



Informations de sécurité

AWS Control Catalog



AWS Control Catalog: Informations de sécurité

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez 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	8
Gestion des accès à l'aide de politiques	12
Fonctionnement d'avec IAM	15
Exemples de politiques basées sur l'identité	23
Résolution des problèmes	26
Validation de conformité	28
Résilience	30
Sécurité de l'infrastructure	30
Configuration et vulnérabilités	30
Surveillance	31
CloudTrail journaux	31
Informations du catalogue de contrôle dans CloudTrail	31
Présentation des entrées des fichiers journaux du catalogue	33
AWS PrivateLink	35
Considérations	35
Création d'un point de terminaison d'interface	35
Création d'une politique de point de terminaison	36
Historique de la documentation	38
.....	xxxix

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 Control Catalog.

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 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 la [Référence de l'API de Control Catalog](#).

Catalogue de sécurité dans Control

Chez, la sécurité du cloud AWS est la priorité numéro 1. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le [modèle de responsabilité partagée](#) décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud — AWS est responsable de la protection de 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 vérificateurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité programmes de [AWS conformité programmes](#) de de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Control Catalog, consultez [AWS Services concernés par le programme de conformité Services AWS](#) .
- Sécurité dans le cloud — Votre responsabilité est fonction du Service AWS 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 lorsque vous utilisez Control Catalog ; Les rubriques suivantes expliquent comment configurer Control Catalog pour répondre à vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres Services AWS qui vous aident à surveiller et à sécuriser votre catalogue de contrôle ; ressources.

Rubriques

- [Protection des données dans Control Catalog](#)
- [Gestion des identités et des accès pour Control Catalog](#)
- [Validation de la conformité pour Control Catalog](#)
- [Résilience dans Control Catalog](#)
- [Sécurité de l'infrastructure dans Control Catalog](#)

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 responsable de la protection de l'infrastructure globale qui fait fonctionner 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 AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécurité AWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (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.
- Utilisez SSL/TLS pour communiquer avec des ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités utilisateur 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 des 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 FIPS (Federal Information Processing Standard) 140-3 lorsque vous accédez à AWS via une interface de ligne de commande ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing 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

AWS Identity and Access Management (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (être connecté) et autorisé (disposer des autorisations) à utiliser les ressources AWS Control Catalog. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

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

Public ciblé

Votre utilisation d' AWS Identity and Access Management (IAM) diffère selon la tâche que vous accomplissez dans AWS Control Catalog.

Utilisateur du service : si vous utilisez le service AWS Control Catalog pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités AWS Control Catalog pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS Control Catalog, consultez [Résolution des problèmes d'identité et d'accès avec Control Catalog](#).

Administrateur du service : si vous êtes le responsable des ressources AWS Control Catalog de votre entreprise, vous bénéficiez probablement d'un accès total à AWS Control Catalog. Votre responsabilité est de déterminer les fonctionnalités et les ressources AWS Control Catalog auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec AWS Control Catalog, consultez [Fonctionnement d'avec IAM](#).

Administrateur IAM : si vous êtes un administrateur IAM, vous souhaitez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS Control Catalog. Pour obtenir des exemples de politiques AWS Control Catalog basées sur l'identité que vous pouvez utiliser dans IAM, consultez. [Exemples de politiques basées sur l'identité pour Control Catalog](#)

Authentification par des identités

L'authentification correspond au processus par lequel vous connectez à AWS l'aide de vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à en AWS tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification de connexion unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos requêtes à l'aide de vos informations d'identification. Si vous n'utilisez pas AWS les outils, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez [AWS Signature Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, vous AWS recommande d'utiliser la Multi-Factor Authentication (MFA) pour améliorer la sécurité de votre compte. Pour plus d'informations, consultez [Authentification multifactorielle](#) dans le Guide de l'utilisateur AWS IAM Identity Center et [Authentification multifactorielle AWS dans IAM](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur racine

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée l'utilisateur Compte AWS racine du. Vous pouvez y accéder en vous connectant à l'aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez

vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez [Tâches nécessitant des informations d'identification d'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à en Services AWS utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité web AWS Directory Service, l'annuaire Identity Center ou tout utilisateur qui accède à en Services AWS utilisant des informations d'identification fournies via une source d'identité. Quand des identités fédérées accèdent à Comptes AWS, elles assument des rôles, ces derniers fournissant des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications Comptes AWS et de vos. Pour obtenir des informations sur IAM Identity Center, 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 dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification](#) dans le Guide de l'utilisateur IAM.

Un [groupe IAM](#) est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations

pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdminset accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. 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 au sein de votre Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour endosser temporairement un rôle IAM dans l'AWS Management Console, vous pouvez [passer d'un rôle utilisateur à un rôle IAM \(console\)](#). Vous pouvez endosser un rôle en appelant une opération de l'interface AWS CLI ou une opération d'API, ou à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- **Accès utilisateur fédéré** : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .
- **Autorisations d'utilisateur IAM temporaires** : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- **Accès intercompte** : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois Services AWS, certains vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les

ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

- Accès services multiples : certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant pour ce service d'exécuter des applications dans Amazon EC2 ou de stocker des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- Transmission de sessions d'accès (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions dans AWS, vous êtes considéré comme principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal qui appelle Service AWS, combinées Service AWS à qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).
- Rôle de service : il s'agit d'un [rôle IAM](#) attribué à un service afin de réaliser 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.
- Rôle lié à un service : 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 s'affichent dans votre Compte AWS et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications s'exécutant sur Amazon EC2 : Vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une EC2 instance et effectuant des demandes d' AWS API AWS CLI ou. Cette solution est préférable au stockage des clés d'accès au sein de l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour de plus amples informations, veuillez consulter [Utiliser un rôle IAM pour accorder des autorisations aux applications s'exécutant sur des EC2 instances Amazon](#) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans en AWS créant des stratégies et en les attachant à AWS des identités ou à des ressources. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, session de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans en AWS tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les stratégies 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.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

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.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les stratégies gérées sont des stratégies autonomes que vous pouvez attacher à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les stratégies gérées incluent les stratégies AWS gérées par et les stratégies gérées par le client. Pour découvrir comment choisir entre une

politique gérée et une politique 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. 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 utilisateurs, des utilisateurs, des utilisateurs fédérés ou des Services AWS.

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

Listes de contrôle d'accès (ACLs)

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

Amazon S3, AWS WAF, et Amazon VPC sont des exemples de services prenant en charge. ACLs. Pour en savoir plus ACLs, consultez [Présentation des listes de contrôle d'accès \(ACL\)](#) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limite d'autorisations** : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur

l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.

- **Stratégies de contrôle de service (SCPs)** : SCPs sont des stratégies JSON qui spécifient les autorisations maximales pour une organisation ou une unité d'organisation (UO) dans AWS Organizations. AWS Organizations est un service Comptes AWS qui vous permet de regrouper et de gérer de façon centralisée plusieurs détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les stratégies de contrôle de service (SCPs) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les [politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.
- **Politiques de contrôle des ressources (RCPs)** : RCPs sont des politiques JSON que vous pouvez utiliser pour définir le nombre maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. La RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris le Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, voir [Politiques de contrôle des ressources \(RCPs\)](#) dans le guide de AWS Organizations l'utilisateur.
- **Politiques de séance** : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. 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 découvrir la façon dont AWS détermine s'il convient d'autoriser une demande lorsque plusieurs types de stratégies sont impliqués, veuillez consulter [Logique d'évaluation de stratégies](#) dans le Guide de l'utilisateur IAM.

Fonctionnement d'avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Control Catalog, découvrez les fonctionnalités IAM que vous pouvez utiliser 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
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AWS Control Catalog et d'autres AWS services fonctionnent avec la plupart des fonctions d'IAM, consultez [AWS services that work with IAM \(Services qui fonctionnent avec IAM\)](#) 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. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. 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 voir des exemples de politiques AWS Control Catalog basées sur l'identité, consultez. [Exemples de politiques basées sur l'identité pour Control Catalog](#)

Politiques basées sur une ressource 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 utilisateurs, des utilisateurs, des utilisateurs fédérés ou des. 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. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans des différents Comptes AWS, un administrateur IAM dans le compte approuvé doit également accorder à l'entité principal (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache

une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. 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 stratégies 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. Les actions de stratégie possèdent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

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 voir des exemples de politiques AWS Control Catalog basées sur l'identité, 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 stratégies 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. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, 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 grâce à 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 d'Amazon Resource Name (ARN) suivant :

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

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

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

Un contrôle commun AWS Control Catalog possède le format d'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 instruction, 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 AWS Control Catalog, telles que la création de ressources, ne peuvent pas être exécutées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

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

Certaines actions d'API AWS Control Catalog prennent en charge plusieurs ressources. Par exemple, `ListCommonControls` accède à un contrôle commun, à un objectif et à un domaine, donc un principal doit disposer d'autorisations d'accès à chacune de ces ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARNs par des virgules.

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

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

Clés de condition de politique pour AWS Control Catalog

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

Les administrateurs peuvent utiliser les stratégies 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` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. 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.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération AND logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez [Éléments d'une politique IAM : variables et identifications](#) dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition AWS globales, veuillez consulter [Clés de contexte de condition AWS globales](#) dans le Guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition AWS Control Catalog, veuillez consulter la rubrique [Clés de condition pour AWS Control Catalog](#) dans le document de référence de l'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 obtenir des exemples de politiques AWS Control Catalog basées sur l'identité, 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) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. ACLs sont semblables 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 des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez attacher des balises à des entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

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 des informations d'identification temporaires avec AWS Control Catalog

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas quand vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les Services AWS fonctionnent avec des informations d'identification temporaires, consultez [Services AWS qui fonctionnent avec IAM](#) dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à la en AWS Management Console utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, ce processus crée automatiquement des informations d'identification temporaires. Vous

créés également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez [Passage d'un rôle utilisateur à un rôle IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS CLI ou de AWS l'API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS vous recommande de générer des informations d'identification temporaires de façon dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#).

Autorisations principales entre services pour AWS Control Catalog

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

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions dans AWS, vous êtes considéré comme mandataire. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal qui appelle Service AWS, combinées Service AWS à qui demande pour effectuer des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande dont l'exécution nécessite des interactions avec d'autres Services AWS ou ressources. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions 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 d'une fonction du service peut altérer la fonctionnalité AWS Control Catalog. Ne modifiez des fonctions du service que quand AWS Control Catalog le conseille.

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 s'affichent dans votre Compte AWS et sont la propriété du 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 ni à modifier les ressources AWS Control Catalog. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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 format de ARNs pour chacun des types de ressources, veuillez consulter [Actions, ressources et clés de condition pour AWS Control Catalog](#) dans la Référence de l'autorisation de service.

Rubriques

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

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter 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 :

- Démarrez avec les politiques AWS gérées et évoluez vers les autorisations de moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations dans de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le AWS client qui sont propres 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 via un spécifique Service AWS, comme AWS 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.
- Exigez l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur racine dans Compte AWS votre, activez l'authentification

multifactorielle pour une sécurité renforcée. 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 stratégie inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou AWS de l'API.

```
{
  "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": "*"
    }
]
}
```

Autorisation accordée aux utilisateurs pour afficher les ressources depuis 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.

```
{
  "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 avec Control Catalog

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous utilisez AWS Control Catalog et IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans Control Catalog](#)
- [Je ne suis pas autorisé à exécuter 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 encore besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à exécuter iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS Control Catalog.

Certains services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou rôle lié à un service. Pour ce faire, un utilisateur doit 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 exécuter une action dans AWS Control Catalog. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer 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 encore 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 stratégies basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces stratégies pour accorder aux personnes l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si AWS Control Catalog prend en charge ces fonctionnalités, consultez [Fonctionnement d'avec IAM](#).
- Pour savoir comment fournir un accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, veuillez consulter Octroi de [l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des tiers Comptes AWS, veuillez consulter Octroi de [l'accès à des Comptes AWS appartenant à 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 la conformité pour Control Catalog

Pour savoir si un Service AWS fait partie ou non du champ d'application de programmes de conformité spécifiques, veuillez consulter [Services AWS dans le champ d'application par programme](#) de 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 les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez [AWS Artifact Téléchargement](#) .

Votre responsabilité de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter la conformité :

- [Conformité et gouvernance de la sécurité](#) : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- [Référence des services éligibles HIPAA](#) : liste les services éligibles HIPAA. Tous les ne Services AWS sont pas éligibles à HIPAA.
- AWS Ressources de [conformité Ressources](#) de de conformité : cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement..
- [AWS Guides de conformité destinés aux clients](#) — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques pour sécuriser les Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (y compris l'Institut national de normalisation et de technologie (NIST), le Conseil de normes de sécurité PCI (Payment Card Industry) et l'Organisation internationale de normalisation (ISO)).
- [Évaluation des ressources à l'aide de règles](#) dans le Guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- [AWS Security Hub](#)— Cela Service AWS fournit une vue complète de votre état de sécurité dans AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez [Référence des contrôles Security Hub](#).
- [Amazon GuardDuty](#) : ce Service AWS détecte les menaces potentielles qui pèsent sur vos Comptes AWS, vos charges de travail, vos conteneurs et vos données en surveillant votre environnement à la recherche d'activités suspectes et malveillantes. GuardDuty peut vous aider à satisfaire diverses exigences de conformité, comme la conformité à la norme PCI DSS, en répondant aux exigences de détection d'intrusion imposées par certains frameworks de conformité.
- [AWS Audit Manager](#): ce service vous Service AWS aide à auditer en continu votre AWS utilisation d'pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Control Catalog

L'infrastructure AWS mondiale d' repose sur les Régions AWS et les zones de disponibilité. Régions AWS Les fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. 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 Régions AWS et les zones de disponibilité, consultez [Infrastructure AWS mondiale d'](#).

Sécurité de l'infrastructure dans Control Catalog

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

Vous pouvez utiliser les appels d'API AWS publiés par pour accéder à Control Catalog via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou 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.

Configuration et analyse des vulnérabilités dans Control Catalog

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

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

Dans le cadre de AWS Control Tower Control Catalog AWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un AWS service. CloudTrail capture les appels d'API pour Control Catalog en tant qu'événements. Ces appels capturés incluent les appels directement à partir de la AWS Control Tower console, par exemple pour activer ou désactiver un contrôle, ainsi que les appels de code adressés aux opérations de l'API du catalogue de contrôle. Si vous créez un journal de suivi, vous pouvez activer la livraison continue des CloudTrail événements dans un compartiment Amazon S3, y compris les événements relatifs aux commandes dans Control Catalog. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Event history (Historique des événements). Grâce aux informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Control Catalog (au moyen de AWS Control Tower), l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

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

Informations du catalogue de contrôle dans CloudTrail

CloudTrail est activé Compte AWS sur votre compte. Lorsqu'une activité a lieu dans Control Catalog, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements AWS de service dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les

événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter [Affichage des événements avec Historique des CloudTrail événements](#).

Pour un enregistrement continu des événements dans votre journal de suivi Compte AWS, y compris les événements de Control Catalog, créez un journal de suivi. Un journal de suivi CloudTrail permet de livrer des fichiers journaux dans 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 de suivi consigne les événements de toutes les Régions dans la AWS partition et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres Services AWS pour analyser plus en profondeur les données d'événement collectées dans les CloudTrail journaux et agir sur celles-ci. 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 effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (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 effectuée par un autre AWS service.

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

Présentation des entrées des fichiers journaux du catalogue

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend 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 de pile ordonnée des appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre 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 utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et le catalogue de contrôle. Vous pouvez accéder au catalogue de AWS contrôle d'accès comme s'il se trouvait dans votre VPC, sans passerelle Internet, périphérique NAT, connexion VPN ou AWS Direct Connect connexion. Les instances de votre VPC ne nécessitent pas 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.

Le catalogue prend en charge les appels vers toutes ses actions d'API via le point de terminaison d'interface.

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

Vous pouvez créer un point de terminaison d'interface pour Control Catalog à l'aide de la console Amazon VPC ou de l' 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 à l'aide du nom de service suivant :

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

Si vous activez le DNS privé pour le point de terminaison d'interface, vous pouvez adresser des demandes d'API au catalogue en utilisant son nom DNS par défaut pour la région. 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 au catalogue Control Catalog via le point de terminaison d'interface. Pour contrôler l'accès autorisé au catalogue de contrôle à partir de votre VPC, attachez une politique de point de terminaison personnalisée au point de terminaison d'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 : stratégie de point de terminaison d'un VPC pour les actions du catalogue de contrôle

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique à votre point de terminaison d'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](#). Les autres opérations d' AWS Control Tower API ne sont pas prises en charge pour AWS PrivateLink.

Historique du Guide de l'information de sécurité de Control Catalog

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

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