Decrypt` autorisations sur la clé KMS gérée par le client.

Ajoutez les déclarations de politique clés KMS suivantes à côté des `AWSControlTowerAdmin` déclarations ci-dessus. *MyControlTowerRole* Remplacez-le par l'ARN du rôle IAM avec lequel vous interagissez AWS Control Tower, tel qu'un rôle d'ensemble d'autorisations IAM Identity Center (par exemple, `AWSReservedSSO_PermissionSetName_*`), un rôle IAM personnalisé pour l'automatisation ou tout autre rôle utilisé pour appeler ou. AWS Control Tower AWS Service Catalog APIs

Déclaration de politique clé de KMS pour les opérations initiées par le client AWS Control Tower :

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityCenterForControlTower",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityStoreForControlTower",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

Déclarations de base relatives à la clé KMS et à la politique IAM pour l'utilisation d'IAM Identity Center sur les instances Amazon EC2

Utilisez le modèle de déclaration de politique clé KMS suivant [Étape 2 : Préparation des déclarations de politique clés de KMS](#) pour permettre aux utilisateurs de l'authentification unique (SSO) des instances Amazon EC2 d'utiliser la clé KMS sur plusieurs comptes.

- Spécifiez les principaux IAM utilisés pour accéder à IAM Identity Center dans le champ Principal. Pour plus d'informations sur les principaux IAM, consultez la section [Spécification d'un principal](#) dans le Guide de l'utilisateur IAM.

- Cette déclaration de politique autorise n'importe laquelle de vos instances IAM Identity Center à utiliser la clé KMS. Pour restreindre l'accès à une instance IAM Identity Center spécifique, consultez [Déclarations de politique clés avancées de KMS](#).
- Pour vous protéger contre les changements de nom de rôle IAM lorsque des ensembles d'autorisations sont recréés, utilisez l'approche décrite dans Exemple de politique de confiance personnalisée.

Déclaration de stratégie de clé KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```



```

    }
  }
}
]
}

```

Utilisez le modèle de déclaration de politique IAM suivant [Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes](#) pour autoriser les instances SSO vers EC2 à utiliser la clé KMS.

Joignez la déclaration de politique IAM à l'ensemble d'autorisations existant dans IAM Identity Center que vous utilisez pour autoriser l'accès SSO aux instances Amazon EC2. Pour des exemples de politique IAM, consultez la section [Connexions au protocole Remote Desktop](#) dans le Guide de l'utilisateur de AWS Systems Manager.

- Remplacez l'exemple d'ARN dans l'élément Resource par l'ARN de votre clé KMS réelle. Pour obtenir de l'aide pour trouver les valeurs des identifiants référencés, consultez [Où trouver les identifiants requis](#).

Politique IAM définie par les autorisations :

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowKMSKeyUseViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}

```

Déclarations de base relatives aux clés KMS et à la politique IAM pour l'utilisation de flux de travail personnalisés avec IAM Identity Center

Utilisez les modèles de déclaration de politique clé KMS suivants [Étape 2 : Préparation des déclarations de politique clés de KMS](#) pour autoriser les flux de travail personnalisés, tels que les applications gérées par le client, dans le compte de AWS Organizations gestion ou le compte d'administration déléguée à utiliser la clé KMS. Notez que la fédération SAML dans les applications gérées par le client ne nécessite pas d'autorisations clés KMS.

- Dans l'élément Principal, spécifiez les principaux IAM utilisés pour accéder au service IAM Identity Center. APIs Pour plus d'informations sur les principaux IAM, consultez la section [Spécification d'un principal](#) dans le Guide de l'utilisateur IAM.
- Ces déclarations de politique permettent à votre flux de travail d'utiliser la clé KMS via n'importe laquelle de vos instances IAM Identity Center. Pour restreindre l'accès à une instance IAM Identity Center spécifique, consultez [Déclarations de politique clés avancées de KMS](#).
- Pour vous protéger contre les changements de nom de rôle IAM lorsque des ensembles d'autorisations sont recréés, utilisez l'approche décrite dans le [Exemple de politique de confiance personnalisée](#)

Déclaration de politique de clé KMS :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    }
  ],
}
```

```

    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

Utilisez le modèle de déclaration de politique IAM suivant [Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes](#) pour permettre au principal IAM associé au flux de travail personnalisé d'utiliser la clé KMS sur tous les comptes. Ajoutez la déclaration de politique IAM au principal IAM.

- Remplacez l'exemple d'ARN dans l'élément Resource par l'ARN de votre clé KMS réelle. Pour obtenir de l'aide pour trouver les valeurs des identifiants référencés, consultez [Où trouver les identifiants requis](#).

Déclaration de politique IAM (requis uniquement pour une utilisation entre comptes) :

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  ]
}

```

```
}  
  }  
}]  
}
```

Exemples de déclarations de politique clés de KMS pour les cas d'utilisation courants

IAM Identity Center avec administrateurs délégués et applications AWS gérées

Cette section contient des exemples de déclarations de politique clés KMS que vous pouvez utiliser pour une instance IAM Identity Center dotée d'administrateurs délégués et d'applications AWS gérées.

Important

Les déclarations de politique clés KMS supposent que votre instance IAM Identity Center n'est utilisée dans aucun autre cas d'utilisation nécessitant des autorisations relatives aux clés KMS. Pour confirmer, vous pouvez passer en revue tous les [cas d'utilisation](#). En outre, pour vérifier si vos applications AWS gérées nécessitent une configuration supplémentaire, voir [the section called “Configuration supplémentaire dans certaines applications AWS gérées”](#)

Copiez les déclarations de politique clé KMS sous le tableau et ajoutez-les à votre politique de clé KMS. Cet exemple utilise les valeurs d'exemple suivantes :

- 111122223333- ID de compte de l'instance IAM Identity Center
- 444455556666- ID de compte d'administration déléguée
- o-a1b2c3d4e5- identifiant AWS de l'organisation
- `arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*`- Un modèle générique représentant le rôle IAM d'un administrateur du IAM Identity Center fourni à partir de l'ensemble d'autorisations. *Admin* Un tel rôle contient le code de région de la région principale (us-east-1 dans cet exemple).
- `arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*`- Un modèle générique représentant le rôle IAM d'un administrateur délégué d'IAM Identity Center fourni à partir du jeu d'autorisations. *DelegatedAdmin* Un tel rôle contient le code de région de la région principale (us-east-1 dans cet exemple).

Si le rôle IAM n'a pas été généré à partir d'un ensemble d'autorisations, le rôle IAM ressemblera à un rôle normal tel que `arn:aws:iam::111122223333:role/idcadmin`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
          ]
        }
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  ],
  {
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    }
  }
}
```

```

    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  },
  "StringLike": {
    "kms:ViaService": "identitystore.*.amazonaws.com",
    "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
  }
}
},
{
  "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": "kms:DescribeKey",
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  }
}
}

```

```

},
{
  "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "sso.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIdentityStoreToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "identitystore.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
}

```

```

    },
    {
      "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}

```



```

    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
},
{
  "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    },
    "StringEquals": {
      "aws:SourceOrgID": "o-a1b2c3d4e5"
    }
  }
}
]
}

```

Déclarations de politique clés avancées de KMS

Utilisez des déclarations de politique clés KMS avancées pour mettre en œuvre des contrôles d'accès plus précis pour votre clé KMS gérée par le client. Ces politiques s'appuient sur le [Déclarations de base relatives aux clés KMS et à la politique IAM](#) en ajoutant des conditions de contexte de chiffrement et des restrictions spécifiques au service. Avant de décider d'utiliser ou non des déclarations de politique clés KMS avancées, assurez-vous de passer en revue les considérations pertinentes.

Utilisation du contexte de chiffrement pour restreindre l'accès

Vous pouvez limiter l'utilisation des clés KMS à une instance IAM Identity Center spécifique en spécifiant une condition de contexte de chiffrement dans vos déclarations de politique clés. Les principales déclarations politiques de base incluent déjà ce contexte avec une valeur générique. Remplacez le caractère générique « * » par un ARN d'instance Identity Center et un ARN Identity Store spécifiques pour garantir que la clé ne fonctionne qu'avec l'instance que vous souhaitez. Vous pouvez également ajouter les mêmes conditions de contexte de chiffrement à la politique IAM configurée pour l'utilisation de la clé KMS entre comptes.

Identity Center

```
"StringEquals": {  
    "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso::instance/  
ssoins-1234567890abcdef"  
}
```

Identity Store

```
"StringEquals": {  
    "kms:EncryptionContext:aws:identitystore:identitystore-arn":  
    "arn:aws:identitystore::111122223333:identitystore/d-1234567890"  
}
```

Si vous avez besoin d'aide pour trouver ces identifiants, consultez [Où trouver les identifiants requis](#).

 Note

Vous ne pouvez utiliser une clé KMS gérée par le client qu'avec une instance organisationnelle d'IAM Identity Center. La clé gérée par le client doit se trouver dans le compte de gestion de AWS l'organisation, ce qui permet de garantir que la clé est utilisée avec une seule instance d'IAM Identity Center. Cependant, le mécanisme de contexte de chiffrement fournit une protection technique indépendante de l'utilisation d'une instance unique. Vous pouvez également utiliser la clé de `aws:SourceArn` condition dans les déclarations de politique relatives aux clés KMS destinées aux responsables des services Identity Center et Identity Store.

Considérations relatives à la mise en œuvre des conditions de contexte de

Avant d'implémenter les conditions de contexte de chiffrement, passez en revue les exigences suivantes :

- **DescribeKey action.** Le contexte de chiffrement ne peut pas être appliqué à l'action « kms : DescribeKey », qui peut être utilisée par les administrateurs d'IAM Identity Center. Lorsque vous configurez votre politique de clé KMS, excluez le contexte de chiffrement pour cette action spécifique afin de garantir le bon fonctionnement de votre instance IAM Identity Center.
- **Configuration de la nouvelle instance.** Si vous activez une nouvelle instance IAM Identity Center avec une clé KMS gérée par le client, consultez [Considérations relatives aux clés KMS gérées par le client et aux politiques avancées en matière de clés KMS](#).
- **Changements de source d'identité.** Lorsque vous modifiez votre source d'identité vers ou depuis Active Directory, le contexte de chiffrement nécessite une attention particulière. Consultez [Considérations relatives à la modification de votre source d'identité](#).

Modèles de politique

Choisissez parmi ces modèles de politiques avancés en fonction de vos exigences en matière de sécurité. Équilibrez les contrôles d'accès granulaires avec les frais administratifs qu'ils engendrent.

Sujets abordés ici :

- [Déclarations de politique KMS pour l'utilisation en lecture seule d'une instance IAM Identity Center spécifique](#). Cette section explique l'utilisation du contexte de chiffrement pour l'accès en lecture seule à IAM Identity Center.

- [Déclarations de politique clés KMS affinées pour l'utilisation des applications AWS gérées](#). Cette section explique comment affiner les politiques relatives aux clés KMS pour les applications AWS gérées à l'aide du contexte de chiffrement et des informations relatives à l'application, telles que le principal du service d'application, l'ARN de l'application et l'ID de AWS compte.

Déclarations de politique KMS pour l'utilisation en lecture seule d'une instance IAM Identity Center spécifique

Cette politique permet [aux auditeurs de sécurité et aux](#) autres membres du personnel qui n'ont besoin que d'un accès en lecture à IAM Identity Center d'utiliser la clé KMS.

Pour utiliser cette politique, procédez comme suit :

1. Remplacez les exemples de principes IAM d'administrateur en lecture seule par vos principes d'administrateur IAM réels
2. Remplacez l'exemple d'ARN de l'instance IAM Identity Center par l'ARN de votre instance réelle
3. Remplacez l'exemple d'ARN d'Identity Store par votre véritable ARN d'Identity Store
4. Si vous utilisez l'[administration déléguée](#), voir [Étape 4 : Configuration des politiques IAM pour l'utilisation de la clé KMS entre comptes](#)

Si vous avez besoin d'aide pour trouver les valeurs de ces identifiants, consultez [Où trouver les identifiants requis](#).

Une fois que vous avez mis à jour le modèle avec vos valeurs, revenez [Étape 2 : Préparation des déclarations de politique clés de KMS](#) à pour préparer des déclarations de politique clés KMS supplémentaires, le cas échéant.

L'action kms: Déchiffrer à elle seule ne limite pas l'accès aux opérations en lecture seule. La politique IAM doit appliquer l'accès en lecture seule au service IAM Identity Center. APIs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
```

```

    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
      }
    }
  },
  {
    "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
      }
    }
  }
]
}

```

Déclarations de politique clés KMS affinées pour l'utilisation des applications AWS gérées

Ces modèles de politique fournissent un contrôle plus précis sur les applications AWS gérées qui peuvent utiliser votre clé KMS.

Note

Certaines applications AWS gérées ne peuvent pas être utilisées avec IAM Identity Center configuré avec une clé KMS gérée par le client. Découvrez les [applications AWS gérées que vous pouvez utiliser avec IAM Identity Center](#).

Ils [Déclarations de base relatives aux clés KMS et à la politique IAM pour l'utilisation des applications AWS gérées](#) permettent AWS à n'importe quelle application gérée depuis n'importe quel compte de la même AWS organisation d'utiliser la clé KMS. Utilisez ces politiques affinées pour restreindre l'accès en :

- Principal du service d'application
- Instance d'application ARNs
- AWS account IDs
- Contexte de chiffrement pour des instances spécifiques d'IAM Identity Center

 Note

Un principal de service est un identifiant unique pour un AWS service, généralement au format `servicename.amazonaws.com` (par exemple, `elasticmapreduce.amazonaws.com` pour Amazon EMR).

Restreindre par compte

Ce modèle de déclaration de politique de clé KMS permet à une application AWS gérée dans des AWS comptes spécifiques d'utiliser la clé KMS à l'aide d'une instance IAM Identity Center spécifique.

Pour utiliser cette politique, procédez comme suit :

1. Remplacez l'exemple de principal de service par le principal de service de votre application réel
2. Remplacez le compte d'exemple IDs par le compte réel sur IDs lequel vos applications AWS gérées sont déployées
3. Remplacez l'exemple d'ARN d'Identity Store par votre véritable ARN d'Identity Store
4. Remplacez l'exemple d'ARN de l'instance IAM Identity Center par l'ARN de votre instance réelle

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
```

```

    "Service": "myapp.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": [
        "111122223333",
        "444455556666"
      ]
    },
    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  }
},
{
  "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
  "Effect": "Allow",
  "Principal": {
    "Service": "myapp.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": [
        "111122223333",
        "444455556666"
      ]
    },
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  }
}

```

```

    }
  }
]
}

```

Restreindre par instance d'application

Ce modèle de déclaration de politique de clé KMS permet à une instance d'application AWS gérée spécifique d'utiliser la clé KMS à l'aide d'une instance IAM Identity Center spécifique.

Pour utiliser cette politique, procédez comme suit :

1. Remplacez l'exemple de principal de service par le principal de service de votre application réel
2. Remplacez l'exemple d'ARN d'application par l'ARN de votre instance d'application réelle
3. Remplacez l'exemple d'ARN d'Identity Store par votre véritable ARN d'Identity Store
4. Remplacez l'exemple d'ARN de l'instance IAM Identity Center par l'ARN de votre instance réelle

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ]
}

```



```

    }
  },
  {
    "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
]
}

```

Considérations relatives aux clés KMS gérées par le client et aux politiques avancées en matière de clés KMS

Lorsque vous implémentez des clés KMS gérées par le client avec IAM Identity Center, tenez compte de ces facteurs qui affectent la configuration, la sécurité et la maintenance continue de votre configuration de chiffrement.

Considérations relatives au choix des principales déclarations de politique KMS de référence par rapport aux déclarations de politique clés

Lorsque vous décidez de rendre les autorisations clés KMS plus spécifiques à l'utilisation [Déclarations de politique clés avancées de KMS](#), tenez compte des frais de gestion et des besoins de sécurité de votre organisation. Des déclarations de politique plus spécifiques permettent de mieux contrôler qui peut utiliser la clé et à quelles fins ; toutefois, elles nécessitent une maintenance continue au fur et à

mesure de l'évolution de la configuration de votre IAM Identity Center. Par exemple, si vous limitez l'utilisation de la clé KMS à des déploiements d'applications AWS gérées spécifiques, vous devrez mettre à jour la politique de clé chaque fois que votre organisation souhaite déployer ou annuler le déploiement d'une application. Des politiques moins restrictives réduisent la charge administrative mais peuvent accorder des autorisations plus étendues que celles nécessaires pour répondre à vos exigences de sécurité.

Considérations relatives à l'activation d'une nouvelle instance IAM Identity Center avec une clé KMS gérée par le client

Les considérations ici s'appliquent si vous utilisez le contexte de chiffrement tel que décrit dans [Déclarations de politique clés avancées de KMS](#) pour restreindre l'utilisation de la clé KMS à une instance IAM Identity Center spécifique.

Lorsque vous activez une nouvelle instance IAM Identity Center avec une clé KMS gérée par le client, le centre d'identité IAM et le magasin d'identités ne ARNs sont disponibles qu'après la configuration. Vous avez les options suivantes :

- Utilisez temporairement des modèles d'ARN génériques, puis remplacez-les par full une ARNs fois l'instance activée. N'oubliez pas de passer StringEquals d'un StringLike opérateur à l'autre selon vos besoins.
 - Pour le SPN du centre d'identité IAM : « `arn : $ {Partition} :sso : :instance/*` ».
 - Pour le SPN d'Identity Store : « `arn : $ {Partition} :identitystore : :$ {Account} :identitystore/*` ».
- Utilisez temporairement « `Purpose:KEY_CONFIGURATION` » dans l'ARN. Cela ne fonctionne que pour l'activation des instances et doit être remplacé par l'ARN réel pour que votre instance IAM Identity Center fonctionne normalement. L'avantage de cette approche est que vous ne pouvez pas oublier de la remplacer une fois l'instance activée.
 - Pour le SPN d'IAM Identity Center, utilisez : « `arn : $ {Partition} :sso : :instance/purpose:KEY_CONFIGURATION` »
 - Pour Identity Store SPN, utilisez : « `arn : $ {Partition} :identitystore : :$ {Account} :identityStore/Purpose:KEY_CONFIGURATION` »

 Important

N'appliquez pas cette configuration à une clé KMS déjà utilisée dans une instance IAM Identity Center existante, car cela pourrait perturber son fonctionnement normal.

- Omettez la condition de contexte de chiffrement de la politique de clé KMS jusqu'à ce que l'instance soit activée.

Ressources de balisage AWS IAM Identity Center

Une balise est une étiquette d'attribut personnalisée que vous ajoutez à une AWS ressource pour faciliter l'identification, l'organisation et la recherche de ressources. Chaque balise se compose de deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Une clé de balise est sensible à la casse et peut contenir 128 caractères au plus.
- Une valeur de balise (par exemple, `111122223333` ou `Production`). Les valeurs de balise peuvent comporter jusqu'à 256 caractères et, comme les clés de balise, sont sensibles à la casse. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur `null`. Si la valeur de balise est identique à l'utilisation d'une chaîne vide.

Les balises vous aident à identifier et à organiser vos AWS ressources. De nombreux AWS services prennent en charge le balisage. Vous pouvez donc attribuer le même tag aux ressources de différents services pour indiquer que les ressources sont liées. Par exemple, vous pouvez attribuer la même balise à un ensemble d'autorisations spécifique dans votre instance d'IAM Identity Center. Pour plus d'informations sur les stratégies de balisage, consultez les [AWS ressources de balisage](#) du Références générales AWS guide et les meilleures pratiques en matière de [balisage](#).

Outre l'identification, l'organisation et le suivi de vos AWS ressources à l'aide de balises, vous pouvez utiliser des balises dans les politiques IAM pour contrôler qui peut consulter vos ressources et interagir avec elles. Pour en savoir plus sur l'utilisation de balises pour contrôler l'accès, consultez la section [Contrôle de l'accès aux AWS ressources à l'aide de balises](#) dans le guide de l'utilisateur IAM. Par exemple, vous pouvez autoriser un utilisateur à mettre à jour un ensemble d'autorisations IAM Identity Center, mais uniquement si le jeu d'autorisations IAM Identity Center comporte une owner balise dont la valeur correspond au nom de cet utilisateur.

Vous ne pouvez appliquer des balises qu'aux ensembles d'autorisations. Vous ne pouvez pas appliquer de balises aux rôles correspondants créés par IAM Identity Center. Comptes AWS Vous pouvez utiliser la console IAM Identity Center AWS CLI ou le IAM Identity Center APIs pour ajouter, modifier ou supprimer des balises pour un ensemble d'autorisations.

Les sections suivantes fournissent des informations supplémentaires sur les balises pour IAM Identity Center.

Rubriques

- [Restrictions liées aux étiquettes](#)
- [Gérez les balises à l'aide de la console IAM Identity Center](#)
- [AWS CLI exemples](#)
- [Gérez les balises à l'aide de l'API IAM Identity Center](#)

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises figurant sur les ressources de l'IAM Identity Center :

- Le nombre maximum de balises que vous pouvez attribuer à une ressource est de 50.
- La longueur de clé maximale est de 128 caractères Unicode.
- La longueur de valeur maximale est de 256 caractères Unicode.
- Les caractères valides pour une clé et une valeur de balise sont les suivants :
a-z, A-Z, 0-9, espace et les caractères suivants : `_` `:/=` `+` `-` et `@`
- Les clés et les valeurs sont sensibles à la casse.
- Ne l'utilisez pas `aws` : comme préfixe pour les clés ; il est réservé à l' AWS usage

Gérez les balises à l'aide de la console IAM Identity Center

Vous pouvez utiliser la console IAM Identity Center pour ajouter, modifier et supprimer des balises associées à votre instance ou à vos ensembles d'autorisations.

Pour gérer les ensembles d'autorisations, les balises d'une console IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Choisissez Ensembles d'autorisations.
3. Choisissez le nom de l'ensemble d'autorisations contenant les balises que vous souhaitez gérer.
4. Dans l'onglet Autorisations, sous Balises, effectuez l'une des opérations suivantes, puis passez à l'étape suivante :
 - a. Si des balises sont déjà attribuées à cet ensemble d'autorisations, choisissez Modifier les balises.
 - b. Si aucun tag n'est attribué à cet ensemble d'autorisations, choisissez Ajouter des tags.

5. Pour chaque nouvelle balise, saisissez les valeurs dans les colonnes Clé et Valeur (facultatif). Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Pour supprimer une étiquette, choisissez le X dans la colonne Supprimer à côté de la balise que vous souhaitez supprimer.

Pour gérer les balises d'une instance d'IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Paramètres.
3. Sélectionnez l'onglet Tags (Identifications).
4. Pour chaque balise, saisissez les valeurs dans les champs Clé et Valeur (facultatif). Lorsque vous avez terminé, cliquez sur le bouton Ajouter un nouveau tag.

Pour supprimer une étiquette, cliquez sur le bouton Supprimer à côté de la balise que vous souhaitez supprimer.

AWS CLI exemples

AWS CLI fournit des commandes que vous pouvez utiliser pour gérer les balises que vous attribuez à votre ensemble d'autorisations.

Affectation de balises

Utilisez les commandes suivantes pour attribuer des balises à votre ensemble d'autorisations.

Exemple **tag-resource** Commande pour un ensemble d'autorisations

Attribuez des balises à un ensemble d'autorisations en utilisant [tag-resource](#) dans le sso jeu de commandes :

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test
```

Cette commande comprend les paramètres suivants :

- **instance-arn**— Le nom de ressource Amazon (ARN) de l'instance IAM Identity Center sous laquelle l'opération sera exécutée.
- **resource-arn**— L'ARN de la ressource contenant les balises à répertorier.
- **tags** – Paires clé-valeur des étiquettes.

Pour affecter plusieurs balises à la fois, spécifiez-les dans une liste séparée par des virgules :

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

Affichage des balises

Utilisez les commandes suivantes pour afficher les balises que vous avez attribuées à votre ensemble d'autorisations.

Exemple **list-tags-for-resource** Commande pour un ensemble d'autorisations

Affichez les balises attribuées à un ensemble d'autorisations à l'aide [list-tags-for-resource](#) de l'ensemble de commandes :

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Suppression de balises

Utilisez les commandes suivantes pour supprimer des balises d'un ensemble d'autorisations.

Exemple **untag-resource** Commande pour un ensemble d'autorisations

Supprimez les balises d'un ensemble d'autorisations en utilisant [untag-resource](#) dans le jeu de commandes :

```
$ aws sso-admin untag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tag-keys Stage CostCenter Owner
```

Pour le paramètre `--tag-keys`, spécifiez une ou plusieurs clés de balise et n'incluez pas les valeurs de balise.

Appliquer des balises lors de la création d'un ensemble d'autorisations

Utilisez les commandes suivantes pour attribuer des balises au moment de créer un ensemble d'autorisations.

Exemple Commande **create-permission-set** avec des identifications

Lorsque vous créez un ensemble d'autorisations à l'aide de la [create-permission-set](#) commande, vous pouvez spécifier des balises avec le `--tags` paramètre suivant :

```
$ aws sso-admin create-permission-set \  
> --instance-arn sso-instance-arn \  
> --name permission=set-name \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

Gérez les balises à l'aide de l'API IAM Identity Center

Utilisez les actions d'API suivantes pour attribuer, afficher et supprimer des balises pour un ensemble d'autorisations ou une instance d'IAM Identity Center.

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)
- [CreatePermissionSet](#)
- [CreateInstance](#)

Intégration de la AWS CLI à IAM Identity Center

AWS L'intégration de l'interface de ligne de commande (CLI) version 2 à IAM Identity Center simplifie le processus de connexion. Les développeurs peuvent se connecter directement à l' AWS CLI aide des mêmes informations d'identification Active Directory ou IAM Identity Center que celles qu'ils utilisent habituellement pour se connecter à IAM Identity Center et accéder aux comptes et rôles qui leur sont assignés. Par exemple, une fois qu'un administrateur a configuré IAM Identity Center pour utiliser Active Directory pour l'authentification, un développeur peut se connecter AWS CLI directement à l'aide de ses informations d'identification Active Directory.

AWS L'intégration de la CLI à IAM Identity Center offre les avantages suivants :

- Les entreprises peuvent permettre à leurs développeurs de se connecter à l'aide des informations d'identification d'IAM Identity Center ou d'Active Directory en connectant IAM Identity Center à leur Active Directory à l'aide de. Directory Service
- Les développeurs peuvent se connecter depuis la CLI pour un accès plus rapide.
- Les développeurs peuvent répertorier les comptes et les rôles auxquels ils ont attribué un accès et passer d'un compte à l'autre.
- Les développeurs peuvent générer et enregistrer automatiquement des profils de rôles nommés dans la configuration de leur CLI et les référencer dans l'interface de ligne de commande pour exécuter des commandes dans les comptes et rôles souhaités.
- La CLI gère automatiquement les informations d'identification à court terme afin que les développeurs puissent démarrer et rester dans la CLI en toute sécurité, sans interruption, et exécuter des scripts de longue durée.

Comment intégrer la AWS CLI à IAM Identity Center

Pour utiliser l'intégration de la AWS CLI avec IAM Identity Center, téléchargez, installez et configurez AWS Command Line Interface la version 2. Pour obtenir des instructions détaillées sur la façon de télécharger et d'intégrer le AWS CLI à IAM Identity Center, voir [Configuration de la AWS CLI pour utiliser IAM Identity Center](#) dans le guide de l'AWS Command Line Interface utilisateur.

Considérations relatives à l'accès AWS Management Console privé

Si votre organisation utilise la fonctionnalité AWS Management Console d'accès privé, vous devez réfléchir à la manière dont vos utilisateurs se connecteront à IAM Identity Center.

Une politique de point de terminaison VPC restreint la connexion à la console de gestion, ce qui empêche vos utilisateurs de se connecter à des sites auxquels Comptes AWS ils ne sont pas autorisés à accéder. Pour plus d'informations, consultez la section [Accès AWS Management Console privé](#) dans le guide de AWS Management Console démarrage.

Les points de terminaison VPC bloquent la connexion à l'IAM Identity Center

Il est important de noter que l'utilisation de points de terminaison VPC bloquera la connexion à l'IAM Identity Center. Cela se produit lorsqu'un utilisateur est déjà connecté à la console de gestion via le point de terminaison VPC. Pour que vos utilisateurs puissent continuer à se connecter à IAM Identity Center, ils doivent utiliser le point de terminaison public pour se AWS connecter, plutôt que le point de terminaison VPC.

Quotas et limites dans IAM Identity Center

Les tableaux suivants décrivent les quotas au sein d'IAM Identity Center. Les demandes d'augmentation de quota doivent provenir d'un compte de gestion ou d'un compte d'administrateur délégué. Pour augmenter un quota, voir [Demande d'augmentation de quota](#).

Note

Nous vous recommandons d'utiliser la AWS CLI et APIs d'administrer IAM Identity Center si vous avez plus de 50 000 utilisateurs, 10 000 groupes ou 500 ensembles d'autorisations. Pour plus d'informations sur la CLI, consultez [Intégration de la AWS CLI à IAM Identity Center](#). Pour plus d'informations APIs, consultez la section [Bienvenue dans le guide de référence de l'API IAM Identity Center](#).

Quotas de candidatures

Ressource	Quota par défaut	Peut être augmenté
Taille du fichier de certificats SAML du fournisseur de services (au format PEM)	2 Ko	Non
Limite d'assertion SAML	50 000 caractères	Non
Limite de taille de fichier du certificat IdP téléchargé vers IAM Identity Center	2500 caractères (UTF-8)	Non
Étendue d'accès par application	25	Non

Compte AWS quotas

Ressource	Quota par défaut	Peut être augmenté
Nombre d'ensembles d'autorisations autorisés dans IAM Identity Center	3500	Oui
Nombre d'ensembles d'autorisations fournis autorisés par Compte AWS	500	Oui
Nombre de stratégies en ligne par jeu d'autorisations	1	Non
Nombre de politiques AWS gérées et gérées par le client par ensemble d'autorisations	25 ¹	Non
Taille maximale de stratégie en ligne par jeu d'autorisations	32 768 octets. La taille maximale des caractères autres que des espaces blancs dans la politique intégrée par ensemble d'autorisations est de 10 240 octets.	Non
Nombre de rôles IAM (ensembles d'autorisations) dans le Compte AWS qui peuvent être mis à jour à la fois	1	Non

¹Gestion des identités et des accès AWS (IAM) définit un quota de 10 politiques gérées par rôle. Pour tirer parti de ce quota, demandez une augmentation du quota IAM. Politiques gérées associées à

un rôle IAM dans la console Service Quotas pour chaque Compte AWS endroit où vous souhaitez déployer l'ensemble d'autorisations.

 Note

[Gérer Comptes AWS avec des ensembles d'autorisations](#) sont fournis en Comptes AWS tant que rôles IAM, ou utilisent des rôles IAM existants dans Comptes AWS, et respectent donc les quotas IAM. Pour plus d'informations sur les quotas associés aux rôles IAM, consultez la section Quotas [IAM et STS](#).

Quotas Active Directory

Ressource	Quota par défaut	Peut être augmenté
Nombre d'annuaires connectés que vous pouvez avoir simultanément	1	Non

Quotas de banque d'identités IAM Identity Center

Ressource	Quota par défaut	Peut être augmenté
Nombre d'utilisateurs pris en charge dans IAM Identity Center	200 000	Oui
Nombre de groupes pris en charge dans IAM Identity Center	100 000	Oui
Nombre de groupes uniques pouvant être utilisés pour évaluer les autorisations d'un utilisateur	1 000	Non

Limites de limitation de l'IAM Identity Center

Ressource	Quota par défaut
Centre d'identité IAM APIs	Les IAM Identity Center APIs ont une limite d'accélération collective de 20 transactions par seconde (TPS). Pour en savoir plus APIs, vous pouvez ouvrir un dossier d'assistance pour demander une augmentation de limite. L'API CreateAccountAssignment d'écriture est limitée à 15 appels asynchrones en attente. Cette limite ne peut pas être augmentée.
Boutique d'identités APIs	Identity Store APIs a une limite de 20 transactions par seconde (TPS) par API. Cette limite s'applique par instance d'Identity Store. Vous pouvez ouvrir un dossier de support pour demander une augmentation de limite.
SCIM APIs	Les SCIM APIs ont des limites d'accélération de 25 transactions par seconde (TPS) pour l'écriture APIs et de 40 TPS pour la lecture. APIs Ces limites s'appliquent par instance d'Identity Store. Vous pouvez ouvrir un dossier de support pour demander une augmentation de limite.

Si votre instance IAM Identity Center est activée en plusieurs fois Régions AWS, les limites de limitation s'appliquent de la même manière à chaque région activée. Par exemple, vous auriez la limite d'accélération de 20 TPS sur l'Identity Store APIs dans chaque région activée. Pour plus d'informations sur les opérations d'API disponibles dans d'autres régions, consultez le [tableau](#) correspondant.

Quotas de demandes de service OIDC

Ressource	Valeur par défaut (requêtes par seconde)	Peut être augmenté
Taux de demandes provenant d'une adresse distante pour enregistrer un OAuth client public S'applique à : RegisterClient	20	Oui
Taux de demande d'un client public enregistré auprès du service OIDC S'applique à : CreateToken, StartDeviceAuthorization	80	Oui
Taux de demandes provenant de tous les clients publics enregistrés auprès de la même instance IAM Identity Center S'applique à : CreateToken	250	Oui
Taux de demandes provenant d'une application IAM Identity Center enregistrée auprès de l'instance IAM Identity Center S'applique à : CreateTokenWithIAM	80	Oui
Taux de génération de jetons à partir de toutes les applications IAM Identity Center enregistrées avec la même	10	AWS Support de contact

Ressource	Valeur par défaut (requêtes par seconde)	Peut être augmenté
instance IAM Identity Center avec la subvention JWT Bearer		
S'applique à : CreateTokenWithIAM		

Si votre instance IAM Identity Center est activée en plusieurs fois Régions AWS, les taux de demandes ci-dessus s'appliquent de la même manière à chaque région activée. Par exemple, si le taux de demandes autorisé pour enregistrer un OAuth client public à partir d'une adresse distante est de 20 demandes par seconde, ce débit est disponible dans chaque région activée. Pour plus d'informations sur les opérations d'API disponibles dans d'autres régions, consultez le [tableau](#) correspondant.

Quotas supplémentaires

Ressource	Quota par défaut	Peut être augmenté
Nombre total Comptes AWS d'applications pouvant être configurées* **	3000	Oui
Nombre total d'instances d'IAM Identity Center par compte	1	Non
Nombre total d'émetteurs de jetons fiables	10	Non
Nombre total de groupes pouvant être affectés à un ensemble d'autorisations par Compte AWS application ou à une application	100	Non

Ressource	Quota par défaut	Peut être augmenté
Nombre total de personnes Régions AWS activées pour une seule instance IAM Identity Center	3	Oui

* Par exemple, vous pouvez configurer 2 750 comptes et 250 applications, soit un total de 3 000 comptes et applications.

** L'opération [ProvisionPermissionSet](#) API peut fournir un ensemble d'autorisations en utilisant l'option ALL_PROVISIONED_ACCOUNTS jusqu'à 3500 Comptes AWS. Si vous devez attribuer un ensemble d'autorisations à plus de 3 500 Comptes AWS, vous pouvez utiliser l'opération ProvisionPermissionSet API avec l'AWS_ACCOUNToption, qui fournit l'ensemble d'autorisations en une seule fois Compte AWS. Vous pouvez passer jusqu'à trois appels simultanés àProvisionPermissionSet.

Résolution des problèmes liés à IAM Identity Center

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la configuration ou de l'utilisation de la console IAM Identity Center.

Problèmes lors de la création d'une instance de compte d'IAM Identity Center

Plusieurs restrictions peuvent s'appliquer lors de la création d'une instance de compte d'IAM Identity Center. Si vous ne parvenez pas à créer une instance de compte via la console IAM Identity Center ou via l'expérience de configuration d'une application AWS gérée prise en charge, vérifiez les cas d'utilisation suivants :

- **Régions AWS** Cochez la case **autre Compte AWS** dans laquelle vous essayez de créer l'instance de compte. Vous êtes limité à une instance d'IAM Identity Center par **Compte AWS**. Pour activer l'application, passez à l'instance **Région AWS avec IAM Identity Center** ou passez à un compte sans instance d'IAM Identity Center.
- Si votre organisation a activé IAM Identity Center avant le 14 septembre 2023, votre administrateur devra peut-être accepter la création d'une instance de compte. Collaborez avec votre administrateur pour activer la création d'instances de compte à partir de la console IAM Identity Center dans le compte de gestion.
- Votre administrateur a peut-être créé une politique de contrôle des services pour limiter la création d'instances de compte d'IAM Identity Center. Travaillez avec votre administrateur pour ajouter votre compte à la liste des autorisations.

Vous recevez un message d'erreur lorsque vous tentez d'afficher la liste des applications cloud préconfigurées pour fonctionner avec IAM Identity Center

L'erreur suivante se produit lorsque vous avez une politique qui autorise un autre centre APIs d'identité IAM, `sso:ListApplications` mais pas les autres. Mettez à jour votre politique pour corriger cette erreur.

L'`ListApplications` autorisation autorise plusieurs APIs :

- L'`ListApplicationsAPI`.
- API interne similaire à l'`ListApplicationProvidersAPI` utilisée dans la console IAM Identity Center.

Pour aider à résoudre le problème de duplication, l'API interne autorise désormais également l'utilisation de l'`ListApplicationProvidersaction`. Pour autoriser l'`ListApplicationsAPI` publique mais refuser l'API interne, votre politique doit inclure une déclaration refusant l'`ListApplicationProvidersaction` :

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplications",  
    "Resource": "<instanceArn>" // (or "*" for all instances)  
  }  
]
```

Pour autoriser l'API interne mais la refuser `ListApplications`, la politique doit uniquement autoriser `ListApplicationProviders`. L'`ListApplicationsAPI` est refusée si elle n'est pas explicitement autorisée.

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  }  
]
```

Lorsque vos politiques sont mises à jour, contactez-nous Support pour que cette mesure proactive soit supprimée.

Problèmes relatifs au contenu des assertions SAML créées par IAM Identity Center

IAM Identity Center fournit une expérience de débogage basée sur le Web pour les assertions SAML créées et envoyées par IAM Identity Center, y compris les attributs contenus dans ces assertions, lors de l'accès, Comptes AWS et pour les applications SAML depuis le portail d'accès. AWS Pour voir les détails d'une assertion SAML générée par IAM Identity Center, procédez comme suit.

1. Connectez-vous au portail d' AWS accès.
2. Lorsque vous êtes connecté au portail, maintenez la touche Shift enfoncée, choisissez la vignette de l'application, puis relâchez la touche Shift.
3. Examinez les informations indiquées sur la page intitulée You are now in administrator mode (Vous êtes maintenant en mode administrateur). Pour conserver ces informations pour référence future, choisissez Copier le code XML et collez le contenu ailleurs.
4. Choisissez Envoyer pour <application>continuer. Cette option envoie l'assertion au fournisseur de services.

Note

Certaines configurations de navigateur et certains systèmes d'exploitation peuvent ne pas prendre en charge cette procédure. Cette procédure a été testée sur Windows 10 à l'aide des navigateurs Firefox, Chrome et Edge.

Des utilisateurs spécifiques ne parviennent pas à se synchroniser avec IAM Identity Center à partir d'un fournisseur SCIM externe

Si votre fournisseur d'identité (IdP) est configuré pour approvisionner les utilisateurs dans IAM Identity Center à l'aide de la synchronisation SCIM, vous risquez de rencontrer des échecs de synchronisation pendant le processus de provisionnement des utilisateurs. Cela peut indiquer que la configuration utilisateur de votre IdP n'est pas compatible avec les exigences de l'IAM Identity Center. Dans ce cas, le SCIM de l'IAM Identity Center APIs renvoie des messages d'erreur fournissant des informations sur la cause première du problème. Vous pouvez trouver ces messages d'erreur dans les journaux ou dans l'interface utilisateur de votre IdP. Vous pouvez également trouver des informations plus détaillées sur les échecs de provisionnement dans les [AWS CloudTrail journaux](#).

Pour plus d'informations sur les implémentations d'IAM Identity Center SCIM, y compris les spécifications des paramètres et opérations obligatoires, facultatifs et non pris en charge pour les objets utilisateur, consultez le guide du développeur de mise en [œuvre d'IAM Identity Center SCIM dans le guide du développeur SCIM](#)

Voici quelques raisons courantes à l'origine de cette erreur :

1. L'objet utilisateur dans l'IdP n'a pas de prénom, de nom de famille ou de nom and/or d'affichage.

Message d'erreur : « 2 erreurs de validation détectées : valeur à '*name.givenName*' la contrainte non satisfaite : le membre doit satisfaire au modèle d'expression régulière : `[\\ p {L} \\ p {M} \\ p {S} \\ p {N} \\ p {P} \\ t \\ n \\ r] +` ; Valeur à '*name.givenName*' la contrainte non satisfaite : le membre doit avoir une longueur supérieure ou égale à 1 »

- Solution : ajoutez un premier (donné), un dernier (famille) et un nom d'affichage pour l'objet utilisateur. En outre, assurez-vous que les mappages de provisionnement SCIM pour les objets utilisateur de votre IdP sont configurés pour envoyer des valeurs non vides pour tous ces attributs.
2. Plusieurs valeurs pour un seul attribut sont envoyées à l'utilisateur (également appelées « attributs à valeurs multiples »). Par exemple, l'utilisateur peut avoir un numéro de téléphone professionnel et un numéro de téléphone personnel spécifiés dans l'IdP, ou plusieurs adresses électroniques ou physiques, et votre IdP est configuré pour essayer de synchroniser plusieurs ou toutes les valeurs pour cet attribut.

Message d'erreur : « L'attribut de liste *emails* dépasse la limite autorisée de 1 »

- Options de solution :
 - i. Mettez à jour vos mappages de provisionnement SCIM pour les objets utilisateur de votre IdP afin de n'envoyer qu'une seule valeur pour un attribut donné. Par exemple, configurez un mappage qui envoie uniquement le numéro de téléphone professionnel de chaque utilisateur.
 - ii. Si les attributs supplémentaires peuvent être supprimés en toute sécurité de l'objet utilisateur au niveau de l'IdP, vous pouvez supprimer les valeurs supplémentaires, en laissant une ou zéro valeur définie pour cet attribut pour l'utilisateur.
 - iii. Si l'attribut n'est pas nécessaire pour effectuer des actions dans AWS, supprimez le mappage correspondant à cet attribut des mappages de provisionnement SCIM pour les objets utilisateur de votre IdP.

3. Votre IdP essaie de faire correspondre les utilisateurs de la cible (IAM Identity Center, dans ce cas) en fonction de plusieurs attributs. Étant donné que l'unicité des noms d'utilisateur est garantie au sein d'une instance IAM Identity Center donnée, il vous suffit de spécifier `username` l'attribut utilisé pour la mise en correspondance.
 - Solution : Assurez-vous que la configuration SCIM de votre IdP n'utilise qu'un seul attribut pour correspondre aux utilisateurs d'IAM Identity Center. Par exemple, le mappage `username` de l'IdP à l'`username` attribut dans SCIM pour le provisionnement vers IAM Identity Center sera correct et suffisant pour la plupart des implémentations.
`userPrincipalName`

Erreur d'utilisateur ou de groupe dupliquée lors du provisionnement d'utilisateurs ou de groupes avec un fournisseur d'identité externe

Si vous rencontrez des problèmes de synchronisation avec IAM Identity Center lorsque vous configurez des utilisateurs ou des groupes auprès d'un fournisseur d'identité externe (IdP), cela peut être dû au fait que les utilisateurs ou groupes de votre IdP externe ne disposent pas de valeurs d'attribut uniques. Les messages d'erreur suivants peuvent s'afficher dans votre IdP externe :

Refusé de créer une nouvelle ressource dupliquée

Vous pouvez rencontrer ce problème dans les scénarios suivants :

- Scénario 1
 - Vous utilisez des attributs personnalisés non uniques dans votre IdP externe pour les attributs qui doivent être uniques dans IAM Identity Center. Les utilisateurs ou groupes IAM Identity Center existants ne parviennent pas à se synchroniser avec votre IdP.
- Scénario 2
 - Vous essayez de créer des utilisateurs dotés d'attributs dupliqués pour des attributs qui doivent être uniques dans IAM Identity Center.
 - Par exemple, vous créez ou possédez un utilisateur IAM Identity Center avec les attributs suivants :
 - Nom d'utilisateur : Jane Doe
 - Adresse e-mail principale : `jane_doe@example.com`
 - Ensuite, vous essayez de créer un autre utilisateur dans votre IdP externe avec les attributs suivants :

- Nom d'utilisateur : Richard Doe
- Adresse e-mail principale : jane_doe@example.com
- L'IdP externe tente de synchroniser et de créer l'utilisateur dans IAM Identity Center. Cependant, ces actions échouent car les deux utilisateurs ont des valeurs dupliquées pour une adresse e-mail principale qui doit être unique.

Le nom d'utilisateur, l'adresse e-mail principale et l'identifiant externe doivent être uniques pour que vos utilisateurs IdP externes puissent se synchroniser correctement avec IAM Identity Center. De même, le nom du groupe doit être unique pour que vos groupes IdP externes soient correctement synchronisés avec IAM Identity Center.

La solution consiste à examiner les attributs de votre source d'identité et à vous assurer qu'ils sont uniques.

Les utilisateurs ne peuvent pas se connecter lorsque leur nom d'utilisateur est au format UPN

Les utilisateurs peuvent ne pas être en mesure de se connecter au portail AWS d'accès en fonction du format qu'ils utilisent pour saisir leur nom d'utilisateur sur la page de connexion. Dans la plupart des cas, les utilisateurs peuvent se connecter au portail utilisateur en utilisant leur nom d'utilisateur simple, leur nom de connexion de bas niveau (DOMAIN \Username) ou leur nom de connexion UPN (). Username@Corp.Example.com L'exception à cette règle est lorsque IAM Identity Center utilise un répertoire connecté qui a été activé avec la MFA et que le mode de vérification a été défini sur Context-aware ou Always-on. Dans ce scénario, les utilisateurs doivent se connecter avec leur nom de connexion de bas niveau (DOMAIN \). Username Pour de plus amples informations, veuillez consulter [MFA pour les utilisateurs de l'annuaire Identity Center](#). Pour obtenir des informations générales sur les formats de nom d'utilisateur utilisés pour se connecter à Active Directory, consultez la section [Formats de nom d'utilisateur](#) sur le site Web de documentation Microsoft.

Je reçois le message d'erreur « Impossible d'effectuer l'opération sur le rôle protégé » lors de la modification d'un rôle IAM

Lorsque vous passez en revue les rôles IAM dans un compte, vous remarquerez peut-être que les noms de rôles commencent par « AWSReserved SSO_ ». Il s'agit des rôles que le service IAM Identity Center a créés dans le compte, et ils proviennent de l'attribution d'un ensemble

d'autorisations au compte. Toute tentative de modification de ces rôles depuis la console IAM entraînera l'erreur suivante :

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoLeName_Here' -  
this role is only modifiable by AWS'
```

Ces rôles ne peuvent être modifiés qu'à partir de la console IAM Identity Center Administrator, qui se trouve dans le compte de gestion de AWS Organizations. Une fois les modifications apportées, vous pouvez les transférer aux AWS comptes auxquels elles sont attribuées.

Les utilisateurs de l'annuaire ne peuvent pas réinitialiser leur mot de passe

Lorsqu'un utilisateur de l'annuaire réinitialise son mot de passe à l'aide du champ Mot de passe oublié ? option lors de la connexion au portail d' AWS accès, leur nouveau mot de passe doit respecter la politique de mot de passe par défaut décrite dans [Exigences relatives aux mots de passe lors de la gestion des identités dans IAM Identity Center](#).

Si un utilisateur saisit un mot de passe conforme à la politique puis reçoit le message d'erreur `We couldn't update your password`, vérifiez s'il AWS CloudTrail a enregistré l'échec. Cela peut être fait en effectuant une recherche dans la console de l'historique des événements CloudTrail ou en utilisant le filtre suivant :

```
"UpdatePassword"
```

Si le message indique ce qui suit, vous devrez peut-être contacter le support :

```
"errorCode": "InternalFailure",  
  "errorMessage": "An unknown error occurred"
```

Une autre cause possible de ce problème réside dans la convention de dénomination qui a été appliquée à la valeur du nom d'utilisateur. Les conventions de dénomination doivent suivre des modèles spécifiques tels que « surname.givenname ». Cependant, certains noms d'utilisateur peuvent être assez longs ou contenir des caractères spéciaux, ce qui peut entraîner la suppression de caractères dans l'appel d'API, entraînant ainsi une erreur. Vous pouvez essayer de réinitialiser le mot de passe avec un utilisateur de test de la même manière pour vérifier si tel est le cas.

Si le problème persiste, contactez le [AWS Support Center](#).

Mon utilisateur est référencé dans un ensemble d'autorisations mais ne peut pas accéder aux comptes ou applications assignés

Ce problème peut se produire si vous utilisez le système de gestion des identités interdomaines (SCIM) pour le provisionnement automatique avec un fournisseur d'identité externe. Plus précisément, lorsqu'un utilisateur, ou le groupe dont il était membre, est supprimé puis recréé en utilisant le même nom d'utilisateur (pour les utilisateurs) ou le même nom (pour les groupes) dans le fournisseur d'identité, un nouvel identifiant interne unique est créé pour le nouvel utilisateur ou le nouveau groupe dans IAM Identity Center. Cependant, IAM Identity Center possède toujours une référence à l'ancien identifiant dans sa base de données d'autorisations, de sorte que le nom de l'utilisateur ou du groupe apparaît toujours dans l'interface utilisateur, mais l'accès échoue. Cela est dû au fait que l'ID d'utilisateur ou de groupe sous-jacent auquel l'interface utilisateur fait référence n'existe plus.

Dans ce cas, pour rétablir l'accès AWS, vous pouvez supprimer l'accès de l'ancien utilisateur ou du Compte AWS groupe auquel il a été attribué à l'origine, puis réattribuer l'accès à l'utilisateur ou au groupe. Cela met à jour l'ensemble d'autorisations avec l'identifiant correct pour le nouvel utilisateur ou le nouveau groupe. De même, pour rétablir l'accès à une application, vous pouvez supprimer l'accès de l'utilisateur ou du groupe de la liste des utilisateurs assignés à cette application, puis ajouter à nouveau l'utilisateur ou le groupe.

Vous pouvez également vérifier si l'échec AWS CloudTrail a été enregistré en recherchant dans vos CloudTrail journaux les événements de synchronisation SCIM faisant référence au nom de l'utilisateur ou du groupe en question.

Je ne parviens pas à configurer correctement mon application à partir du catalogue d'applications

Si vous avez ajouté une application depuis le catalogue d'applications d'IAM Identity Center, sachez que chaque fournisseur de services fournit sa propre documentation détaillée. Vous pouvez accéder à ces informations depuis l'onglet Configuration de l'application dans la console IAM Identity Center.

Si le problème est lié à la configuration de la confiance entre l'application du fournisseur de services et IAM Identity Center, assurez-vous de consulter le manuel d'instructions pour connaître les étapes de dépannage.

Erreur « Une erreur inattendue s'est produite » lorsqu'un utilisateur tente de se connecter à l'aide d'un fournisseur d'identité externe

Cette erreur peut se produire pour plusieurs raisons, mais l'une des raisons les plus courantes est une incohérence entre les informations utilisateur contenues dans la demande SAML et les informations relatives à l'utilisateur dans IAM Identity Center.

Pour qu'un utilisateur d'IAM Identity Center puisse se connecter correctement lorsqu'il utilise un IdP externe comme source d'identité, les conditions suivantes doivent être remplies :

- Le format SAML NameID (configuré chez votre fournisseur d'identité) doit être « e-mail »
- La valeur NameID doit être une chaîne correctement formatée (RFC2822) (user@domain.com)
- La valeur NameID doit correspondre exactement au nom d'utilisateur d'un utilisateur existant dans IAM Identity Center (peu importe que l'adresse e-mail dans IAM Identity Center corresponde ou non, la correspondance entrante est basée sur le nom d'utilisateur)
- L'implémentation de la fédération SAML 2.0 par IAM Identity Center ne prend en charge qu'une seule assertion dans la réponse SAML entre le fournisseur d'identité et IAM Identity Center. Il ne prend pas en charge les assertions SAML chiffrées.
- Les instructions suivantes s'appliquent si cette option [Attributs pour le contrôle d'accès](#) est activée dans votre compte IAM Identity Center :
 - Le nombre d'attributs mappés dans la demande SAML doit être inférieur ou égal à 50.
 - La demande SAML ne doit pas contenir d'attributs à valeurs multiples.
 - La demande SAML ne doit pas contenir plusieurs attributs portant le même nom.
 - L'attribut ne doit pas contenir de XML structuré comme valeur.
 - Le format du nom doit être un format spécifié par SAML et non un format générique.

Note

IAM Identity Center n'effectue pas de création « juste à temps » d'utilisateurs ou de groupes pour les nouveaux utilisateurs ou groupes via la fédération SAML. Cela signifie que l'utilisateur doit être précréé dans IAM Identity Center, soit manuellement, soit via un provisionnement automatique, afin de se connecter à IAM Identity Center.

Cette erreur peut également se produire lorsque le point de terminaison Assertion Consumer Service (ACS) configuré dans votre fournisseur d'identité ne correspond pas à l'URL ACS fournie par votre instance IAM Identity Center. Assurez-vous que ces deux valeurs correspondent exactement.

En outre, vous pouvez résoudre de manière plus approfondie les problèmes de connexion au fournisseur d'identité externe en accédant au nom ExternalId PDirectory de l'événement Login AWS CloudTrail et en filtrant sur celui-ci.

Erreur « Impossible d'activer les attributs du contrôle d'accès »

Cette erreur peut se produire si l'utilisateur qui active ABAC ne dispose pas des `iam:UpdateAssumeRolePolicy` autorisations requises pour l'activer [Attributs pour le contrôle d'accès](#).

Je reçois un message « Navigateur non pris en charge » lorsque je tente d'enregistrer un appareil pour le MFA

WebAuthn est actuellement compatible avec les navigateurs Web Google Chrome, Mozilla Firefox, Microsoft Edge et Apple Safari, ainsi que sur les plateformes Windows 10 et Android. Certains composants du WebAuthn support peuvent varier, tels que la prise en charge de l'authentificateur de plateforme sur les navigateurs macOS et iOS. Si les utilisateurs tentent d'enregistrer des WebAuthn appareils sur un navigateur ou une plateforme non pris en charge, certaines options non prises en charge seront grisées, ou ils recevront un message d'erreur indiquant que toutes les méthodes prises en charge ne sont pas prises en charge. Dans ces cas, reportez-vous à [FIDO2: Web Authentication \(WebAuthn\)](#) pour plus d'informations sur le browser/platform support. Pour plus d'informations sur WebAuthn IAM Identity Center, consultez [FIDO2 authentificateurs](#).

Le groupe « Utilisateurs du domaine » Active Directory ne se synchronise pas correctement avec IAM Identity Center

Le groupe d'utilisateurs du domaine Active Directory est le « groupe principal » par défaut pour les objets utilisateur AD. Les groupes principaux Active Directory et leurs adhésions ne peuvent pas être lus par IAM Identity Center. Lorsque vous attribuez l'accès aux ressources ou aux applications IAM Identity Center, utilisez des groupes autres que le groupe des utilisateurs du domaine (ou d'autres groupes assignés en tant que groupes principaux) pour que l'appartenance au groupe soit correctement reflétée dans la banque d'identités IAM Identity Center.

Erreur d'identification MFA non valide

Cette erreur peut se produire lorsqu'un utilisateur tente de se connecter à IAM Identity Center à l'aide d'un compte fourni par un fournisseur d'identité externe (par exemple, Okta ou Microsoft Entra ID) avant que son compte ne soit entièrement provisionné auprès d'IAM Identity Center à l'aide du protocole SCIM. Une fois le compte utilisateur configuré auprès d'IAM Identity Center, ce problème doit être résolu. Vérifiez que le compte a été fourni à IAM Identity Center. Dans le cas contraire, consultez les journaux de provisionnement dans le fournisseur d'identité externe.

Je reçois un message « Une erreur inattendue s'est produite » lorsque je tente de m'inscrire ou de me connecter à l'aide d'une application d'authentification

Les systèmes de mot de passe à usage unique basé sur le temps (TOTP), tels que ceux utilisés par IAM Identity Center en combinaison avec des applications d'authentification basées sur du code, reposent sur la synchronisation de l'heure entre le client et le serveur. Assurez-vous que l'appareil sur lequel votre application d'authentification est installée est correctement synchronisé avec une source de temps fiable, ou réglez manuellement l'heure sur votre appareil pour qu'elle corresponde à une source fiable, telle que NIST (<https://www.time.gov/>) ou d'autres équivalents. local/regional

Je reçois un message d'erreur « Ce n'est pas toi, c'est nous » lorsque j'essaie de me connecter à IAM Identity Center

Cette erreur indique qu'il existe un problème de configuration avec votre instance d'IAM Identity Center ou avec le fournisseur d'identité externe (IdP) qu'IAM Identity Center utilise comme source d'identité. Nous vous recommandons de vérifier les points suivants :

- Vérifiez les paramètres de date et d'heure sur l'appareil que vous utilisez pour vous connecter. Nous vous recommandons de définir la date et l'heure à régler automatiquement. Si ce n'est pas le cas, nous vous recommandons de synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol) connu.
- Vérifiez que le certificat IdP téléchargé vers IAM Identity Center est le même que celui fourni par votre IdP. Vous pouvez vérifier le certificat depuis la console IAM Identity Center en accédant aux paramètres. Dans l'onglet Source d'identité, sélectionnez Action, puis sélectionnez Gérer

l'authentification. Si les certificats IdP et IAM Identity Center ne correspondent pas, importez un nouveau certificat dans IAM Identity Center.

- Assurez-vous que le format NameID du fichier de métadonnées de votre fournisseur d'identité est le suivant :
 - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Si vous utilisez AD Connector from AWS Directory Service comme fournisseur d'identité, vérifiez que les informations d'identification du compte de service sont correctes et n'ont pas expiré. Consultez [Mettre à jour les informations d'identification de votre compte de service AD Connector AWS Directory Service](#) pour plus d'informations.

Mes utilisateurs ne reçoivent pas d'e-mails d'IAM Identity Center

Tous les e-mails envoyés par le service IAM Identity Center proviendront soit de `no-reply@signin.aws`, soit de `no-reply@login.awsapps.com`. Votre système de messagerie doit être configuré de manière à accepter les e-mails provenant de ces adresses électroniques d'expéditeurs et à ne pas les traiter comme du courrier indésirable ou du spam.

Erreur : vous ne pouvez pas delete/modify/remove/assign accéder aux ensembles d'autorisations fournis dans le compte de gestion

Ce message indique que la [Administration déléguée](#) fonctionnalité a été activée et que l'opération que vous avez tentée précédemment ne peut être exécutée avec succès que par une personne disposant d'autorisations de compte de gestion AWS Organizations. Pour résoudre ce problème, connectez-vous en tant qu'utilisateur disposant de ces autorisations et réessayez d'exécuter la tâche ou attribuez cette tâche à une personne disposant des autorisations appropriées. Pour de plus amples informations, veuillez consulter [Enregistrez un compte membre](#).

Erreur : jeton de session introuvable ou non valide

Cette erreur peut se produire lorsqu'un client, tel qu'un navigateur Web AWS CLI, essaie d'utiliser une session révoquée ou invalidée côté serveur. AWS Toolkit Pour résoudre ce problème, retournez sur l'application client ou sur le site Web et réessayez, y compris en vous reconnectant si vous y êtes invité. Cela peut parfois vous obliger à annuler également les demandes en attente, telles qu'une tentative de connexion en attente AWS Toolkit depuis votre IDE.

Les membres du groupe issus de domaines approuvés ne se synchronisent pas avec IAM Identity Center

Si un groupe de sécurité se synchronise correctement avec IAM Identity Center, mais que ses membres d'un domaine local approuvé n'apparaissent pas dans le centre d'identité IAM, cela peut être dû au fait que le groupe réside dans AWS Managed Microsoft AD et contient Foreign Security Principal (FSPs) représentant les utilisateurs d'un domaine sécurisé.

Essayez les étapes suivantes pour résoudre les problèmes :

- Synchronisez les groupes directement depuis le domaine approuvé : au lieu de synchroniser un groupe AWS Managed Microsoft AD contenant des membres provenant de plusieurs domaines, créez et synchronisez le groupe directement à partir du domaine local approuvé. Cette approche fonctionne car IAM Identity Center peut accéder à des objets utilisateur réels dans le domaine source.
- Vérifiez les autorisations du compte de service : assurez-vous que le compte de service IAM Identity Center dispose des autorisations requises sur les objets utilisateur du domaine sécurisé : ReadProperties et de l' ListContents autorisation.

Résoudre les problèmes liés aux clés gérées par le client dans AWS IAM Identity Center

Cette rubrique décrit les erreurs courantes liées aux clés gérées par le client que vous pouvez rencontrer lors de l'utilisation AWS IAM Identity Center et fournit des étapes de dépannage pour les résoudre.

Accès refusé : problème d'autorisation de déchiffrement KMS

Erreur : « L'utilisateur xxxxxxxx n'est pas autorisé à effectuer : kms: Déchiffrer la ressource associée à ce texte chiffré car aucune politique basée sur l'identité n'autorise l'action de déchiffrement » kms:

L'utilisateur ou le principal IAM ne dispose pas de l'kms : Decryptautorisation requise dans sa politique IAM ou dans sa politique de clé KMS.

Résolution des problèmes avec AWS CloudTrail :

1. Recherchez des kms . amazonaws . com événements dans CloudTrail

2. Rechercher le nom de l'événement Decrypt
3. Passez en revue les errorMessage champs errorCode et
4. Vérifiez userIdentity quel principal a tenté l'opération

Pour résoudre ce problème, accordez à l'utilisateur ou à l'IAM principal des autorisations kms:Decrypt d'accès dans sa politique IAM et sa politique de clé KMS. Pour de plus amples informations, veuillez consulter [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#).

AWS échecs de connexion aux applications gérées avec une clé KMS gérée par le client activée dans IAM Identity Center

Si aucun utilisateur d'Identity Center ne peut se connecter aux applications AWS gérées et qu'une clé KMS gérée par le client est activée dans votre instance IAM Identity Center, vérifiez que la politique de clé KMS autorise les applications AWS gérées à utiliser la clé KMS gérée par le client. Pour de plus amples informations, veuillez consulter [Déclarations de base relatives aux clés KMS et à la politique IAM](#).

AWS échec de l'installation d'applications gérées et de and/or l'attribution des utilisateurs lorsque la clé KMS gérée par le client est activée dans IAM Identity Center

Erreur : « L'utilisateur xxxxxxxx n'est pas autorisé à effectuer : kms: Déchiffrer la ressource associée à ce texte chiffré car aucune politique basée sur l'identité n'autorise l'action de déchiffrement » kms:

L'utilisateur ou le principal IAM ne dispose pas de l'kms:Decrypt autorisation requise dans sa politique IAM ou dans sa politique de clé KMS.

Résolution des problèmes avec CloudTrail :

1. Rechercher le nom de l'événement Decrypt
2. Passez en revue les errorMessage champs errorCode et
3. Vérifiez userIdentity quel principal a tenté l'opération

Pour résoudre ce problème, accordez à l'utilisateur ou à l'IAM principal des autorisations kms:Decrypt d'accès dans sa politique IAM et sa politique de clé KMS. Pour de plus amples

informations, veuillez consulter [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#).

Problème d'autorisations KMS : configuration de la clé gérée par le client avec AWS IAM Identity Center

L'utilisateur ou le principal IAM ne dispose pas d'une ou de plusieurs autorisations KMS requises (`kms:Decrypt`, `kms:Encrypt`, `kms:GenerateDataKey`, `kms:DescribeKey`) lors de l'activation de la clé gérée par le client.

Résolution des problèmes avec CloudTrail :

1. Rechercher `Decrypt`, `EncryptGenerateDataKey`, ou `DescribeKey` événements
2. Passez en revue les `errorMessage` champs `errorCode` et
3. Vérifiez `userIdentity` quel principal a tenté l'opération

Pour résoudre ce problème, accordez toutes les autorisations KMS requises à l'utilisateur ou au principal IAM dans sa politique basée sur l'identité ou sa politique de clé KMS. Pour de plus amples informations, veuillez consulter [Implémentation de clés KMS gérées par le client dans AWS IAM Identity Center](#).

AWS échecs de connexion au portail d'accès avec une clé KMS gérée par le client activée dans IAM Identity Center

Erreur : « Code d'erreur : 0001 - l'accès au IdentityCenter service est bloqué. Contactez votre IdentityCenter administrateur pour connaître les étapes à suivre. »

Si les utilisateurs ne peuvent pas se connecter au portail AWS d'accès et qu'une clé KMS gérée par le client est activée dans votre instance IAM Identity Center, vérifiez que la politique des clés KMS accorde les autorisations nécessaires à Identity Center et à Identity Store. Pour de plus amples informations, veuillez consulter [Déclarations de base relatives aux clés KMS et à la politique IAM](#).

Résoudre les problèmes de configuration multirégionale dans AWS IAM Identity Center

Cette rubrique décrit les erreurs courantes liées à la configuration multirégionale que vous pouvez rencontrer lors de l'utilisation AWS IAM Identity Center et fournit des étapes de dépannage pour les résoudre.

La région vers laquelle je souhaite répliquer mon instance IAM Identity Center n'est pas disponible dans la console IAM Identity Center

Vous devez d'abord créer une réplique de clé pour votre clé KMS gérée par le client dans la région dans laquelle vous souhaitez répliquer votre instance IAM Identity Center. Une fois la clé de réplique créée, vous verrez la région dans la liste des régions disponibles pour les répliques. Pour de plus amples informations, veuillez consulter [the section called “Étape 1 : Création d'une réplique de clé”](#).

AWS échecs de connexion à une application gérée dans une région supplémentaire

Si aucun utilisateur d'IAM Identity Center ne peut se connecter aux applications AWS gérées dans une région supplémentaire après avoir ajouté la région dans IAM Identity Center, vérifiez que vous avez configuré l'URL du service de consommation d'assertions (ACS) de la région supplémentaire dans le fournisseur d'identité externe, comme décrit dans [the section called “Étape 3 : Mettre à jour la configuration de l'IdP externe”](#). Vérifiez également que vos utilisateurs sont connectés à la région.

Historique du document

Le tableau suivant décrit les ajouts importants à la AWS IAM Identity Center documentation. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

- Dernière mise à jour majeure de la documentation : 21 octobre 2025

Modification	Description	Date
Support multirégional	Ajout du support multirégional, y compris la réplication vers des régions supplémentaires, Compte AWS l'accès et l'utilisation d'applications AWS gérées dans des régions supplémentaires.	2 février 2026
Politique AWS gérée mise à jour	Mise à jour de la politique AWSIdentityCenterExternalManagementPolicy AWS gérée pour modifier l'ARN pour le provisionnement du locataire.	5 décembre 2025
Nouveau sujet AWS relatif aux politiques gérées	Ajout de détails sur la politique AWSIdentityCenterExternalManagementPolicy AWS gérée.	21 novembre 2025
Conseils d'audit et de réconciliation relatifs au provisionnement automatique	Ajout de conseils pour l'audit et le rapprochement des utilisateurs, des groupes et des appartenances à des groupes provisionnés automatiquement par SCIM	17 octobre 2025

à l'aide d'Identity Store et de commandes. APIs AWS CLI

[Quotas de demandes de service OIDC](#)

Ajout de quotas de demandes de service OIDC, y compris des limites de débit pour l'enregistrement des OAuth clients, la création de jetons et d'autres opérations OIDC.

13 octobre 2025

[Mises à jour pour les politiques AWS gérées](#)

IAM Identity Center a mis à jour les politiques gérées AWS IAM Identity Center MasterAccountAdministrator, AWSSSOMemberAccountAdministrator, AWSSSODirectoryAdministrator, AWSSSODirectoryReadOnly, et AWSSSODirectoryReadOnly pour inclure AWS KMS les autorisations requises pour les instances IAM Identity Center qui utilisent des clés gérées par le client pour le chiffrement.

17 septembre 2025

[Clés gérées par le client pour le chiffrement au repos](#)

Ajout de la prise en charge des clés KMS gérées par le client pour chiffrer les données d'identité du personnel au repos.

17 septembre 2025

<u>Exemple de politique basée sur les ressources pour autoriser la création de jetons</u>	Ajout d'un exemple de politique basée sur les ressources qui permet la création de jetons pour les applications clientes autorisées.	16 septembre 2025
<u>Support pour les sessions d'arrière-plan des utilisateurs</u>	Ajout de contenu pour les sessions d'arrière-plan des utilisateurs.	11 août 2025
<u>Sessions de console à identité améliorée</u>	Terminologie mise à jour pour les sessions de console à identité améliorée (auparavant appelées sessions basées sur l'identité).	12 mai 2025
<u>Commencer la réorganisation</u>	Contenu de démarrage réorganisé pour améliorer la clarté et l'expérience utilisateur.	6 mai 2025
<u>Déconseiller IAM Identity Center AD Sync</u>	Vous ne pouvez plus approvisionner les utilisateurs d'Active Directory avec IAM Identity Center AD Sync. Au lieu de cela, vous pouvez utiliser AD Sync configurable par IAM Identity Center.	17 avril 2025
<u>Contenu mis à jour pour la session authentifiée</u>	Mise à jour des durées de session IAM Identity Center lorsque la session utilisateur est supprimée.	2 avril 2025

Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSSS0ServiceRolePolicy AWS gérée.	11 février 2025
Amélioration du flux de travail d'activation d'IAM Identity Center	Flux de travail mis à jour pour activer les instances d'organisation et les instances de compte d'IAM Identity Center.	11 février 2025
Mises à jour pour l'activation d'IAM Identity Center	Contenu et procédures mis à jour pour activer les instances d'organisation et les instances de compte d'IAM Identity Center.	10 octobre 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	2 octobre 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSSS0MasterAccountAdministrator AWS gérée.	26 septembre 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	4 septembre 2024
Mises à jour de la rubrique « Qu'est-ce qu'IAM Identity Center ? » topic	Mise à jour du contenu décrivant les avantages et les fonctionnalités d'IAM Identity Center.	19 août 2024

Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	12 juillet 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	27 juin 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	17 mai 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	30 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSSSOMasterAccountAdministrator AWS gérée.	26 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSSSOMemberAccountAdministrator AWS gérée.	26 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSSSODeveloperAccessAWS gérée.	26 avril 2024

Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	26 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	24 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	19 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	11 avril 2024
Mises à jour pour les politiques AWS gérées	Autorisations mises à jour pour la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	26 novembre 2023
Nouveau sujet AWS relatif aux politiques gérées	Ajout de détails sur la politique AWSIAMIdentityCenterAllowListForIdentityContext AWS gérée.	15 novembre 2023

[Conseils améliorés pour démarrer avec IAM Identity Center](#)

Ajout de nouveau contenu pour démarrer avec IAM Identity Center et créer un utilisateur administratif

23 septembre 2022

[Utilisateurs et groupes mis à jour dans la référence d'API Identity Center](#)

Cette mise à jour inclut des références aux nouveaux outils Create, Update and Delete APIs dans le guide de référence de l'API Identity Center.

31 août 2022

[AWS Authentication unique \(AWS SSO\) renommée en AWS IAM Identity Center](#)

AWS présente AWS IAM Identity Center. IAM Identity Center étend les fonctionnalités de Gestion des identités et des accès AWS (IAM) pour vous aider à gérer de manière centralisée les comptes et l'accès aux applications pour les utilisateurs de votre personnel. Les fonctionnalités d'IAM Identity Center incluent les attributions d'applications, les autorisations multi-comptes et un portail d' AWS accès.

26 juillet 2022

[Support des limites d'autorisations et des politiques gérées par le client dans les ensembles d'autorisations](#)

Ajout de contenu pour l'utilisation de politiques AWS gérées et gérées par le client Gestion des identités et des accès AWS (IAM) avec des ensembles d'autorisations.

14 juillet 2022

<u>Support pour les AWS régions activées manuellement</u>	Ajout de contenu pour l'utilisation d'IAM Identity Center dans les régions activées manuellement.	15 juin 2022
<u>Mises à jour pour les politiques AWS gérées</u>	Autorisations mises à jour pour la politique <code>AWSSS0ServiceRolePolicy</code> AWS gérée.	11 mai 2022
<u>Support pour l'administration déléguée</u>	Ajout de contenu pour la fonctionnalité d'administration déléguée.	11 mai 2022
<u>Mises à jour pour les politiques AWS gérées</u>	Autorisations mises à jour pour le <code>AWSSS0MasterAccountAdministrator</code> <code>AWSSS0MemberAccountAdministrator</code> , et les politiques <code>AWSSS0ReadOnly</code> AWS gérées.	28 avril 2022
<u>Support pour la synchronisation AD configurable</u>	Ajout de contenu pour la fonctionnalité configurable de synchronisation AD.	14 avril 2022
<u>Nouveau sujet AWS relatif aux politiques gérées</u>	Ajout de détails sur la politique <code>AWSSS0MasterAccountAdministrator</code> AWS gérée.	4 août 2021
<u>Mises à jour des quotas</u>	Ajustements des tableaux de quotas.	21 décembre 2020

Nouveaux exemples de politiques	De nouveaux exemples de politiques gérées par le client ont été ajoutés et des mises à jour ont été apportées à la section des autorisations requises.	21 décembre 2020
Support pour le contrôle d'accès basé sur les attributs (ABAC)	Ajout de contenu pour la fonctionnalité ABAC.	24 novembre 2020
Support à l'inscription forcée au MFA	Mises à jour pour obliger les utilisateurs à inscrire un appareil MFA lors de la connexion.	23 novembre 2020
Support pour WebAuthn	Du contenu a été ajouté pour WebAuthn une nouvelle fonctionnalité.	20 novembre 2020
Support pour Ping Identity	Ajout de contenu à intégrer aux Ping Identity produits en tant que fournisseur d'identité externe pris en charge.	26 octobre 2020
Support pour OneLogin	Ajout de contenu à intégrer en OneLogin tant que fournisseur d'identité externe pris en charge.	31 juillet 2020
Prise en charge pour Okta	Ajout de contenu à intégrer en Okta tant que fournisseur d'identité externe pris en charge.	28 mai 2020

<u>Support pour les fournisseurs d'identité externes</u>	Modification des références du répertoire à la source d'identité, ajout de contenu pour prendre en charge les fournisseurs d'identité externes.	26 novembre 2019
<u>Nouveaux paramètres MFA</u>	Suppression de la rubrique de validation en deux étapes et ajout d'une nouvelle rubrique MFA à sa place.	24 octobre 2019
<u>Nouveau paramètre pour ajouter la validation en deux étapes</u>	Ajout de contenu expliquant comment activer la validation en deux étapes pour les utilisateurs.	16 janvier 2019
<u>Support de la durée de session sur les AWS comptes</u>	Ajout de contenu expliquant comment définir la durée de session d'un AWS compte.	30 octobre 2018
<u>Nouvelle option pour utiliser le répertoire Identity Center</u>	Ajout de contenu permettant de choisir le répertoire Identity Center ou de se connecter à un répertoire existant dans Active Directory.	17 octobre 2018
<u>Support de l'état du relais et de la durée de session sur les applications</u>	Ajout de contenu sur l'état du relais et la durée de session pour les applications.	10 octobre 2018

[Support supplémentaire pour les nouvelles applications](#)

Ajouté 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, et UserEcho au catalogue d'applications.

3 août 2018

[Support pour l'accès multicompte aux comptes de gestion](#)

Ajout de contenu expliquant comment déléguer l'accès à plusieurs comptes aux utilisateurs d'un compte de gestion.

9 juillet 2018

[Support pour les nouvelles applications](#)

Ajouté DocuSign, Keeper Security, et SugarCRM au catalogue d'applications.

16 mars 2018

[Obtenir des informations d'identification temporaires pour l'accès à la CLI](#)

Ajout d'informations sur la façon d'obtenir des informations d'identification temporaires pour exécuter AWS CLI des commandes.

le 22 février 2018

[Nouveau guide](#)

Il s'agit de la première version du guide de l'utilisateur d'IAM Identity Center.

7 décembre 2017

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le [AWS glossaire](#) dans la Glossaire AWS référence.

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.