



Informations de sécurité

Catalogue AWS Control



Catalogue AWS Control: Informations de sécurité

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 Control Catalog ?	1
Vue d'ensemble de l'ontologie	1
Accès au catalogue de contrôle	3
Sécurité	4
Protection des données	5
Chiffrement des données	6
Chiffrement en transit	6
Gestion des clés	6
Confidentialité du trafic inter-réseaux	6
Gestion des identités et des accès	6
Public ciblé	7
Authentification par des identités	7
Gestion de l'accès à l'aide de politiques	9
Fonctionnement de Control Catalog avec IAM	10
Exemples de politiques basées sur l'identité	17
Résolution des problèmes	20
Validation de conformité	23
Résilience	23
Sécurité de l'infrastructure	23
Configuration et vulnérabilités	24
Contrôle	25
CloudTrail journaux	25
Informations du catalogue de contrôle dans CloudTrail	25
Comprendre les entrées du fichier journal de Control Catalog	27
AWS PrivateLink	29
Considérations	29
Création d'un point de terminaison d'interface	29
Création d'une politique de point de terminaison	30
Historique de la documentation	32
.....	xxxiii

Qu'est-ce que Control Catalog ?

Bienvenue dans le guide d'informations de sécurité de Control Catalog. Le catalogue de contrôles fait partie de AWS Control Tower, qui répertorie les contrôles pour plusieurs AWS services. Il s'agit d'un catalogue consolidé de AWS contrôles. Vous n'avez pas besoin de configurer AWS Control Tower pour utiliser le catalogue de contrôle.

Avec le catalogue de contrôles, vous pouvez visualiser les commandes en fonction des cas d'utilisation courants, notamment en matière de sécurité, de coût, de durabilité et de fonctionnement.

Dans ce document, vous trouverez les informations de sécurité et de conformité que vous devez connaître lorsque vous utilisez les APIs informations fournies par Control Catalog.

Le catalogue de contrôles intègre une ontologie de contrôle, qui est un système de classification standard pour les contrôles.

Vue d'ensemble de l'ontologie

AWS a développé un système de classification standard pour aider à classer, organiser et créer des mappages entre les contrôles. Cette ontologie peut être utilisée pour mapper les contrôles aux normes réglementaires existantes et nouvelles, y compris 24 cadres, ainsi qu'aux normes réglementaires telles que PCI, HIPAA, etc. Nous nous adaptons également aux normes du secteur telles que le NIST et l'ISO, ainsi qu'aux frameworks spécifiques à Amazon, notamment le framework Well-Architected.

L'ontologie comporte quatre aspects fondamentaux

- Classification des contrôles par domaine de contrôle, objectif de contrôle et contrôles communs. L'ontologie permet d'organiser et de regrouper les contrôles associés en trois niveaux :
 - L1 : domaine de contrôle,
 - L2 : objectif de contrôle,
 - L3 : Contrôle commun.

Ces niveaux ont une relation hiérarchique stricte. En d'autres termes, chaque domaine a plusieurs objectifs de contrôle, mais chaque objectif de contrôle doit avoir un seul domaine parent. Chaque objectif de contrôle possède plusieurs contrôles communs, mais chaque contrôle commun a un seul objectif parent.

- Cartographie selon les normes réglementaires. L'ontologie repose sur un concept appelé contrôle standard (L4) qui représente une exigence spécifique au sein d'une norme réglementaire ou industrielle. Ces contrôles standard sont mappés aux contrôles communs qui permettent de répondre à ces exigences spécifiques.

Par exemple, PCI-DSS v3.2.1. ID 4.1 Utilisez des protocoles de cryptographie et de sécurité robustes pour protéger les données sensibles des titulaires de cartes lors de la transmission sur des réseaux publics ouverts et NIST 800.53.r5 ID SC-16 La transmission des attributs de sécurité et de confidentialité est deux contrôles standard, tous deux mappés au contrôle commun Chiffrer les données en transit.

- Implémentations de contrôle et preuves de contrôle. L'ontologie repose sur un concept d'implémentations de contrôle (L6) qui peut représenter soit une implémentation de contrôle spécifique dans AWS, par exemple, un AWS Control Tower contrôle, une AWS Security Hub CSPM vérification, une AWS Config règle, etc., soit une implémentation externe non technique AWS, telle que le guidage de processus. Un concept distinct de preuve de contrôle (L7) représente les sources de données qui peuvent être utilisées comme preuve pour les contrôles effectués par AWS Audit Manager des outils tiers ou par les clients eux-mêmes. Ces sources de preuves peuvent être AWS des sources telles que AWS CloudTrail des événements, des journaux d'appels d'API et des résultats d'évaluation des AWS Config règles. Il peut également s'agir de sources externes telles que la documentation client.
- Le concept d'un contrôle central (L5). Le contrôle de base est une couche cartographique qui consolide toutes les implémentations de contrôle (L6), les sources de preuves correspondantes (L7), les contrôles standard associés (L4) et les contrôles communs (L3) en un seul objet holistique. Le contrôle de base est davantage un document de mappage qu'un contrôle lui-même. Cela permet de répondre à la question de me montrer toutes les informations relatives au contrôle X. Chaque contrôle de base peut avoir plusieurs implémentations de contrôle (L6) et plusieurs sources de preuves (L7).

En résumé, l'ontologie du catalogue de AWS contrôles contient sept couches. Trois sont des couches de classification hiérarchiques (domaines de contrôle, objectifs de contrôle, contrôles communs). Une autre couche (contrôles standard) décrit les exigences réglementaires ou industrielles. Une couche de mappage (contrôle central) décrit un résultat de contrôle pour un type de ressource donné. Deux couches (implémentations de contrôle, preuves de contrôle) décrivent les implémentations de contrôle spécifiques et les sources de preuves.

Cette ontologie a été conçue par une AWS équipe d'auditeurs certifiés, sur la base de leur expérience de travail avec des centaines de clients dans le cadre d'audits de conformité. Les

concepts de domaines de contrôle, d'objectifs de contrôle, de contrôles communs et de contrôles standard (L1-L4) sont utilisés dans l'ensemble de l'industrie. Ils correspondent aux modèles industriels courants et aux recommandations du NIST. Les trois couches restantes (L5-L7) ont été conçues sur la base de AWS concepts existants, tels que les types de ressources et les contrôles gérés.

Accès au catalogue de contrôle

Control Catalog est disponible via la console et via l'interface de programmation d'applications (API) Control Catalog. Cette API fournit un moyen programmatique d'identifier et de filtrer les contrôles courants et les métadonnées associées qui sont à votre disposition en tant que AWS client. Pour plus d'informations, consultez le manuel de [référence de l'API Control Catalog](#).

Catalogue de sécurité dans Control

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures 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 ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS 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 [AWS conformité Programmes](#) de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Control Catalog, voir [AWS Services concernés par programme de conformité Services AWS](#) .
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce 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 de Control Catalog ;. Les rubriques suivantes expliquent comment configurer Control Catalog afin d'atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres ressources Services AWS qui vous aident à surveiller et à sécuriser vos ressources Control Catalog.

Rubriques

- [Protection des données dans Control Catalog](#)
- [Gestion des identités et des accès pour Control Catalog](#)
- [Validation de conformité pour Control Catalog](#)
- [Resilience in Control Catalog](#)
- [Catalogue de sécurité de l'infrastructure dans Control](#)

Protection des données dans Control Catalog

Le [modèle de responsabilité AWS partagée](#) s'applique à la protection des données dans AWS Control Catalog. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog [Modèle de responsabilité partagée d'AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les 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 qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

Nous vous recommandons fortement 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 libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec AWS Control Catalog ou autre Services AWS

à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données

AWS Control Catalog ne stocke aucune donnée client.

Chiffrement au repos

AWS Control Catalog ne chiffre pas les données des clients. Aucune donnée client n'étant conservée ou conservée par AWS Control Catalog, il n'existe aucune directive spécifique concernant le chiffrement.

Chiffrement en transit

AWS Control Catalog ne chiffre pas les données des clients. Étant donné qu'aucune donnée sensible n'est échangée ou conservée par AWS Control Catalog, il n'existe aucune directive spécifique pour le chiffrement en transit.

Gestion des clés

La gestion des clés de chiffrement ne s'applique pas à AWS Control Catalog.

Confidentialité du trafic inter-réseaux

La confidentialité du trafic interréseau ne s'applique pas à AWS Control Catalog.

Gestion des identités et des accès pour Control Catalog

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources du catalogue de contrôle AWS. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion de l'accès à l'aide de politiques](#)
- [Fonctionnement de Control Catalog avec IAM](#)
- [Exemples de politiques basées sur l'identité pour Control Catalog](#)
- [Résolution des problèmes d'identité et d'accès au catalogue de contrôle](#)

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir [Résolution des problèmes d'identité et d'accès au catalogue de contrôle](#))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir [Fonctionnement de Control Catalog avec IAM](#))
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir [Exemples de politiques basées sur l'identité pour Control Catalog](#))

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez [Connexion à votre Compte AWS](#) dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez [Signature AWS Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez [Tâches qui requièrent les informations d'identification de l'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir [Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires](#) dans le guide de l'utilisateur IAM.

[Les groupes IAM](#) spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en [passant d'un rôle d'utilisateur à un rôle IAM \(console\)](#) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de

compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez [Politiques de contrôle de service](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir [Politiques de contrôle des ressources \(RCPs\)](#) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de l'utilisateur IAM.

Fonctionnement de Control Catalog avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Control Catalog, découvrez quelles fonctionnalités IAM peuvent être utilisées avec AWS Control Catalog.

Fonctionnalités IAM que vous pouvez utiliser avec Control Catalog

Fonctionnalité IAM	Support d'AWS Control Catalog
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principaux	Non
Rôles du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AWS Control Catalog et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les [AWS services compatibles avec IAM](#) dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AWS Control Catalog

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez [Références des éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour AWS Control Catalog

Pour consulter des exemples de politiques basées sur l'identité d'AWS Control Catalog, consultez. [Exemples de politiques basées sur l'identité pour Control Catalog](#)

Politiques basées sur les ressources dans AWS Control Catalog

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Actions de politique pour AWS Control Catalog

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions d'AWS Control Catalog, consultez la section [Actions définies par AWS Control Catalog](#) dans la référence d'autorisation de service.

Les actions de politique dans AWS Control Catalog utilisent le préfixe suivant avant l'action :

```
controlcatalog
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [  
  "controlcatalog:ListCommonControls",  
  "controlcatalog:ListDomains"  
]
```

Vous pouvez aussi préciser plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot List, incluez l'action suivante.

```
"Action": "controlcatalog:List*"
```

Pour consulter des exemples de politiques basées sur l'identité d'AWS Control Catalog, consultez [Exemples de politiques basées sur l'identité pour Control Catalog](#)

Ressources relatives aux politiques pour AWS Control Catalog

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON Resource indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources du catalogue AWS Control et de leurs caractéristiques ARNs, consultez la section [Ressources définies par AWS Control Catalog](#) dans la référence

d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez [Actions définies par AWS Control Catalog](#).

Un domaine AWS Control Catalog possède le format Amazon Resource Name (ARN) suivant :

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

Un objectif AWS Control Catalog possède le format ARN suivant :

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

Un contrôle commun d'AWS Control Catalog possède le format ARN suivant :

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

Pour plus d'informations sur le format de ARNs, consultez [Amazon Resource Names \(ARNs\)](#).

Par exemple, pour spécifier le `i-1234567890abcdef0` domaine dans votre relevé, utilisez l'ARN suivant.

```
"Resource": "arn:aws:controlcatalog:::domain/i-1234567890abcdef0"
```

Pour spécifier toutes les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*).

```
"Resource": "arn:aws:controlcatalog:::domain/*"
```

Certaines actions d'AWS Control Catalog, telles que celles relatives à la création de ressources, ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

Certaines actions de l'API AWS Control Catalog prennent en charge plusieurs ressources. Par exemple, il `ListCommonControls` accède à un contrôle commun, à un objectif et à un domaine, de sorte qu'un principal doit être autorisé à accéder à chacune de ces ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules.

```
"Resource": [  
  "commonControl",  
  "objective",  
  "domain"
```

Pour consulter des exemples de politiques basées sur l'identité d'AWS Control Catalog, consultez.

[Exemples de politiques basées sur l'identité pour Control Catalog](#)

Clés de conditions de politique pour AWS Control Catalog

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition d'AWS Control Catalog, consultez la section [Clés de condition pour AWS Control Catalog](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez [Actions définies par AWS Control Catalog](#).

Pour consulter des exemples de politiques basées sur l'identité d'AWS Control Catalog, consultez.

[Exemples de politiques basées sur l'identité pour Control Catalog](#)

ACLs dans AWS Control Catalog

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec AWS Control Catalog

Prise en charge d'ABAC (balises dans les politiques) : non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'[élément de condition](#) d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez [Définition d'autorisations avec l'autorisation ABAC](#) dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez [Utilisation du contrôle d'accès par attributs \(ABAC\)](#) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS Control Catalog

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#) et [Services AWS compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour AWS Control Catalog

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section [Sessions de transmission d'accès](#).

Rôles de service pour AWS Control Catalog

Prend en charge les rôles de service : Non

Un rôle de service est un [rôle IAM](#) qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

Warning

La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités d'AWS Control Catalog. Modifiez les rôles de service uniquement lorsque AWS Control Catalog fournit des instructions à cet effet.

Rôles liés à un service pour AWS Control Catalog

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez [Services AWS qui fonctionnent avec IAM](#). Recherchez un service dans le tableau qui inclut un Yes dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Control Catalog

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources du catalogue AWS Control. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Control Catalog, y compris le ARNs format de chaque type de ressource, consultez la section [Actions, ressources et clés de condition pour AWS Control Catalog](#) dans la référence d'autorisation de service.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)
- [Autoriser les utilisateurs à consulter les ressources d'AWS Control Catalog](#)

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS Control Catalog dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez [politiques gérées par AWS](#) ou [politiques gérées par AWS pour les activités professionnelles](#) dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule 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. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles.

Pour plus d'informations, consultez [Validation de politiques avec IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",

```

```
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

Autoriser les utilisateurs à consulter les ressources d'AWS Control Catalog

La politique suivante accorde des autorisations pour répertorier les domaines, les objectifs et les contrôles courants à partir d'AWS Control Catalog.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageControlCatalogAccess",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

Résolution des problèmes d'identité et d'accès au catalogue de contrôle

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d'AWS Control Catalog et d'IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans Control Catalog](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite donner à des personnes extérieures à moi l' Compte AWS accès aux ressources de mon catalogue de contrôle](#)

Je ne suis pas autorisé à effectuer une action dans Control Catalog

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM mateojackson tente d'utiliser la console pour afficher des informations détaillées sur une ressource *my-example-widget* fictive, mais ne dispose pas des autorisations `controlcatalog:GetWidget` fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
controlcatalog:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur mateojackson doit être mise à jour pour autoriser l'accès à la ressource *my-example-widget* à l'aide de l'action `controlcatalog:GetWidget`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole` action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AWS Control Catalog.

Certains vos Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé marymajor essaie d'utiliser la console pour effectuer une action dans AWS Control Catalog. Toutefois, l'action nécessite que le

service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite donner à des personnes extérieures à moi l' Compte AWS accès aux ressources de mon catalogue de contrôle

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si AWS Control Catalog prend en charge ces fonctionnalités, consultez [Fonctionnement de Control Catalog avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section [Fournir un accès à des ressources Comptes AWS détenues par des tiers](#) dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez [Fournir un accès à des utilisateurs authentifiés en externe \(fédération d'identité\)](#) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Validation de conformité pour Control Catalog

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](#).

Resilience in Control Catalog

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS 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 à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Catalogue de sécurité de l'infrastructure dans Control

En tant que service géré, Control Catalog est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc [Amazon Web Services : présentation des processus de sécurité](#).

Vous utilisez des appels d'API AWS publiés pour accéder au catalogue de contrôle via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous vous recommandons le certificat TLS 1.2 ou une version ultérieure. Les clients doivent aussi prendre en charge les 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.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Analyse de configuration et de vulnérabilité dans Control Catalog

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le [modèle de responsabilité AWS partagée](#).

Surveillance d'AWS Control Catalog

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'AWS Control Catalog et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Control Catalog, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter le [Guide de l'utilisateur AWS CloudTrail](#).

Journalisation des appels d'API Control Catalog à l'aide AWS CloudTrail

Dans le cadre de AWS Control Tower Control Catalog AWS CloudTrail, un service est intégré à un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture tous les appels d'API pour Control Catalog sous forme d'événements. Les appels capturés incluent des appels provenant directement de la AWS Control Tower console, par exemple pour activer ou désactiver un contrôle, et des appels de code vers les opérations de l'API Control Catalog. Si vous créez un suivi, vous pouvez activer la diffusion continue d'CloudTrail événements vers un compartiment Amazon S3, y compris les événements relatifs aux contrôles de Control Catalog. 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 Control Catalog (au moyen de AWS Control Tower), l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations du catalogue de contrôle dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Control Catalog, 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 à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre site Compte AWS, y compris des événements pour Control Catalog, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions 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 en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [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](#)

Toutes les actions du Control Catalog sont enregistrées CloudTrail et sont documentées dans le manuel de [référence de l'API Control Catalog](#). Par exemple, les appels aux `ListCommonControlsListObjectives`, et `ListDomains` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

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 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.

Pour de plus amples informations, veuillez consulter l'[élément userIdentity CloudTrail](#) .

Comprendre les entrées du fichier journal de Control Catalog

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. 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 fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListDomains` action.

```
{
  eventVersion:"1.05",
  userIdentity:{
    type:"IAMUser",
    principalId:"principalId",
    arn:"arn:aws:iam::accountId:user/userName",
    accountId:"111122223333",
    accessKeyId:"accessKeyId",
    userName:"userName",
    sessionContext:{
      sessionIssuer:{
      },
      webIdFederationData:{
      },
      attributes:{
        mfaAuthenticated:"false",
        creationDate:"2020-11-19T07:32:06Z"
      }
    }
  },
  eventTime:"2020-11-19T07:32:36Z",
  eventSource:"controlcatalog.amazonaws.com",
  eventName:"ListDomains",
  awsRegion:"us-west-2",
  sourceIPAddress:"sourceIPAddress",
  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,
  requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
```

```
eventID:"a782029a-959e-4549-81df-9f6596775cb0",  
readOnly:false,  
eventType:"AwsApiCall",  
recipientAccountId:"recipientAccountId"  
}
```

Catalogue de contrôle d'accès à l'aide d'un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et Control Catalog. Vous pouvez accéder au catalogue de AWS contrôle comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder au catalogue de contrôle.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à Control Catalog.

Pour plus d'informations, consultez la section [Accès Services AWS par AWS PrivateLink le biais](#) du AWS PrivateLink guide.

Considérations relatives à AWS Control Catalog

Avant de configurer un point de terminaison d'interface pour Control Catalog, consultez les [considérations](#) du AWS PrivateLink guide.

Control Catalog permet d'appeler toutes ses actions d'API via le point de terminaison de l'interface.

Création d'un point de terminaison d'interface pour Control Catalog

Vous pouvez créer un point de terminaison d'interface pour Control Catalog à l'aide de la console Amazon VPC ou du AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez [Création d'un point de terminaison d'interface](#) dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour Control Catalog en utilisant le nom de service suivant :

```
com.amazonaws.region.controlcatalog
```

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à Control Catalog en utilisant son nom DNS régional par défaut. Par exemple, `service-name.us-east-1.amazonaws.com`.

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d'interface. La politique de point de terminaison par défaut autorise un accès complet à Control Catalog via le point de terminaison de l'interface. Pour contrôler l'accès autorisé à Control Catalog depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :


- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

Pour plus d'informations, consultez [Contrôle de l'accès aux services à l'aide de politiques de point de terminaison](#) dans le Guide AWS PrivateLink .

Exemple : politique de point de terminaison VPC pour les actions du catalogue de contrôle

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle accorde l'accès aux actions du catalogue de AWS contrôle répertoriées pour tous les principaux sur toutes les ressources.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

 Note

Les opérations `GetControl` et `ListControls` API nécessitent une autorisation différente, l'autorisation complète par défaut. Pour un exemple, consultez [la politique de point de terminaison par défaut](#).

Historique des documents pour le guide d'informations de sécurité de Control Catalog

Le tableau suivant décrit les versions de documentation de Control Catalog.

Modification	Description	Date
Première version	Publication initiale du catalogue de contrôle APIs et du guide d'informations de sécurité.	8 avril 2024

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.