Guide de l’utilisateur

# AWS Organizations

# AWS Organizations: Guide de l’utilisateur

# Table of Contents

# Qu'est-ce que c'est AWS Organizations ?

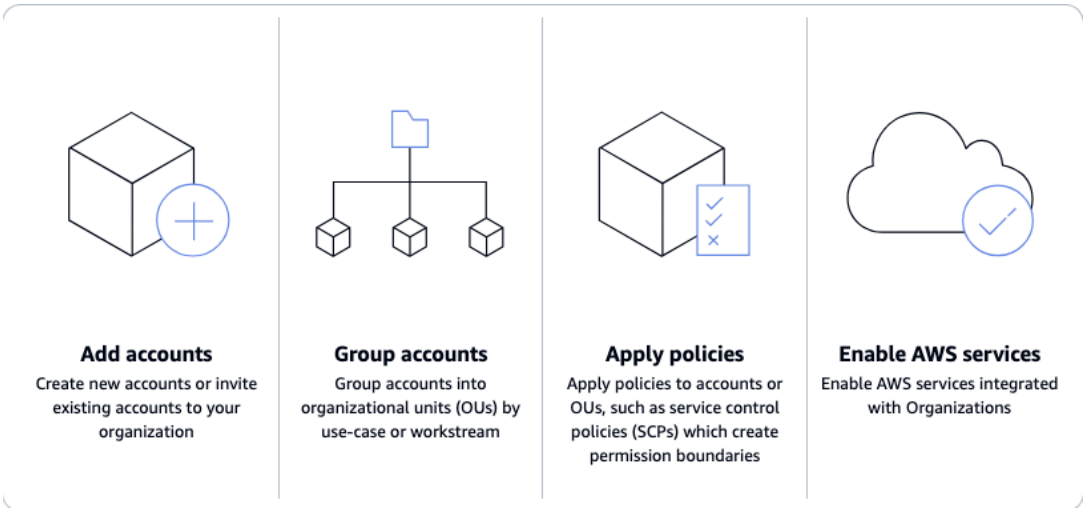
Gérez votre environnement de manière centralisée à mesure que vous augmentez vos AWS ressources

AWS Organizations vous permet de gérer et de gouverner votre environnement de manière centralisée à mesure que vous développez et faites évoluer vos AWS ressources. Organizations vous permet de créer des comptes et d'allouer des ressources, de regrouper des comptes pour organiser vos flux de travail, d'appliquer des politiques de gouvernance et de simplifier la facturation en utilisant un mode de paiement unique pour tous vos comptes.

Organizations est intégrée à d'autres Services AWS afin que vous puissiez définir des configurations centralisées, des mécanismes de sécurité, des exigences d'audit et le partage des ressources entre les comptes de votre organisation. Pour de plus amples informations, veuillez consulter Utilisation AWS Organizations avec d'autres Services AWS.

Le schéma suivant fournit une explication détaillée de la manière dont vous pouvez utiliser AWS Organizations :

- Ajouter des comptes
- Comptes de groupe
- Appliquer les politiques
- Activer Services AWS.




Rubriques

# Fonctionnalités pour AWS Organizations

AWS Organizations propose les fonctionnalités suivantes :

Gérez votre Comptes AWS

Comptes AWS sont des limites naturelles pour les autorisations, la sécurité, les coûts et les charges de travail. L'utilisation d'un environnement multi-comptes est une bonne pratique recommandée lors de la mise à l'échelle de votre environnement cloud. Vous pouvez simplifier la création de comptes en créant de nouveaux comptes par programmation à l'aide de AWS Command Line Interface (AWS CLI), ou SDKs APIs, et en fournissant de manière centralisée les ressources et autorisations recommandées à ces comptes. AWS CloudFormation StackSets

Définissez et gérez votre organisation

Lorsque vous créez de nouveaux comptes, vous pouvez les regrouper en unités organisationnelles (OUs) ou en groupes de comptes destinés à une seule application ou à un seul service. Appliquez des politiques de balises pour classer ou suivre les ressources de votre organisation, et fournissez un contrôle d'accès basé sur les attributs pour les utilisateurs ou les applications. En outre, vous pouvez déléguer la responsabilité du support Services AWS à des comptes afin que les utilisateurs puissent les gérer au nom de votre organisation.

Sécurisez et surveillez vos comptes

Vous pouvez fournir des outils et un accès centralisés à votre équipe de sécurité afin de gérer les besoins de sécurité au nom de l'organisation. Par exemple, vous pouvez fournir un accès de sécurité en lecture seule à tous les comptes, détecter et atténuer les menaces avec Amazon GuardDuty, contrôler les accès involontaires aux ressources avec IAM Access Analyzer et sécuriser les données sensibles avec Amazon Macie.

Contrôlez l'accès et les autorisations

Configurez AWS IAM Identity Centerpour fournir un accès Comptes AWS et des ressources à l'aide de votre Active Directory, et personnalisez les autorisations en fonction de rôles professionnels distincts. Vous pouvez également appliquer les politiques de l'organisation aux utilisateurs, aux comptes ou OUs. Par exemple, les politiques de contrôle des services (SCPs) vous permettent de contrôler l'accès aux AWS ressources, aux services et aux régions au sein de votre organisation. Les politiques de contrôle des ressources (RCPs) vous permettent de prévenir de manière centralisée l'utilisation involontaire de vos AWS ressources. Les politiques relatives aux applications de chat vous permettent de contrôler l'accès aux comptes de votre organisation à partir d'applications de chat telles que Slack et Microsoft Teams.

Partagez les ressources entre les comptes

Vous pouvez partager AWS des ressources au sein de votre organisation à l'aide de AWS Resource Access Manager (AWS RAM). Par exemple, vous pouvez créer vos sous-réseaux Amazon Virtual Private Cloud (Amazon VPC) une seule fois et les partager au sein de votre organisation. Vous pouvez également accepter des licences logicielles de manière centralisée et partager un catalogue de services informatiques et de produits personnalisés sur plusieurs comptes avec AWS Service Catalog. AWS License Manager

Auditez votre environnement pour vérifier sa conformité

Vous pouvez AWS CloudTraill'activer sur plusieurs comptes, ce qui crée un journal de toutes les activités de votre environnement cloud qui ne peut pas être désactivé ou modifié par les comptes des membres. En outre, vous pouvez définir des politiques pour appliquer les sauvegardes à la cadence que vous avez spécifiée ou définir des paramètres de configuration recommandés pour les ressources entre les comptes et Régions AWS avec AWS Config. AWS Backup

Gérez la facturation et les coûts de manière centralisée

Organizations vous fournit une facture consolidée unique. En outre, vous pouvez consulter l'utilisation des ressources sur l'ensemble des comptes AWS Cost Explorer, suivre les coûts d'utilisation et optimiser votre utilisation des ressources informatiques Optimiseur de calcul AWS.

# Cas d'utilisation pour AWS Organizations

Voici quelques cas d'utilisation pour AWS Organizations :

Automatisez la création Comptes AWS et catégorisez les charges de travail

Vous pouvez automatiser la création de Comptes AWS pour lancer rapidement de nouvelles charges de travail. Ajoutez les comptes à des groupes définis par l'utilisateur pour une application instantanée des politiques de sécurité, des déploiements d'infrastructures sans contact et des audits. Créez des groupes distincts pour classer les comptes de développement et de production et utilisez-les AWS CloudFormation StackSetspour fournir des services et des autorisations à chaque groupe.

Définir et appliquer les politiques d'audit et de conformité

Vous pouvez appliquer des politiques de contrôle des services (SCPs) pour garantir que vos utilisateurs n'exécutent que les actions qui répondent à vos exigences de sécurité et de conformité. Créez un journal central de toutes les actions effectuées au sein de votre organisation à l'aide de AWS CloudTrail. Affichez et appliquez les configurations de ressources standard sur l'ensemble des comptes et sur Régions AWS l'utilisation AWS Config. Appliquez automatiquement des sauvegardes régulières à l'aide de AWS Backup. Utilisez-le AWS Control Towerpour appliquer des règles de gouvernance prédéfinies en matière de sécurité, d'exploitation et de conformité pour vos charges AWS de travail.

Fournissez des outils et des accès à vos équipes de sécurité tout en encourageant le développement

Créez un groupe de sécurité et donnez-lui un accès en lecture seule à toutes vos ressources pour identifier et atténuer les problèmes de sécurité. Vous pouvez autoriser ce groupe à gérer Amazon GuardDuty afin qu'il puisse surveiller et atténuer activement les menaces qui pèsent sur vos charges de travail, et autoriser IAM Access Analyzer à identifier rapidement les accès involontaires à vos ressources.

Partagez des ressources communes entre les comptes

Organizations vous permet de partager facilement des ressources centrales critiques entre vos comptes. Par exemple, vous pouvez partager votre central AWS Directory Service for Microsoft Active Directoryafin que les applications puissent accéder à votre banque d'identité centrale.

Partagez les ressources centrales essentielles entre vos comptes

Partagez-le AWS Directory Service for Microsoft Active Directoryen tant que banque d'identité centrale pour vos applications. Utilisez-le AWS Service Catalogpour partager des services informatiques sur des comptes désignés afin que les utilisateurs puissent rapidement découvrir et déployer des services approuvés. Assurez-vous que les ressources d'application sont créées sur vos sous-réseaux Amazon Virtual Private Cloud (Amazon VPC) en les définissant une seule fois

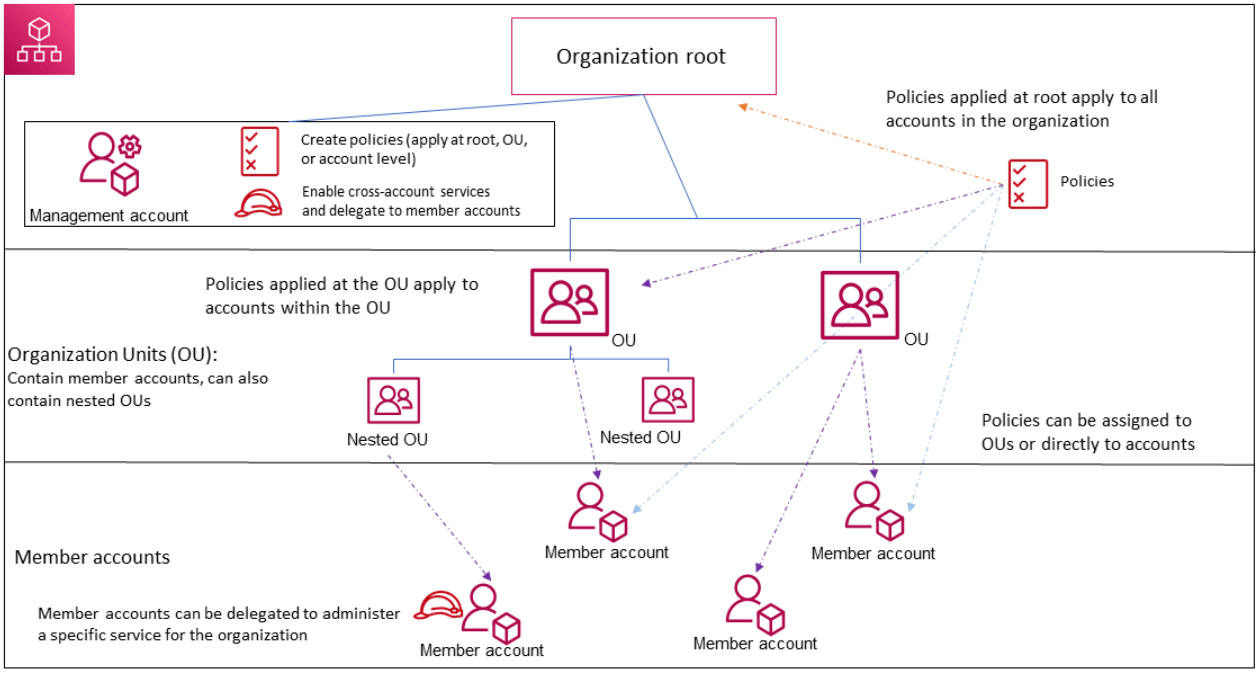
de manière centralisée et en les partageant au sein de votre organisation à l'aide AWS Resource Access Manager de ().AWS RAM

# Terminologie et concepts pour AWS Organizations

Cette rubrique explique certains des concepts clés de AWS Organizations.

Le schéma suivant montre une organisation composée de cinq comptes organisés en quatre unités organisationnelles (OUs) sous la racine. L'organisation dispose également de plusieurs politiques qui sont associées à certains comptes OUs ou directement à ceux-ci.

Pour une description de chacun de ces éléments, reportez-vous aux définitions de cette rubrique.




Rubriques

- Ensembles de fonctions disponibles
- Structure de l'organisation
- Invitations et poignées de main
- Politiques de l'organisation

# Ensembles de fonctions disponibles

Toutes les fonctionnalités (recommandé)

Toutes les fonctionnalités sont l'ensemble de fonctionnalités par défaut disponible pour AWS Organizations. Vous pouvez définir des politiques et des exigences de configuration centralisées pour l'ensemble d'une organisation, créer des autorisations ou des fonctionnalités personnalisées au sein de l'organisation, gérer et organiser vos comptes sous une seule facture et déléguer des responsabilités à d'autres comptes au nom de l'organisation. Vous pouvez également utiliser des intégrations avec d'autres Services AWS pour définir des configurations centralisées, des mécanismes de sécurité, des exigences d'audit et le partage des ressources entre tous les comptes membres de votre organisation. Pour de plus amples informations, veuillez consulter Utilisation AWS Organizations avec d'autres Services AWS.

Le mode Toutes les fonctionnalités fournit toutes les fonctionnalités de facturation consolidée ainsi que les fonctionnalités administratives.

Facturation consolidée

La facturation consolidée est l'ensemble de fonctionnalités qui fournit des fonctionnalités de facturation partagée, mais n'inclut pas les fonctionnalités plus avancées de AWS Organizations. Par exemple, vous ne pouvez pas permettre à d'autres AWS services de s'intégrer à votre organisation pour qu'ils fonctionnent sur tous ses comptes, ou utiliser des politiques pour restreindre les actions des utilisateurs et des rôles des différents comptes.

Vous pouvez activer toutes les fonctionnalités pour une organisation qui, à l'origine, ne prenait en charge que les fonctionnalités de facturation consolidée. Pour activer toutes les fonctions, tous les comptes membres invités doivent approuver la modification en acceptant l'invitation envoyée lorsque le compte de gestion commence le processus. Pour de plus amples informations, veuillez consulter Activation de toutes les fonctionnalités pour une organisation avec AWS Organizations.

# Structure de l'organisation

Organisation

Une organisation est un ensemble d'organisations Comptes AWSque vous pouvez gérer de manière centralisée et organiser dans une structure hiérarchique arborescente avec une racine en haut et des unités organisationnelles imbriquées sous la racine. Chaque compte peut être directement à la racine ou placé dans l'un des comptes de la hiérarchie. OUs

Chaque organisation est composée de :

- Un compte de gestion
- Aucun compte membre ou plus
- Aucune unité organisationnelle ou plus (OUs)
- Aucune politique ou plus.

Une organisation possède la fonctionnalité déterminée par l'ensemble des fonctions que vous activez.

Root

Une racine administrative (root) est contenue dans le compte de gestion et constitue le point de départ de l'organisation de votre compte Comptes AWS. La racine est le conteneur le plus haut dans la hiérarchie de votre organisation. Sous cette racine, vous pouvez créer des unités organisationnelles (OUs) pour regrouper logiquement vos comptes et les OUs organiser selon une hiérarchie qui correspond le mieux à vos besoins.

Si vous appliquez une politique de gestion à la racine, elle s'applique à toutes les unités organisationnelles (OUs) et à tous les comptes, y compris le compte de gestion de l'organisation.

Si vous appliquez une politique d'autorisation (par exemple, une politique de contrôle des services (SCP)) à la racine, elle s'applique à toutes les unités organisationnelles (OUs) et à tous les comptes de membres de l'organisation. Elle ne s'applique pas au compte de gestion de l'organisation.

> **Note**
>
> Vous ne pouvez avoir qu'une seule racine. AWS Organizations crée automatiquement la racine pour vous lorsque vous créez une organisation.

Unité d'organisation (UO)

Une unité organisationnelle (UO) est un groupe Comptes AWSau sein d'une organisation. Une UO peut également en contenir d'autres OUs qui vous permettent de créer une hiérarchie. Par exemple, vous pouvez regrouper tous les comptes appartenant au même département dans une unité d'organisation départementale. De même, vous pouvez regrouper tous les comptes exécutant des services de sécurité dans une unité d'organisation de sécurité.

OUs sont utiles lorsque vous devez appliquer les mêmes contrôles à un sous-ensemble de comptes de votre organisation. L'imbrication OUs permet de réduire la taille des unités de gestion. Par exemple, vous pouvez en créer OUs pour chaque charge de travail, puis en créer deux imbriqués OUs dans chaque unité organisationnelle de charge de travail afin de séparer les charges de production de celles de pré-production. Ceux-ci OUs héritent des politiques de l'unité d'organisation parent, en plus de tous les contrôles assignés directement à l'unité d'organisation au niveau de l'équipe. En incluant la racine et en Comptes AWS créant le niveau le plus bas OUs, votre hiérarchie peut comporter cinq niveaux de profondeur.

Compte AWS

An Compte AWSest un conteneur pour vos AWS ressources. Vous créez et gérez vos AWS ressources dans un Compte AWS, et Compte AWS fournit des fonctionnalités administratives pour l'accès et la facturation.

L'utilisation de plusieurs Comptes AWS est une bonne pratique pour faire évoluer votre environnement, car elle fournit une limite de facturation pour les coûts, isole les ressources pour des raisons de sécurité, donne de la flexibilité aux individus et aux équipes, en plus de s'adapter aux nouveaux processus.

> **Note**
>
> Un AWS compte est différent d'un utilisateur. Un utilisateur est une identité que vous créez à l'aide de Gestion des identités et des accès AWS (IAM) et prend la forme d'un utilisateur IAM avec des informations d'identification à long terme ou d'un rôle IAM avec des informations d'identification à court terme. Un seul AWS compte peut contenir, et c'est généralement le cas, de nombreux utilisateurs et rôles.

Il existe deux types de comptes dans une organisation : un compte unique désigné comme compte de gestion et un ou plusieurs comptes membres.

Compte de gestion

Un compte de gestion est le compte Compte AWS que vous utilisez pour créer votre organisation. Depuis le compte de gestion, vous pouvez effectuer les opérations suivantes :

- Créez d'autres comptes dans votre organisation
- Inviter et gérer les invitations d'autres comptes à rejoindre votre organisation
- Désigner des comptes d'administrateur délégué

- Supprimer des comptes de votre organisation
- Associez des politiques à des entités telles que des racines, des unités organisationnelles (OUs) ou des comptes au sein de votre organisation
- Activez l'intégration avec AWS les services pris en charge pour fournir des fonctionnalités de service sur tous les comptes de l'organisation.

Le compte de gestion est le propriétaire ultime de l'organisation, ayant le contrôle final sur les politiques de sécurité, d'infrastructure et financières. Ce compte joue le rôle d'un compte payeur et est chargé de payer tous les frais accumulés par les comptes de son organisation.

> **Remarques**
>
> - Vous ne pouvez pas modifier le compte de gestion de votre organisation.
> - Il n'est pas nécessaire que le compte de gestion se trouve directement sous la racine, il peut être placé n'importe où dans l'organisation.

### Compte membre

Un compte de membre est un compte Compte AWS, autre que le compte de gestion, qui fait partie d'une organisation. Si vous êtes administrateur d'une organisation, vous pouvez créer des comptes membres au sein de l'organisation et inviter des comptes existants à rejoindre l'organisation. Vous pouvez également appliquer des politiques aux comptes des membres.

> **Note**
>
> Le compte d'un membre ne peut appartenir qu'à une seule organisation à la fois. Vous pouvez désigner les comptes des membres comme des comptes d'administrateurs délégués.

### Administrateur délégué

Nous vous recommandons de n'utiliser le compte de gestion et ses utilisateurs et rôles que pour les tâches qui doivent être effectuées par ce compte. Nous vous recommandons de stocker vos ressources AWS dans d'autres comptes membres de l'organisation et de les garder en dehors du compte de gestion. Cela est dû au fait que les fonctionnalités de sécurité telles que

les politiques de contrôle des services des Organisations (SCPs) ne limitent aucun utilisateur ou rôle dans le compte de gestion. Le fait de séparer vos ressources de votre compte de gestion peut également vous aider à comprendre les frais figurant sur vos factures. À partir du compte de gestion de l'organisation, vous pouvez désigner un ou plusieurs comptes membres comme compte d'administrateur délégué pour vous aider à mettre en œuvre cette recommandation. Il existe deux types d'administrateurs délégués :

- Administrateur délégué pour les organisations : à partir de ces comptes, vous pouvez gérer les politiques de l'organisation et associer des politiques aux entités (racines ou comptes) au sein de l'organisation. OUs Le compte de gestion peut contrôler les autorisations de délégation à des niveaux granulaires. Pour de plus amples informations, veuillez consulter Administrateur délégué pour AWS Organizations.
- Administrateur délégué pour un AWS service : à partir de ces comptes, vous pouvez gérer les AWS services qui s'intègrent aux Organizations. Le compte de gestion peut enregistrer différents comptes membres en tant qu'administrateurs délégués pour différents services, selon les besoins. Ces comptes disposent d'autorisations administratives pour un service spécifique, ainsi que d'autorisations pour les actions en lecture seule d'Organizations. Pour de plus amples informations, consultez Administrateur délégué pour Services AWS ce travail avec les Organizations.

## Invitations et poignées de main

Invitation

Une invitation est une demande faite par le compte de gestion d'une organisation à un autre compte. Par exemple, le processus consistant à demander à un compte autonome de rejoindre une organisation est une invitation.

Les invitations sont mises en œuvre sous forme de poignées de main. Vous risquez de ne pas voir les handshakes lorsque vous utilisez la console AWS Organizations . Mais si vous utilisez l' AWS Organizations API AWS CLI or, vous devez travailler directement avec des poignées de main.

Handshake

Une poignée de main est l'échange sécurisé d'informations entre deux AWS comptes : un expéditeur et un destinataire.

Les poignées de main suivantes sont prises en charge :

- INVITATION : poignée de main envoyée à un compte autonome pour qu'il rejoigne l'organisation de l'expéditeur.
- ENABLE_ALL_FEATURES : poignée de main envoyée aux comptes des membres invités pour activer toutes les fonctionnalités de l'organisation.
- APPROVE_ALL_FEATURES : poignée de main envoyée au compte de gestion lorsque tous les comptes de membres invités ont approuvé l'activation de toutes les fonctionnalités.

Vous devez généralement interagir directement avec les handshakes uniquement si vous utilisez l' AWS Organizations API ou des outils de ligne de commande tels que le. AWS CLI

## Politiques de l'organisation

Une politique est un « document » contenant une ou plusieurs instructions qui définissent les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS. AWS Organizations prend en charge les politiques d'autorisation et les politiques de gestion.

### Politiques d'autorisation

Les politiques d'autorisation vous aident à gérer de manière centralisée la sécurité Comptes AWS au sein d'une organisation.

Politique de contrôle des services

Une politique de contrôle des services est un type de politique qui permet de contrôler de manière centralisée les autorisations maximales disponibles pour les utilisateurs IAM et les rôles IAM au sein d'une organisation.

Cela signifie que SCPs vous devez spécifier des contrôles centrés sur le principal. SCPs créez un garde-fou en matière d'autorisations ou fixez des limites au maximum d'autorisations accordées aux principaux sur vos comptes de membres. Vous utilisez un SCP lorsque vous souhaitez appliquer de manière centralisée des contrôles d'accès cohérents aux principaux de votre organisation.

Cela peut inclure la spécification des services auxquels vos utilisateurs et rôles IAM peuvent accéder, des ressources auxquelles ils peuvent accéder ou des conditions dans lesquelles ils peuvent faire des demandes (par exemple, depuis des régions ou des réseaux spécifiques). Pour de plus amples informations, veuillez consulter SCPs.

### Politique de contrôle des ressources (RCP)

Une politique de contrôle des ressources est un type de politique qui permet de contrôler de manière centralisée le maximum d'autorisations disponibles pour les ressources d'une organisation.

Cela signifie qu'il faut RCPs spécifier des contrôles centrés sur les ressources. RCPs créez un garde-fou en matière d'autorisations, ou fixez des limites, aux autorisations maximales disponibles pour les ressources de vos comptes membres. Utilisez un RCP lorsque vous souhaitez appliquer de manière centralisée des contrôles d'accès cohérents à l'ensemble des ressources de votre organisation.

Cela peut inclure la restriction de l'accès à vos ressources afin que seules les identités appartenant à votre organisation puissent y accéder, ou la spécification des conditions dans lesquelles des identités externes à votre organisation peuvent accéder à vos ressources. Pour de plus amples informations, veuillez consulter RCPs.

## Politiques de gestion

Les politiques de gestion vous aident à configurer et à gérer Services AWS de manière centralisée leurs fonctionnalités au sein d'une organisation.

- Les politiques déclaratives vous permettent de déclarer et d'appliquer de manière centralisée les configurations souhaitées pour une donnée Service AWS à grande échelle au sein d'une organisation. Une fois connectée, la configuration est toujours maintenue lorsque le service ajoute de nouvelles fonctionnalités ou APIs.
- Les politiques de sauvegarde vous permettent de gérer et d'appliquer de manière centralisée des plans de sauvegarde aux AWS ressources des comptes d'une organisation.
- Les politiques relatives aux balises vous permettent de standardiser les balises associées aux AWS ressources dans les comptes d'une organisation.
- Les politiques relatives aux applications de chat vous permettent de contrôler l'accès aux comptes d'une organisation à partir d'applications de chat telles que Slack et Microsoft Teams.
- Les politiques de désinscription des services d'IA vous permettent de contrôler la collecte de données pour les services d' AWS IA pour tous les comptes d'une organisation.
- Les politiques du Security Hub vous permettent de combler les lacunes en matière de couverture de sécurité conformément aux exigences de sécurité de votre entreprise et de les appliquer de manière centralisée à l'ensemble de l'organisation.

- Les politiques Amazon Inspector vous permettent d'activer et de gérer Amazon Inspector de manière centralisée pour tous les comptes de votre AWS organisation.
- Les politiques d'Amazon Bedrock vous permettent d'appliquer automatiquement les mesures de protection configurées dans Amazon Bedrock Guardrails à tous les éléments de la structure de votre organisation pour tous les appels d'inférence de modèles adressés à Amazon Bedrock.
- Les politiques de déploiement des mises à niveau vous permettent de gérer de manière centralisée et d'échelonner les mises à niveau automatiques sur plusieurs AWS ressources et comptes de votre organisation.
- Les politiques Amazon S3 vous permettent de gérer de manière centralisée les configurations des ressources Amazon S3 à grande échelle sur l'ensemble des comptes d'une organisation.
- AWS Shield Les politiques du Network Security Director vous permettent d'activer et de gérer de manière centralisée le AWS Shield Network Security Director sur l'ensemble des comptes d'une organisation.

# Quotas et limites de service pour AWS Organizations

Cette rubrique décrit les quotas et les limites de service pour AWS Organizations.

## Instructions d'attribution de noms

Les instructions suivantes concernent les noms que vous créez dans AWS Organizations, notamment les noms des comptes, des unités organisationnelles (OUs), des racines et des politiques :

- Les noms doivent être composés de caractères Unicode.
- La longueur maximale de chaîne des noms varie selon l'objet. Pour plus d'informations sur la limite réelle pour chaque objet, consultez la référence d'AWS Organizations API et recherchez l'opération d'API qui crée l'objet, puis examinez les détails du `Name` paramètre de cette opération. Par exemple : Nom du compte ou Nom de l'unité d'organisation.

## Considérations

Les codes de quota de service peuvent changer au fil du temps en raison des mises à jour. Cela n'a aucune incidence sur les valeurs ou les noms des quotas. Pour trouver le code de quota correspondant à un quota spécifique, utilisez l'ListServiceQuotasopération et recherchez la `QuotaCode` réponse dans la sortie pour le quota souhaité.

# Valeurs minimales et maximales

Les valeurs maximales par défaut pour les entités dans AWS Organizations sont les suivantes.

> **Note**
>
> Tenez compte des informations suivantes concernant AWS Organizations les quotas :
>
> - Vous pouvez demander des augmentations de certaines de ces valeurs à l'aide de la console Service Quotas.
> - AWS Organizations les limites s'appliquent au niveau de l'organisation, sauf indication contraire. De nombreux quotas s'appliquent uniquement aux actions effectuées depuis le compte AWS Organizations de gestion.
> - AWS Organizations est un service mondial hébergé physiquement dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`). Par conséquent, vous devez utiliser `us-east-1` pour accéder à ces quotas lorsque vous utilisez la console Service Quotas AWS CLI, le ou un AWS SDK.

| Description | Limite |
| --- | --- |
| Nombre maximum de comptes | 10 — Le nombre maximum de comptes autorisés dans une organisation. Ce quota est ajustable et peut être augmenté à l'aide de la console Service Quotas.<br><br>Remarque : Seul le compte de gestion d'une organisation peut soumettre cette demande d'augmentation de quota. Des augmentations de limite peuvent être accordées jusqu'à 50 000 comptes en fonction des qualifications et des exigences du client. Les comptes et organisations nouvellement créés peuvent avoir un quota inférieur à la valeur par défaut de 10 comptes.<br><br>Une invitation envoyée à un compte est comptabilisée par rapport à ce quota. Elle est décomptée si le compte invité décline l'invitation, si le compte de gestion annule l'invitation ou si celle-ci expire.<br><br>Lorsqu'un compte est fermé, il ne cesse de compter dans ce quota jusqu'à ce qu'il soit définitivement fermé. Pour plus d'informations |

| Description | Limite |
| --- | --- |
| | sur la fermeture définitive d'un compte, consultez la section Période postérieure à la fermeture dans le Guide de Gestion de compte AWS référence.<br><br>Certains services ont des limites de compte distinctes du nombre maximum de comptes autorisés dans une organisation. Pour plus d'informations, consultez la section Limites par AWS service. |
| Âge minimum pour la suppression des comptes créés | Chaque région prise en charge : 7 — Le nombre minimum de jours pendant lesquels un compte créé doit exister avant que vous puissiez le supprimer de l'organisation. |
| Nombre de racines dans une organisation | 1 |
| Nombre de personnes OUs dans une organisation | 2000 |
| Nombre de politiques dans une organisation | Politiques de contrôle des services : 10 000<br><br>Politiques de contrôle des ressources : 1000<br><br>Politiques déclaratives : 1000<br><br>Politiques de sauvegarde : 1000<br><br>Politiques de tag : 1000<br><br>Politiques relatives aux applications de chat : 1000<br><br>Politiques de désinscription des services d'IA : 1000<br><br>Politiques du Security Hub : 1000 |

| Description | Limite |
| --- | --- |
| Taille maximale d'un document de politique | Politiques de contrôle des services : 5 120 octets<br><br>Politiques de contrôle des ressources : 5120 caractères<br><br>Politiques déclaratives : 10 000 caractères<br><br>Politiques de sauvegarde : 10 000 caractères<br><br>Politiques relatives aux applications de chat : 10 000 caractères<br><br>Politiques de désactivation des services IA : 2500 caractères<br><br>Politiques de balises : 10 000 caractères<br><br>Politiques du Security Hub : 10 000 caractères<br><br>Remarque : Si vous enregistrez la politique en utilisant les AWS Management Console espaces blancs supplémentaires (tels que les espaces et les sauts de ligne) entre les éléments JSON et en dehors des guillemets, ils sont supprimés et ne sont pas pris en compte. Si vous enregistrez la politique à l'aide d'une opération du SDK ou du AWS CLI, elle est enregistrée exactement comme vous l'avez indiqué et aucun caractère n'est automatiquement supprimé. |
| Imbrication maximale d'UO dans une racine | Cinq niveaux de OUs profondeur sous une racine. |

| Description | Limite |
| --- | --- |
| Nombre maximal de tentatives d'invitation sur une période de 24 heures | Soit 20, soit le nombre maximal de comptes autorisés dans votre organisation, selon la valeur la plus élevée de ces deux valeurs. Les invitations acceptées ne sont pas prises en compte dans ce quota. Dès qu'une invitation est acceptée, vous pouvez envoyer une autre invitation le même jour.<br><br>Si le nombre maximal de comptes autorisés dans votre organisation est inférieur à 20, vous obtenez une exception « limite de comptes dépassée » si vous essayez d'inviter plus de comptes que votre organisation peut contenir. Cependant, vous pouvez annuler des invitations et en envoyer de nouvelles jusqu'à un maximum de 20 tentatives en une journée. |
| Nombre de comptes membres que vous pouvez créer simultané ment | 5 : dès qu'un compte est abandonné, vous pouvez en démarrer un autre, mais seuls cinq comptes peuvent être en cours à la fois. |
| Nombre de comptes que vous pouvez fermer dans un délai de 30 jours | 20 % des comptes membres appartiennent à des organisations ou 250, selon le montant le plus élevé, avec un maximum de 1 000. Il ne s'agit pas d'un quota ajustable.<br><br>• < 1 250 comptes — Vous pouvez fermer jusqu'à 250 comptes de membres<br>• 1 250 à 5 000 comptes — Vous pouvez fermer jusqu'à 20 % des comptes de vos membres<br>• > 5 000 comptes — Vous pouvez fermer jusqu'à 1 000 comptes de membres<br><br>Une fois ce quota atteint, vous pouvez fermer des comptes supplémentaires ou attendre que votre quota soit réinitialisé. Pour plus d'informations, consultez la section Clôture d'un AWS compte dans le Guide de gestion des AWS comptes. |

| Description | Limite |
| --- | --- |
| Nombre de comptes membres que vous pouvez clôturer simultanément | 3 – Seules trois clôtures de comptes peuvent être en cours au même moment. Dès qu'une est terminée, vous pouvez clôturer un autre compte. |
| Nombre d'entités auxquelles vous pouvez attacher une politique | Illimité |
| Nombre de balises que vous pouvez attacher à une racine, une UO ou un compte | 50 |
| Taille maximale de la politique de délégation basée sur les ressources | 40 000 caractères |

## Limites par AWS service

La plupart Services AWS soutiennent le nombre maximum de comptes indiqué que vous pouvez avoir dans une organisation. Cependant, certains services ont des limites de comptes distinctes du nombre maximum de comptes autorisés dans une organisation.

Le tableau suivant indique les services avec des limites de compte distinctes.

| AWS service | Limite | Peut être augmenté | Documentation du service |
| --- | --- | --- | --- |
| AWS Directory Service (Le partage de répertoire est disponible pour AWS Managed Microsoft AD) | La capacité des comptes de partage d'annuaires varie en fonction de l'édition. | Oui | Directory Service Quotas |

| AWS service | Limite | Peut être augmenté | Documentation du service |
|---|---|---|---|
| AWS Audit Manager | 250 | Oui | AWS Audit Manager Quotas |
| Amazon Detective | 1200 | Oui | Quotas Amazon Detective |
| AWS IAM Identity Center | 3000 | Oui | AWS IAM Identity Center Quotas |
| AWS Application Migration Service | 5000 | Non | AWS Quotas |
| AWS Security Hub | 10 000 | Non | AWS Security Hub Quotas |
| Amazon Macie | 10 000 | Non | Quotas Amazon Macie |
| AWS Control Tower | 10 000 | Non | AWS Control Tower Quotas |
| Amazon Inspector | 10 000 | Non | Quotas Amazon Inspector |
| AWS Firewall Manager | 10 000 | Oui | AWS Firewall Manager Quotas |
| Amazon DevOps Guru | 10 000 | Oui | Quotas Amazon DevOps Guru |

## Délai d'expiration des handshakes

Les délais d'attente pour les poignées de main sont les suivants. AWS Organizations

| Description | Limite |
|---|---|
| Invitation à rejoindre une organisation | 15 jours |
| Demande d'activer toutes les fonctions dans une organisation | 90 jours |

| Description | Limite |
| --- | --- |
| Le handshake est supprimé et ne s'affiche plus dans les listes | 30 jours après la fin du handshake |

## Nombre de politiques que vous pouvez attacher à une entité

Le nombre maximum dépend du type de politique ainsi que de l'entité à laquelle vous attachez la politique. Le tableau suivant montre chaque type de politique et le nombre d'entités auquel chacun peut être attaché.

> **Note**
>
> Ces chiffres s'appliquent uniquement aux polices directement rattachées à une unité d'organisation ou à un compte. Les politiques qui s'appliquent à une unité d'organisation ou à un compte par héritage ne sont pas prises en compte dans ces limites. Toutes les limites des politiques sont des limites strictes.

| Type de politique | Minimum attaché à une entité | Maximum attaché à la racine | Maximum attaché par unité d'organisation | Maximum attaché par compte |
| --- | --- | --- | --- | --- |
| Politique de contrôle des services | 1 — Chaque entité doit avoir au moins un SCP attaché à tout moment lorsque vous l'activez SCPs. Vous ne pouvez pas supprimer la dernière politique de contrôle des services d'une entité. | 5 | 5 | 5 |

| Type de politique | Minimum attaché à une entité | Maximum attaché à la racine | Maximum attaché par unité d'organisation | Maximum attaché par compte |
|---|---|---|---|---|
| Politique de contrôle des ressources | 1 — La `RCPFullAWSAccess` politique est automatiquement attachée à la racine, à chaque unité d'organisation et à chaque compte de votre organisation lorsque vous l'activez RCPs. Vous ne pouvez pas dissocier cette politique et elle est prise en compte dans le quota de 5 politiques. | 5 | 5 | 5 |
| Politique déclarative | 0 USD | 10 | 10 | 10 |
| Politique de sauvegarde | 0 USD | 10 | 10 | 10 |
| Politique de balises | 0 USD | 10 | 10 | 10 |
| Politique relative aux applications de chat | 0 | 5 | 5 | 5 |
| Politique de désactivation des services IA | 0 | 5 | 5 | 5 |

| Type de politique | Minimum attaché à une entité | Maximum attaché à la racine | Maximum attaché par unité d'organisation | Maximum attaché par compte |
|---|---|---|---|---|
| Politique du Security Hub | 0 USD | 10 | 10 | 10 |

> **Note**
>
> Vous ne pouvez avoir qu'une seule racine dans une organisation.

## Limites d'étranglement

Les tableaux suivants les répertorient AWS Organizations APIs par catégorie de gestion et indiquent leurs taux d'accélération respectifs au niveau du compte et de l'organisation.

AWS Organizations utilise l'algorithme Token Bucket pour implémenter la régulation des API. Avec cet algorithme, votre compte dispose d'un compartiment contenant un nombre spécifique de jetons. Le nombre de jetons contenus dans le compartiment représente votre quota de limitation à chaque seconde.

Le taux est le rythme fixe auquel les jetons sont ajoutés au compartiment de jetons par seconde.

La rafale est le nombre maximum de jetons pouvant être ajoutés et le nombre maximum de jetons pouvant être utilisés par seconde.

Par exemple, l'`DescribeAccount`API est limitée pour une seule demande Compte AWS à 20 demandes par seconde comme taux de référence et à 30 demandes par seconde comme taux de rafale. Le taux de rafale de 30 demandes par seconde vous permet de dépasser temporairement le taux de référence de 20 demandes par seconde.

Vous pouvez effectuer 20 demandes au cours de la première seconde, ce qui correspond au taux de référence. Au cours de la seconde qui suit, vous pouvez faire 30 demandes, ce qui dépasse la base de référence tout en respectant le taux de rafale de 30. Toutefois, au cours de la troisième seconde, si vous essayez de faire plus de 20 demandes, vous serez limité car vous avez dépassé le taux de référence et la capacité de rafale a été utilisée.

Le taux de rafale vous permet de gérer les pics de trafic temporaires sans vous limiter, à condition que le nombre moyen de demandes par seconde reste dans les limites de base au fil du temps.

## Limites de gestion des comptes

Le tableau suivant répertorie les informations AWS Organizations APIs relatives à la gestion des comptes.

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| CloseAccount | 0,05, 1 | |
| CreateAccount, CreateGov CloudAccount | 0,1, 3 | |
| DescribeAccount | 20, 30 | 24, 36 |
| DescribeCreateAccountStatus | 2, 2 | 2, 3 |
| LeaveOrganization | 1, 1 | |
| ListCreateAccountStatus | 5, 8 | 6, 10 |

## Limites de gestion des poignées de main

Le tableau suivant répertorie la poignée de main AWS Organizations APIs pour le compte.

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| AcceptHandshake | 1, 2 | 5, 5 |
| DescribeHandshake | 1, 2 | 6, 10 |
| CancelHandshake | 2, 3 | |
| DeclineHandshake | 1, 1 | 5, 5 |
| InviteAccountToOrganization | 3, 5 | |

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| ListHandshakesForAccount, ListHandshakesForOrganization | 5, 8 | 6, 10 |

## Limites de gestion de l'organisation

Le tableau suivant répertorie les informations relatives à AWS Organizations APIs la gestion de l'organisation.

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| CreateOrganization, DeleteOrganization, EnableFullControl | 1, 1 | |
| CreateOrganizationalUnit, DescribeOrganization | 1, 2 | |
| MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit | 2, 3 | |
| DescribeOrganizationalUnit | 2, 2 | 2, 3 |
| ListAccounts | 8, 12 | 9, 15 |
| ListChildren | 6, 10 | 7, 12 |
| ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent | 5, 8 | 6, 10 |
| ListRoots | 1, 2 | 1, 3 |

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| ListTagsForResource | 10, 15 | 12, 18 ANS |
| RemoveAccountFromOrganization | 2, 2 | |
| TagResource, UntagResource | 4, 6 | |

## Limites de gestion des politiques

Le tableau suivant répertorie les informations AWS Organizations APIs relatives à la gestion des politiques.

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy | 2, 3 | |
| DescribePolicy | 2, 2 | 2, 3 |
| DisablePolicyType, EnablePolicyType | 1, 1 | |
| ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy | 5, 8 | 6, 10 |
| UpdatePolicy | 2, 3 | |

## Limites de gestion des services

Le tableau suivant répertorie les informations AWS Organizations APIs relatives à la gestion des services.

| AWS Organizations API | Limite par compte (taux, rafale) | Limite par organisation (taux, rafale) |
|---|---|---|
| Activer AWSService l'accès, désactiver AWSService l'accès | 1, 2 | |
| Liste AWSServiceAccessForOrganization, ListDelegatedServicesForAccount | 1, 3 | 1, 4 |
| ListDelegatedAdministrators | 5, 8 | 6, 10 |
| RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator | 1, 2 | |

## Support régional pour AWS Organizations

AWS Organizations est disponible dans toutes les régions AWS commerciales et dans AWS GovCloud (US) Regions les régions de Chine.

Pour une liste des différences de fonctionnalités dans AWS GovCloud (US) Regions, voir AWS Organizations dans AWS GovCloud (US).

Pour une liste des différences de fonctionnalités dans les régions de Chine, voir AWS Organizations Chine.

Les points de terminaison de service pour les Organizations sont situés :

- Dans l'est des États-Unis (Virginie du Nord) pour les organisations commerciales
- In AWS GovCloud (US-West) pour les organisations AWS GovCloud (US)
- En Chine (Ningxia) pour les organisations chinoises, exploitée par Ningxia Western Cloud Data Technology Co. Ltd (NWCD).

Toutes les entités de l'organisation sont accessibles dans le monde entier, à l'exception des organisations gérées en Chine, de la même manière que Gestion des identités et des accès AWS

(IAM) fonctionne aujourd'hui. Vous n'avez pas besoin de spécifier Région AWS quand vous créez et gérez votre organisation, mais vous devrez créer une organisation distincte pour les comptes utilisés en Chine. Les utilisateurs de votre Comptes AWS site peuvent l'utiliser Services AWS dans n'importe quelle région géographique où ce service est disponible.

> **Note**
>
> Les politiques relatives aux balises ne sont prises en charge que dans un sous-ensemble de régions
> Les politiques de balises sont un type de politique qui peut vous aider à standardiser les balises entre les ressources des comptes de votre organisation. Les politiques relatives aux balises ne sont prises en charge que dans un sous-ensemble de régions où Organizations est pris en charge. Pour obtenir la liste des régions dans lesquelles les politiques relatives aux balises sont prises en charge, voir Politiques relatives aux balises | Régions de support.

## Liste des produits disponibles Régions AWS

Le tableau suivant répertorie toutes les options disponibles Régions AWS.

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| US East (Ohio) | us-east-2 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| USA Est (Virginie du Nord) | us-east-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| USA Ouest (Californie du Nord) | us-west-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Afrique (Le Cap) | af-south-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Hong Kong) | ap-east-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Hyderabad) | ap-south-2 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Jakarta) | ap-southeast-3 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Malaisie) | ap-southeast-5 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Melbourne) | ap-southeast-4 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Nouvelle Zélande) | ap-southeast-6 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Asie-Pacifique (Osaka) | ap-northeast-3 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Singapour) | ap-southeast-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Taipei) | ap-east-2 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Thaïlande) | ap-southeast-7 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Asie-Pacifique (Tokyo) | ap-northeast-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Canada (Centre) | ca-central-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Canada-Ouest (Calgary) | ca-west-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Francfort) | eu-central-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Irlande) | eu-west-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Londres) | eu-west-2 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Espagne) | eu-south-2 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | organizations.us-east-1.amazonaws.com | HTTPS |
| | | organizations-fips.us-east-1.amazonaws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Israël (Tel Aviv) | il-central-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Mexique (Centre) | mx-central-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Moyen-Orient (Bahreïn) | me-south-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Moyen-Orient (EAU) | me-central-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| Amérique du Sud (São Paulo) | sa-east-1 | organizations.us-east-1.amazonaws.com<br>organizations-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| AWS GovCloud (USA Est) | us-gov-east-1 | organizations.us-gov-west-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-Ouest) | us-gov-west-1 | organizations.us-gov-west-1.amazonaws.com | HTTPS |

# Facturation et tarification pour AWS Organizations

AWS Organizations est offert sans frais supplémentaires. Vous êtes facturé uniquement pour les AWS ressources utilisées par les utilisateurs et les rôles de vos comptes de membre. Par exemple,

vous payez les frais standard pour les instances Amazon EC2 qui sont utilisées par les utilisateurs ou rôles de vos comptes membres. Pour plus d'informations sur la tarification des autres AWS services, consultez la section AWS Tarification.

### Qui prend en charge les frais d'utilisation encourus par les utilisateurs d'un compte AWS membre de mon organisation ?

Le propriétaire du compte de gestion est responsable du paiement de toutes les utilisations, données et ressources utilisées par les comptes de l'organisation.

### Ma facture reflètera-t-elle la structure des unités organisationnelles que j'ai créée dans mon organisation ?

Votre facture ne reflétera pas la structure que vous avez définie dans votre organisation. Vous pouvez utiliser des balises de répartition des coûts individuelles Comptes AWS pour classer et suivre vos AWS coûts, et cette répartition sera visible dans la facture consolidée de votre organisation.

## Support et commentaires pour AWS Organizations

Nous apprécions vos commentaires. Vous pouvez publier vos commentaires et vos questions sur le forum AWS Organizations d'assistance. Pour plus d'informations sur les forums de AWS support, consultez l'aide des forums.

### Autres AWS ressources

- AWS Formations et cours — Liens vers des cours spécialisés et basés sur les rôles, ainsi que vers des ateliers d'autoformation pour vous aider à perfectionner vos AWS compétences et à acquérir une expérience pratique.
- AWS Outils de développement : liens vers des outils et des ressources de développement qui fournissent de la documentation, des exemples de code, des notes de publication et d'autres informations pour vous aider à créer des applications innovantes avec AWS.
- AWS Support Centre — Le centre de création et de gestion de vos dossiers de AWS Support. Comprend également des liens vers d'autres ressources utiles, telles que des forums, des informations techniques FAQs, l'état de santé des services et AWS Trusted Advisor.
- AWS Support : page Web principale contenant des informations sur le AWS support one-on-one, un canal d'assistance rapide destiné à vous aider à créer et à exécuter des applications dans le cloud.

- Contactez-nous — Un point de contact central pour les demandes concernant la AWS facturation, le compte, les événements, les abus et autres problèmes.
- AWS Conditions du site — Informations détaillées sur nos droits d'auteur et notre marque commerciale ; votre compte, votre licence et l'accès au site ; et d'autres sujets.

# Bonnes pratiques pour un environnement multi-comptes

Suivez ces recommandations pour vous aider à configurer et à gérer un environnement multi-comptes dans AWS Organizations.

Rubriques



## Compte et informations d'identification

### Activez la gestion de l'accès root pour simplifier la gestion des informations d'identification des utilisateurs root pour les comptes des membres

Nous vous recommandons d'activer la gestion de l'accès root pour vous aider à surveiller et à supprimer les informations d'identification des utilisateurs root pour les comptes des membres. La gestion de l'accès root empêche la récupération des informations d'identification de l'utilisateur root, améliorant ainsi la sécurité des comptes dans votre organisation.

- Supprimez les informations d'identification de l'utilisateur root pour les comptes membres afin d'empêcher la connexion à l'utilisateur root. Cela empêche également les comptes membres de récupérer l'utilisateur root.
- Supposons une session privilégiée pour effectuer les tâches suivantes sur les comptes des membres :
  - Supprimez une politique de compartiment mal configurée qui empêche tous les principaux d'accéder à un compartiment Amazon S3.
  - Supprimez une politique Amazon Simple Queue Service qui refuse à tous les principaux l'accès à une file d'attente Amazon SQS.
  - Autoriser un compte membre à récupérer ses informations d'identification d'utilisateur root. La personne ayant accès à l'e-mail de l'utilisateur root à la boîte de réception pour le compte membre peut réinitialiser le mot de passe de l'utilisateur root et se connecter en tant qu'utilisateur root du compte membre.

Une fois la gestion de l'accès root activée, les comptes membres nouvellement créés sont secure-by-default dépourvus d'informations d'identification d'utilisateur root, ce qui élimine le besoin d'une sécurité supplémentaire, telle que l'authentification MFA après le provisionnement.

Pour plus d'informations, voir Centraliser les informations d'identification des utilisateurs root pour les comptes des membres dans le Guide de l'Gestion des identités et des accès AWS utilisateur.

## Garder le numéro de téléphone du contact à jour

Pour récupérer l'accès à votre Compte AWS, il est essentiel de disposer d'un numéro de téléphone valide et actif vous permettant de recevoir des SMS ou des appels. Nous vous recommandons d'utiliser un numéro de téléphone dédié pour être sûr de AWS pouvoir vous contacter à des fins d'assistance et de rétablissement de votre compte. Vous pouvez facilement consulter et gérer les numéros de téléphone de votre compte via le AWS Management Console ou la gestion de compte APIs.

Il existe différentes manières d'obtenir un numéro de téléphone dédié qui vous permettra de AWS vous contacter. Nous vous recommandons vivement d'obtenir une carte SIM et un téléphone physique dédiés. Conservez le téléphone et la carte SIM en toute sécurité et à long terme afin de garantir que le numéro de téléphone reste disponible pour la récupération du compte. Assurez-vous également que l'équipe responsable des factures de téléphonie mobile comprend l'importance de ce numéro, même s'il reste inactif pendant de longues périodes. Il est essentiel que ce numéro de téléphone reste confidentiel au sein de votre organisation pour une protection supplémentaire.

Documentez le numéro de téléphone sur la page de la console Informations de AWS contact et partagez ses informations avec les équipes spécifiques qui doivent le connaître au sein de votre organisation. Cette approche permet de minimiser le risque associé au transfert du numéro de téléphone vers une autre carte SIM. Stockez le téléphone conformément à votre politique de sécurité des informations existante. Toutefois, ne stockez pas le téléphone au même endroit que les autres informations d'identification connexes. Tout accès au téléphone ou à son emplacement de stockage doit être consigné et surveillé. Si le numéro de téléphone associé à un compte change, mettez en place des processus de mise à jour du numéro de téléphone dans votre documentation existante.

## Utiliser une adresse e-mail de groupe pour les comptes root

Utilisez une adresse e-mail gérée par votre entreprise. Utilisez une adresse e-mail gérée par votre entreprise. Dans le cas où vous AWS devez contacter le propriétaire du compte, par exemple pour confirmer l'accès, le message électronique est distribué à plusieurs parties. Cette approche aide à

réduire le risque de retards dans l'intervention, même si les personnes sont en vacances, malades ou ont quitté l'entreprise.

# Structure de l'organisation et charges de travail

## Gestion de vos comptes au sein d'une seule organisation

Nous vous recommandons de créer une organisation unique et de gérer tous vos comptes au sein de cette organisation. Une organisation est une frontière de sécurité qui vous permet de maintenir la cohérence entre les comptes dans votre environnement. Vous pouvez appliquer de manière centralisée des stratégies ou des configurations de niveau de service à tous les comptes d'une organisation. Si vous voulez appliquer des règles cohérentes, une visibilité centrale et des contrôles programmatiques dans votre environnement multi-comptes, il est préférable de le faire au sein d'une seule organisation.

## Regrouper les charges de travail en fonction de l'objectif de l'entreprise et non de la structure hiérarchique

Nous vous recommandons d'isoler les environnements de charge de travail de production et les données dans le cadre de votre environnement orienté charge de travail OUs de haut niveau. Vous OUs devez vous baser sur un ensemble de contrôles communs plutôt que de refléter la structure hiérarchique de votre entreprise. Outre la production OUs, nous vous recommandons de définir une ou plusieurs applications hors production OUs contenant des comptes et des environnements de charge de travail utilisés pour développer et tester des charges de travail. Pour obtenir des conseils supplémentaires, voir Organisation axée sur la charge de travail OUs.

## Utiliser plusieurs comptes pour organiser vos charges de travail

An Compte AWS fournit une sécurité naturelle, un accès et des limites de facturation pour vos AWS ressources. L'utilisation de plusieurs comptes présente des avantages, car elle vous permet de répartir les quotas au niveau du compte et les limites de taux de demande d'API, ainsi que d'autres avantages énumérés ici. Nous vous recommandons d'utiliser un certain nombre de comptes de base à l'échelle de l'organisation, tels que les comptes pour la sécurité, la journalisation et l'infrastructure. Pour les comptes de charge de travail, vous devez séparer les charges de travail de production des charges de test/development travail dans des comptes distincts.

# Gestion des services et des coûts

## Activez AWS les services au niveau de l'organisation à l'aide de la console de service ou API/CLI des opérations

À titre de bonne pratique, nous vous recommandons d'activer ou de désactiver tous les services auxquels vous souhaitez vous intégrer AWS Organizations en utilisant la console de ce service ou des opérations d'API/commandes CLI équivalentes. Grâce à cette méthode, le AWS service peut effectuer toutes les étapes d'initialisation requises pour votre organisation, telles que la création des ressources requises et le nettoyage des ressources lors de la désactivation du service. Gestion de compte AWS est le seul service qui nécessite l'utilisation de la AWS Organizations console ou APIs son activation. Pour consulter la liste des services intégrés à AWS Organizations, voirServices AWS que vous pouvez utiliser avec AWS Organizations.

## Utiliser les outils de facturation pour suivre les coûts et optimiser l'utilisation des ressources

Lorsque vous gérez une organisation, vous recevez une facture consolidée qui couvre tous les frais des comptes de votre organisation. Pour les utilisateurs professionnels qui ont besoin d'accéder à la visibilité des coûts, vous pouvez fournir un rôle dans le compte de gestion avec des autorisations restreintes en lecture seule pour examiner les outils de facturation et de coûts. Par exemple, vous pouvez créer un ensemble d'autorisations donnant accès aux rapports de facturation, ou utiliser AWS Cost Explorer Service (un outil permettant de visualiser les tendances des coûts au fil du temps), et les services d'optimisation des coûts tels qu'Amazon S3 Storage Lens et AWS Compute Optimizer.

## Planifier la stratégie de balisage et l'application des balises dans l'ensemble des ressources de votre organisation

Au fur et à mesure que vos comptes et vos charges de travail évoluent, les balises peuvent s'avérer utiles pour le suivi des coûts, le contrôle d'accès et l'organisation des ressources. Pour les stratégies de dénomination relatives au balisage, suivez les instructions de la section Marquage de vos AWS ressources. Outre les ressources, vous pouvez créer des balises sur la racine, les comptes et les politiques de l'organisation. OUs Pour plus d'informations, consultez Créer votre stratégie de balisage (français non garanti).

# Commencer avec AWS Organizations

Les rubriques suivantes fournissent des informations qui vous aideront à commencer à utiliser AWS Organizations. Vous pouvez également utiliser les didacticiels suivants pour commencer à effectuer des tâches en utilisant AWS Organizations.

Didacticiel : Création et configuration d'une organisation

Lancez-vous en step-by-step suivant les instructions pour créer votre organisation, inviter vos premiers comptes membres, créer une hiérarchie d'unités d'organisation contenant vos comptes et appliquer certaines politiques de contrôle des services (SCPs).

Tutoriel : Surveillez les modifications importantes apportées à votre organisation avec Amazon EventBridge

Surveillez les principaux changements dans votre organisation en configurant Amazon EventBridge pour qu'il déclenche une alarme sous la forme d'un e-mail, d'un SMS ou d'une entrée de journal lorsque des actions que vous avez désignées se produisent dans votre organisation. Par exemple, de nombreuses organisations veulent savoir quand un nouveau compte est créé ou quand un compte tente de quitter l'organisation.

Rubriques



# S'inscrire à AWS

Rubriques

## Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

## Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

# Accès AWS Organizations

Vous pouvez travailler avec AWS Organizations l'une des méthodes suivantes :

AWS Management Console

La AWS Organizations console est une interface basée sur un navigateur que vous pouvez utiliser pour gérer votre organisation et vos AWS ressources. Vous pouvez effectuer n'importe quelle tâche de votre organisation à l'aide de la console.

AWS Outils de ligne de commande

Avec les outils de ligne de AWS commande, vous pouvez émettre des commandes sur la ligne de commande de votre système pour exécuter AWS Organizations des AWS tâches. L'utilisation de la ligne de commande peut être plus rapide et plus pratique que la console. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts exécutant des tâches AWS .

AWS fournit deux ensembles d'outils de ligne de commande :

- AWS Command Line Interface

  Le AWS Command Line Interface (AWS CLI) est un outil unifié pour gérer votre Services AWS. Avec un seul outil à télécharger et à configurer, vous pouvez en contrôler plusieurs Services AWS depuis la ligne de commande et les automatiser par le biais de scripts.

  Pour plus d'informations sur l'installation et l'utilisation du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

- AWS Tools for Windows PowerShell

  Les outils pour Windows PowerShell permettent aux développeurs et aux administrateurs de gérer leurs ressources Services AWS et leurs ressources dans l'environnement PowerShell de script. Vous pouvez gérer vos AWS ressources à l'aide des mêmes PowerShell outils que ceux que vous utilisez pour gérer vos environnements Windows, Linux et macOS.

  Pour plus d'informations sur l'installation et l'utilisation des outils pour Windows PowerShell, consultez le guide de Outils AWS pour PowerShell l'utilisateur.

AWS SDKs

Il AWS SDKs s'agit de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (par exemple, Java, Python, Ruby, .NET, iOS et Android). Ils se

SDKs chargent de tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur les AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

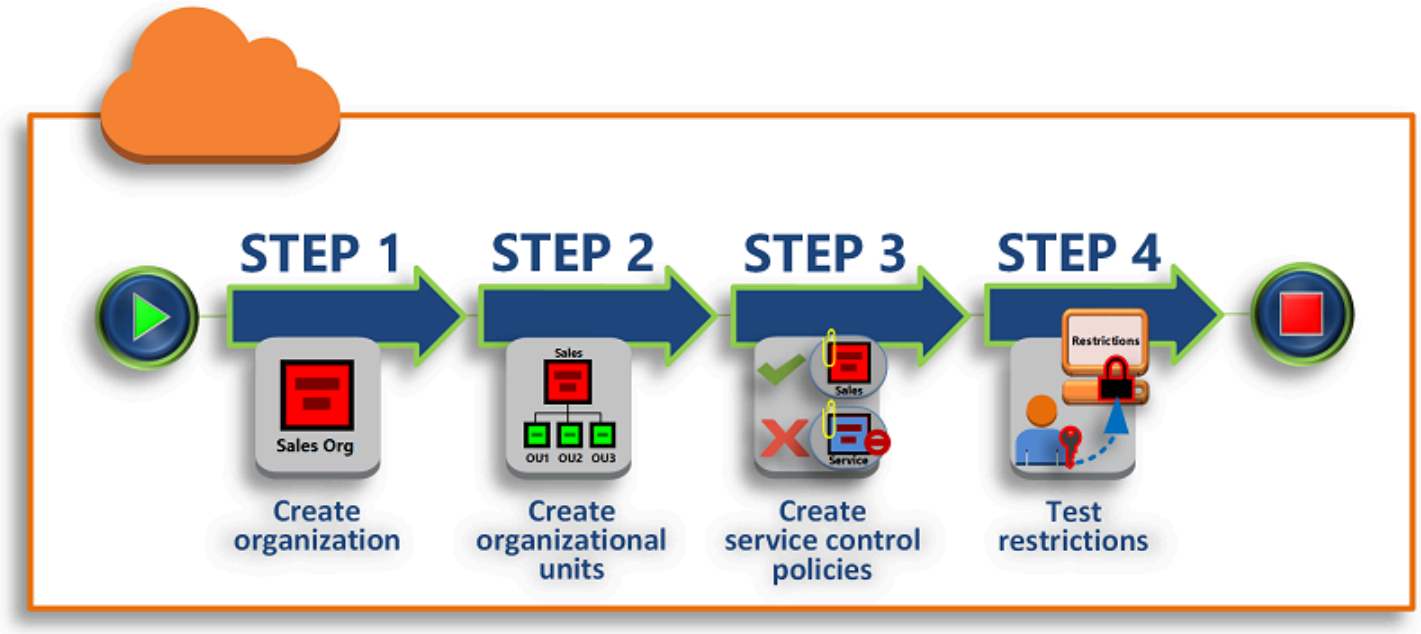
AWS Organizations API de requête HTTPS

L'API de requête AWS Organizations HTTPS vous donne un accès programmatique à AWS Organizations et AWS. L'API de requête HTTPS vous permet d'envoyer des demandes HTTPS directement au service. Lorsque vous utilisez l'API HTTPS, vous devez inclure du code pour signer numériquement les demandes à l'aide de vos informations d'identification. Pour plus d'informations, consultez Appel de l'API à l'aide de demandes de requête HTTP et la Référence des API AWS Organizations.

# Didacticiel : Création et configuration d'une organisation

Dans ce didacticiel, vous allez créer votre organisation et la configurer avec deux comptes AWS membres. Vous créez l'un des comptes membres dans votre organisation et vous invitez l'autre compte à rejoindre celle-ci. Ensuite, vous utilisez la technique de liste d'autorisations pour spécifier que les administrateurs de ce compte peuvent déléguer uniquement les services et actions répertoriés explicitement. Cela permet aux administrateurs de valider tout nouveau service AWS introduit avant d'autoriser son utilisation par un autre membre de votre entreprise. Ainsi, si un nouveau service est AWS introduit, il reste interdit jusqu'à ce qu'un administrateur ajoute le service à la liste des services autorisés dans la politique appropriée. Le didacticiel explique également comment utiliser une liste de refus pour garantir qu'aucun utilisateur d'un compte membre ne puisse modifier la configuration des journaux d'audit AWS CloudTrail créés.

L'illustration suivante montre les principales étapes du didacticiel.




### Étape 1 : Créer votre organisation

Au cours de cette étape, vous créez une organisation avec votre compte de gestion actuel Compte AWS . Vous en invitez également un Compte AWS à rejoindre votre organisation et vous créez un deuxième compte en tant que compte membre.

### Étape 2 : Créer les unités d'organisation

Vous devez ensuite créer deux unités organisationnelles (OUs) dans votre nouvelle organisation et y placer les comptes des membres OUs.

### Étape 3 : Créer les politiques de contrôle des services

Vous pouvez appliquer des restrictions aux actions pouvant être déléguées aux utilisateurs et aux rôles dans les comptes des membres en utilisant les politiques de contrôle des services (SCPs). Au cours de cette étape, vous en créez deux SCPs et vous les associez au OUs dans votre organisation.

### Étape 4 : Tester les politiques de votre organisation

Vous pouvez vous connecter en tant qu'utilisateur à partir de chacun des comptes de test et voir les effets qu' SCPs ils ont sur les comptes.

Aucune des étapes de ce didacticiel n'entraîne de frais pour votre AWS facture. AWS Organizations est un service gratuit.

## Conditions préalables

Ce didacticiel part du principe que vous avez accès à deux sites existants Comptes AWS (vous en créez un troisième dans le cadre de ce didacticiel) et que vous pouvez vous connecter à chacun d'eux en tant qu'administrateur.

Le didacticiel fait référence aux comptes comme suit :

- `111111111111` : compte que vous utilisez pour créer l'organisation. Ce compte devient le compte de gestion. Le propriétaire de ce compte dispose de l'adresse e-mail `OrgAccount111@example.com`.
- `222222222222` : compte que vous invitez à rejoindre l'organisation en tant que compte membre. Le propriétaire de ce compte dispose de l'adresse e-mail `member222@example.com`.
- `333333333333` : compte que vous créez en tant que membre de l'organisation. Le propriétaire de ce compte dispose de l'adresse e-mail `member333@example.com`.

Remplacez les valeurs ci-dessus par celles qui sont associées à vos comptes de test. Nous vous recommandons de ne pas utiliser des comptes de production pour ce didacticiel.

## Étape 1 : Créer votre organisation

Au cours de cette étape, vous vous connectez au compte 111111111111 en tant qu'administrateur, créez une organisation avec ce compte comme compte de gestion et invitez un compte existant, 222222222222, à rejoindre l'organisation en tant que compte membre.

AWS Management Console

1. Connectez-vous en AWS tant qu'administrateur du compte 111111111111 et ouvrez la console.AWS Organizations
2. Sur la page d'introduction, choisissez Créer une organisation.
3. Dans la boîte de dialogue de confirmation, choisissez Créer une organisation.

> **Note**
>
> Par défaut, l'organisation est créée avec toutes les fonctions activées. Vous pouvez également choisir de créer votre organisation avec uniquement les fonctions de facturation consolidée activées.

AWS crée l'organisation et vous montre la Comptes AWSpage. Si vous êtes sur une autre page, choisissez Comptes AWS dans le panneau de navigation de gauche.

Si l'adresse e-mail du compte que vous utilisez n'a jamais été vérifiée par AWS, un e-mail de vérification est automatiquement envoyé à l'adresse associée à votre compte de gestion. Il peut y avoir un délai avant la réception de l'e-mail de vérification.

4. Validez votre adresse e-mail dans un délai de 24 heures. Pour de plus amples informations, veuillez consulter Vérification de l'adresse e-mail avec AWS Organizations.

Vous disposez à présent d'une organisation avec votre compte comme seul membre. Il s'agit du compte de gestion de l'organisation.

## Inviter un compte existant à rejoindre votre organisation

Maintenant que vous disposez d'une organisation, vous pouvez commencer à la remplir avec des comptes. Dans les étapes de cette section, vous invitez un compte existant à rejoindre votre organisation en tant que membre.

AWS Management Console

Pour inviter un compte existant à rejoindre votre organisation

1. Accédez à la page Comptes AWS, puis choisissez Ajouter un Compte AWS.
2. Sur la Compte AWS page Ajouter un objet, choisissez Inviter un existant Compte AWS.
3. Dans la zone Adresse e-mail ou ID de compte d'un Compte AWS à inviter, saisissez l'adresse e-mail du propriétaire du compte que vous souhaitez inviter, sous une forme similaire à ceci : **`member222@example.com`**. Sinon, si vous connaissez le numéro Compte AWS d'identification, vous pouvez le saisir à la place.
4. Saisissez le texte de votre choix dans la zone Message à inclure dans l'e-mail d'invitation. Ce texte est inclus dans l'e-mail qui est envoyé au propriétaire du compte.
5. Choisissez Envoyer une invitation. AWS Organizations envoie l'invitation au propriétaire du compte.

> **Important**
>
> Développez le message d'erreur si possible. Si l'erreur indique que vous avez dépassé vos limites de compte pour l'organisation ou que vous ne pouvez pas ajouter un compte parce que votre organisation est toujours en cours d'initialisation, attendez une heure après avoir créé l'organisation, puis réessayez. Si vous obtenez toujours la même erreur, contactez le Support AWS.

6. Dans le cadre de ce didacticiel, vous devez maintenant accepter votre propre invitation. Effectuez l'une des actions suivantes pour accéder à la page Invitations dans la console :

   - Ouvrez l'e-mail AWS envoyé depuis le compte de gestion et cliquez sur le lien pour accepter l'invitation. Lorsque vous êtes invité à vous connecter, connectez-vous en tant qu'administrateur du compte membre invité.
   - Ouvrez la console AWS Organizations et accédez à la page Invitations.

7. Dans la page Comptes AWS, choisissez Accepter, puis Confirmer.

> **Tip**
>
> L'invitation peut arriver avec du retard et vous devrez peut-être attendre avant de pouvoir l'accepter.

8. Déconnectez-vous de votre compte membre, puis reconnectez-vous en tant qu'administrateur de votre compte de gestion.

## Création d'un compte membre

Au cours des étapes décrites dans cette section, vous créez un Compte AWS membre automatiquement membre de l'organisation. Dans le didacticiel, ce compte identifié 333333333333.

AWS Management Console

Pour créer un compte membre

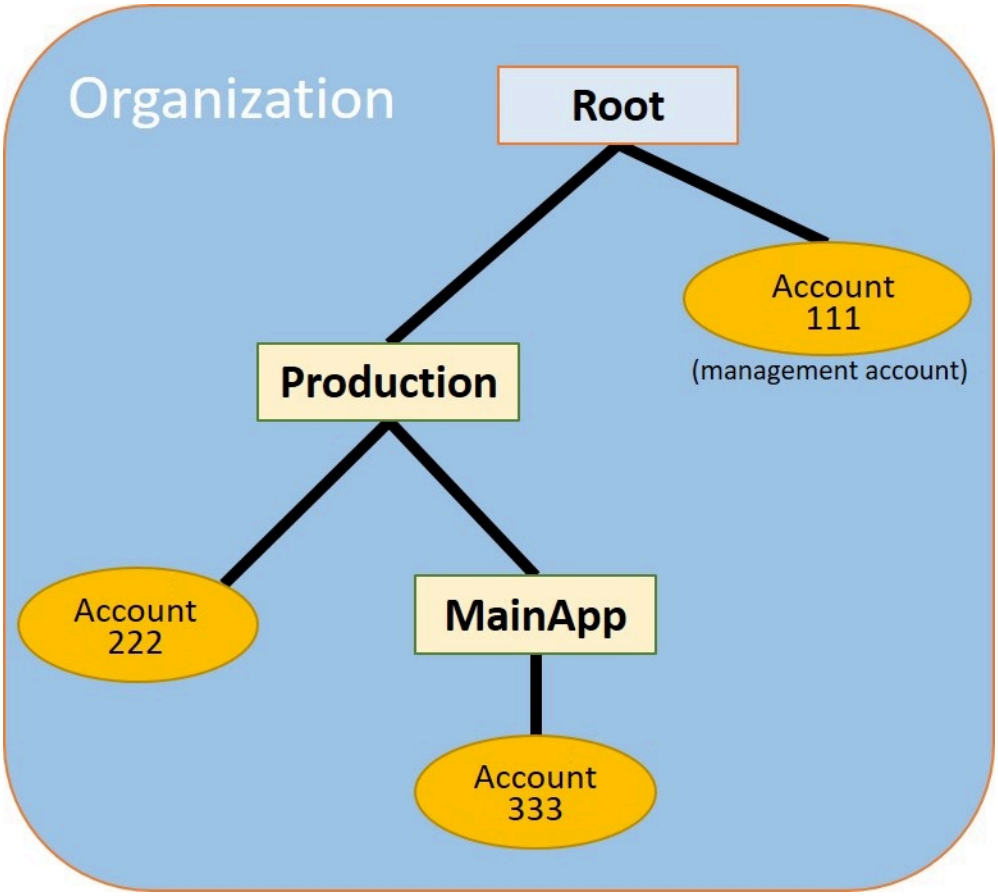
1. Sur la AWS Organizations console, sur la Comptes AWSpage, choisissez Ajouter Compte AWS.
2. Dans la page Ajouter un Compte AWS, choisissez Créer un Compte AWS.

3. Dans le champ Nom du Compte AWS , saisissez un nom pour le compte, tel que **`MainApp Account`**.
4. Pour Adresse e-mail de l'utilisateur racine du compte, saisissez l'adresse e-mail de la personne qui doit recevoir les communications au nom du compte. Cette valeur doit être unique globalement. Deux comptes ne peuvent pas avoir la même adresse e-mail. Par exemple, vous pouvez utiliser quelque chose comme **`mainapp@example.com`**.
5. Pour Nom du rôle IAM, vous pouvez laisser ce champ vide afin d'utiliser automatiquement le nom de rôle par défaut `OrganizationAccountAccessRole` ou vous pouvez fournir votre propre nom. Ce rôle vous permet d'accéder au nouveau compte membre lorsque celui-ci est connecté en tant qu'utilisateur IAM dans le compte de gestion. Dans le cadre de ce didacticiel, laissez ce champ vide pour demander à AWS Organizations de créer le rôle avec le nom par défaut.
6. Choisissez Créer Compte AWS. Vous devrez peut-être patienter quelques instants et actualiser la page pour que le nouveau compte apparaisse sur la page Comptes AWS.

> **Important**
>
> Si vous obtenez une erreur indiquant que vous avez dépassé vos limites de compte pour l'organisation ou que vous ne pouvez pas ajouter un compte parce que votre organisation est toujours en cours d'initialisation, patientez jusqu'à une heure après avoir créé l'organisation et réessayez. Si vous obtenez toujours la même erreur, contactez le Support AWS.

## Étape 2 : Créer les unités d'organisation

Au cours des étapes décrites dans cette section, vous allez créer des unités organisationnelles (OUs) et y placer vos comptes de membres. À la fin, votre hiérarchie ressemble à l'illustration suivante. Le compte de gestion reste dans la racine. Un compte membre est transféré vers l'unité d'organisation de production, et l'autre compte de membre est transféré vers l' MainApp unité d'organisation, qui est un enfant de Production.




AWS Management Console

Pour créer et remplir le OUs

> **Note**
>
> Dans les étapes suivantes, vous interagissez avec des objets pour lesquels vous pouvez choisir soit le nom de l'objet lui-même, soit la case d'option en regard de l'objet.
>
> - Si vous choisissez le nom de l'objet, vous ouvrez une nouvelle page qui affiche les détails des objets.
> - Si vous choisissez le bouton d'option en regard de l'objet, vous identifiez l'objet sur lequel agira une autre action, par exemple le choix d'une option de menu.
>
> Dans les étapes qui suivent, vous choisirez la case d'option afin de pouvoir agir ensuite sur l'objet associé en faisant des choix dans les menus.

1. Dans la console AWS Organizations, accédez à la page Comptes AWS.
2. Cochez la case
   
   en regard du conteneur Racine.
3. Choisissez le menu déroulant Actions, puis sous Unité organisationnelle, choisissez Créer un nouveau.
4. Dans la page Créer une unité d'organisation dans la racine, pour Nom de l'unité d'organisation, saisissez **`Production`**, puis choisissez Créer une unité d'organisation.
5. Cochez la case
   
   en regard de votre nouvelle UO Production.
6. Choisissez Actions, puis, sous Unité d'organisation, choisissez Créer.
7. Dans la page Créer une unité d'organisation dans Production, pour **`MainApp`**Nom de l'unité d'organisation, saisissez , puis choisissez Créer une unité d'organisation.

   Vous pouvez désormais y transférer vos comptes de membres OUs.
8. Revenez à la page Comptes AWS, puis développez l'arborescence sous votre UO Production en choisissant le triangle
   
   en regard de cette UO. Cela affiche l'MainAppUO en tant qu'enfant de Production.
9. À côté de 333333333333, cochez la case
   
   (et non le nom), choisissez Actions, puis, sous Compte AWS, choisissez Déplacer.
10. Sur la page Déplacer Compte AWS « 333333333333 », choisissez le triangle situé à côté de Production pour le développer. À côté de MainApp, choisissez le bouton radio
    
    (pas son nom), puis choisissez Déplacer Compte AWS.
11. À côté de 222222222222, cochez la case
    
    (et non le nom), choisissez Actions, puis, sous Compte AWS, choisissez Déplacer.
12. Sur la page Déplacer Compte AWS « 222222222222 », à côté de Production, choisissez le bouton radio (pas son nom), puis choisissez Déplacer. Compte AWS

# Étape 3 : Créer les politiques de contrôle des services

Dans les étapes décrites dans cette section, vous créez trois politiques de contrôle des services (SCPs) et vous les associez à la racine et OUs à la afin de limiter les actions des utilisateurs des comptes de l'organisation. Le premier SCP empêche toute personne appartenant à l'un des comptes membres de créer ou de modifier AWS CloudTrail les journaux que vous configurez. Le compte de gestion n'est affecté par aucun SCP. Par conséquent, après avoir appliqué le CloudTrail SCP, vous devez créer des journaux à partir du compte de gestion.

## Activation du type de politique de contrôle des services pour l'organisation

Pour pouvoir attacher une politique de tout type à une racine ou à n'importe quelle unité d'organisation au sein d'une racine, vous devez activer le type de politique pour l'organisation. Les types de politiques ne sont pas activés par défaut. Les étapes de cette section vous montrent comment activer le type de politique de contrôle des services (SCP) pour la racine de votre organisation.

AWS Management Console

Pour activer SCPs les activités de votre organisation

1. Accédez à la page Politiques, puis choisissez Politiques de contrôle des services.
2. Dans la page Politiques de contrôle des services, choisissez Activer les politiques de contrôle des services.

   Une bannière verte apparaît pour vous informer que vous pouvez désormais créer SCPs dans votre organisation.

## Créez votre SCPs

Maintenant que les politiques de contrôle des services sont activées dans votre organisation, vous pouvez créer les trois politiques dont vous avez besoin pour ce didacticiel.

AWS Management Console

Pour créer le premier SCP qui bloque les actions CloudTrail de configuration

1. Accédez à la page Politiques, puis choisissez Politiques de contrôle des services.
2. Sur la page Politiques de contrôle des services, choisissez Créer une politique.

3. Pour Policy name (Nom de la politique), saisissez **`Block CloudTrail Configuration Actions`**.
4. Dans la section Politique, dans la liste des services de droite, sélectionnez CloudTrail le service. Choisissez ensuite les actions suivantes : AddTagsCreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging, et UpdateTrail.
5. Toujours dans le volet droit, choisissez Ajouter une ressource CloudTrailet spécifiez toutes les ressources. Choisissez ensuite Ajouter une ressource.

   L'instruction de politique sur la gauche devrait ressembler à ce qui suit.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Choisissez Create Policy (Créer une politique).

La deuxième politique définit une liste d'autorisations de tous les services et opérations que vous souhaitez activer pour les utilisateurs et rôles dans l'unité d'organisation Production. Lorsque vous avez terminé, les utilisateurs de l'UO Production peuvent accéder uniquement aux services et actions répertoriés.

AWS Management Console

Pour créer la deuxième politique, qui autorise les services approuvés pour l'UO Production,

1. Sur la page Politiques de contrôle des services, choisissez Créer une politique.
2. Pour Nom de la politique, saisissez **`Allow List for All Approved Services`**.
3. Placez votre curseur dans le panneau droit de la section Politique et collez-y une politique similaire à celle-ci.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. Choisissez Create Policy (Créer une politique).

La politique finale fournit une liste de refus des services dont l'utilisation est bloquée dans l'unité d' MainApp organisation. Dans le cadre de ce didacticiel, vous bloquez l'accès à Amazon DynamoDB pour tous les comptes figurant dans l'unité d'organisation. MainApp

AWS Management Console

Pour créer la troisième politique qui refuse l'accès aux services qui ne peuvent pas être utilisés dans l'unité d' MainApp organisation

1. Sur la page Politiques de contrôle des services, choisissez Créer une politique.
2. Pour Nom de la politique, saisissez **`Deny List for MainApp Prohibited Services`**.
3. Dans la section Politique sur la gauche, choisissez Amazon DynamoDB pour le service. Pour l'action, choisissez Toutes les actions.
4. Toujours dans le panneau de gauche, choisissez Ajouter une ressource et spécifiez DynamoDB et Toutes les ressources. Choisissez ensuite Ajouter une ressource.

   L'instruction de politique sur la droite se met à jour et ressemble à ce qui suit.

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [ "dynamodb:*" ],
      "Resource": [ "*" ]
    }
  ]
}
```

5. Choisissez Créer une politique pour enregistrer la SCP.

## Attachez-le SCPs à votre OUs

Maintenant qu'ils SCPs existent et sont activés pour votre racine, vous pouvez les attacher à la racine et OUs.

AWS Management Console

Pour associer les politiques à la racine et au OUs

1. Accédez à la page Comptes AWS.

2. Sur la page Comptes AWS, choisissez Root (Racine) (le nom, pas la case d'option) pour accéder à sa page de détails.
3. Dans la page de détails Racine, choisissez l'onglet Politiques, puis, sous Politiques de contrôle des services, choisissez Attacher.
4. Dans la page Attacher une politique de contrôle des services, choisissez la case d'option en regard de la politique de contrôle des services nommée `Block CloudTrail Configuration Actions`, puis choisissez Attacher. Dans ce didacticiel, vous l'attachez à la racine afin qu'il affecte tous les comptes membres afin d'empêcher quiconque de modifier la façon dont vous l'avez configuré CloudTrail.

   La page de détails de la racine, onglet Politiques, indique désormais que deux SCPs sont attachés à la racine : celui que vous venez d'attacher et le `FullAWSAccess` SCP par défaut.
5. Retournez à la page Comptes AWS, puis choisissez l'UO Production (le nom, pas la case d'option) pour accéder à sa page de détails.
6. Dans la page de détails de l'UO Production, choisissez l'onglet Politiques.
7. Sous Politiques de contrôle des services, choisissez Attacher.
8. Dans la page Attacher une politique de contrôle des services, choisissez la case d'option en regard de `Allow List for All Approved Services`, puis choisissez Attacher. Cela permet aux utilisateurs ou rôles des comptes membres de l'UO Production d'accéder aux services approuvés.
9. Cliquez à nouveau sur l'onglet Politiques pour voir que deux SCPs sont attachés à l'unité d'organisation : celui que vous venez de joindre et le `FullAWSAccess` SCP par défaut. Cependant, comme la politique de contrôle des services `FullAWSAccess` est également une liste d'autorisations qui autorise tous les services et actions, vous devez maintenant détacher cette politique pour vous assurer que seuls vos services approuvés sont autorisés.
10. Pour supprimer la politique par défaut de l'unité d'organisation de production, cliquez sur le bouton radio Complet AWSAccess, choisissez Détacher, puis dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

    Une fois que vous avez supprimé cette politique par défaut, tous les comptes membres sous l'UO Production perdent immédiatement l'accès aux actions et services qui ne sont pas dans la SCP de liste d'autorisations que vous avez attachée lors des étapes précédentes. Toutes les demandes d'utilisation d'actions qui ne sont pas incluses dans la SCP Liste d'autorisations pour tous les services approuvés sont refusées. Cela est vrai même si un administrateur d'un

compte accorde l'accès à un autre service en attachant une politique d'autorisations IAM à un utilisateur dans l'un des comptes membres.

11. Vous pouvez désormais joindre le SCP nommé `Deny List for MainApp Prohibited services` pour empêcher toute personne figurant dans les comptes de l'unité d'organisation MainApp d'utiliser l'un des services restreints.

    Pour ce faire, accédez à la Comptes AWSpage, choisissez l'icône en forme de triangle pour développer la branche de l'unité d'organisation de production, puis MainAppchoisissez l'unité d'organisation (son nom, pas le bouton radio) pour accéder à son contenu.

12. Sur la page de MainAppdétails, choisissez l'onglet Politiques.
13. Sous Politiques de contrôle des services, choisissez Joindre, puis dans la liste des politiques disponibles, cliquez sur le bouton radio à côté de Liste de refus pour les services MainApp interdits, puis choisissez Attacher une politique.

## Étape 4 : Tester les politiques de votre organisation

Vous pouvez maintenant vous connecter en tant qu'utilisateur de l'un des comptes membres et essayer d'effectuer différentes actions AWS :

- Si vous vous connectez en tant qu'utilisateur du compte de gestion, vous pouvez effectuer toutes les opérations qui sont autorisées par les politiques d'autorisation IAM. Ils SCPs n'affectent aucun utilisateur ou rôle dans le compte de gestion, quelle que soit la racine ou l'unité d'organisation dans laquelle se trouve le compte.
- Si vous vous connectez en tant qu'utilisateur sur le compte 222222222222, vous pouvez effectuer toutes les actions autorisées par la liste des autorisations. AWS Organizations refuse toute tentative d'exécution d'une action dans un service ne figurant pas dans la liste des services autorisés. AWS Organizations Refuse également toute tentative d'exécution de l'une des actions de CloudTrail configuration.
- Si vous vous connectez en tant qu'utilisateur du compte 333333333333, vous pouvez effectuer toutes les actions permises par la liste d'autorisations et qui ne sont pas bloquées par la liste de refus. AWS Organizations refuse toute tentative d'exécuter une action qui n'est pas dans la politique de liste d'autorisations et d'exécuter une action qui est dans la politique de liste de refus. AWS Organizations Refuse également toute tentative d'exécution de l'une des actions de CloudTrail configuration.

# Tutoriel : Surveillez les modifications importantes apportées à votre organisation avec Amazon EventBridge

Ce didacticiel explique comment configurer Amazon EventBridge, anciennement Amazon CloudWatch Events, pour surveiller les modifications apportées par votre organisation. Vous commencez par configurer une règle qui est déclenchée lorsque des utilisateurs appellent des opérations AWS Organizations spécifiques. Ensuite, vous configurez Amazon EventBridge pour exécuter une AWS Lambda fonction lorsque la règle est déclenchée, et vous configurez Amazon SNS pour envoyer un e-mail contenant des détails sur l'événement.

L'illustration suivante montre les principales étapes du didacticiel.

Étape 1 : Configuration d'un journal d'activité et d'un sélecteur d'événements

Créez un journal, appelé sentier, dans AWS CloudTrail. Vous le configurez pour capturer tous les appels d'API.

Étape 2 : Configuration d'une fonction Lambda

Créez une AWS Lambda fonction qui enregistre les détails de l'événement dans un compartiment S3.

Étape 3 : Création d'une rubrique Amazon SNS qui envoie des e-mails aux abonnés

Créez une rubrique Amazon SNS qui envoie des e-mails à ses abonnés, puis abonnez-vous vous-même à la rubrique.

Étape 4 : créer une EventBridge règle Amazon

Créez une règle qui indique EventBridge à Amazon de transmettre les détails des appels d'API spécifiés à la fonction Lambda et aux abonnés aux rubriques SNS.

Étape 5 : testez votre EventBridge règle Amazon

Testez votre nouvelle règle en exécutant l'une des opérations surveillées. Dans ce didacticiel, l'opération surveillée est la création d'une unité d'organisation (UO). Vous affichez l'entrée de journal créée par la fonction Lambda et vous consultez l'e-mail qu'Amazon SNS envoie aux abonnés.

> **Conseil**
>
> Vous pouvez également utiliser ce didacticiel comme guide pour configurer des opérations similaires, telles que l'envoi de notifications par e-mail une fois la création du compte terminée. Comme la création du compte est une opération asynchrone, vous n'êtes pas informé par défaut lorsqu'elle se termine. Pour plus d'informations sur l'utilisation AWS CloudTrail et Amazon EventBridge avec AWS Organizations, consultezConnexion et surveillance AWS Organizations.

## Conditions préalables

Ce didacticiel suppose ce qui suit :

- Vous pouvez vous connecter en AWS Management Console tant qu'utilisateur IAM depuis le compte de gestion de votre organisation. L'utilisateur IAM doit être autorisé à créer et à configurer une connexion CloudTrail, une fonction dans Lambda, une rubrique dans Amazon SNS et une règle dans Amazon. EventBridge Pour plus d'informations sur l'octroi d'autorisations, consultez Gestion des accès dans le Guide de l'utilisateur IAM ou dans le guide du service pour lequel vous souhaitez configurer l'accès.
- Vous avez accès à un compartiment Amazon Simple Storage Service (Amazon S3) existant (ou vous êtes autorisé à créer un compartiment) pour recevoir CloudTrail le journal que vous avez configuré à l'étape 1.

> **Important**
>
> Actuellement, AWS Organizations il est hébergé uniquement dans la région de l'est des États-Unis (Virginie du Nord) (même s'il est disponible dans le monde entier). Pour effectuer les étapes de ce didacticiel, vous devez configurer le AWS Management Console pour utiliser cette région.

# Étape 1 : Configuration d'un journal d'activité et d'un sélecteur d'événements

Au cours de cette étape, vous vous connectez au compte de gestion et vous configurez un journal (appelé journal d'activité) dans AWS CloudTrail. Vous configurez également un sélecteur d'événements sur le parcours pour capturer tous les appels d' read/write API afin qu'Amazon EventBridge ait des appels à déclencher.

Pour créer un journal de suivi

1. Connectez-vous en AWS tant qu'administrateur du compte de gestion de l'organisation, puis ouvrez la CloudTrail console à l'adressehttps://console.aws.amazon.com/cloudtrail/.
2. Sur la barre de navigation dans le coin supérieur droit de la console, choisissez la région USA Est (Virginie du Nord). Si vous choisissez une autre région, AWS Organizations elle n'apparaît pas comme une option dans les paramètres de EventBridge configuration d'Amazon et CloudTrail ne capture aucune information à ce sujet AWS Organizations.
3. Dans le panneau de navigation, choisissez Journaux d'activité.
4. Choisissez Créer un journal d'activité).
5. Pour Nom du journal d'activité, saisissez **`My-Test-Trail`**.
6. Exécutez l'une des options suivantes pour spécifier où CloudTrail doit être livré ses journaux :

   - Si vous devez créer un compartiment, choisissez Create new S3 bucket (Créer un compartiment S3), puis, pour Trail log bucket and folder (Compartiment et dossier des journaux de suivi), saisissez le nom du nouveau compartiment.

     > **Note**
     >
     > Les noms de compartiment S3 doivent être globalement uniques.

   - Si vous disposez déjà d'un compartiment, choisissez Use existing S3 bucket (Utiliser un compartiment S3 existant), puis choisissez le nom du compartiment dans la liste de compartiments S3.
7. Choisissez Suivant.
8. Sur la page Choisir les événements du journal, dans la section Événements de gestion, choisissez Read (Lire) et Write (Écrire).
9. Choisissez Suivant.

10. Passez en revue vos sélections, puis choisissez Create trail (Créer un journal d'activité).

Amazon vous EventBridge permet de choisir entre plusieurs méthodes différentes pour envoyer des alertes lorsqu'une règle d'alarme correspond à un appel d'API entrant. Ce didacticiel explique deux méthodes : l'appel d'une fonction Lambda qui peut consigner l'appel d'API, et l'envoi d'informations vers une rubrique Amazon SNS qui envoie un e-mail ou un SMS aux abonnés de la rubrique. Dans les deux prochaines étapes, vous allez créer les composants dont vous avez besoin : la fonction Lambda et la rubrique Amazon SNS.

## Étape 2 : Configuration d'une fonction Lambda

Au cours de cette étape, vous créez une fonction Lambda qui enregistre l'activité de l'API qui lui est envoyée par la EventBridge règle Amazon que vous configurez ultérieurement.

Pour créer une fonction Lambda qui enregistre les événements Amazon EventBridge

1. Ouvrez la AWS Lambda console à l'adressehttps://console.aws.amazon.com/lambda/.
2. Si vous débutez avec Lambda, choisissez Get Started Now (Démarrez maintenant) sur la page d'accueil ; sinon choisissez Create function (Créer une fonction).
3. Sur la page Créer une fonction, choisissez Use a blueprint (Utiliser un plan).
4. Dans la zone de recherche Blueprints (Plans), saisissez **`hello`** comme filtre et choisissez le plan hello-world.
5. Choisissez Configure (Configurer).
6. Sur la page Basic information (Informations de base), effectuez les opérations suivantes :
   a. Pour le nom de la fonction Lambda, saisissez **`LogOrganizationEvents`** dans la zone de texte Name (Nom).
   b. Pour Role (Rôle), choisissez Create a new role with basic Lambda permissions (Créer un nouveau rôle avec les autorisations Lambda de base). Ce rôle accorde à votre fonction Lambda les autorisations nécessaires pour accéder aux données dont celle-ci a besoin et pour écrire son journal de sortie.
7. Modifiez le code pour la fonction Lambda, comme illustré dans l'exemple suivant.

```
console.log('Loading function');

exports.handler = async (event, context) => {
```

```
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

Cet exemple de code consigne l'événement avec une chaîne de marqueur **`LogOrganizationEvents`**, suivie de la chaîne JSON qui constitue l'événement.

8. Choisissez Créer une fonction.

## Étape 3 : Création d'une rubrique Amazon SNS qui envoie des e-mails aux abonnés

Au cours de cette étape, vous allez créer une rubrique Amazon SNS qui envoie des informations à ses abonnés. Vous faites de cette rubrique une cible de la EventBridge règle Amazon que vous créerez ultérieurement.

Pour créer une rubrique Amazon SNS afin d'envoyer un e-mail aux abonnés

1. Ouvrez la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/.
2. Dans le panneau de navigation, choisissez Topics (Rubriques).
3. Choisissez Create new topic (Créer une rubrique).
   a. Pour Topic name (Nom de la rubrique), saisissez **`OrganizationsCloudWatchTopic`**.
   b. Pour Display name (Nom complet), saisissez **`OrgsCWEvnt`**.
   c. Choisissez Create topic (Créer la rubrique).
4. Vous pouvez désormais créer un abonnement pour la rubrique. Choisissez l'ARN de la rubrique que vous venez de créer.
5. Choisissez Create subscription (Créer un abonnement).
   a. Sur la page Create Subscription, pour Protocol (Protocole), choisissez Email (E-mail).
   b. Saisissez votre adresse e-mail dans Endpoint (Point de terminaison).
   c. Choisissez Créer un abonnement. AWS envoie un e-mail à l'adresse e-mail que vous avez spécifiée à l'étape précédente. Attendez que l'e-mail arrive, puis choisissez le lien Confirm subscription (Confirmer l'abonnement) contenu dans l'e-mail pour confirmer que vous avez bien reçu l'e-mail.

d. Revenez dans la console et actualisez la page. Le message Pending confirmation (En attente de confirmation) disparaît et est remplacé par l'ID d'abonnement désormais valide.

## Étape 4 : créer une EventBridge règle Amazon

Maintenant que la fonction Lambda requise existe dans votre compte, vous créez une EventBridge règle Amazon qui l'invoque lorsque les critères de la règle sont remplis.

Pour créer une EventBridge règle

1. Ouvrez la EventBridge console Amazon à l'adressehttps://console.aws.amazon.com/events/.
2. Définissez la console sur la région USA Est (Virginie du Nord), faute de quoi les informations sur Organizations ne sont pas disponibles. Sur la barre de navigation dans le coin supérieur droit de la console, choisissez la région USA Est (Virginie du Nord).
3. Pour obtenir des instructions sur la création de règles, consultez la section Règles d'Amazon EventBridge dans le guide de EventBridge l'utilisateur Amazon.

## Étape 5 : testez votre EventBridge règle Amazon

Au cours de cette étape, vous créez une unité organisationnelle (UO), vous respectez la EventBridge règle Amazon, vous générez une entrée dans le journal et vous vous envoyez un e-mail contenant des informations sur l'événement.

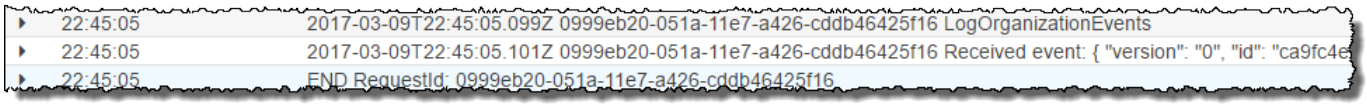
AWS Management Console

Pour créer une unité d'organisation

1. Ouvrez la AWS Organizations console sur la Comptes AWSpage.
2. Cochez la case
   
   Root OU (UO Racine), choisissez Actions, puis sous Unité d'organisation, choisissez Create new (Créer une nouvelle).
3. Pour le nom de l'unité d'organisation, saisissez **`TestCWEOU`**, puis choisissez Create organizational unit (Créer l'unité d'organisation).

Pour voir l'entrée du EventBridge journal

1. Ouvrez la CloudWatch console à l'adressehttps://console.aws.amazon.com/cloudwatch/.
2. Dans la page de navigation, choisissez Logs (Journaux).
3. Sous Log Groups, choisissez le groupe associé à votre fonction Lambda :/. aws/lambda/ LogOrganizationEvents
4. Chaque groupe contient un ou plusieurs flux, et il devrait y avoir un groupe pour aujourd'hui. Choisissez-le.
5. Affichez le journal. Vous devriez voir des lignes similaires aux suivantes.




6. Sélectionnez la ligne du milieu de l'entrée pour voir l'intégralité du texte JSON de l'événement reçu. Vous pouvez voir tous les détails de la demande d'API dans les éléments `requestParameters` et `responseElements` de la sortie.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
```

```
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId",
                "path": "o-exampleOrgId/r-exampleRootId/ou-exampleRootId-
exampleOUId/"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```


7. Vérifiez si votre compte e-mail contient un message d'Orgs CWEvnt (le nom d'affichage de votre rubrique Amazon SNS). Le corps de l'e-mail contient la même sortie de texte JSON que l'entrée de journal qui est illustrée dans l'étape précédente.

## Nettoyage : supprimer les ressources devenues inutiles

Pour éviter d'encourir des frais, vous devez supprimer toutes les AWS ressources que vous avez créées dans le cadre de ce didacticiel et que vous ne souhaitez pas conserver.

Pour assainir votre AWS environnement

1. Utilisez la CloudTrail console pour supprimer le parcours nommé **`My-Test-Trail`** que vous avez créé à l'étape 1.
2. Si vous avez créé un compartiment Amazon S3 à l'étape 1, utilisez la console Amazon S3 pour le supprimer.
3. Utilisez la console Lambda pour supprimer la fonction nommée **`LogOrganizationEvents`** que vous avez créée à l'étape 2.
4. Utilisez la Console Amazon SNS pour supprimer la rubrique Amazon SNS nommée **`OrganizationsCloudWatchTopic`**que vous avez créée lors de l'étape 3.
5. Utilisez la CloudWatch console pour supprimer la EventBridge règle nommée **`OrgsMonitorRule`** que vous avez créée à l'étape 4.

6. Enfin, utilisez la console Organizations pour supprimer l'unité d'organisation nommée **`TestCWEOU`** que vous avez créée à l'étape 5.

Vous avez terminé. Dans ce didacticiel, vous avez EventBridge configuré votre organisation pour surveiller les modifications. Vous avez configuré une règle qui est déclenchée lorsque des utilisateurs appellent des opérations AWS Organizations spécifiques. La règle exécutait une fonction Lambda qui consignait l'événement et envoyait un e-mail contenant des détails sur l'événement.

## Utilisation AWS Organizations avec un AWS SDK

AWS des kits de développement logiciel (SDKs) sont disponibles pour de nombreux langages de programmation courants. Chaque kit SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

| Documentation SDK | Exemples de code |
| --- | --- |
| AWS SDK pour C++ | AWS SDK pour C++ exemples de code |
| AWS CLI | AWS CLI exemples de code |
| AWS SDK pour Go | AWS SDK pour Go exemples de code |
| AWS SDK pour Java | AWS SDK pour Java exemples de code |
| AWS SDK pour JavaScript | AWS SDK pour JavaScript exemples de code |
| AWS SDK pour Kotlin | AWS SDK pour Kotlin exemples de code |
| AWS SDK pour .NET | AWS SDK pour .NET exemples de code |
| AWS SDK pour PHP | AWS SDK pour PHP exemples de code |
| Outils AWS pour PowerShell | Outils AWS pour PowerShell exemples de code |
| AWS SDK pour Python (Boto3) | AWS SDK pour Python (Boto3) exemples de code |
| AWS SDK pour Ruby | AWS SDK pour Ruby exemples de code |

| Documentation SDK | Exemples de code |
| --- | --- |
| AWS SDK pour Rust | AWS SDK pour Rust exemples de code |
| AWS SDK pour SAP ABAP | AWS SDK pour SAP ABAP exemples de code |
| AWS SDK pour Swift | AWS SDK pour Swift exemples de code |

**Exemple de disponibilité**

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

# Gérer une organisation avec AWS Organizations

Une organisation est un ensemble d'organisations Comptes AWS que vous pouvez gérer de manière centralisée et organiser dans une structure hiérarchique arborescente avec une racine en haut et des unités organisationnelles imbriquées sous la racine. Chaque compte peut être directement à la racine ou placé dans l'un des comptes de la hiérarchie. OUs

Chaque organisation est composée de :

- Un compte de gestion
- Aucun compte membre ou plus
- Aucune unité organisationnelle ou plus (OUs)
- Aucune politique ou plus.

Une organisation possède la fonctionnalité déterminée par l'ensemble des fonctions que vous activez.

Rubriques



## Création d'une organisation avec AWS Organizations

Vous pouvez créer une organisation en utilisant votre Compte AWS compte de gestion. Lorsque vous créez une organisation, vous pouvez choisir si l'organisation prend en charge toutes les fonctionnalités (recommandé) ou uniquement la facturation consolidée. Par défaut, l'organisation que vous créez prend en charge toutes les fonctionnalités.

# Créer une organisation.

Vous pouvez créer une organisation à l'aide du SDK AWS Management Console ou à l'aide d'une commande du SDK AWS CLI ou de l'un de ses composants APIs.

> **Autorisations minimales**
>
> Pour créer une organisation avec votre organisation actuelle Compte AWS, vous devez disposer des autorisations suivantes :
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> Vous pouvez restreindre cette autorisation au mandataire du service `organizations.amazonaws.com`.

AWS Management Console

Pour créer une organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Par défaut, l'organisation est créée avec toutes les fonctions activées. Vous pouvez toutefois effectuer l'une ou l'autre des étapes suivantes :

   - Pour créer une organisation dans laquelle toutes les fonctions sont activées, dans la page d'introduction, choisissez Créer une organisation.
   - Pour créer une organisation avec des fonctionnalités de facturation consolidée uniquement, sur la page d'introduction et sous Créer une organisation, choisissez fonctions de facturation consolidée, puis, dans la boîte de dialogue de confirmation, choisissez Créer une organisation.

   Si vous choisissez accidentellement la mauvaise option, vous pouvez immédiatement aller à la page Paramètres, puis choisir Supprimer l'organisation et recommencer.
3. L'organisation est créée et la page Comptes AWS s'affiche. Le seul compte présent est votre compte de gestion, et il est actuellement placé dans l'unité d'organisation (UO) racine.

Au besoin, Organizations envoie automatiquement un e-mail de vérification à l'adresse associée à votre compte de gestion. Il peut y avoir un délai avant la réception de l'e-mail de vérification. Validez votre adresse e-mail dans un délai de 24 heures. Pour de plus amples informations, consultez Vérification de l'adresse e-mail avec AWS Organizations. Vous pouvez créer d'autres comptes dans votre organisation sans plus valider l'adresse e-mail de votre compte de gestion. En revanche, pour inviter des comptes existants, vous devez d'abord effectuer la vérification e-mail.

> **Note**
>
> Si ce compte a précédemment validé son adresse e-mail, cela ne se reproduit plus lorsque vous utilisez le compte pour créer une organisation.

AWS CLI & AWS SDKs

Les exemples de code suivants illustrent comment utiliser `CreateOrganization`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
```

```
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateOrganizationà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Exemple 1 : pour créer une organisation

Bill souhaite créer une organisation à l'aide des informations d'identification du compte 111111111111. L'exemple suivant montre que le compte devient le compte principal de la nouvelle organisation. Comme il ne spécifie aucun ensemble de fonctionnalités, la nouvelle organisation utilise par défaut toutes les fonctionnalités activées et les politiques de contrôle des services sont activées à la racine.

```
aws organizations create-organization
```

La sortie inclut un objet d'organisation contenant des détails sur la nouvelle organisation :

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Exemple 2 : pour créer une organisation avec uniquement les fonctionnalités de facturation consolidée activées

L'exemple suivant crée une organisation qui prend uniquement en charge les fonctionnalités de facturation consolidée :

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

La sortie inclut un objet d'organisation contenant des détails sur la nouvelle organisation :

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Pour plus d'informations, consultez Création d'une organisation dans le Guide de l'utilisateur AWS Organizations.

- Pour plus de détails sur l'API, reportez-vous CreateOrganizationà la section Référence des AWS CLI commandes.

Après avoir créé une organisation, vous pouvez y ajouter des comptes de la manière suivante à partir du compte de gestion :

- Créez d'autres Comptes AWS qui sont automatiquement ajoutés à l'organisation en tant que comptes membres.
- Après avoir vérifié votre adresse e-mail, invitez les utilisateurs existants Comptes AWS à rejoindre votre organisation en tant que comptes membres.

# Vérification de l'adresse e-mail avec AWS Organizations

Après avoir créé une organisation et avant de pouvoir inviter des comptes à la rejoindre, vous devez confirmer que vous possédez l'adresse e-mail fournie pour le compte de gestion de l'organisation.

Lorsque vous créez une organisation, si le compte de gestion n'a pas été vérifié auparavant, envoie AWS automatiquement un e-mail de vérification à l'adresse e-mail spécifiée. Il peut y avoir un délai avant la réception de l'e-mail de vérification.

## Vérifier votre adresse e-mail

Dans les 24 heures, suivez les instructions de l'e-mail pour valider votre adresse e-mail. Si plus de 24 heures se sont écoulées, voir Renvoyer l'e-mail de vérification.

# Renvoyez l'e-mail de vérification avec AWS Organizations

Si vous ne vérifiez pas votre adresse e-mail dans les 24 heures, vous pouvez renvoyer la demande de vérification. Après avoir vérifié votre adresse e-mail, vous pouvez inviter d'autres personnes Comptes AWS à rejoindre votre organisation. Si vous ne recevez pas l'e-mail de vérification, vérifiez que votre adresse e-mail est correcte et, si nécessaire, modifiez-la.

- Pour déterminer quelle adresse e-mail est associée à votre compte de gestion, consultez Afficher les détails d'une organisation depuis le compte de gestion.

- Pour modifier l'adresse e-mail associée à votre compte de gestion, consultez Gestion d'un Compte AWS dans le Guide de l'utilisateur AWS Billing .

AWS Management Console

Pour renvoyer la demande de vérification

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez à la page Paramètres, puis choisissez Envoyer la demande de vérification. L'option n'est présente que si le compte de gestion n'a pas encore été vérifié.
3. Validez votre adresse e-mail dans un délai de 24 heures.

Une fois que vous avez validé votre adresse e-mail, vous pouvez inviter des Comptes AWS à rejoindre votre organisation. Pour de plus amples informations, veuillez consulter Gérer les invitations à un compte avec AWS Organizations.

## Modification de l'adresse e-mail d'une organisation avec AWS Organizations

Pour modifier l'adresse e-mail associée à votre compte de gestion, voir Mettre à jour le Compte AWS nom, l'adresse e-mail ou le mot de passe de l'utilisateur root dans le Guide de Gestion de compte AWS référence.

Si vous modifiez l'adresse e-mail du compte de gestion, le statut du compte redevient « adresse e-mail non vérifiée » et vous devez suivre le processus de vérification pour votre nouvelle adresse e-mail.

> **Note**
>
> Si vous avez invité des comptes à rejoindre votre organisation avant de modifier l'adresse e-mail du compte de gestion et que ces invitations n'ont pas encore été acceptées, elles ne peuvent pas être acceptées tant que vous n'avez pas vérifié la nouvelle adresse e-mail du compte de gestion. Vous devez d'abord renvoyer la demande de vérification. Une fois que

vous avez terminé le processus en répondant à l'e-mail, les comptes que vous avez invités peuvent accepter les invitations.

# Activation de toutes les fonctionnalités pour une organisation avec AWS Organizations

AWS Organizations dispose de deux ensembles de fonctionnalités disponibles :

- Toutes les fonctionnalités — Cet ensemble de fonctionnalités est la méthode préférée et par défaut AWS Organizations, et il inclut toutes les fonctionnalités de consolidation de la facturation. Lorsque vous créez une organisation, toutes les fonctions sont activées par défaut. Lorsque toutes les fonctionnalités sont activées, vous pouvez utiliser les fonctionnalités avancées de gestion de compte disponibles dans Organizations, telles que l'intégration aux AWS services pris en charge et aux politiques de l'organisation.
- Fonctionnalités de facturation consolidée — Cet ensemble de fonctionnalités est limité à la génération d'une facture unique au sein d'une organisation. Aucune autre fonctionnalité de gestion n'est disponible avec la facturation consolidée.

Si vous créez une organisation dotée de l'ensemble de fonctionnalités de facturation consolidée, vous pourrez ultérieurement activer toutes les fonctionnalités. Cependant, vous ne pouvez pas passer de toutes les fonctionnalités à la facturation consolidée une fois que toutes les fonctionnalités sont activées.

Migration standard et migration assistée

Les deux approches de migration vers toutes les fonctionnalités sont la migration standard et la migration assistée.

La migration standard est le processus en libre-service mis à la disposition de tous les AWS Organizations clients pour activer le mode toutes les fonctionnalités.

La migration assistée est un processus à la disposition des clients du plan Enterprise Support qui AWS souhaitent migrer leur organisation vers le mode toutes les fonctionnalités en votre nom.

> **Note**
>
> Processus unidirectionnels et processus d'annulation

- La migration depuis les fonctions de facturation consolidée vers toutes les fonctions est à sens unique. Si toutes les fonctions sont activées dans votre organisation, vous ne pouvez pas revenir aux seules fonctions de facturation consolidée.
- Une fois que vous avez entamé le processus de migration assistée, celui-ci ne peut pas être annulé. Vous devrez attendre 90 jours avant l'expiration du processus si vous souhaitez plutôt suivre le processus standard.

Rubriques



## Considérations

Avant de passer d'une organisation qui prend uniquement en charge les fonctionnalités de facturation consolidée à une organisation prenant en charge toutes les fonctionnalités, tenez compte des points suivants :

Les comptes invités doivent approuver la migration

Lorsque vous lancez le processus d'activation de toutes les fonctionnalités, AWS Organizations envoie une demande à chaque compte membre que vous avez invité à rejoindre votre organisation. Chaque compte invité doit approuver l'activation de toutes les fonctions en acceptant la demande. Ce n'est qu'alors que vous pouvez terminer le processus d'activation de toutes les fonctions dans votre organisation. Si un compte refuse la demande, vous devez supprimer le compte de votre organisation ou renvoyer la demande. La demande doit être acceptée pour que vous puissiez terminer l'activation de toutes les fonctions. Les comptes que vous avez créés à l'aide d' AWS Organizations ne reçoivent pas de demande car ils n'ont pas besoin d'approuver le contrôle supplémentaire.

Les comptes invités sont informés des fonctionnalités actuellement activées

Le propriétaire d'un compte invité est informé par l'invitation s'il rejoint une organisation avec la facturation consolidée uniquement ou si toutes les fonctions sont activées. Vous pouvez continuer à inviter des comptes à votre organisation tout en activant toutes les fonctions.

Si vous invitez un compte pendant le processus d'activation de toutes les fonctions, l'invitation indique que l'organisation qu'ils rejoignent a toutes les fonctions activées. Si vous annulez le processus d'activation de toutes les fonctions avant que le compte accepte l'invitation, cette invitation est annulée. Vous devez de nouveau inviter le compte à devenir membre d'une organisation avec uniquement les fonctions de facturation consolidée.

Si vous invitez un compte et que l'invitation n'a pas encore été acceptée avant que vous commenciez le processus d'activation de toutes les fonctions, cette invitation est annulée car l'invitation indique que l'organisation a uniquement des fonctions de facturation consolidées. Vous devez de nouveau inviter le compte à devenir membre d'une organisation avec toutes les fonctions activées.

Le processus de création de comptes dans une organisation n'est pas affecté par la migration

Vous pouvez continuer à créer des comptes dans l'organisation. Ce processus n'est pas affecté par cette modification.

Le rôle **`AWSServiceRoleForOrganizations`** lié au service est obligatoire

AWS Organizations vérifie que chaque compte de membre possède un rôle lié au service nommé. `AWSServiceRoleForOrganizations` Ce rôle est obligatoire dans tous les comptes pour que vous puissiez activer toutes les fonctions. Si vous avez supprimé ce rôle dans un compte invité, le fait d'accepter l'invitation à activer toutes les fonctions recrée le rôle. Si vous avez supprimé le rôle dans un compte créé en utilisant AWS Organizations, ce compte reçoit une invitation spécifique pour recréer ce rôle. Toutes ces invitations doivent être acceptées pour que l'organisation puisse achever le processus d'activation de toutes les fonctions.

## Processus de migration standard pour activer toutes les fonctionnalités avec Organizations

Cette rubrique explique comment activer toutes les fonctionnalités dans le cadre du processus de migration standard.

### Étape 1 : demander aux comptes invités d'approuver la migration (compte de gestion)

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez démarrer le processus d'activation de toutes les fonctions. Pour ce faire, exécutez les étapes suivantes.

> **Autorisations minimales**
>
> Pour activer toutes les fonctions de votre organisation, vous devez disposer de l'autorisation suivante :
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations

AWS Management Console

Pour demander à vos comptes membres invités d'accepter d'activer toutes les fonctions dans l'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Paramètres, choisissez Commencer le processus pour activer toutes les fonctionnalités.
3. Dans la page Activer toutes les fonctionnalités, confirmez que vous comprenez que vous ne pouvez pas revenir aux seules fonctionnalités de facturation consolidée après votre changement en choisissant Commencer le processus pour activer toutes les fonctionnalités.

   AWS Organizations envoie une demande à chaque compte invité (non créé) de l'organisation pour demander l'autorisation d'activer toutes les fonctionnalités de l'organisation. Si certains de vos comptes ont été créés à l'aide du rôle lié au service nommé AWS Organizations et que l'administrateur du compte membre l'a supprimé`AWSServiceRoleForOrganizations`, AWS Organizations envoie à ce compte une demande pour recréer le rôle.

   La console affiche la liste Statut d'approbation de la demande pour les comptes invités.

   > **Tip**
   >
   > Pour revenir à cette page plus tard, ouvrez la page Paramètres et, dans la section Demande envoyée le date, choisissez Afficher le statut.

4. La page Activer toutes les fonctions indique le statut actuel de la demande pour chaque compte de l'organisation. Les comptes ayant accepté la demande ont le statut ACCEPTÉ. Les comptes qui n'ont pas encore accepté affichent le statut OUVERT.

AWS CLI & AWS SDKs

Pour demander à vos comptes membres invités d'accepter d'activer toutes les fonctions dans l'organisation

Vous pouvez utiliser l'une des commandes suivantes pour activer toutes les fonctions dans une organisation :

- AWS CLI: enable-all-features

  La commande suivante lance le processus d'activation de toutes les fonctions dans l'organisation.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

La sortie montre les détails du handshake que les comptes membres invités doivent accepter.

- AWS SDKs: EnableAllFeatures

> **Remarques**
>
> - Un compte à rebours de 90 jours commence lorsque la demande est envoyée aux comptes membres. Tous les comptes doivent approuver la demande dans ce délai sinon la demande expire. Dans ce cas, toutes les demandes liées à cette tentative sont annulées et vous devez tout recommencer à partir de l'étape 2.
> - Après que vous ayez demandé l'activation de toutes les fonctionnalités, toutes les invitations de compte en attente sont annulées.
> - Vous pouvez toujours envoyer des invitations et créer des comptes pendant le processus de migration des fonctionnalités.

Une fois que tous les comptes invités de l'organisation ont approuvé la demande, vous pouvez finaliser le processus et activer toutes les fonctions. Vous pouvez également finaliser immédiatement le processus si votre organisation ne possède aucun compte membre invité. Pour finaliser le processus, continuez de la manière décrite sous Étape 3 : finaliser le processus de migration pour activer toutes les fonctionnalités (compte de gestion).

### Étape 2 : Approuver la demande d'activation de toutes les fonctionnalités ou de recréation du rôle lié au service (compte invité)

Lorsque vous êtes connecté à l'un des comptes membres invités de l'organisation, vous pouvez approuver une demande à partir du compte de gestion. Si, à l'origine, votre compte a été invité à rejoindre l'organisation, cette invitation vise à activer toutes les fonctions et inclut implicitement l'approbation de recréer le rôle `AWSServiceRoleForOrganizations`, si nécessaire. Si votre compte a plutôt été créé en utilisant le rôle `AWSServiceRoleForOrganizations` lié au service AWS Organizations et que vous l'avez supprimé, vous recevez une invitation uniquement pour recréer le rôle. Pour ce faire, exécutez les étapes suivantes.

> **Important**
>
> Si vous activez toutes les fonctionnalités, le compte de gestion de l'organisation peut appliquer à votre compte membre des contrôles basés sur des politiques. Ces contrôles

peuvent limiter les actions des utilisateurs dans votre compte et même les vôtres en tant qu'administrateur. De telles restrictions peuvent empêcher votre compte de quitter l'organisation.

Autorisations minimales

Pour approuver une demande d'activation de toutes les fonctionnalités de votre compte de membre, celui-ci doit disposer des autorisations suivantes :

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:ListHandshakesForAccount` — requis uniquement si vous utilisez la console Organizations
- `iam:CreateServiceLinkedRole` — requis uniquement si le rôle `AWSServiceRoleForOrganizations` doit être recréé dans le compte membre

AWS Management Console

Pour accepter la demande d'activation de toutes les fonctions de l'organisation

1. Connectez-vous à la AWS Organizations console sur la AWS Organizations console. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans un compte membre.
2. Lisez ce qu'implique l'acceptation de la demande d'activer toutes les fonctions dans l'organisation pour votre compte, puis choisissez Accepter. La page continue d'afficher le processus comme incomplet jusqu'à ce que tous les comptes de l'organisation acceptent la demande et que l'administrateur du compte de gestion finalise le processus.

AWS CLI & AWS SDKs

Pour accepter la demande d'activation de toutes les fonctions de l'organisation

Pour accepter la demande, vous devez accepter le handshake avec `"Action": "APPROVE_ALL_FEATURES"`.

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

  L'exemple suivant montre comment répertorier les handshakes disponibles pour votre compte. La valeur de `"Id"` figurant à la quatrième ligne de la sortie est la valeur dont vous avez besoin pour la commande suivante.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
```

```
            ]
        }
    ]
}
```

L'exemple suivant utilise l'ID du handshake de la commande précédente pour accepter celui-ci.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
```

```
}
```

- AWS SDKs:
  - list-handshakes-for-account
  - AcceptHandshake

## Étape 3 : finaliser le processus de migration pour activer toutes les fonctionnalités (compte de gestion)

Tous les comptes membres invités doivent approuver la demande d'activer toutes les fonctions. S'il n'y a aucun compte membre invité dans l'organisation, la page Progression de l'activation de toutes les fonctions indique avec une bannière verte que vous pouvez finaliser le processus.

> **Autorisations minimales**
>
> Pour finaliser le processus d'activation de toutes les fonctions pour l'organisation, vous devez disposer de l'autorisation suivante :
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations

AWS Management Console

Pour finaliser le processus d'activation de toutes les fonctions

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Paramètres, si tous les comptes invités acceptent la demande d'activation de toutes les fonctions, une zone verte apparaît en haut de la page pour vous en informer. Dans cette zone verte, choisissez Procéder à la finalisation.
3. Dans la page Activer toutes les fonctions, choisissez Finaliser, puis, dans la boîte de dialogue de confirmation, choisissez de nouveau Finaliser.
4. L'organisation a désormais toutes les fonctions activées.

AWS CLI & AWS SDKs

Pour finaliser le processus d'activation de toutes les fonctions

Pour finaliser le processus, vous devez accepter le handshake avec `"Action": "ENABLE_ALL_FEATURES"`.

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

L'exemple suivant montre comment répertorier les handshakes disponibles pour l'organisation. La valeur de `"Id"` figurant à la quatrième ligne de la sortie est la valeur dont vous avez besoin pour la commande suivante.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS SDKs:
  - ListHandshakesForOrganization
  - AcceptHandshake

## Processus de migration assistée pour activer toutes les fonctionnalités avec Organizations

Si vous êtes un client Enterprise, il peut être difficile de terminer le processus de migration standard en raison du grand nombre de comptes que vous pouvez gérer. Par exemple, vous pourriez avoir des difficultés à obtenir l'autorisation de migrer tous les comptes invités dans les grandes organisations.

La migration assistée facilite ce processus en permettant aux clients disposant d'un plan de Support aux entreprises de demander la AWS migration de leur organisation vers toutes les fonctionnalités en

votre nom. Ce processus nécessite que vous signiez un accord attestant que vous êtes propriétaire de tous les comptes. Ensuite, tous les comptes membres de l'organisation seront informés par e-mail de la migration, et les notifications par e-mail déclencheront une période d'attente de 14 jours. Cette période d'attente donne aux comptes le temps de quitter l'organisation avant que la migration vers toutes les fonctionnalités ne prenne effet.

AWS Management Console

Pour migrer vers toutes les fonctionnalités grâce à la migration assistée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Paramètres, choisissez Activer toutes les fonctionnalités, puis sélectionnez Migration assistée.
3. Lisez les termes et conditions du contrat, choisissez Accepter, puis Commencer le processus pour activer toutes les fonctionnalités permettant de démarrer la migration.

> **Note**
>
> Le lancement du processus de migration assistée remplace le processus de migration standard
> Si vous activez actuellement toutes les fonctionnalités à l'aide du processus de migration standard, celui-ci sera annulé et le processus de migration assistée démarrera.
> Le processus de migration assistée est unidirectionnel et ne peut pas être annulé
> Une fois que vous avez entamé le processus de migration assistée, celui-ci ne peut pas être annulé. Vous devrez attendre 90 jours avant l'expiration du processus si vous souhaitez plutôt suivre le processus standard.

Si vous utilisez la migration assistée, vous n'avez pas à vous soucier d'accéder à votre compte invité en tant qu'utilisateur root pour accepter la migration vers toutes les fonctionnalités.

Vous pouvez contacter votre responsable de compte technique (TAM) pour obtenir les détails exacts, les progrès et les délais de la migration assistée.

# Afficher les détails d'une organisation depuis le compte de gestion

Lorsque vous vous connectez au compte de gestion de l'organisation dans la console AWS Organizations, vous pouvez afficher les détails de l'organisation.

> **Autorisations minimales**
>
> Pour afficher les détails d'une organisation, vous devez disposer de l'autorisation suivante :
>
> - `organizations:DescribeOrganization`

AWS Management Console

Pour afficher les détails de votre organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez à la page Paramètres. Cette page affiche des détails relatifs à l'organisation, notamment l'ID de l'organisation ainsi que le nom de compte et l'adresse e-mail affectés au compte de gestion de l'organisation.

AWS CLI & AWS SDKs

Pour afficher les détails de votre organisation

Vous pouvez utiliser l'une des commandes suivantes pour afficher les détails d'une organisation :

- AWS CLI : describe-organization

  L'exemple suivant présente les informations incluses dans la sortie de cette commande.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
```

```
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

> **Important**
>
> Le champ `AvailablePolicyTypes` est obsolète et ne contient pas d'informations précises sur les politiques activées dans votre organisation. Pour afficher la liste exacte et complète des types de politiques réellement activés pour l'organisation, utilisez la commande `ListRoots`, comme décrit dans la partie AWS CLI de la section suivante.

- AWS SDKs: DescribeOrganization

# Supprimer une organisation avec AWS Organizations

Lorsque vous n'avez plus besoin de votre organisation, vous pouvez la supprimer. La suppression d'une organisation ne ferme pas le compte de gestion, mais supprime le compte de gestion de l'organisation et supprime l'organisation elle-même.

L'ancien compte de gestion devient un compte autonome Compte AWS qui n'est plus géré par AWS Organizations. Trois options s'offrent alors à vous :

- Vous pouvez continuer à l'utiliser en tant que compte autonome
- Vous pouvez l'utiliser pour créer une autre organisation
- Vous pouvez accepter une invitation d'une autre organisation pour ajouter le compte à cette organisation en tant que compte membre.

Rubriques

# Considérations

Les organisations supprimées ne peuvent pas être restaurées

Si vous supprimez une organisation, vous ne pouvez pas la récupérer. Si vous avez créé des politiques au sein de l'organisation, elles sont également supprimées.

Organisations ne peuvent être supprimées qu'une fois que tous les comptes membres ont été supprimés

Vous ne pouvez supprimer une organisation qu'après en avoir supprimé tous les comptes membres. Si vous avez créé certains de vos comptes de membre en utilisant AWS Organizations, il se peut que vous ne puissiez pas supprimer ces comptes. Vous ne pouvez supprimer un compte membre que s'il dispose de toutes les informations requises pour fonctionner comme Compte AWS autonome. Pour plus d'informations sur la façon de fournir ces informations et de supprimer le compte, consultez Quitter une organisation depuis un compte membre avec AWS Organizations.

Les comptes de membres « suspendus » ne peuvent pas être supprimés d'une organisation

Si vous avez fermé un compte membre avant de le supprimer de l'organisation, il entre dans un `Closed` état pendant un certain temps et vous ne pouvez pas le supprimer de l'organisation tant qu'il n'est pas définitivement fermé. Cela peut prendre jusqu'à 90 jours et peut vous empêcher de supprimer l'organisation tant que tous les comptes de membres ne sont pas complètement clôturés.

Le fait de supprimer le compte de gestion d'une organisation en supprimant l'organisation peut affecter le compte de la manière suivante :

- Le compte est responsable du paiement de ses propres frais uniquement et n'est plus responsable des frais encourus par un autre compte.
- L'intégration à d'autres services peut être désactivée. Par exemple, AWS IAM Identity Center nécessite le fonctionnement d'une organisation. Ainsi, si vous supprimez un compte d'une organisation qui prend en charge IAM Identity Center, les utilisateurs de ce compte ne peuvent plus utiliser ce service.

Le compte de gestion d'une organisation n'est jamais affecté par les politiques de contrôle des services (SCPs). Les autorisations ne sont donc pas modifiées une fois qu' SCPs elles ne sont plus disponibles.

Sauvegardez tous les rapports

Assurez-vous d'exporter ou de sauvegarder les rapports du compte de gestion, en particulier les rapports de facturation. Les rapports et l'historique au niveau de l'organisation ne sont pas stockés lorsque vous supprimez une organisation. Toutes les données de coûts (telles que l'ensemble de données Cost Explorer) sont supprimées. Il est recommandé d'exporter l'intégralité de l'historique de facturation.

Pour plus d'informations, consultez les rapports sur les coûts et l'utilisation, les rapports Cost Explorer, les rapports Savings Plans et l'utilisation et la couverture des instances réservées (RI).

## Supprimer une organisation

Suivez la procédure ci-dessous pour supprimer une organisation qui transforme l'ancien compte de gestion en un compte autonome Compte AWS qui n'est plus géré par. AWS Organizations

> **Autorisations minimales**
>
> Pour supprimer une organisation, vous devez vous connecter en tant qu'utilisateur ou rôle dans le compte de gestion et vous devez disposer des autorisations suivantes :
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations

AWS Management Console

Pour supprimer une organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Avant de pouvoir supprimer l'organisation, vous devez tout d'abord supprimer tous les comptes de l'organisation. Pour de plus amples informations, consultez Supprimer un compte membre d'une organisation avec AWS Organizations.
3. Accédez à la page Paramètres, puis choisissez Supprimer l'organisation.
4. Dans la boîte de dialogue Supprimer l'organisation, entrez l'ID de l'organisation qui s'affiche dans la ligne au-dessus de la zone de texte. Ensuite, choisissez Supprimer l'organisation.

> **Important**
>
> Cette opération ne ferme pas le compte de gestion, mais le transforme en un Compte AWS autonome. Pour fermer le compte, suivez les étapes indiquées à Fermeture d'un compte membre dans une organisation avec AWS Organizations.

AWS CLI & AWS SDKs

Les exemples de code suivants illustrent comment utiliser `DeleteOrganization`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteOrganizationà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour supprimer une organisation

L'exemple suivant montre comment supprimer une organisation. Pour effectuer cette opération, vous devez être administrateur du compte principal de l'organisation. L'exemple suppose que vous avez précédemment supprimé tous les comptes et politiques des membres de l'organisation : OUs

```
aws organizations delete-organization
```

- Pour plus de détails sur l'API, reportez-vous DeleteOrganizationà la section Référence des AWS CLI commandes.

# Gestion des comptes dans une organisation avec AWS Organizations

An Compte AWSest un conteneur pour vos AWS ressources. Vous créez et gérez vos AWS ressources dans un Compte AWS.

Cette rubrique décrit comment gérer les comptes pour AWS Organizations.

Rubriques



## Gérer le compte de gestion avec AWS Organizations

Un compte de gestion est le compte Compte AWS que vous utilisez pour créer votre organisation.

Le compte de gestion est le propriétaire ultime de l'organisation, ayant le contrôle final sur les politiques de sécurité, d'infrastructure et financières. Ce compte joue le rôle d'un compte payeur et est chargé de payer tous les frais accumulés par les comptes de son organisation.

Cette rubrique décrit comment gérer le compte de gestion avec AWS Organizations.

Rubriques

# Bonnes pratiques relatives au compte de gestion

Suivez ces recommandations pour vous aider à protéger la sécurité du compte de gestion dans AWS Organizations. Ces recommandations supposent que vous respectez également les bonnes pratiques qui consistent à avoir recours à l'utilisateur racine uniquement pour les tâches qui le nécessitent vraiment.

Rubriques



## Limiter l'accès au compte de gestion

Le compte de gestion est essentiel à toutes les tâches administratives mentionnées, telles que la gestion des comptes, les politiques, l'intégration avec d'autres AWS services, la facturation consolidée, etc. Par conséquent, vous devez restreindre et limiter l'accès au compte de gestion aux seuls utilisateurs administrateurs qui ont besoin de droits pour apporter des modifications à l'organisation.

## Vérifier et suivre les personnes ayant accès au compte de gestion

Pour vous assurer de conserver l'accès au compte de gestion, vérifiez périodiquement le personnel de votre entreprise qui a accès à l'adresse e-mail, au mot de passe, à la MFA et au numéro de téléphone qui lui sont associés. Alignez la vérification sur les procédures métier existantes. Ajoutez une vérification mensuelle ou trimestrielle de ces informations pour vous assurer que seules les bonnes personnes y ont accès. Assurez-vous que le processus de récupération ou de réinitialisation de l'accès aux informations d'identification de l'utilisateur racine ne dépend pas d'une personne spécifique. Tous les processus devraient tenir compte de l'éventualité que des personnes ne soient pas disponibles.

## Utiliser le compte de gestion uniquement pour les tâches qui nécessitent le compte de gestion.

Nous vous recommandons d'utiliser le compte de gestion et ses utilisateurs et rôles pour les tâches qui ne peuvent être exécutées que par ce compte. Stockez toutes vos AWS ressources dans un autre Comptes AWS service de l'organisation et gardez-les hors du compte de gestion. L'une des principales raisons de conserver vos ressources dans d'autres comptes est que les politiques de contrôle des services des Organisations (SCPs) ne permettent pas de restreindre les utilisateurs ou les rôles dans le compte de gestion. La séparation de vos ressources de votre compte de gestion vous aide également à comprendre les frais qui vous sont facturés.

Pour obtenir la liste des tâches qui doivent être appelées depuis le compte de gestion, voir Opérations que vous ne pouvez appeler que depuis le compte de gestion de l'organisation.

## Éviter de déployer des charges de travail dans le compte de gestion de l'organisation

Les opérations privilégiées peuvent être effectuées dans le compte de gestion d'une organisation et SCPs ne s'appliquent pas au compte de gestion. C'est pourquoi vous devez limiter les ressources et données cloud contenues dans le compte de gestion à celles qui doivent être gérées dans le compte de gestion.

## Déléguer des responsabilités en dehors du compte de gestion pour la décentralisation

Dans la mesure du possible, nous recommandons de déléguer des responsabilités et des services en dehors du compte de gestion. Accordez à vos équipes des autorisations dans leurs propres comptes pour gérer les besoins de l'organisation, sans qu'il soit nécessaire d'accéder au compte de gestion. En outre, vous pouvez enregistrer plusieurs administrateurs délégués pour les services qui prennent en charge cette fonctionnalité, par exemple AWS Service Catalog pour le partage de logiciels au sein de l'organisation ou CloudFormation StackSets pour la création et le déploiement de piles.

Pour plus d'informations, consultez Architecture de référence de sécurité, Organisation de votre AWS environnement à l'aide de plusieurs comptes, et Services AWS que vous pouvez utiliser avec AWS Organizations pour des suggestions sur l'enregistrement de comptes membres en tant qu'administrateurs délégués pour différents AWS services.

Pour plus d'informations sur la configuration des administrateurs délégués, consultez Activation d'un compte d'administrateur délégué pour Gestion de compte AWS (français non garanti) et Administrateur délégué pour AWS Organizations.

# Fermeture d'un compte de gestion dans votre organisation

Pour fermer le compte de gestion de votre organisation, vous devez d'abord fermer ou supprimer tous les comptes membres de l'organisation. La fermeture du compte de gestion supprime également l'instance AWS Organizations et toutes les politiques que vous avez créées au sein de cette organisation après l'expiration de la période postérieure à la fermeture.

## Fermer le compte de gestion

Pour fermer un compte de gestion, procédez comme suit.

> **Important**
>
> Avant de fermer votre compte de gestion, nous vous recommandons vivement de prendre en compte les facteurs à prendre en compte et de comprendre l'impact de la fermeture d'un compte. Pour plus d'informations, consultez ce que vous devez savoir avant de fermer votre compte et À quoi vous attendre après la fermeture de votre compte dans le Guide de gestion de AWS compte.

AWS Management Console

Pour fermer un compte de gestion depuis la page Comptes

> **Note**
>
> Vous ne pouvez pas fermer un compte de gestion directement depuis la AWS Organizations console.

1. Connectez-vous en AWS Management Console tant qu'utilisateur root pour le compte de gestion que vous souhaitez fermer. Vous ne pouvez pas fermer un compte lorsque vous êtes connecté en tant qu'utilisateur ou en tant que rôle IAM.
2. Vérifiez qu'il ne reste aucun compte de membre actif dans votre organisation. Pour ce faire, accédez à la AWS Organizations console. Si votre compte de membre est toujours actif, vous devrez suivre les instructions fournies dans Fermeture d'un compte membre dans une organisation avec AWS Organizations ou Supprimer un compte membre d'une organisation avant de passer à l'étape suivante.

3. Dans la barre de navigation située dans le coin supérieur droit, choisissez le nom ou le numéro de votre compte, puis sélectionnez Compte.
4. Sur la page Compte, cliquez sur le bouton Fermer le compte. Lisez les instructions de fermeture de compte et assurez-vous de bien les comprendre.
5. Cliquez sur le bouton Fermer le compte pour lancer le processus de fermeture du compte.
6. Dans quelques minutes, vous devriez recevoir un e-mail de confirmation indiquant que votre compte a été fermé.

AWS CLI & AWS SDKs

Cette tâche n'est pas prise en charge dans AWS CLI ou par une opération d'API provenant de l'un des AWS SDKs. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

# Gérer les comptes des membres avec AWS Organizations

Un compte de membre est un compte Compte AWS, autre que le compte de gestion, qui fait partie d'une organisation.

Cette rubrique décrit comment gérer les comptes des membres avec AWS Organizations.

Rubriques

# Bonnes pratiques relatives aux comptes membres

Suivez ces recommandations pour vous aider à protéger la sécurité des comptes membres de votre organisation. Ces recommandations supposent que vous respectez également les bonnes pratiques qui consistent à avoir recours à l'utilisateur racine uniquement pour les tâches qui le nécessitent vraiment.

Rubriques

- Définir le nom et les attributs du compte
- Mise à l'échelle efficace de l'utilisation de votre environnement et de vos comptes
- Activez la gestion de l'accès root pour simplifier la gestion des informations d'identification des utilisateurs root pour les comptes membres

## Définir le nom et les attributs du compte

Pour vos comptes membres, utilisez une structure de dénomination et une adresse e-mail qui reflètent l'utilisation du compte. Par exemple, `Workloads+fooA+dev@domain.com` pour `WorkloadsFooADev`, `Workloads+fooB+dev@domain.com` pour `WorkloadsFooBDev`. Si vous avez défini des balises personnalisées pour votre organisation, nous vous recommandons d'attribuer ces balises à des comptes qui reflètent l'utilisation du compte, le centre de coûts, l'environnement et le projet. Cela facilite l'identification, l'organisation et la recherche des comptes.

## Mise à l'échelle efficace de l'utilisation de votre environnement et de vos comptes

Au fur et à mesure que vous évoluez, avant de créer de nouveaux comptes, assurez-vous qu'il n'existe pas déjà de comptes répondant à des besoins similaires, afin d'éviter toute duplication inutile. Comptes AWS devrait être fondé sur des exigences d'accès communes. Si vous prévoyez de réutiliser les comptes, comme un compte d'environnement de test (sandbox) ou équivalent, nous vous recommandons de nettoyer les ressources ou charges de travail inutiles des comptes, mais de conserver les comptes pour une utilisation ultérieure.

Avant de fermer des comptes, notez qu'ils sont soumis à des limites de quotas de fermeture. Pour de plus amples informations, veuillez consulter Quotas et limites de service pour AWS Organizations. Pensez à mettre en œuvre un processus de nettoyage pour réutiliser les comptes au lieu de les fermer et d'en créer de nouveaux lorsque c'est possible. De cette façon, vous éviterez les coûts liés à l'exploitation des ressources et à l'atteinte des limites des CloseAccount API.

## Activez la gestion de l'accès root pour simplifier la gestion des informations d'identification des utilisateurs root pour les comptes membres

Nous vous recommandons d'activer la gestion de l'accès root pour vous aider à surveiller et à supprimer les informations d'identification des utilisateurs root pour les comptes des membres. La gestion de l'accès root empêche la récupération des informations d'identification de l'utilisateur root, améliorant ainsi la sécurité des comptes dans votre organisation.

- Supprimez les informations d'identification de l'utilisateur root pour les comptes membres afin d'empêcher la connexion à l'utilisateur root. Cela empêche également les comptes membres de récupérer l'utilisateur root.
- Supposons une session privilégiée pour effectuer les tâches suivantes sur les comptes des membres :
  - Supprimez une politique de compartiment mal configurée qui empêche tous les principaux d’accéder à un compartiment Amazon S3.
  - Supprimez une politique Amazon Simple Queue Service qui refuse à tous les principaux l’accès à une file d’attente Amazon SQS.
  - Autoriser un compte membre à récupérer ses informations d'identification d'utilisateur root. La personne ayant accès à l'e-mail de l'utilisateur root à la boîte de réception pour le compte membre peut réinitialiser le mot de passe de l'utilisateur root et se connecter en tant qu'utilisateur root du compte membre.

Une fois la gestion de l'accès root activée, les comptes membres nouvellement créés sont secure-by-default dépourvus d'informations d'identification d'utilisateur root, ce qui élimine le besoin d'une sécurité supplémentaire, telle que l'authentification MFA après le provisionnement.

Pour plus d'informations, voir Centraliser les informations d'identification des utilisateurs root pour les comptes des membres dans le Guide de l'Gestion des identités et des accès AWS utilisateur.

Utiliser une politique de contrôle des services (SCP) pour restreindre ce que l'utilisateur racine de vos comptes membres peut faire

Nous vous recommandons de créer une politique de contrôle des services (SCP) dans l'organisation et de l'attacher à la racine de l'organisation de manière à ce qu'elle s'applique à tous les comptes membres. Pour plus d'informations, consultez Sécurisez les informations d’identification d'utilisateur root de votre compte Organizations.

Vous pouvez refuser toutes les actions de l'utilisateur root, à l'exception d'une action spécifique que vous devez effectuer dans votre compte membre. Par exemple, le SCP suivant empêche l'utilisateur root d'un compte membre d'effectuer des appels d'API de AWS service, à l'exception de « Mettre à jour une politique de compartiment S3 mal configurée et refusant l'accès à tous les principaux » (l'une des actions nécessitant des informations d'identification root). Pour plus d'informations, consultez la rubrique Tâches nécessitant des informations d'identification d'utilisateur root du Guide de l'utilisateur IAM.

JSON

```
{
 "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "NotAction":[
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy",
            "s3:DeleteBucketPolicy"
                 ],
            "Resource": "*",
            "Condition": {
 "ArnLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
            }
        }
    ]
 }
```

Dans la majorité des cas, toutes les tâches administratives peuvent être exécutées par un rôle Gestion des identités et des accès AWS (IAM) dans le compte membre disposant des autorisations d'administrateur appropriées. Tout rôle de ce type doit avoir des contrôles appropriés appliqués pour limiter, journaliser et surveiller les activités.

# Création d'un compte membre dans une organisation avec AWS Organizations

Cette rubrique décrit comment créer au Comptes AWS sein de votre organisation dans AWS Organizations. Pour plus d'informations sur la création d'un single Compte AWS, consultez le Centre de ressources pour la mise en route.

## Considérations à prendre en compte avant de créer un compte membre

Organizations crée automatiquement le rôle IAM **`OrganizationAccountAccessRole`** pour le compte membre

Lorsque vous créez un compte membre dans votre organisation, Organizations crée automatiquement le rôle IAM `OrganizationAccountAccessRole` dans le compte membre qui permet aux utilisateurs et aux rôles du compte de gestion d'exercer un contrôle administratif total sur le compte membre. Tous les comptes supplémentaires attachés à la même politique gérée seront automatiquement mis à jour chaque fois que la politique sera mise à jour. Ce rôle est soumis à toutes les politiques de contrôle des services (SCPs) qui s'appliquent au compte du membre.

Organizations crée automatiquement le rôle lié au service **`AWSServiceRoleForOrganizations`** pour le compte membre

Lorsque vous créez un compte membre dans votre organisation, Organizations crée automatiquement un rôle lié au service `AWSServiceRoleForOrganizations` dans le compte membre qui permet l'intégration à certains AWS services. Vous devez configurer les autres services pour permettre l'intégration. Pour de plus amples informations, veuillez consulter AWS Organizations et rôles liés aux services.

Les comptes membres ne peuvent être créés qu'à la racine d'une organisation

Les comptes de membres d'une organisation ne peuvent être créés qu'à la racine d'une organisation. Après avoir créé un compte membre racine d'une organisation, vous pouvez le déplacer entre les deux OUs. Pour de plus amples informations, veuillez consulter Déplacement de comptes vers une unité organisationnelle (UO) ou entre la racine et OUs avec AWS Organizations.

Les politiques associées à la racine s'appliquent immédiatement

Si des politiques sont associées à la racine, elles s'appliquent immédiatement à tous les utilisateurs et rôles du compte créé.

Si vous avez activé le service Trust pour un autre AWS service de votre organisation, ce service fiable peut créer des rôles liés au service ou effectuer des actions sur n'importe quel compte membre de l'organisation, y compris le compte que vous avez créé.

Les comptes membres doivent s'inscrire pour recevoir des e-mails marketing

Les comptes de membres que vous créez dans le cadre d'une organisation ne sont pas automatiquement abonnés aux e-mails AWS marketing. Pour inscrire vos comptes à la réception d'e-mails de marketing, consultez https://pages.awscloud.com/communication-preferences.

Les comptes membres des organisations gérées par AWS Control Tower doivent être créés dans AWS Control Tower

Si votre organisation est gérée par AWS Control Tower, nous vous recommandons de créer vos comptes membres à l'aide de la fabrique de AWS Control Tower comptes de la AWS Control Tower console ou à l'aide du AWS Control Tower APIs.

Si vous créez un compte membre dans Organizations alors que l'organisation est gérée par AWS Control Tower, le compte ne sera pas inscrit auprès de ce compte AWS Control Tower. Pour de plus amples informations, consultez Référence à des ressources en dehors de AWS Control Tower dans le Guide de l'utilisateur de AWS Control Tower .

## Création d'un compte membre

Une fois connecté au compte de gestion de l'organisation, vous pouvez créer des comptes de membres qui font partie de votre organisation.

Lorsque vous créez un compte à l'aide de la procédure suivante, copie AWS Organizations automatiquement les coordonnées principales suivantes du compte de gestion vers le nouveau compte membre :

- Numéro de téléphone
- Nom de la société
- URL du site Web
- Adresse

Organizations copie également le langage de communication et les informations Marketplace (fournisseur du compte dans certains cas Régions AWS) à partir du compte de gestion.

Autorisations minimales

Pour créer un compte membre dans votre organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:CreateAccount`

AWS Management Console

Pour créer une Compte AWS annonce intégrée automatiquement à votre organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, choisissez Ajouter un Compte AWS.
3. Sur la page Ajouter un Compte AWS, choisissez Créer un Compte AWS (cette option est choisie par défaut).
4. Sur la page Créer un Compte AWS, pour Compte AWS Nom saisissez le nom que vous souhaitez attribuer au compte. Ce nom vous aide à distinguer le compte de tous les autres comptes de l'organisation et il est différent de l'alias IAM ou de l'e-mail du propriétaire.
5. Pour Adresse e-mail du propriétaire du compte, saisissez l'adresse e-mail du propriétaire du compte. Cette adresse e-mail ne peut pas déjà être associée à une autre Compte AWS car elle devient le nom d'utilisateur de l'utilisateur root du compte.
6. (Facultatif) Spécifiez le nom à attribuer au rôle IAM qui est automatiquement créé dans le nouveau compte. Ce rôle accorde au compte de gestion de l'organisation l'autorisation d'accéder au compte membre nouvellement créé. Si vous ne spécifiez pas de nom, AWS Organizations donne au rôle le nom par défaut de`OrganizationAccountAccessRole`. Nous vous recommandons d'utiliser le nom par défaut sur tous vos comptes pour assurer la cohérence.

   Important

   N'oubliez pas ce nom de rôle. Vous en aurez besoin ultérieurement pour accorder l'accès au nouveau compte aux utilisateurs et rôles du compte de gestion.

7. (Facultatif) Dans la section Balises, ajoutez une ou plusieurs balises au nouveau compte en choisissant Ajouter une balise, puis en saisissant une clé et une valeur facultative. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à un compte.
8. Choisissez Créer Compte AWS.

   - Si vous obtenez une erreur qui indique que vous avez dépassé votre quota de comptes pour l'organisation, consultez J'obtiens un message « Quota dépassé » lorsque j'essaie d'ajouter un compte à mon organisation..
   - Si vous obtenez une erreur qui indique que vous ne pouvez pas ajouter un compte parce que votre organisation est toujours en cours d'initialisation, attendez une heure, puis réessayez.
   - Vous pouvez également consulter le AWS CloudTrail journal pour savoir si la création du compte a été réussie. Pour de plus amples informations, veuillez consulter Connexion et surveillance AWS Organizations.
   - Si vous obtenez toujours la même erreur, contactez AWS Support.

   La page Comptes AWS apparaît ; votre nouveau compte a été ajouté à la liste.
9. Maintenant que le compte existe et qu'il dispose d'un rôle IAM qui accorde l'accès administrateur aux utilisateurs du compte de gestion, vous pouvez y accéder en suivant les étapes indiquées dans Accès aux comptes des membres d'une organisation avec AWS Organizations.

AWS CLI & AWS SDKs

Les exemples de code suivants illustrent comment utiliser `CreateAccount`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
```

```
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates a new AWS Organizations account.
    /// </summary>
    public class CreateAccount
    {
        /// <summary>
        /// Initializes an Organizations client object and uses it to create
        /// the new account with the name specified in accountName.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- Pour plus de détails sur l'API, voir CreateAccountla section Référence des AWS SDK pour .NET API.

## CLI

### AWS CLI

Pour créer un compte membre qui fait automatiquement partie de votre organisation

L'exemple suivant montre comment créer un compte membre dans une organisation. Le compte membre est configuré avec le nom Compte de production et l'adresse e-mail susan@example.com. Organizations crée automatiquement un rôle IAM en utilisant le nom par défaut, OrganizationAccountAccessRole car le paramètre RoleName n'est pas spécifié. En outre, le paramètre qui permet aux utilisateurs ou aux rôles IAM disposant d'autorisations suffisantes d'accéder aux données de facturation du compte est défini sur la valeur par défaut ALLOW car le IamUserAccessToBilling paramètre n'est pas spécifié. Organizations envoie automatiquement à Susan un e-mail « Bienvenue à AWS » :

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

La sortie inclut un objet de demande qui indique que l'état est désormais `IN_PROGRESS` :

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Vous pouvez ultérieurement demander l'état actuel de la demande en fournissant la valeur de réponse Id à la describe-create-account-status commande comme valeur du create-account-request-id paramètre.

Pour plus d'informations, consultez la section Création d'un AWS compte dans votre organisation dans le Guide de l'utilisateur AWS des Organizations.

- Pour plus de détails sur l'API, reportez-vous CreateAccountà la section Référence des AWS CLI commandes.

## Accès aux comptes des membres d'une organisation avec AWS Organizations

Lorsque vous créez un compte dans votre organisation, en plus de l'utilisateur racine, AWS Organizations crée automatiquement un rôle IAM nommé par défaut `OrganizationAccountAccessRole`. Vous pouvez spécifier un autre nom lorsque vous le créez, mais nous vous recommandons de le nommer de manière cohérente sur tous vos comptes. AWS Organizations ne crée aucun autre utilisateur ou rôle.

Pour accéder aux comptes de votre organisation, vous devez utiliser l'une des méthodes suivantes :

Autorisations minimales

Pour accéder à un compte Compte AWS depuis n'importe quel autre compte de votre organisation, vous devez disposer des autorisations suivantes :

- `sts:AssumeRole` - L'élément `Resource` doit être défini sur un astérisque (*) ou sur l'ID du compte associé à l'utilisateur ayant besoin d'accéder au nouveau compte membre.

Using the root user (Not recommended for everyday tasks)

Lorsque vous créez un nouveau compte membre dans votre organisation, le compte ne possède aucun identifiant d'utilisateur root par défaut. Les comptes membres ne peuvent pas se connecter à leur utilisateur racine ni récupérer le mot de passe de leur utilisateur racine si la récupération de compte n'est pas activée.

Vous pouvez centraliser l'accès root pour les comptes membres afin de supprimer les informations d'identification des utilisateurs root pour les comptes membres existants de votre organisation. La suppression des informations d'identification de l'utilisateur root supprime le mot de passe de l'utilisateur root, les clés d'accès, les certificats de signature et désactive l'authentification multifactorielle (MFA). Ces comptes membres ne disposent pas d'informations d'identification de l'utilisateur racine, ne peuvent pas se connecter en tant qu'utilisateur racine et ne peuvent pas récupérer le mot de passe de l'utilisateur racine. Les nouveaux comptes que vous créez dans Organizations ne disposent par défaut d'aucunes informations d'identification d'utilisateur racine.

Contactez votre administrateur si vous devez effectuer une tâche qui nécessite les informations d'identification de l'utilisateur root sur un compte membre où les informations d'identification de l'utilisateur root ne sont pas présentes.

Pour accéder à votre compte de membre en tant qu'utilisateur root, vous devez suivre le processus de récupération du mot de passe. Pour plus d'informations, consultez la section J'ai oublié mon mot de passe utilisateur root Compte AWS dans le guide de AWS connexion de l'utilisateur.

Si vous devez accéder à un compte membre en utilisant l'utilisateur root, suivez les bonnes pratiques suivantes :

- N'utilisez pas l'utilisateur root pour accéder à votre compte, sauf pour créer d'autres utilisateurs et rôles avec des autorisations plus limitées. Ensuite, connectez-vous en tant que l'un de ces utilisateurs ou rôles.
- Activez l'authentification multifactorielle (MFA) sur l'utilisateur root. Réinitialisez le mot de passe et attribuez un dispositif MFA à l'utilisateur racine.

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. Pour des recommandations de sécurité supplémentaires pour les utilisateurs root, consultez les meilleures pratiques pour les utilisateurs root Compte AWS dans le guide de l'utilisateur IAM.

Using trusted access for IAM Identity Center

Utilisez AWS IAM Identity Centeret activez un accès sécurisé pour IAM Identity Center avec AWS Organizations. Cela permet aux utilisateurs de se connecter au portail d' AWS accès avec leurs informations d'identification professionnelles et d'accéder aux ressources du compte de gestion ou des comptes membres qui leur ont été attribués.

Pour plus d'informations, consultez Autorisations de plusieurs comptes dans le Guide de l'utilisateur AWS IAM Identity Center . Pour plus d'informations sur la configuration de l'accès de confiance à IAM Identity Center, consultez AWS IAM Identity Center et AWS Organizations.

Using the IAM role OrganizationAccountAccessRole

Si vous créez un compte à l'aide des outils fournis dans le cadre de AWS Organizations, vous pouvez accéder au compte en utilisant le nom de rôle préconfiguré `OrganizationAccountAccessRole` qui existe dans tous les nouveaux comptes que vous créez de cette manière. Pour de plus amples informations, veuillez consulter Accès à un compte de membre OrganizationAccountAccessRole doté de AWS Organizations.

Si vous invitez un compte existant à rejoindre votre organisation et qu'il accepte l'invitation, vous pouvez ensuite décider de créer un rôle IAM qui permet au compte de gestion d'accéder au compte membre invité. Ce rôle est censé être identique au rôle automatiquement ajouté à un compte créé avec AWS Organizations.

Pour créer ce rôle, consultez Création OrganizationAccountAccessRole d'un compte invité avec AWS Organizations.

Après avoir créé le rôle, vous pouvez y accéder grâce à la procédure décrite dans Accès à un compte de membre OrganizationAccountAccessRole doté de AWS Organizations.

Rubriques



## Création OrganizationAccountAccessRole d'un compte invité avec AWS Organizations

Par défaut, si vous créez un compte membre dans le cadre de votre organisation, AWS crée automatiquement dans le compte un rôle qui accorde des autorisations d'administrateur aux utilisateurs IAM du compte de gestion qui peuvent assumer le rôle. Par défaut, ce rôle est nommé `OrganizationAccountAccessRole`. Pour de plus amples informations, consultez Accès à un compte de membre OrganizationAccountAccessRole doté de AWS Organizations.

Cependant, un rôle administrateur n'est pas automatiquement créé pour les comptes membres que vous invitez à rejoindre votre organisation. Vous devez le faire manuellement, comme indiqué dans la procédure suivante. Cela permet essentiellement de dupliquer le rôle automatiquement configuré pour les comptes créés. Nous vous recommandons d'utiliser le même nom (`OrganizationAccountAccessRole`) pour les rôles créés manuellement afin de faciliter la cohérence et la mémorisation.

AWS Management Console

Pour créer un rôle d' AWS Organizations administrateur dans un compte membre

1. Connectez-vous à la console IAM à https://console.aws.amazon.com/iam/l'adresse. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte membre. L'utilisateur ou le rôle doit être autorisé à créer des rôles et des politiques IAM.
2. Dans la console IAM, accédez à Rôles, puis sélectionnez Créer un rôle.
3. Choisissez Compte AWS, puis sélectionnez Autre Compte AWS.
4. Entrez le numéro d'identification à 12 chiffres du compte de gestion auquel vous souhaitez accorder l'accès administrateur. Dans la section Options, veuillez noter ce qui suit :

- Pour ce rôle, dans la mesure où les comptes sont internes à votre société, ne choisissez pas Exiger un ID externe. Pour plus d'informations sur l'option ID externe, voir Quand dois-je utiliser un ID externe ? dans le guide de l'utilisateur IAM.
- Si l'authentification MFA est activée et configurée, vous pouvez éventuellement exiger une authentification à l'aide d'un périphérique MFA. Pour plus d'informations sur l'authentification multifactorielle, consultez la section Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'utilisateur IAM.

5. Choisissez Suivant.
6. Sur la page Ajouter des autorisations, choisissez la politique AWS gérée nommée, `AdministratorAccess` puis cliquez sur Suivant.
7. Sur la page Nom, révision et création, spécifiez un nom de rôle et une description facultative. Nous vous recommandons d'utiliser `OrganizationAccountAccessRole`, par souci de cohérence avec le nom par défaut attribué au rôle dans les nouveaux comptes. Pour valider vos modifications, choisissez Créer un rôle.
8. Votre nouveau rôle s'affiche sur la liste des rôles disponibles. Choisissez le nom du nouveau rôle pour en afficher les détails et prêtez une attention particulière à l'adresse URL fournie. Communiquez cette URL aux utilisateurs du compte membre qui ont besoin d'accéder au rôle. Notez également le nom ARN de rôle car il est nécessaire à l'étape 15.
9. Connectez-vous à la console IAM à https://console.aws.amazon.com/iam/l'adresse. Cette fois, connectez-vous en tant qu'utilisateur du compte de gestion, qui dispose des autorisations pour créer des politiques et attribuer des politiques à des utilisateurs ou des groupes.
10. Accédez à Politiques, puis choisissez Créer une politique.
11. Pour Service, choisissez STS.
12. Pour Actions, commencez par saisir **`AssumeRole`** dans la zone Filtrer, puis sélectionnez la case en regard de celle-ci lorsqu'elle s'affiche.
13. Sous Ressources, assurez-vous que Spécifique est sélectionné, puis choisissez Ajouter ARNs.
14. Entrez le numéro d'identification du compte AWS membre, puis le nom du rôle que vous avez créé précédemment aux étapes 1 à 8. Choisissez Ajouter ARNs.
15. Si vous accordez l'autorisation d'assumer le rôle dans plusieurs comptes membres, répétez les étapes 14 et 15 pour chaque compte.
16. Choisissez Suivant.

17. Sur la page Réviser et créer, entrez le nom de la nouvelle politique, puis choisissez Créer une politique pour enregistrer vos modifications.
18. Choisissez Groupes d'utilisateurs dans le volet de navigation, puis choisissez le nom du groupe (et non la case à cocher) que vous souhaitez utiliser pour déléguer l'administration du compte membre.
19. Sélectionnez l'onglet Autorisations.
20. Choisissez Ajouter des autorisations, choisissez Joindre des politiques, puis sélectionnez la politique que vous avez créée aux étapes 11 à 18.

Les utilisateurs membres du groupe sélectionné peuvent désormais utiliser les informations URLs que vous avez capturées à l'étape 9 pour accéder au rôle de chaque compte membre. Ils peuvent accéder à ces comptes membres de la même façon qu'ils le feraient pour accéder à un compte créé dans l'organisation. Pour de plus amples informations sur l'utilisation du rôle pour administrer un compte membre, consultez Accès à un compte de membre OrganizationAccountAccessRole doté de AWS Organizations.

## Accès à un compte de membre OrganizationAccountAccessRole doté de AWS Organizations

Lorsque vous créez un compte membre à l'aide de la AWS Organizations console, un rôle IAM nommé `OrganizationAccountAccessRole` dans le compte est AWS Organizations automatiquement créé. Ce rôle possède les autorisations d'administration complètes du compte membre. La portée de l'accès pour ce rôle inclut tous les principaux du compte de gestion, si bien que le rôle est configuré pour accorder cet accès au compte de gestion de l'organisation.

Vous pouvez créer un rôle identique pour un compte membre invité en suivant les étapes indiquées dans Création OrganizationAccountAccessRole d'un compte invité avec AWS Organizations.

Pour utiliser ce rôle afin d'accéder au compte membre, vous devez vous connecter en tant qu'utilisateur du compte de gestion disposant des autorisations pour assumer le rôle. Pour configurer ces autorisations, exécutez la procédure suivante. Nous vous recommandons d'accorder des autorisations à des groupes plutôt qu'à des utilisateurs pour faciliter la maintenance.

AWS Management Console

Pour accorder des autorisations à des membres d'un groupe IAM dans le compte de gestion afin d'accéder au rôle

1. Connectez-vous à la console IAM en https://console.aws.amazon.com/iam/tant qu'utilisateur disposant des autorisations d'administrateur dans le compte de gestion. Cette action est obligatoire pour déléguer des autorisations au groupe IAM dont les utilisateurs accéderont au rôle dans le compte membre.
2. Commencez par créer la politique gérée dont vous aurez besoin ultérieurement dans ???.

   Dans le panneau de navigation, choisissez Politiques, puis Créer une politique.
3. Dans l'onglet Éditeur visuel, choisissez Choisir un service, entrez **STS** dans le champ de recherche pour filtrer la liste, puis choisissez l'option STS.
4. Dans la section Actions, entrez **assume** dans la zone de recherche pour filtrer la liste, puis choisissez l'AssumeRoleoption.
5. Dans la section Ressources, sélectionnez Spécifique, puis Ajouter ARNs
6. Dans la section Spécifier les ARN, choisissez Autre compte pour Resource in.
7. Entrez l'identifiant du compte membre que vous venez de créer
8. Pour Nom du rôle de ressource avec chemin, entrez le nom du rôle que vous avez créé dans la section précédente (nous vous recommandons de le nommer`OrganizationAccountAccessRole`).
9. Choisissez Ajouter ARNs lorsque la boîte de dialogue affiche le bon ARN.
10. (Facultatif) Si vous souhaitez exiger l'authentification multi-facteur (MFA) ou restreindre l'accès au rôle à partir d'une plage d'adresses IP spécifiée, développez la section Conditions de demande et sélectionnez les options à appliquer.
11. Choisissez Suivant.
12. Sur la page Réviser et créer, entrez le nom de la nouvelle politique. Par exemple : **`GrantAccessToOrganizationAccountAccessRole`**. Vous pouvez également ajouter une description si vous le souhaitez.
13. Choisissez Créer une politique pour enregistrer votre nouvelle politique gérée.
14. Maintenant que vous disposez de la politique, vous pouvez l'attacher à un groupe.

Dans le volet de navigation, choisissez Groupes d'utilisateurs, puis choisissez le nom du groupe (et non la case à cocher) dont vous souhaitez que les membres puissent assumer le rôle dans le compte membre. Si nécessaire, vous pouvez créer un nouveau groupe.

15. Choisissez l'onglet Autorisations, puis Ajouter des autorisations, et enfin Attacher des politiques.
16. (Facultatif) Dans la zone Rechercher, vous pouvez commencer à taper le nom de votre politique pour filtrer la liste jusqu'à ce que le nom de la politique que vous venez de créer aux étapes Step 2 à Step 13 apparaisse. Vous pouvez également filtrer toutes les politiques AWS gérées en choisissant Tous les types, puis en choisissant Gestion par le client.
17. Cochez la case à côté de votre politique, puis choisissez Joindre des politiques.

Les utilisateurs IAM membres du groupe sont désormais autorisés à passer au nouveau rôle dans la AWS Organizations console en suivant la procédure suivante.

AWS Management Console

Pour endosser le rôle pour le compte membre

Lorsqu'il utilise le rôle, l'utilisateur dispose des autorisations d'administration dans le nouveau compte membre. Indiquez à vos utilisateurs IAM qui sont membres du groupe d'effectuer les opérations suivantes pour endosser le nouveau rôle.

1. Dans le coin supérieur droit de la AWS Organizations console, choisissez le lien contenant votre nom de connexion actuel, puis choisissez Changer de rôle.
2. Entrez l'ID de compte et le nom de rôle fournis par votre administrateur.
3. Pour Nom d'affichage, entrez le texte que vous souhaitez afficher dans la barre de navigation dans le coin supérieur droit à la place de votre nom d'utilisateur quand vous utilisez ce rôle. Vous pouvez éventuellement choisir une couleur.
4. Choisissez Changer de rôle. À présent, toutes les actions que vous exécutez sont effectuées avec les autorisations accordées au rôle que vous avez endossé. Vous ne disposez plus des autorisations associées à votre utilisateur IAM d'origine jusqu'à ce que vous changiez de nouveau de rôle.
5. Lorsque vous avez terminé d'exécuter les actions qui exigent les autorisations de ce rôle, vous pouvez revenir à votre utilisateur IAM normal. Choisissez le nom du rôle dans le coin supérieur droit (quel que soit le nom que vous avez spécifié comme nom d'affichage), puis cliquez sur Retour à. *UserName*

# Fermeture d'un compte membre dans une organisation avec AWS Organizations

Si vous n'avez plus besoin d'un compte membre dans votre organisation, vous pouvez le fermer depuis la AWS Organizations console en suivant les instructions de cette rubrique. Vous ne pouvez fermer un compte membre à l'aide de la AWS Organizations console que si votre organisation est en mode Toutes les fonctionnalités.

Vous pouvez également fermer un compte Compte AWS directement depuis la page Compte AWS Management Console après vous être connecté en tant qu'utilisateur root. Pour step-by-step obtenir des instructions, consultez la section Fermer un Compte AWS dans le Guide de gestion de AWS compte.

Pour fermer un compte de gestion, voirFermeture d'un compte de gestion dans votre organisation.

## Fermer le compte d'un membre

Une fois connecté au compte de gestion de l'organisation, vous pouvez clôturer des comptes membres qui font partie de votre organisation. Pour ce faire, exécutez les étapes suivantes.

> **Important**
>
> Avant de fermer votre compte de membre, nous vous recommandons vivement de prendre en compte les facteurs à prendre en compte et de comprendre l'impact de la fermeture d'un compte. Pour plus d'informations, consultez ce que vous devez savoir avant de fermer votre compte et À quoi vous attendre après la fermeture de votre compte dans le Guide de gestion de AWS compte.

### AWS Management Console

Pour fermer un compte membre depuis la AWS Organizations console

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM ou en tant qu'utilisateur root (ce n'est pas recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Comptes AWS, trouvez et choisissez le nom du compte membre que vous souhaitez clôturer. Vous pouvez naviguer dans la hiérarchie des unités organisationnelles (OU), consulter une liste plate de comptes sans la structure des OU.

3. Choisissez Close (Clôturer) en regard du nom du compte en haut de la page. Cette option n'est disponible que lorsqu'une AWS organisation est en mode Toutes les fonctionnalités.

> **Note**
>
> Si votre organisation utilise le mode de facturation consolidée, le bouton Fermer ne s'affichera pas dans la console. Pour fermer un compte en mode de facturation consolidée, connectez-vous au compte que vous souhaitez fermer en tant qu'utilisateur root. Sur la page Comptes, cliquez sur le bouton Fermer le compte, entrez votre identifiant de compte, puis cliquez sur le bouton Fermer le compte.

4. Lisez les instructions de fermeture de compte et assurez-vous de bien les comprendre.
5. Entrez l'identifiant du compte du membre, puis choisissez Fermer le compte.

> **Note**
>
> Tout compte de membre que vous fermez affichera une `CLOSED` étiquette à côté de son nom dans la AWS Organizations console jusqu'à 90 jours après la date de fermeture initiale. Après 90 jours, le compte du membre sera définitivement fermé et ne sera plus affiché dans la AWS Organizations console. Veuillez noter que la suppression du compte de l'organisation peut prendre quelques jours après sa fermeture définitive.

Pour fermer un compte membre depuis la page Comptes

Vous pouvez éventuellement fermer un compte AWS membre directement depuis la page Comptes du AWS Management Console. Pour step-by-step obtenir des conseils, suivez les instructions décrites dans Fermer et Compte AWS dans le Guide de gestion de AWS compte.

AWS CLI & AWS SDKs

Pour fermer un Compte AWS

Vous pouvez utiliser l'une des commandes suivantes pour clôturer un compte AWS :

- AWS CLI : close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS SDKs: CloseAccount

## Protéger les comptes des membres contre la fermeture avec AWS Organizations

Pour protéger les comptes des membres contre toute fermeture accidentelle, créez une politique IAM qui précise quels comptes sont exemptés. Cette politique empêche la fermeture des comptes de membres protégés.

Créez une politique IAM pour refuser la fermeture du compte en utilisant l'une des méthodes suivantes :

- Répertoriez explicitement les comptes protégés dans l'`Resource`élément de la politique en utilisant leur ARNs.
- Marquez les comptes individuels et utilisez la clé de condition `aws:ResourceTag` globale pour empêcher la fermeture des comptes étiquetés.

> **Note**
>
> Les politiques de contrôle des services (SCPs) n'affectent pas les principes IAM du compte de gestion.

### Exemples de politiques IAM qui empêchent la clôture de comptes membres

Les exemples de code suivants montrent deux méthodes différentes que vous pouvez utiliser pour empêcher les comptes des membres de fermer leur compte.

Prevent member accounts with tags from getting closed

Vous pouvez attacher la politique suivante à une identité de votre compte de gestion. Cette politique empêche les principaux du compte de gestion de clôturer tout compte membre labelisé avec la clé de condition globale d'identification `aws:ResourceTag`, le`AccountTypeKey` et`Criticalvaleur` de balise.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Prevent member accounts listed in this policy from getting closed

Vous pouvez attacher la politique suivante à une identité de votre compte de gestion. Cette politique empêche les principaux du compte de gestion de clôturer les comptes membres explicitement spécifiés dans l'élément `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

# Supprimer un compte membre d'une organisation avec AWS Organizations

La suppression d'un compte membre ne ferme pas le compte, mais le retire de l'organisation. Le compte de l'ancien membre devient un compte autonome Compte AWS qui n'est plus géré par AWS Organizations.

Par la suite, le compte n'est plus soumis à aucune politique et est responsable du paiement de ses propres factures. Le compte de gestion de l'organisation n'est plus facturé pour les dépenses accumulées par le compte après son retrait de l'organisation.

## Considérations

Les rôles d'accès IAM créés par le compte de gestion ne sont pas automatiquement supprimés

Lorsque vous supprimez un compte membre de l'organisation, tout rôle IAM créé pour permettre l'accès au compte de gestion de l'organisation n'est pas automatiquement supprimé. Si vous souhaitez mettre fin à cet accès à partir du compte de gestion de l'ancienne organisation, vous devez supprimer manuellement le rôle IAM. Pour plus d'informations sur la suppression d'un rôle, consultez Suppression de rôles ou de profils d'instance dans le Guide de l'utilisateur IAM.

Vous ne pouvez supprimer un compte de votre organisation que s'il contient les informations nécessaires à son fonctionnement en tant que compte autonome.

Vous ne pouvez supprimer un compte de votre organisation que si le compte possède les informations requises pour pouvoir fonctionner comme compte autonome. Lorsque vous créez un compte dans une organisation à l'aide de la AWS Organizations console, de l'API ou de AWS CLI commandes, toutes les informations requises pour les comptes autonomes ne sont pas automatiquement collectées.

Pour chaque compte que vous souhaitez rendre autonome, vous devez choisir un plan d'assistance, fournir et vérifier les informations de contact requises, et fournir un mode de paiement actuel. AWS utilise le mode de paiement pour facturer toute AWS activité facturable (autre que le niveau AWS gratuit) survenant alors que le compte n'est pas rattaché à une organisation. Pour supprimer un compte qui ne possède pas encore ces informations, suivez les étapes de Quitter une organisation depuis un compte membre avec AWS Organizations.

Vous devez attendre au moins quatre jours après la création du compte

Pour supprimer un compte que vous avez créé dans l'organisation, vous devez attendre au moins quatre jours après sa création. Les comptes invités ne sont pas soumis à cette période d'attente.

Le titulaire du compte qui quitte le compte devient responsable de tous les nouveaux frais encourus.

Au moment où le compte quitte l'organisation avec succès, le propriétaire du compte Compte AWS devient responsable de tous les nouveaux AWS frais encourus et le mode de paiement du compte est utilisé. Le compte de gestion de l'organisation n'est plus responsable.

Le compte ne peut pas être un compte d'administrateur délégué pour aucun AWS service activé pour l'organisation.

Le compte que vous souhaitez supprimer ne doit pas être un compte d'administrateur délégué pour aucun AWS service activé pour votre organisation. Si le compte est un administrateur délégué, vous devez d'abord remplacer le compte administrateur délégué par un autre compte qui reste dans l'organisation. Pour plus d'informations sur la façon de désactiver ou de modifier le compte d'administrateur délégué pour un AWS service, consultez la documentation de ce service.

Le compte n'a plus accès aux données de coût et d'utilisation

Quand un compte membre quitte une organisation, ce compte n'a plus accès aux données de coût et d'utilisation du temps où il était membre de l'organisation. Par contre, le compte de gestion de l'organisation peut continuer à accéder aux données. Si le compte rejoint à nouveau l'organisation, il peut à nouveau accéder à ces données.

Les tags associés au compte sont supprimés

Lorsqu'un compte membre quitte une organisation, toutes les balises attachées au compte sont supprimées.

Les principaux associés au compte ne sont plus concernés par les politiques de l'organisation.

Les mandataires du compte ne sont plus affectés par les politiques de contrôle des services (SCP) s'appliquaient dans l'organisation. Cela signifie que les restrictions imposées par SCPs ont disparu et que les utilisateurs et les rôles du compte peuvent disposer de plus d'autorisations qu'auparavant. Les autres types de politiques d'organisation ne peuvent plus être appliqués ni traités.

Le compte n'est plus couvert par les accords d'organisation

Si un compte membre est supprimé d'une organisation, ce compte n'est plus couvert par les accords d'organisation. Les administrateurs de compte de gestion doivent communiquer cette suppression aux comptes membres avant de supprimer les comptes membres de l'organisation, afin que les comptes membres puissent mettre en place de nouveaux accords, si nécessaire. La liste des accords

d'organisation actifs peut être consultée dans la AWS Artifact console sur la page Accords d'AWS Artifact organisation.

L'intégration à d'autres services peut être désactivée

L'intégration à d'autres services peut être désactivée. Si vous supprimez un compte d'une organisation dont l'intégration à un AWS service est activée, les utilisateurs de ce compte ne peuvent plus utiliser ce service.

## Supprimer un compte membre d'une organisation

Lorsque vous vous connectez au compte de gestion de l'organisation, vous pouvez supprimer de l'organisation les comptes membres dont vous n'avez plus besoin. Pour ce faire, procédez comme suit : Cette procédure s'applique uniquement aux comptes membres. Pour supprimer le compte de gestion, vous devez supprimer l'organisation.

Autorisations minimales

Pour supprimer plusieurs comptes membres de votre organisation, vous devez vous connecter en tant qu'utilisateur ou rôle dans le compte de gestion avec les autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:RemoveAccountFromOrganization`

Si vous choisissez la connexion en tant qu'utilisateur ou rôle dans un compte membre à l'étape 5, cet utilisateur ou rôle doit détenir les autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations.
- `organizations:LeaveOrganization` — Notez que l'administrateur de l'organisation peut appliquer à votre compte une politique qui supprime cette autorisation, vous empêchant ainsi de supprimer votre compte de l'organisation.
- Si vous vous connectez en tant qu'utilisateur IAM et que les informations de paiement sont absentes du compte, l'utilisateur doit détenir les autorisations `aws-portal:ModifyBilling` et `aws-portal:ModifyPaymentMethods` (si le compte n'a pas encore migré vers des autorisations détaillées) OU les autorisations

`payments:CreatePaymentInstrument` et `payments:UpdatePaymentPreferences` (si le compte a migré vers des autorisations détaillées). En outre, l'accès de l'utilisateur IAM à la facturation doit être activé sur le compte membre. Si vous ne l'avez pas encore activé, consultez Activation de l'accès à la console de facturation et de gestion des coûts dans le Guide de l'utilisateur AWS Billing .

AWS Management Console

Pour supprimer un compte membre de votre organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, cochez la case
   ☑
   en regard du compte membre à supprimer de votre organisation. Vous pouvez parcourir la hiérarchie de l'unité d'organisation ou activer l'option Afficher Comptes AWS uniquement pour afficher une liste plate de comptes sans la structure de l'unité d'organisation. Si vous avez beaucoup de comptes, vous devrez peut-être choisir Charger plus de comptes dans « nom-UO » au bas de la liste pour trouver tous ceux que vous souhaitez supprimer.

   Dans la page Comptes AWS, trouvez et choisissez le nom du compte membre à supprimer de votre organisation. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver le compte que vous souhaitez.
3. Choisissez Actions, puis, sous Compte AWS, choisissez Supprimer de l'organisation.
4. Dans la section Supprimer le compte « nom du compte » (# account-id-num) de l'organisation ? dans la boîte de dialogue, choisissez Supprimer le compte.
5. Si AWS Organizations vous ne supprimez pas un ou plusieurs comptes, c'est généralement parce que vous n'avez pas fourni toutes les informations requises pour que le compte fonctionne en tant que compte autonome. Procédez comme suit :

   a. Connectez-vous aux comptes ayant échoué. Nous vous recommandons de vous connecter au compte membre en choisissant Copier le lien, puis en collant ce lien dans la barre d'adresse d'une nouvelle fenêtre de navigation privée. Si vous ne voyez pas le lien Copier, utilisez ce lien pour accéder à la AWS page d'inscription et effectuer les

étapes d'inscription manquantes. Si vous n'utilisez pas de fenêtre privée, vous êtes déconnecté du compte de gestion et ne pourrez pas revenir à cette boîte de dialogue.

b. Le navigateur vous ramène directement au processus de connexion pour réaliser toute étape manquante pour ce compte. Complétez toutes les étapes présentées. Elles peuvent inclure les éléments suivants :

   - Fournir les informations de contact
   - Fournir un moyen de paiement valide
   - Vérifier le numéro de téléphone
   - Sélectionner une option de plan de support

c. Une fois la dernière étape d'inscription terminée, votre navigateur est AWS automatiquement redirigé vers la AWS Organizations console du compte membre. Choisissez Quitter l'organisation, puis confirmez votre choix dans la boîte de dialogue de confirmation. Vous êtes redirigé vers la page de démarrage (Getting Started) de la console AWS Organizations dans laquelle vous pouvez consulter les invitations en attente pour votre compte à rejoindre d'autres organisations.

d. Supprimez de l'organisation les rôles IAM qui accordent l'accès à votre compte.

> **Important**
>
> Si votre compte a été créé dans l'organisation, Organizations a créé automatiquement dans le compte un rôle IAM qui a activé l'accès par le compte de gestion de l'organisation. Si le compte a été invité à rejoindre l'organisation, Organizations n'a pas créé automatiquement un tel rôle, mais vous ou un autre administrateur en avez peut-être créé un pour obtenir les mêmes avantages. Dans un cas comme dans l'autre, lorsque vous supprimez le compte de l'organisation, un tel rôle n'est pas supprimé automatiquement. Si vous souhaitez mettre fin à cet accès à partir du compte de gestion de l'ancienne organisation, vous devez supprimer manuellement ce rôle IAM. Pour plus d'informations sur la suppression d'un rôle, consultez Suppression de rôles ou de profils d'instance dans le Guide de l'utilisateur IAM.

AWS CLI & AWS SDKs

Pour supprimer un compte membre de votre organisation

Vous pouvez utiliser l'une des commandes suivantes pour supprimer un compte membre :

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS SDKs: RemoveAccountFromOrganization

Une fois le compte membre supprimé de l'organisation, veillez à supprimer de l'organisation les rôles IAM qui accordent l'accès à votre compte.

> **Important**
>
> Si votre compte a été créé dans l'organisation, Organizations a créé automatiquement dans le compte un rôle IAM qui a activé l'accès par le compte de gestion de l'organisation. Si le compte a été invité à rejoindre l'organisation, Organizations n'a pas créé automatiquement un tel rôle, mais vous ou un autre administrateur en avez peut-être créé un pour obtenir les mêmes avantages. Dans un cas comme dans l'autre, lorsque vous supprimez le compte de l'organisation, un tel rôle n'est pas supprimé automatiquement. Si vous souhaitez mettre fin à cet accès à partir du compte de gestion de l'ancienne organisation, vous devez supprimer manuellement ce rôle IAM. Pour plus d'informations sur la suppression d'un rôle, consultez Suppression de rôles ou de profils d'instance dans le Guide de l'utilisateur IAM.

Les comptes des membres peuvent plutôt être supprimés en utilisant leave-organization. Pour de plus amples informations, veuillez consulter Quitter une organisation depuis un compte membre avec AWS Organizations.

## Quitter une organisation depuis un compte membre avec AWS Organizations

Lorsque vous vous connectez à un compte membre, vous pouvez quitter une organisation. Le compte de gestion ne peut pas quitter l'organisation en utilisant cette technique. Pour supprimer le compte de gestion, vous devez supprimer l'organisation.

## Considérations

Le statut d'un compte auprès d'une organisation influe sur les données de coût et d'utilisation visibles

Les comptes conservent l'accès à toutes les anciennes factures qui leur ont été livrées et à toutes les données de facturation qu'ils génèrent, indépendamment des changements d'adhésion des organisations. Cependant, la visibilité des données de Cost Explorer est liée à l'adhésion actuelle des organisations. Le tableau ci-dessous montre comment trois transitions de compte courantes affectent la visibilité des données :

| | Disponibilité des factures | Disponibilité des factures (par exemple, page des factures) | Disponibilité de Cost Explorer |
|---|---|---|---|
| Scénario 1<br><br>Le compte membre quitte l'organisation A et devient un compte autonome | Le compte conserve l'accès à toutes les factures historiques qui lui sont livrées. | Le compte conserve l'accès à toutes les données historiques des factures qu'il a générées en tant que membre de l'organisation A. | Le compte perd l'accès aux données historiques sur les coûts et l'utilisation qu'il a générées en tant que membre de l'organisation A. |
| Scénario 2<br><br>Le compte membre quitte l'organisation A et rejoint l'organisation B | Le compte conserve l'accès à toutes les factures historiques qui lui sont livrées. | Le compte conserve l'accès à toutes les données historiques des factures qu'il a générées en tant que membre de l'organisation A. | Le compte perd l'accès aux données historiques sur les coûts et l'utilisation qu'il a générées en tant que membre de l'organisation A. |
| Scénario 3<br><br>Le compte rejoint une organisation à laquelle il appartenait auparavant | Le compte conserve l'accès à toutes les factures historiques qui lui sont livrées. | Le compte conserve l'accès à toutes les données historiques des factures qu'il a générées (qu'elles soient générées en tant que compte autonome ou en tant | Le compte a de nouveau accès aux données relatives aux coûts et à l'utilisation pendant toute la période pendant laquelle il était membre de l'organisation, mais il perd l'accès à tous les coûts et utilisati |

| | Disponibilité des factures | Disponibilité des factures (par exemple, page des factures) | Disponibilité de Cost Explorer |
|---|---|---|---|
| | | que membre d'une autre organisation). | ons historiques générés en dehors de son organisation actuelle. |

Le compte n'est plus couvert par les accords d'organisation acceptés en son nom

Si vous quittez une organisation, vous ne serez plus couvert par les accords d'organisation qui ont été acceptés en votre nom par le compte de gestion de l'organisation. Vous pouvez consulter la liste de ces accords d'organisation dans la AWS Artifact console sur la page Accords d'AWS Artifact organisation. Avant de quitter l'organisation, vous devez déterminer (avec l'aide de vos équipes juridiques, de confidentialité ou de conformité le cas échéant) s'il est nécessaire pour vous de disposer de nouveaux accords.

Les limites de quota du compte peuvent changer et avoir un impact

Le fait de quitter une organisation en tant que compte membre peut affecter les limites de quotas de service disponibles pour ce compte. Si vous avez des charges de travail automatisées qui nécessitent des limites plus élevées, veuillez revoir vos quotas dans la console des quotas de service après avoir quitté l'organisation afin de garantir une expérience ininterrompue. Veuillez contacter le AWS Support centre après avoir quitté l'organisation pour obtenir de l'aide.

## Quitter une organisation depuis un compte membre

Pour quitter une organisation, suivez la procédure ci-dessous.

Autorisations minimales

Pour quitter une organisation , vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations.
- `organizations:LeaveOrganization` — Notez que l'administrateur de l'organisation peut appliquer à votre compte une politique qui supprime cette autorisation, vous empêchant ainsi de supprimer votre compte de l'organisation.

- Si vous vous connectez en tant qu'utilisateur IAM et que les informations de paiement sont absentes du compte, l'utilisateur doit détenir les autorisations `aws-portal:ModifyBilling` et `aws-portal:ModifyPaymentMethods` (si le compte n'a pas encore migré vers des autorisations détaillées) OU les autorisations `payments:CreatePaymentInstrument` et `payments:UpdatePaymentPreferences` (si le compte a migré vers des autorisations détaillées). En outre, l'accès de l'utilisateur IAM à la facturation doit être activé sur le compte membre. Si vous ne l'avez pas encore activé, consultez Activation de l'accès à la console de facturation et de gestion des coûts dans le Guide de l'utilisateur AWS Billing .

AWS Management Console

Pour quitter une organisation depuis votre compte membre

1. Connectez-vous à la AWS Organizations console sur la AWS Organizations console. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans un compte membre.

   Par défaut, vous n'avez pas accès au mot de passe de l'utilisateur root dans un compte membre créé à l'aide de AWS Organizations. Si nécessaire, récupérez le mot de passe de l'utilisateur root en suivant les étapes décrites dans la section Utilisation de l'utilisateur root (déconseillé pour les tâches quotidiennes) dansAccès aux comptes des membres d'une organisation avec AWS Organizations.
2. Sur la page Tableau de bord Organizations, choisissez Quitter l'organisation.
3. Dans la boîte de dialogue Confirmer le départ de l'organisation ?, choisissez Quitter l'organisation. Lorsque vous y êtes invité, confirmez votre choix de supprimer le compte. Après avoir confirmé, vous êtes redirigé vers la page Getting Started de la AWS Organizations console, où vous pouvez consulter toutes les invitations en attente pour votre compte afin de rejoindre d'autres organisations.

   Si le message Vous ne pouvez pas encore quitter l'organisation s'affiche, cela signifie que votre compte ne dispose pas de toutes les informations requises pour fonctionner en tant que compte autonome. Dans ce cas, passez à l'étape suivante.
4. Si la boîte de dialogue Confirmer le départ de l'organisation ? affiche le message Vous ne pouvez pas encore quitter l'organisation, cliquez sur le lien Compléter les étapes de création de compte.

Si vous ne voyez pas le lien Terminer les étapes d'inscription au compte, utilisez ce lien pour accéder à la AWS page S'inscrire et terminer les étapes d'inscription manquantes.

5. Sur la page Inscription à AWS, entrez toutes les informations requises pour faire du compte un compte autonome. Ces informations incluent notamment :

   - Le nom et l'adresse du contact
   - Un mode de paiement valide
   - Un numéro de téléphone vérifié
   - Les options du plan de support

6. Lorsque la boîte de dialogue indique que le processus d'inscription est terminé, choisissez Quitter l'organisation.

   Une boîte de dialogue de confirmation s'affiche. Confirmez votre choix de supprimer le compte. Vous êtes redirigé vers la page Getting Started de la AWS Organizations console, où vous pouvez consulter toutes les invitations en attente pour que votre compte rejoigne d'autres organisations.

7. Supprimez de l'organisation les rôles IAM qui accordent l'accès à votre compte.

   > **Important**
   >
   > Si votre compte a été créé dans l'organisation, Organizations a créé automatiquement dans le compte un rôle IAM qui a activé l'accès par le compte de gestion de l'organisation. Si le compte a été invité à rejoindre l'organisation, Organizations n'a pas créé automatiquement un tel rôle, mais vous ou un autre administrateur en avez peut-être créé un pour obtenir les mêmes avantages. Dans un cas comme dans l'autre, lorsque vous supprimez le compte de l'organisation, un tel rôle n'est pas supprimé automatiquement. Si vous souhaitez mettre fin à cet accès à partir du compte de gestion de l'ancienne organisation, vous devez supprimer manuellement ce rôle IAM. Pour plus d'informations sur la suppression d'un rôle, consultez Suppression de rôles ou de profils d'instance dans le Guide de l'utilisateur IAM.

AWS CLI & AWS SDKs

Pour quitter une organisation en tant que compte membre

Vous pouvez utiliser l'une des commandes suivantes pour quitter une organisation :

- AWS CLI : leave-organization

  Dans l'exemple suivant, le compte dont les informations d'identification sont utilisées pour exécuter la commande quitte l'organisation.

  ```
  $ aws organizations leave-organization
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS SDKs: LeaveOrganization

Une fois le compte membre retiré de l'organisation, veillez à supprimer de l'organisation les rôles IAM qui accordent l'accès à votre compte.

> **Important**
>
> Si votre compte a été créé dans l'organisation, Organizations a créé automatiquement dans le compte un rôle IAM qui a activé l'accès par le compte de gestion de l'organisation. Si le compte a été invité à rejoindre l'organisation, Organizations n'a pas créé automatiquement un tel rôle, mais vous ou un autre administrateur en avez peut-être créé un pour obtenir les mêmes avantages. Dans un cas comme dans l'autre, lorsque vous supprimez le compte de l'organisation, un tel rôle n'est pas supprimé automatiquement. Si vous souhaitez mettre fin à cet accès à partir du compte de gestion de l'ancienne organisation, vous devez supprimer manuellement ce rôle IAM. Pour plus d'informations sur la suppression d'un rôle, consultez Suppression de rôles ou de profils d'instance dans le Guide de l'utilisateur IAM.

Les comptes membres peuvent également être supprimés par un utilisateur du compte de gestion à la remove-account-from-organizationplace. Pour de plus amples informations, veuillez consulter Supprimer un compte membre d'une organisation.

## Mettre à jour le nom du compte d'un membre avec AWS Organizations

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez mettre à jour le nom du compte d'un membre. Pour savoir comment mettre à jour le nom du compte d'un

membre, suivez les étapes décrites dans la section Mettre à jour le nom du compte de n'importe quel Compte AWS membre de votre organisation dans le Guide de Gestion de compte AWS référence.

## Mise à jour de l'adresse e-mail de l'utilisateur root () pour un compte membre avec AWS Organizations

Pour une sécurité et une résilience administrative accrues, les principaux IAM du compte de gestion (qui disposent des autorisations IAM nécessaires) peuvent mettre à jour de manière centralisée l'adresse e-mail d'un utilisateur root (adresse ) (également appelée adresse e-mail principale) pour n'importe lequel de leurs comptes membres sans avoir à se connecter à chaque compte individuellement. Cela permet aux administrateurs du compte de gestion (ou d'un compte administrateur délégué) de mieux contrôler leurs comptes de membres. Cela garantit également que les adresses e-mail des utilisateurs root, les adresses de tous les comptes membres de votre choix AWS Organizations peuvent être tenues à jour, même si vous avez perdu l'accès à l'adresse e-mail d'origine de l'utilisateur root, à l'adresse e-mail ou aux informations d'identification administratives.

Lorsque l'adresse e-mail de l'utilisateur root (adresse ) est modifiée de manière centralisée par un administrateur de compte de gestion, le mot de passe et la configuration MFA restent les mêmes qu'avant le changement. Notez que le MFA peut être contourné par un utilisateur qui contrôle l'adresse e-mail de l'utilisateur root d'un compte, l'adresse e-mail du contact principal.

Pour mettre à jour l'adresse e-mail de l'utilisateur root () d'un compte membre de votre organisation, celle-ci doit avoir préalablement activé le mode toutes les fonctionnalités. AWS Organizations en mode de facturation consolidée ou sur des comptes ne faisant pas partie d'une organisation, ne peuvent pas mettre à jour leur adresse e-mail d'utilisateur racine (adresse ) de manière centralisée. Les utilisateurs qui souhaitent modifier l'adresse e-mail de l'utilisateur root (adresse ) pour les comptes non pris en charge par l'API doivent continuer à utiliser la console de facturation pour gérer leur adresse e-mail utilisateur root (adresse e-mail ).

Pour step-by-step savoir comment mettre à jour l'adresse e-mail de l'utilisateur root de votre compte membre (adresse e-mail e-mail de l'utilisateur root pour n'importe quel Compte AWS membre de votre organisation dans le Guide de Gestion de compte AWS référence.

# Gérer les invitations à un compte avec AWS Organizations

Après avoir créé une organisation et vérifié que vous possédez l'adresse e-mail associée au compte de gestion, vous pouvez inviter des personnes existantes Comptes AWS à rejoindre votre organisation. Utilisez la AWS Organizations console pour lancer et gérer les invitations que vous

envoyez à d'autres comptes. Vous ne pouvez envoyer une invitation à d'autres comptes qu'à partir du compte de gestion de votre organisation.

Lorsque vous invitez un compte, AWS Organizations envoie une invitation au propriétaire du compte, qui peut décider d'accepter ou de refuser l'invitation.

Si vous êtes l'administrateur d'une Compte AWS, vous pouvez également accepter ou refuser une invitation d'une organisation. Si vous acceptez, votre compte devient membre de cette organisation.

Pour créer un compte qui fait automatiquement partie d'une organisation, consultezCréation d'un compte membre dans une organisation avec AWS Organizations.

> **Important**
>
> Tous les comptes d'une organisation doivent provenir de la même AWS partition que le compte de gestion. Les comptes de la Régions AWS partition commerciale ne peuvent pas appartenir à une organisation dont les comptes proviennent de la partition des régions de la Chine ou des comptes de la partition AWS GovCloud (US) des régions.

Rubriques



## Considérations

Limitations du nombre d'invitations que vous pouvez envoyer par jour

Pour connaître les limites du nombre d'invitations que vous pouvez envoyer par jour, consultezValeurs minimales et maximales. Les invitations acceptées ne sont pas prises en compte dans ce quota. Dès qu'une invitation est acceptée, vous pouvez envoyer une autre invitation le même jour. Chaque invitation doit recevoir une réponse dans un délai de 15 jours, sinon, elle expire.

Une invitation qui est envoyée à un compte est comptabilisée par rapport au quota de comptes de votre organisation. Le décompte est réinitialisé si le compte invité refuse, si le compte de gestion annule l'invitation ou si l'invitation expire.

Un compte ne peut rejoindre qu'une seule organisation

Un compte ne peut rejoindre qu'une seule organisation. Si vous recevez plusieurs invitations, vous ne pouvez en accepter qu'une seule.

L'historique de facturation et les rapports restent enregistrés dans le compte de gestion

L'historique de facturation et les rapports relatifs à tous les comptes sont conservés dans le compte de gestion d'une organisation. Avant de transférer le compte vers une nouvelle organisation, exportez ou sauvegardez les historiques de facturation et de rapports des comptes membres que vous souhaitez conserver. Cela peut inclure les rapports sur les coûts et l'utilisation, les rapports Cost Explorer, les rapports Savings Plans, ainsi que l'utilisation et la couverture des instances réservées (RI).

Le compte de gestion est responsable de tous les frais accumulés par les comptes des membres

Une fois qu'un compte a accepté l'invitation à rejoindre une organisation, le compte de gestion de l'organisation devient responsable de tous les frais accumulés par le nouveau compte membre. Le moyen de paiement associé au compte membre n'est plus utilisé. Au lieu de cela, le moyen de paiement associé au compte de gestion de l'organisation paie tous les frais encourus par le compte membre.

Organizations crée automatiquement le rôle lié au service **`AWSServiceRoleForOrganizations`**

AWS Organizations crée un rôle lié à un service appelé `AWSServiceRoleForOrganizations` à prendre en charge les intégrations entre AWS Organizations et d'autres services. AWS Pour de plus amples informations, veuillez consulter AWS Organizations et rôles liés aux services. Le compte invité doit avoir ce rôle si votre organisation prend en charge toutes les fonctionnalités. Vous pouvez supprimer ce rôle si l'organisation ne prend en charge que l'ensemble de fonctionnalités de facturation consolidée. Si vous supprimez ce rôle et que vous activez ultérieurement toutes les fonctionnalités de votre organisation, vous AWS Organizations recréez ce rôle pour le compte.

Organizations ne crée pas automatiquement le rôle IAM **`OrganizationAccountAccessRole`**

Pour les comptes de membres invités, le rôle `OrganizationAccountAccessRole`IAM AWS Organizations n'est pas automatiquement créé. Ce rôle accorde aux utilisateurs du compte de gestion l'accès administratif au compte membre. Si vous souhaitez activer ce niveau de contrôle administratif, vous pouvez ajouter manuellement le rôle au compte invité. Pour de plus amples informations, veuillez consulter Création OrganizationAccountAccessRole d'un compte invité avec AWS Organizations.

> **Note**
>
> Lorsque vous créez un compte dans votre organisation au lieu d'inviter un compte existant à le rejoindre, le rôle IAM est AWS Organizations automatiquement créé `OrganizationAccountAccessRole` par défaut.

Les politiques associées à la racine ou à l'unité d'organisation contenant le compte s'appliquent immédiatement

Si vous avez des politiques associées à la racine ou à l'unité organisationnelle (UO) qui contient le compte invité, ces politiques s'appliquent immédiatement à tous les utilisateurs et rôles du compte invité.

Vous pouvez activer la confiance en matière de service pour un autre AWS service de votre organisation. Lorsque vous le faites, ce service approuvé peut créer des rôles liés au service ou exécuter des actions dans n'importe quel compte membre de l'organisation, y compris dans un compte invité.

Organisations disposant uniquement de l'ensemble de fonctionnalités de facturation consolidée peuvent toujours inviter des comptes

Vous pouvez inviter un compte à rejoindre une organisation où seules les fonctions de facturation consolidée sont activées. Si vous souhaitez activer ultérieurement toutes les fonctions de l'organisation, les comptes invités doivent approuver la modification.

## Envoyer des invitations à un compte avec AWS Organizations

Vous devez confirmer que vous possédez l'adresse e-mail associée au compte de gestion avant de pouvoir inviter des comptes à votre organisation. Pour de plus amples informations, veuillez consulter Vérification de l'adresse e-mail avec AWS Organizations. Une fois que vous avez validé votre adresse e-mail, effectuez les opérations suivantes pour inviter des comptes à votre organisation.

> **Autorisations minimales**
>
> Pour inviter un Compte AWS homme à rejoindre votre organisation, vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization` (console uniquement)

- `organizations:InviteAccountToOrganization`

### AWS Management Console

Pour inviter un autre compte à rejoindre votre organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Si vous avez déjà vérifié votre adresse e-mail auprès de AWS, ignorez cette étape.

   Si vous n'avez pas encore validé votre adresse e-mail, suivez les instructions sous e-mail de vérification dans les 24 heures après la création de l'organisation. Il peut y avoir un certain délai avant la réception de l'e-mail de vérification. Vous ne pouvez pas inviter un compte à rejoindre votre organisation tant que vous n'avez pas validé votre adresse e-mail.
3. Accédez à la page Comptes AWS, puis choisissez Ajouter un compte AWS .
4. Dans la page Ajouter un Compte AWS, choisissez Inviter un compte AWS existant.
5. Sur la AWS page Inviter un compte existant, dans le champ Adresse e-mail ou identifiant du compte Compte AWS à inviter, entrez soit l'adresse e-mail associée au compte à inviter, soit son numéro d'identification de compte.
6. (Facultatif) Dans Message à inclure dans l'e-mail d'invitation, saisissez le texte que vous souhaitez inclure dans l'e-mail d'invitation envoyé au propriétaire du compte invité.
7. (Facultatif) Dans Ajouter des balises, spécifiez une ou plusieurs balises qui seront automatiquement appliquées au compte une fois que son administrateur aura accepté l'invitation. Pour cela, choisissez Ajouter une balise, puis saisissez une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à un Compte AWS.
8. Choisissez Send invitation (Envoyer une invitation).

> **Important**
>
> Si vous obtenez un message indiquant que vous avez dépassé vos quotas de comptes pour l'organisation ou que vous ne pouvez pas ajouter un compte parce que votre organisation est toujours en cours d'initialisation, contactez AWS Support.

9. La console vous redirige vers la page Invitations, où vous pouvez consulter toutes les invitations ouvertes et acceptées. L'invitation que vous venez de créer s'affiche en haut de la liste avec son statut défini sur OUVERTE.

   AWS Organizations envoie une invitation à l'adresse e-mail du propriétaire du compte que vous avez invité à rejoindre l'organisation. Ce message électronique inclut un lien vers la AWS Organizations console, où le propriétaire du compte peut consulter les détails et choisir d'accepter ou de refuser l'invitation. Le propriétaire du compte invité peut également ignorer le message électronique, accéder directement à la AWS Organizations console, consulter l'invitation et l'accepter ou la refuser.

   L'invitation à ce compte est immédiatement comptabilisée par rapport au nombre maximal de comptes que vous pouvez avoir dans votre organisation. AWS Organizations n'attend pas que le compte ait accepté l'invitation. Si le compte invité refuse, le compte de gestion annule l'invitation. Si le compte invité ne répond pas dans le délai spécifié, l'invitation expire. Dans les deux cas, l'invitation n'est plus comptabilisée dans votre quota.

AWS CLI & AWS SDKs

Pour inviter un autre compte à rejoindre votre organisation

Vous pouvez utiliser l'une des commandes suivantes pour inviter un autre compte à rejoindre votre organisation :

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
```

```
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```


- AWS SDKs: InviteAccountToOrganization

## Gérer les invitations à des comptes en attente avec AWS Organizations

Lorsque vous êtes connecté à votre compte de gestion, vous pouvez afficher tous les Comptes AWS liés dans votre organisation et annuler des invitations en attente (ouvertes). Pour ce faire, exécutez les étapes suivantes.

**Autorisations minimales**

Pour gérer les invitations en attente pour votre organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

### AWS Management Console

Pour afficher ou annuler des invitations envoyées depuis votre organisation à d'autres comptes

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez à la page Invitations.

   Cette page affiche toutes les invitations qui sont envoyées depuis votre organisation et leur statut actuel.

   Si aucune invitation ne s'affiche, vérifiez si le compte invité est le compte de gestion d'une autre organisation. Seuls les comptes membres et les comptes autonomes peuvent recevoir des invitations. Les comptes de gestion ne peuvent pas recevoir d'invitations.

   Si vous souhaitez inviter un compte qui est un compte de gestion dans une autre organisation, il est recommandé de faire de ce compte un compte autonome.

   **Note**

   Les invitations acceptées, annulées et refusées continuent de s'afficher dans la liste pendant 30 jours. Elles sont ensuite supprimées et ne s'affichent plus dans la liste.

3. Choisissez la case d'option

en regard de l'invitation que vous souhaitez annuler, puis choisissez Annuler l'invitation. Si la case d'option est grisée, cette invitation ne peut pas être annulée.

Le statut de l'invitation passe de OUVERTE à ANNULÉE.

AWS envoie un e-mail au propriétaire du compte indiquant que vous avez annulé l'invitation. Le compte ne peut plus rejoindre l'organisation, sauf si vous envoyez une nouvelle invitation.

AWS CLI & AWS SDKs

Pour afficher ou annuler des invitations envoyées depuis votre organisation à d'autres comptes

Vous pouvez utiliser les commandes suivantes pour afficher ou annuler des invitations :

- AWS CLI: list-handshakes-for-organization, annuler-poignée de main
- L'exemple suivant montre les invitations envoyées par cette organisation à d'autres comptes.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
```

```
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
```

```
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

L'exemple suivant montre comment annuler une invitation à un compte.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
```

```
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDKs: ListHandshakesForOrganization, CancelHandshake

# Accepter ou refuser des invitations à un compte avec AWS Organizations

Si vous recevez une invitation à rejoindre une organisation, vous pouvez accepter ou refuser l'invitation.

## Considérations

Le statut d'un compte auprès d'une organisation influe sur les données de coût et d'utilisation visibles

Si un compte membre quitte une organisation et devient un compte autonome, ce compte n'a plus accès aux données de coût et d'utilisation du temps où il était membre de l'organisation. Le compte a accès uniquement aux données générées alors qu'il est autonome.

Si un compte membre quitte l'organisation A pour rejoindre l'organisation B, ce compte n'a plus accès aux données de coût et d'utilisation du temps où il était membre de l'organisation A. Le compte a accès uniquement aux données générées alors qu'il est membre de l'organisation B.

Si un compte joint à nouveau une organisation à laquelle il appartenait, il a de nouveau accès à ses données historiques de coût et d'utilisation.

Seuls les comptes membres et les comptes autonomes peuvent accepter ou refuser une invitation

Seuls les comptes de membres et les comptes autonomes peuvent accepter ou refuser une invitation à rejoindre une organisation. Si une invitation est envoyée à un compte de gestion qui fait déjà partie d'une organisation, ce compte ne pourra pas consulter l'invitation tant qu'il n'aura pas supprimé tous les comptes membres de son organisation et supprimé l'organisation.

CloudTrail la journalisation a lieu dans le compte effectuant l'action

Si un compte membre ou un compte autonome accepte ou refuse une invitation à créer un compte, cette action sera enregistrée dans le CloudTrail journal du compte intérimaire. Si le compte intérimaire est un compte membre, cette action ne sera pas enregistrée dans les CloudTrail journaux du compte de gestion. Cela est cohérent avec la CloudTrail connexion à des scénarios connexes (ex. Le compte du membre quittant l'organisation sera connecté au compte de membre (suivi du compte de membre, suppression du compte du membre, suivi du compte de gestion).

## Accepter ou refuser une invitation à créer un compte

Pour accepter ou refuser l'invitation, procédez comme suit.

Autorisations minimales

Pour accepter ou refuser une invitation à rejoindre une organisation , vous devez disposer des autorisations suivantes :

- `organizations:ListHandshakesForAccount`— Nécessaire pour voir la liste des invitations dans la AWS Organizations console.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `organizations:LeaveOrganization`— Obligatoire uniquement lorsque vous acceptez une invitation alors que votre compte est déjà membre d'une organisation.
- `iam:CreateServiceLinkedRole`— Requis uniquement lorsque l'acceptation de l'invitation nécessite la création d'un rôle lié au service dans le compte du membre pour faciliter l'intégration avec les autres. Services AWS Pour de plus amples informations, veuillez consulter AWS Organizations et rôles liés aux services.

AWS Management Console

Pour accepter ou refuser une invitation

1. Une invitation à rejoindre une organisation est envoyée à l'adresse e-mail du propriétaire du compte. Si vous êtes le propriétaire d'un compte et que vous recevez une invitation par e-mail, suivez les instructions de l'e-mail d'invitation ou accédez à la console AWS Organizations dans votre navigateur et choisissez Invitations ou accédez directement à la page Invitations du compte membre.
2. Si vous y êtes invité, connectez-vous au compte invité en tant qu'utilisateur IAM, assumez un rôle IAM, ou connectez-vous en tant qu'utilisateur racine du compte (non recommandé).
3. La page Invitations du compte membre affiche les invitations ouvertes de votre compte à rejoindre des organisations.

   Choisissez Accepter l'invitation ou Refuser l'invitation selon le cas.

   - Si vous choisissez Accepter l'invitation à l'étape précédente, la console vous redirige vers la page Présentation de l'organisation avec les détails de l'organisation dont votre compte est désormais membre. Vous pouvez voir l'ID de l'organisation et l'adresse e-mail du propriétaire.

> **Note**
>
> Les invitations acceptées continuent de s'afficher dans la liste pendant 30 jours. Elles sont ensuite supprimées et ne s'affichent plus dans la liste.

AWS Organizations crée automatiquement un rôle lié au service dans le nouveau compte membre pour faciliter l'intégration entre AWS Organizations les autres. Services AWS Pour de plus amples informations, veuillez consulter AWS Organizations et rôles liés aux services.

AWS envoie un e-mail au propriétaire du compte de gestion de l'organisation indiquant que vous avez accepté l'invitation. Il envoie également au propriétaire du compte membre un e-mail indiquant que le compte est désormais membre de l'organisation.

- Si vous avez choisi Refuser l'invitation à l'étape précédente, votre compte reste affiché sur la page Invitations du compte membre, qui répertorie les autres invitations en attente.

  AWS envoie un e-mail au propriétaire du compte de gestion de l'organisation indiquant que vous avez refusé l'invitation.

> **Note**
>
> Les invitations refusées continuent de s'afficher dans la liste pendant 30 jours. Elles sont ensuite supprimées et ne s'affichent plus dans la liste.

AWS CLI & AWS SDKs

Pour accepter ou refuser une invitation

Vous pouvez utiliser les commandes suivantes pour accepter ou refuser une invitation :

- AWS CLI : accept-handshake, decline-handshake

  L'exemple suivant montre comment accepter une invitation à rejoindre une organisation.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
```

```
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

L'exemple suivant montre comment refuser une invitation à rejoindre une organisation.

- AWS SDKs: AcceptHandshake, DeclineHandshake

# Migrer un compte vers une autre organisation avec AWS Organizations

Vous pouvez effectuer une migration Compte AWS d'une organisation à une autre à tout moment. Par exemple, la migration d'un compte peut être utile dans le cas d'une fusion et d'une acquisition lorsque vous devez regrouper une ou plusieurs organisations au sein Comptes AWS d'une seule organisation.

Quel que soit votre cas d'utilisation, la migration d'un compte entre organisations nécessite que vous envoyiez une invitation depuis le compte de gestion de la nouvelle organisation et que vous utilisiez le compte invité pour accepter l'invitation à rejoindre la nouvelle organisation.

> **Note**
>
> Les comptes fermés ou suspendus ne peuvent pas être migrés.
> Vous ne pouvez pas migrer un compte fermé ou suspendu. Pour réactiver un compte, contactez Support.
> Âge requis de quatre jours
> Pour migrer un compte que vous avez créé dans une organisation, vous devez attendre au moins quatre jours après sa création. Les comptes invités ne sont pas soumis à cette période d'attente.
> Réplication des données entre comptes
> Le guide AWS prescriptif suivant fournit des informations sur les stratégies de réplication des données entre Comptes AWS : réplication de ressources ou migration entre. Comptes AWS

## Ce que vous devez faire avant de migrer un compte

Avant de migrer Compte AWS d'une organisation à une autre, assurez-vous d'avoir effectué les étapes suivantes.

## Étape 1 : Vérifiez que vous disposez des autorisations IAM nécessaires pour migrer un compte

Étape 1

Assurez-vous d'avoir appliqué les autorisations nécessaires pour migrer un compte vers les organisations respectives.

Pour quitter une organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` (console uniquement)
- `organizations:LeaveOrganization`

Pour plus d'informations, voir Quitter une organisation de votre compte membre.

Pour inviter un membre Compte AWS à rejoindre une organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` (console uniquement)
- `organizations:InviteAccountToOrganization`

Pour plus d'informations, voir Inviter un Compte AWS homme à rejoindre votre organisation.

Pour migrer un compte, vous ne pouvez pas avoir de politiques IAM ou de politiques de contrôle des services qui empêchent la migration

Si vous êtes le compte de gestion ou un administrateur délégué, vous pouvez contrôler l'accès aux AWS ressources en associant des politiques d'autorisation aux identités IAM (utilisateurs, groupes et rôles) au sein d'une organisation. Pour plus d'informations, consultez les politiques IAM pour AWS Organizations.

Avant de migrer un compte :

- Vérifiez qu'aucune politique IAM ou politique de contrôle des services (SCPs) ne vous empêche de migrer le compte.
- Identifiez les politiques IAM et les politiques de contrôle des services (SCPs) existantes que vous devez répliquer dans l'organisation dans laquelle vous migrez le compte.
- Identifiez les politiques IAM existantes qui spécifient l'ID de votre organisation. Par exemple, `aws:PrincipalOrgID`.

Pour plus d'informations, consultez les sections Gestion des politiques IAM dans le Guide de l'utilisateur IAM et Politiques de contrôle des services () SCPs.

## Étape 2 : Vérifiez que vous avez supprimé les autorisations IAM qui permettent d'accéder à l'ancien compte de gestion

Étape 2

Assurez-vous d'avoir supprimé les autorisations IAM qui permettent d'accéder à l'ancien compte de gestion, telles que`OrganizationAccountAccessRole`.

Lorsque vous supprimez un compte membre d'une organisation, aucun rôle IAM créé pour permettre l'accès par le compte de gestion de l'organisation n'est pas automatiquement supprimé. Si vous souhaitez mettre fin à cet accès à partir du compte de gestion de l'ancienne organisation, vous devez supprimer manuellement le rôle IAM.

Pour plus d'informations sur la suppression d'un rôle, consultez Suppression de rôles ou de profils d'instance dans le Guide de l'utilisateur IAM.

## Étape 3 : Sauvegarder tous les rapports

Étape 3

Assurez-vous d'exporter ou de sauvegarder les rapports du compte de gestion, en particulier les rapports de facturation. Les rapports et l'historique au niveau de l'organisation ne sont pas stockés lorsque vous migrez un compte. Il est recommandé d'exporter l'intégralité de l'historique de facturation. Vous pouvez toujours accéder aux rapports relatifs au compte membre, tels que l'historique des AWS CloudTrail événements et l'historique de facturation du compte.

> **Important**
>
> Tous les rapports et historiques au niveau de l'organisation, tels que les informations de facturation de l'organisation figurant dans le compte de gestion, seront supprimés après le retrait d'un compte d'une organisation.

Pour plus d'informations, consultez les rapports sur les coûts et l'utilisation, les rapports Cost Explorer, les rapports Savings Plans et l'utilisation et la couverture des instances réservées (RI).

### Étape 4 : Vérifier les dépendances de l'organisation

Étape 4

Assurez-vous que le compte de migration ne comporte aucune dépendance liée à l'organisation.

Dépendances à vérifier :

- Si le compte est un administrateur délégué, vous devez annuler l'enregistrement des autorisations d'administrateur délégué avant de migrer le compte. Pour plus d'informations, consultez la section Services que vous pouvez utiliser avec AWS Organizations.
- S'il s'agit du compte de gestion, vous devez supprimer tous les comptes membres de l'organisation et supprimer l'organisation avant de procéder à la migration. Après avoir supprimé l'organisation, votre compte de gestion fonctionnera comme un compte autonome. Après la migration, le compte de gestion sera un compte membre de la nouvelle organisation. Pour plus d'informations, voir Supprimer une organisation.
- Si des autorisations IAM dépendent du compte, vous devrez ajuster les autorisations de l'ancienne organisation après avoir migré le compte vers la nouvelle organisation afin que l'ancienne organisation puisse fonctionner comme avant. Pour plus d'informations, consultez la section Gestion des autorisations d'accès pour votre organisation.
- Si vous utilisez des balises de compte ou d'unité organisationnelle (UO), vous devrez les recréer dans la nouvelle organisation.

### (Facultatif) Étape 5 : Consultez les instructions si vous utilisez AWS Control Tower

(Facultatif) Étape 5

Si vous migrez un compte vers ou depuis une organisation gérée par AWS Control Tower, consultez le guide AWS prescriptif suivant : Migrer un compte AWS membre de vers. AWS Organizations AWS Control Tower

## Ce que vous devez faire pour migrer un compte

Le processus de migration exige que la nouvelle organisation envoie une invitation au compte de migration, et que le compte de migration accepte l'invitation de la nouvelle organisation à rejoindre la nouvelle organisation.

Pour migrer un compte

1. Envoyez une invitation depuis le compte de gestion de la nouvelle organisation vers le compte de migration. Pour plus d'informations sur l'invitation de comptes, voir Inviter un Compte AWS utilisateur à rejoindre votre organisation.
2. Acceptez l'invitation à rejoindre la nouvelle organisation. Pour plus d'informations, voir Accepter une invitation d'une organisation. Les comptes migrés d'une autre organisation à une autre seront automatiquement ajoutés à la racine de la nouvelle organisation. Avant de déplacer un compte vers une unité organisationnelle (UO) de la nouvelle organisation, il est recommandé de vérifier que le compte migrateur dispose des politiques d'organisation et des autorisations d'unité d'organisation appropriées.
3. Si vous souhaitez migrer le compte de gestion, vous devez supprimer tous les comptes membres de l'organisation et supprimer l'organisation avant de migrer le compte de gestion vers la nouvelle organisation. Après avoir supprimé l'ancienne organisation, votre compte de gestion fonctionnera comme un compte autonome et pourra accepter l'invitation de la nouvelle organisation à rejoindre la nouvelle organisation. Si vous acceptez l'invitation, le compte de gestion sera un compte membre de la nouvelle organisation.

## Ce que vous devez faire après avoir migré un compte

Après avoir migré votre compte d'une organisation à une autre, assurez-vous d'avoir effectué les étapes suivantes.

Examen après la migration

1. Évaluez toutes les configurations de l'outil de facturation pour le compte migré, telles que les catégories de coûts, les budgets et les alarmes de facturation.
2. Consultez et mettez à jour les informations monétaires suivantes pour tous les comptes que vous avez migrés d'une organisation à une autre :
   a. Si nécessaire, mettez à jour les paramètres fiscaux du compte.
   b. Assurez-vous que le Support plan de migration du compte correspond au compte payeur de la nouvelle organisation.
   c. Passez en revue les éventuelles exonérations fiscales que vous souhaiteriez appliquer au compte que vous avez migré.

3. Validez et confirmez les politiques IAM et les politiques de contrôle des services (SCPs) existantes pour le compte migré. Par exemple, vous devrez peut-être mettre à jour l'ID de l'organisation pour certaines politiques IAM afin de refléter la nouvelle organisation.
4. Mettez à jour les balises de répartition des coûts pour la nouvelle organisation dans laquelle vous avez migré le compte. Vous devrez mettre à jour toutes les anciennes balises de répartition des coûts collectées par compte que vous avez migré.
5. Toutes les instances réservées et les plans d'épargne seront migrés en même temps que le compte. Ils ne sont pas conservés dans l'ancienne organisation. Contactez-nous Support si ceux-ci doivent être transférés à l'ancienne organisation.

# Afficher les détails d'un compte dans AWS Organizations

Lorsque vous vous connectez au compte de gestion de l'organisation dans la AWS Organizations console, vous pouvez consulter les informations relatives à vos comptes de membres.

> **Autorisations minimales**
>
> Pour consulter les détails d'un Compte AWS, vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
> - `organizations:ListAccounts` — requis uniquement si vous utilisez la console Organizations

AWS Management Console

Pour afficher les détails d'un Compte AWS

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez à la page Comptes AWS et choisissez le nom du compte (pas la case d'option) que vous souhaitez examiner. Si le compte que vous souhaitez est un

enfant d'une unité d'organisation, vous devrez peut-être choisir l'icône en triangle

à côté d'une unité d'organisation pour la développer et voir ses enfants. Répétez jusqu'à trouver le compte.

La zone Détails du compte affiche les informations relatives au compte.

### AWS CLI & AWS SDKs

Pour afficher les détails d'un Compte AWS

Vous pouvez utiliser les commandes suivantes pour afficher les détails d'un compte :

- AWS CLI:
  - liste-accounts : répertorie les détails de tous les comptes de l'organisation
  - describe-account : répertorie uniquement les détails du compte spécifié

  Les deux commandes renvoient les mêmes détails pour chaque compte inclus dans la réponse.

  L'exemple suivant montre comment extraire les détails d'un compte spécifié.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00",
        "Paths": [
            "o-aa111bb222/r-a1b2/123456789012/"
        ]
    }
}
```

- AWS SDKs:
  - ListAccounts

- DescribeAccount

# Exporter les détails de tous les comptes dans AWS Organizations

Avec AWS Organizations, les utilisateurs du compte de gestion et les administrateurs délégués d'une organisation peuvent exporter un fichier .csv contenant tous les détails du compte au sein d'une organisation. Par conséquent, les administrateurs de l'organisation peuvent facilement consulter les comptes et filtrer par état : `PENDING_ACTIVATION`ACTIVE,SUSPENDED,`PENDING_CLOSURE`, ou`CLOSED`. S'il existe de nombreux comptes dans votre organisation, l'option de téléchargement de fichier .csv permet d'afficher et de trier facilement les détails des comptes dans une feuille de calcul. Nous vous recommandons de générer de nouvelles exportations CSV plutôt que d'utiliser des versions précédemment enregistrées pour conserver les informations du compte courant.

> **Important**
>
> Nous avons retiré le `Status` paramètre de compte de l'`Accounts`objet de la AWS Organizations console le 9 septembre 2025. Le fichier d'exportation du compte affiche désormais le `State` paramètre au lieu du `Status` paramètre. Tous les processus en aval utilisant le fichier exporté `Organization_accounts_information.csv` doivent être mis à jour pour utiliser le `State` paramètre au lieu de`Status`.

> **Note**
>
> Seuls les principaux du compte de gestion peuvent télécharger la liste des comptes.

## Exportez une liste de tous les Comptes AWS membres de votre organisation

Lorsque vous vous connectez au compte de gestion de l'organisation, vous pouvez obtenir une liste de tous les comptes faisant partie de votre organisation sous forme de fichier .csv. Cette liste contient les détails des différents comptes. Toutefois, elle n'indique pas à quelle unité organisationnelle (UO) un compte appartient.

Voici les informations figurant dans le fichier .csv pour chaque compte :

- Account ID (ID de compte) – Identifiant de compte numérique. Par exemple : 123456789012
- ARN – Amazon Resource Name du compte. Par exemple : `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- Email (Adresse e-mail) – Adresse e-mail associée au compte. Par exemple : marymajor@exemple.com
- Name (Nom) – Nom de compte fourni par le créateur du compte. Par exemple : compte de test d'étape
- Status (Statut) – Statut du compte au sein de l'organisation. Les valeurs possibles sont `PENDING`, `ACTIVE` ou `SUSPENDED`.
- État - État du compte opérationnel au sein de l'organisation. La valeur peut être `PENDING_ACTIVATIONACTIVE`,`SUSPENDED`,`PENDING_CLOSURE`, ou`CLOSED`.
- Joined method (Méthode d'adhésion) – Indique comment le compte a été créé. Les valeurs possibles sont `INVITED` ou `CREATED`.
- Joined timestamp (Horodatage de l'adhésion) – Date et heure auxquelles le compte a rejoint l'organisation.

> **Autorisations minimales**
>
> Pour pouvoir exporter un fichier .csv contenant tous les comptes membres de l'organisation, vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

Pour exporter un fichier .csv pour tous les membres Comptes AWS de votre organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Choisissez Actions, et pour Compte AWS, choisissez Export account list (Exporter la liste des comptes). La bannière bleue en haut de la page indique « Export is in progress! » (L'exportation est en cours).

3. Lorsque le fichier est prêt, la bannière passe au vert et indique : « Download is ready » (Le téléchargement est prêt). Choisissez Télécharger le rapport CSV. Le dossier `Organization_accounts_information.csv` est téléchargé sur votre appareil.

AWS CLI & AWS SDKs

La seule façon d'exporter le fichier .csv avec les détails des comptes est d'utiliser la AWS Management Console. Vous ne pouvez pas exporter le fichier .csv de liste des comptes à partir d' AWS CLI.

# Surveillez l'état de votre Comptes AWS

AWS Organizations permet d'évaluer rapidement l'état de santé et le statut opérationnel de tous les comptes de votre organisation. Vous pouvez consulter ces informations à l'aide de la colonne État de la AWS Organizations console ou par programmation. AWS Organizations APIs Cela vous permet de suivre l'évolution de chacun Compte AWS dans son cycle de vie, de sa création à sa fermeture.

Le suivi continu de l'état du compte offre les avantages suivants :

- Identifiez rapidement les comptes qui nécessitent une attention ou une action
- Simplifiez les processus de gestion de votre compte
- Prenez des décisions éclairées concernant l'allocation des ressources et le contrôle d'accès
- Améliorez la sécurité globale et la conformité au sein de votre entreprise

Le tableau ci-dessous décrit les cinq états de compte possibles et leurs implications pour votre compte Comptes AWS :

États du compte

| State | Description |
| --- | --- |
| EN ATTENTE D'ACTIVATION | Dans cet état, le compte est inutilisable car le processus d'inscription au compte a été lancé mais n'a jamais été terminé. Le titulaire du compte doit effectuer les étapes d'inscription restantes, telles que la vérification par téléphone ou les informations de paiement. Une fois ces étapes terminées, le compte passe à l'état ACTIF. |

| State | Description |
| --- | --- |
| ACTIF | Cet état indique que le compte est pleinement opérationnel et disponible. Les utilisateurs peuvent accéder aux AWS services et aux ressources normaleme nt conformément aux autorisations du compte et aux politiques de l'organis ation. Des AWS activités régulières telles que le lancement de ressources, la gestion de services et le paiement de frais peuvent avoir lieu dans cet état. |
| INTERROMPU | Dans cet état, le compte est inutilisable car AWS son accès est restreint. Le titulaire du compte peut toujours consulter les informations de facturation et contacter Support, qui pourra expliquer pourquoi le compte est suspendu. |
| EN ATTENTE DE FERMETURE | Cet état temporaire indique une demande active de fermeture du compte, mais le processus de fermeture n'est pas encore terminé. Le compte reste fonctionnel et peut toujours être utilisé pour accéder aux AWS services pendant le traitement de la demande de fermeture. Après AWS avoir traité la demande de fermeture, le compte passe à l'état FERMÉ. |
| CLOSED | Cet état indique que le compte a été fermé à la demande du titulaire du compte ou par AWS et s'affiche à côté du nom du compte dans la AWS Organizations console pendant 90 jours après le début de la fermeture. Pendant cette période, vous ne pouvez pas accéder aux AWS services, mais vous pouvez nous contacter Support pour rétablir le compte ou récupérer des données importantes. À l'expiration du délai de 90 jours suivant la fermeture , le compte est définitivement fermé et ne sera plus affiché sur la console. AWS Organizations |

## Afficher l'état d'un Compte AWS

Vous pouvez consulter les informations sur l'état du compte à l'aide de la AWS Organizations console ou par programmation à l'aide des touches `DescribeAccount` `ListAccounts`, et. `ListAccountsForParent` APIs

> **Important**
>
> Le `Status` paramètre du compte AWS Organizations sera retiré le 9 septembre 2026. Bien que le compte `State` et les `Status` paramètres du

compte soient actuellement disponibles dans le AWS Organizations APIs (`DescribeAccount`,`ListAccounts`,`ListAccountsForParent`), nous vous recommandons de mettre à jour vos scripts ou tout autre code pour utiliser le `State` paramètre plutôt `Status` qu'avant le 9 septembre 2026.

### AWS Management Console

Pour afficher l'état d'un Compte AWS

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez à la Comptes AWSpage et notez la valeur dans la colonne État à côté du compte membre que vous souhaitez examiner. Si le compte que vous souhaitez voir est un enfant d'une unité d'organisation, vous devrez peut-être choisir l'icône en forme de triangle à

   côté d'une unité d'organisation pour l'agrandir et voir ses enfants. Répétez jusqu'à trouver le compte.

   > **Note**
   >
   > Vous pouvez également consulter la valeur du champ État sur la page des détails du compte de la AWS Organizations console.

### AWS CLI & AWS SDKs

Pour afficher l'état d'un Compte AWS

Vous pouvez utiliser les commandes suivantes pour consulter l'état d'un compte :

> **Note**
>
> Pour afficher les valeurs de l'état du compte dans les réponses de l'API, utilisez la AWS CLI version 2.29.0 ou ultérieure, ou une version du SDK publiée après le 9 septembre 2025. Nous vous recommandons d'utiliser la dernière version AWS CLI ou la version du SDK comme meilleure pratique. Pour plus d'informations, reportez-vous AWS SDKs à la

section « Cycle de vie des versions des outils » dans le guide de référence « AWS SDKs and Tools ».

- AWS CLI:
  - liste-accounts : répertorie les détails de tous les comptes de l'organisation
  - list-accounts-for-parent— répertorie les détails de tous les comptes de l'organisation contenus par la racine ou l'unité organisationnelle (UO) cible spécifiée
  - describe-account : répertorie uniquement les détails du compte spécifié

  Ces commandes renvoient les mêmes informations pour chaque compte inclus dans la réponse.

  L'exemple suivant montre comment récupérer les informations relatives à un compte spécifié, y compris sa `State` valeur.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "State": "CLOSED",
        "Status": "SUSPENDED",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00",
        "Paths": [
            "o-aa111bb222/r-a1b2/123456789012/"
        ]
    }
}
```

- AWS SDKs:
  - ListAccounts
  - ListAccountsForParent
  - DescribeAccount

# Mettre à jour les contacts alternatifs pour un compte dans AWS Organizations

Vous pouvez mettre à jour les contacts alternatifs pour les comptes de votre organisation à l'aide de la console AWS Organizations, ou par programmation à l'aide de la AWS CLI ou. AWS SDKs Pour savoir comment mettre à jour les contacts secondaires, voir Mettre à jour les contacts secondaires de n'importe quel membre de votre organisation Compte AWS dans le manuel de référence sur la gestion des AWS comptes.

# Mettre à jour les informations de contact principales d'un compte dans AWS Organizations

Vous pouvez mettre à jour les coordonnées principales des comptes de votre organisation à l'aide de la console AWS Organizations, ou par programmation à l'aide de la AWS CLI ou. AWS SDKs Pour savoir comment mettre à jour les informations du contact principal, voir Mettre à jour le contact principal de n'importe quel membre de votre organisation Compte AWS dans le manuel de référence sur la gestion des AWS comptes.

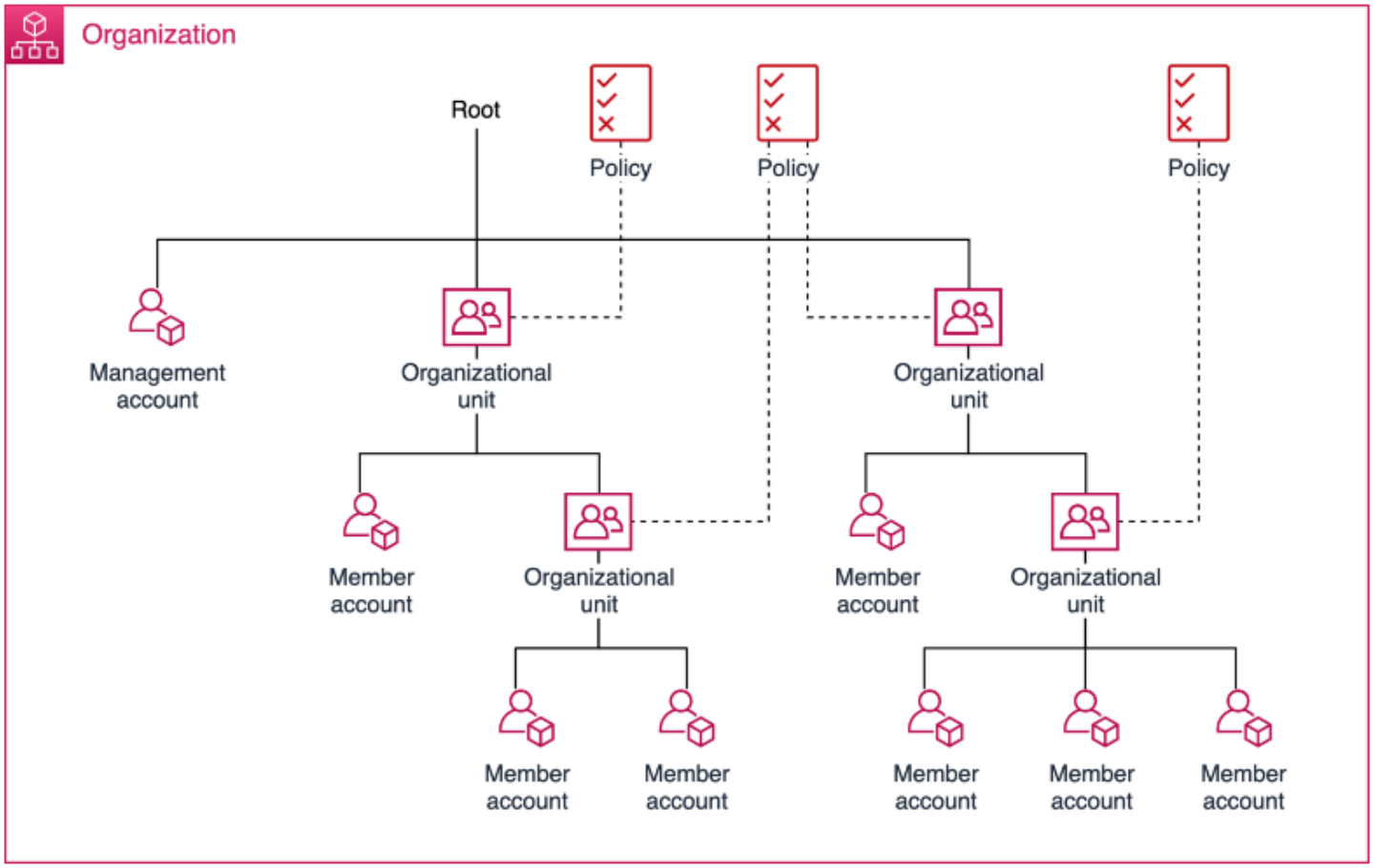
# Mise à jour Régions AWS pour un compte dans AWS Organizations

Vous pouvez activer la mise à jour Régions AWS pour les comptes de votre organisation à l'aide de la AWS Organizations console. Pour savoir comment activer la mise à jour Régions AWS, consultez la section Activer ou désactiver Régions AWS dans votre compte dans le manuel de référence sur la gestion des AWS comptes.

# Gestion des unités organisationnelles (OUs) avec AWS Organizations

Vous pouvez utiliser les unités organisationnelles (OUs) pour regrouper les comptes afin de les administrer en tant qu'unité unique. Cela permet de simplifier considérablement la gestion de vos comptes. Par exemple, vous pouvez attacher un contrôle basé sur une stratégie à une unité d'organisation. Tous les comptes au sein de cette unité d'organisation hériteront ainsi automatiquement de la stratégie. Vous pouvez en créer plusieurs OUs au sein d'une même organisation, et vous pouvez en créer OUs au sein d'une autre OUs. Chaque unité d'organisation peut contenir plusieurs comptes et vous pouvez déplacer des comptes d'une unité à une autre. Toutefois, les noms des unités d'organisation doivent être uniques au sein d'une unité opérationnelle parent ou racine.

Le schéma suivant montre une organisation composée de sept comptes organisés en quatre OUs sous la racine. L'organisation dispose également de quelques politiques qui s'appliquent à OUs.



> **Note**
>
> Il existe une racine dans l'organisation, qui AWS Organizations crée pour vous lorsque vous configurez votre organisation pour la première fois.

Rubriques



# Bonnes pratiques pour la gestion des unités organisationnelles (OUs) avec AWS Organizations

Suivez ces recommandations pour vous aider à gérer un environnement multi-comptes à l' AWS Organizations aide des unités organisationnelles (OUs).

Rubriques

# Compréhension AWS Organizations

La base d'un AWS environnement multi-comptes bien conçu est AWS Organizations de vous permettre de gérer et de gouverner plusieurs comptes de manière centralisée. Une unité organisationnelle (UO) est un regroupement logique de comptes au sein d'une organisation. OUs vous permettent d'organiser vos comptes selon une hiérarchie et vous aident à appliquer des contrôles de gestion. Les politiques des organisations définissent les contrôles que vous pouvez appliquer à un groupe de Comptes AWS. Par exemple, une politique de contrôle des services (SCP) est une politique qui définit les Service AWS actions, telles que Amazon EC2 Run Instance, que les comptes de votre organisation peuvent effectuer.

Bien que vous puissiez commencer votre AWS parcours avec un seul compte, il est AWS recommandé de configurer plusieurs comptes à mesure que vos charges de travail augmentent en taille et en complexité. L'utilisation d'un environnement multi-comptes est une AWS bonne pratique qui peut offrir plusieurs avantages :

- Innovation rapide avec des exigences diverses : vous pouvez affecter des ressources Comptes AWS à différentes équipes, projets ou produits au sein de votre entreprise afin de garantir que chacune d'entre elles puisse innover rapidement tout en tenant compte de ses propres exigences en matière de sécurité.
- Facturation simplifiée : L'utilisation de plusieurs Comptes AWS modes de facturation peut simplifier la façon dont vous répartissez vos AWS coûts en vous aidant à identifier le produit ou la gamme de services AWS responsable d'une facturation.
- Contrôles de sécurité flexibles : vous pouvez en utiliser plusieurs Comptes AWS pour isoler les charges de travail ou les applications qui ont des exigences de sécurité spécifiques ou qui doivent respecter des directives strictes en matière de conformité, telles que HIPAA ou PCI.
- Adaptez-vous aux processus métier : vous pouvez Comptes AWS en organiser plusieurs de manière à refléter au mieux les divers besoins des processus métier de votre entreprise, qui ont des exigences opérationnelles, réglementaires et budgétaires différentes.

## Unité organisationnelle de base recommandée () OUs

Votre unité organisationnelle (OUs) doit être basée sur une fonction ou un ensemble de contrôles communs au lieu de refléter la structure hiérarchique de votre entreprise. AWS recommande de commencer en tenant compte de la sécurité et de l'infrastructure. La plupart des entreprises disposent d'équipes centralisées au service de l'ensemble de l'organisation pour répondre à ces

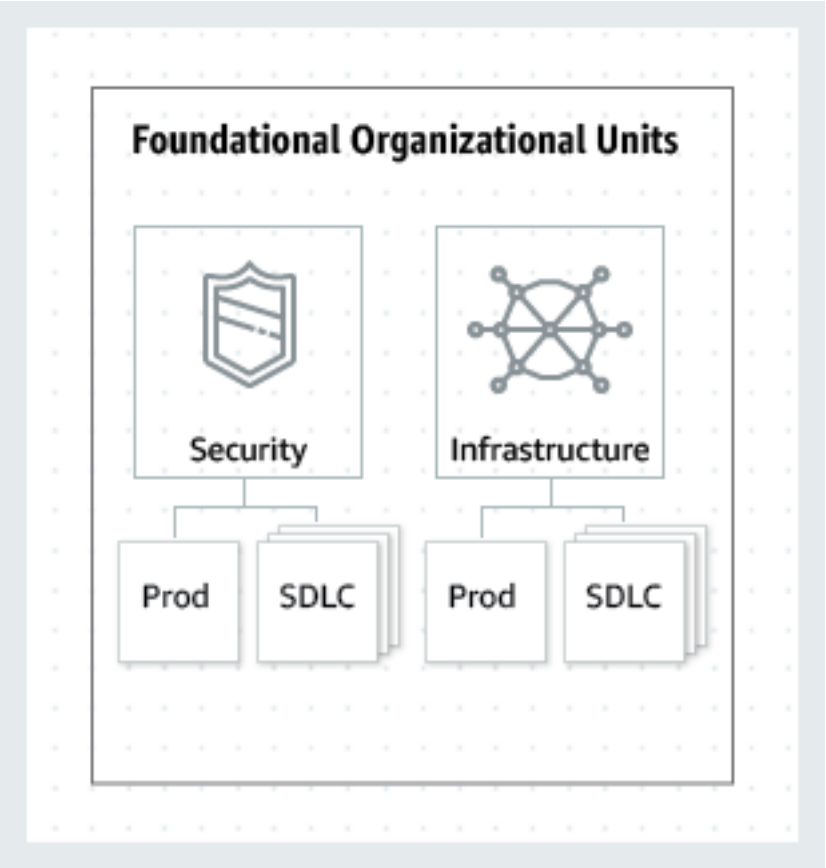
besoins. Nous vous recommandons de créer un ensemble de bases OUs pour ces fonctions spécifiques :

- Sécurité : utilisé pour les services de sécurité. Créez des comptes pour les archives de journaux, l'accès sécurisé en lecture seule, les outils de sécurité et Break-Glass.
- Infrastructure : utilisée pour les services d'infrastructure partagés tels que les réseaux et les services informatiques. Créez des comptes pour chaque type de service d'infrastructure dont vous avez besoin.

Étant donné que la plupart des entreprises ont des exigences politiques différentes en matière de charges de travail de production, l'infrastructure et la sécurité peuvent avoir été imbriquées OUs pour la non-production (SDLC) et pour la production (Prod). Les comptes de l'unité d'organisation SDLC hébergent des charges de travail non liées à la production et ne doivent pas avoir de dépendances de production par rapport à d'autres comptes. S'il existe des variations dans les politiques de l'UO entre les étapes du cycle de vie, le SDLC peut être divisé en plusieurs OUs (par exemple, développement et pré-production). Les comptes de l'unité d'organisation de production hébergent les charges de travail de production.

Appliquez des politiques au niveau de l'unité d'organisation pour régir l'environnement Prod et SDLC en fonction de vos besoins. En général, il est préférable d'appliquer des politiques au niveau de l'unité d'organisation plutôt qu'au niveau du compte individuel, car cela simplifie la gestion des politiques et les éventuels dépannages.

Le schéma suivant montre les bases OUs (Prod et SDLC) de la sécurité et de l'infrastructure :




## Unité organisationnelle supplémentaire recommandée (OUs)

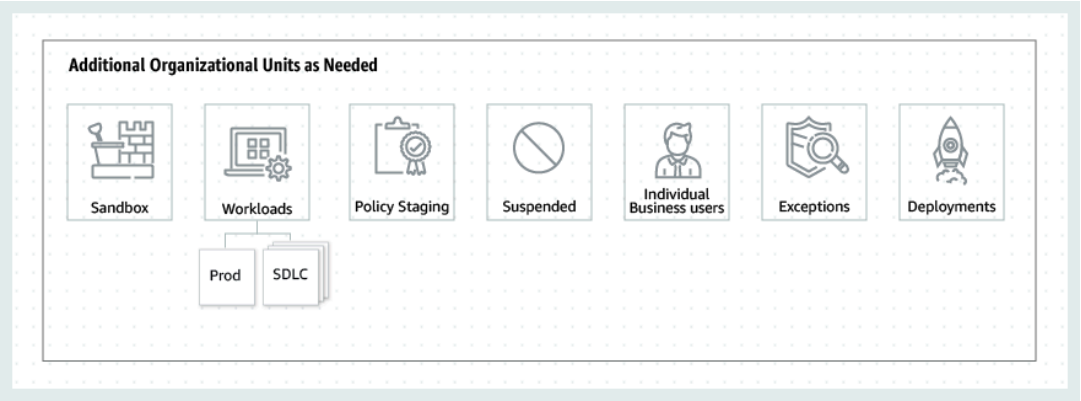
Une fois les services centraux en place, nous vous recommandons de créer des OUs services directement liés à la création ou à la gestion de vos produits ou services. De nombreux AWS clients construisent les éléments suivants OUs après avoir établi une base :

- Sandbox : contient des Comptes AWS espaces que les développeurs individuels peuvent utiliser pour expérimenter Services AWS. Assurez-vous que ces comptes peuvent être détachés des réseaux internes.
- Charges de travail : contient Comptes AWS les contenus qui hébergent vos services applicatifs externes. Vous devez vous structurer OUs selon les environnements SDLC et Prod (similaires à ceux de base OUs) afin d'isoler et de contrôler étroitement les charges de travail de production.

Nous vous recommandons également d'en ajouter d'autres OUs pour la maintenance et l'extension continue en fonction de vos besoins spécifiques. Voici quelques thèmes courants basés sur les pratiques des AWS clients existants :

- Établissement des politiques : détient AWS des comptes sur lesquels vous pouvez tester les modifications de politique proposées avant de les appliquer à grande échelle à l'organisation. Commencez par mettre en œuvre les modifications au niveau du compte dans l'unité d'organisation prévue, puis appliquez-les lentement aux autres comptes et au reste de l'organisation. OUs
- Suspendu : contient des contenus Comptes AWS qui ont été fermés et attendent d'être supprimés de l'organisation. Attachez un SCP à cette unité d'organisation qui refuse toutes les actions. Assurez-vous que les comptes sont étiquetés avec des informations à des fins de traçabilité s'ils doivent être restaurés.
- Utilisateurs professionnels individuels : unité d'organisation à accès limité destinée aux Comptes AWS utilisateurs professionnels (et non aux développeurs) susceptibles de devoir créer des applications liées à la productivité de l'entreprise, par exemple configurer un compartiment S3 pour partager des rapports ou des fichiers avec un partenaire.
- Exceptions : Comptes AWS blocages utilisés pour les cas d'utilisation professionnels comportant des exigences de sécurité ou d'audit hautement personnalisées, différentes de celles définies dans l'unité d'organisation Workloads. Par exemple, configurer une application ou une fonctionnalité Compte AWS spécifique pour une nouvelle application ou fonctionnalité confidentielle. SCPs Utilisez-le au niveau du compte pour répondre à des besoins personnalisés. Envisagez de configurer un système Detect and React à l'aide d'Amazon EventBridge et de AWS Config ses règles.
- Déploiements : contient des Comptes AWS informations destinées à une intégration continue et continue delivery/deployment (CI/CD deployments). You can create this OU if you have a different governance and operational model for CI/CD deployments as compared to accounts in the Workloads OUs (Prod and SDLC). Distribution of CI/CD helps reduce the organizational dependency on a shared CI/CD environment operated by a central team. For each set of SDLC/ Prod Comptes AWS pour une application dans l'unité d'organisation Workloads, créez un compte dans l'unité d'organisation des CI/CD déploiements).
- Transitionnel : il s'agit d'une zone de stockage temporaire pour les comptes et les charges de travail existants avant de les déplacer vers les zones standard de votre organisation. Cela peut être dû au fait que les comptes font partie d'une acquisition, étaient auparavant gérés par un tiers, ou à des comptes hérités d'une ancienne structure organisationnelle.

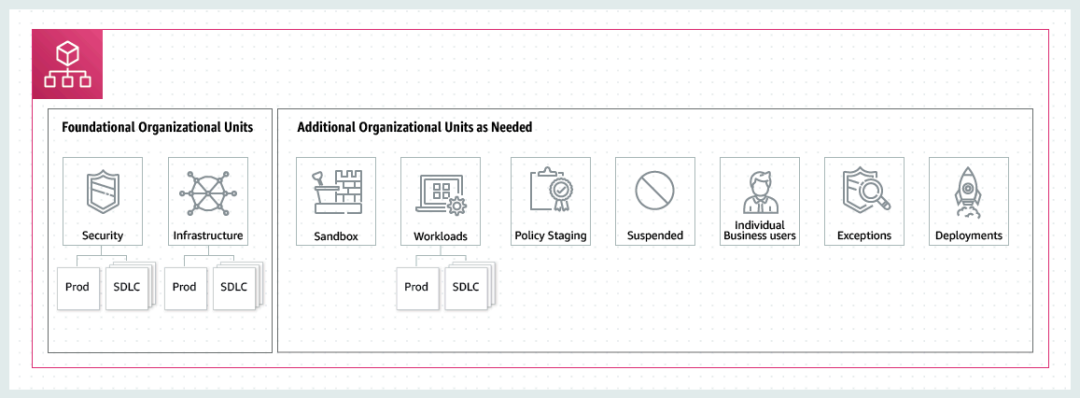
Le schéma suivant montre les informations supplémentaires OUs relatives au sandbox, aux charges de travail, à l'élaboration des politiques, aux utilisateurs professionnels suspendus, aux exceptions, aux déploiements et aux comptes de transition :




## Conclusion

Une stratégie multi-comptes bien conçue peut vous aider à innover AWS, tout en garantissant que vous répondez à vos besoins en matière de sécurité et d'évolutivité. Le cadre décrit dans cette rubrique représente les AWS meilleures pratiques que vous devez utiliser comme point de départ pour votre AWS voyage.

Le schéma suivant montre les éléments fondamentaux OUs et supplémentaires OUs recommandés :




# Naviguer dans la hiérarchie des racines et des unités organisationnelles (UO) avec AWS Organizations

Pour accéder à une version différente OUs ou à la racine lorsque vous déplacez des comptes ou que vous associez des politiques, vous pouvez utiliser la vue « arborescente » par défaut.

AWS Management Console

Pour naviguer dans l'organisation sous la forme d'une arborescence

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Comptes AWS, en haut de la section Organization (Organisation), sélectionnez le bouton bascule Hierarchy (Hiérarchie) (à la place de List (Liste)).
3. L'arborescence apparaît initialement avec la racine, affichant uniquement le premier niveau d'enfant OUs et de comptes. Pour développer l'arborescence et afficher des niveaux inférieurs, choisissez l'icône Développer ( en regard de n'importe quelle entité parente. Pour réduire l'encombrement et réduire une branche de l'arborescence, choisissez l'icône Réduire ( ) à côté d'une entité parente développée.
4. Choisissez le nom d'une unité d'organisation ou d'une racine pour en afficher les détails et effectuer certaines opérations. Sinon, vous pouvez choisir la case d'option en regard du nom et effectuer certaines opérations sur cette entité dans le menu Actions.

Vous pouvez également afficher la liste des seuls comptes de votre organisation sous forme de tableau, sans avoir à accéder d'abord à une unité d'organisation pour les trouver. Dans cette vue, vous ne pouvez ni voir OUs ni manipuler les politiques qui leur sont associées.

AWS Management Console

Pour afficher l'organisation sous la forme d'une liste non hiérarchique des comptes

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la Comptes AWSpage, en haut de la section Organisation, cliquez sur l'icône Afficher Comptes AWS uniquement pour l'activer. .
3. La liste des comptes s'affiche sans hiérarchie.

# Afficher les détails d'une unité organisationnelle (UO) avec AWS Organizations

Lorsque vous vous connectez au compte de gestion de l'organisation dans la AWS Organizations console, vous pouvez consulter les détails du compte de gestion OUs de votre organisation.

> **Autorisations minimales**
>
> Pour afficher les détails d'une unité d'organisation (UO), vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
> - `organizations:ListOrganizationsUnitsForParent` — requis uniquement si vous utilisez la console Organizations
> - `organizations:ListRoots` — requis uniquement si vous utilisez la console Organizations

AWS Management Console

Pour afficher les détails d'une unité d'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, choisissez le nom de l'unité d'organisation (pas sa case d'option) que vous souhaitez examiner. Si l'unité d'organisation est un enfant d'une autre unité d'organisation, choisissez l'icône en triangle à côté de son UO parente pour la développer et afficher les UO au niveau suivant de la hiérarchie. Répétez cette opération jusqu'à ce que vous trouviez l'unité d'organisation voulue.

   La zone Détails de l'unité d'organisation affiche les informations relatives à l'unité d'organisation.

AWS CLI & AWS SDKs

Pour afficher les détails d'une unité d'organisation

Vous pouvez utiliser l'une des commandes suivantes pour afficher les détails d'une unité d'organisation :

- AWS CLI, AWS SDKs:
  - list-roots
  - list-children
  - describe-organizational-unit

L'exemple suivant montre comment rechercher l'ID d'une unité d'organisation à l'aide de l' AWS CLI. Vous trouvez l'ID de l'UO en parcourant la hiérarchie en commençant par la commande `list-roots`, puis en exécutant `list-children` sur la racine et itérativement sur chacun de ses enfants jusqu'à ce que vous trouviez l'UO que vous voulez.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Une fois que vous avez l'ID de l'unité d'organisation, l'exemple suivant montre comment récupérer les détails de l'unité d'organisation.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps",
        "Path": "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/"
    }
}
```

- AWS SDKs:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

# Création d'une unité organisationnelle (UO) avec AWS Organizations

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez créer une unité d'organisation à la racine de votre organisation. OUs peut être imbriqué jusqu'à cinq niveaux de profondeur. Pour créer une unité d'organisation, procédez comme suit :

**Important**

Si cette organisation est gérée avec AWS Control Tower, créez la vôtre OUs avec la AWS Control Tower console ou APIs. Si vous créez l'UO dans Organizations, cette UO n'est pas enregistrée auprès de AWS Control Tower. Pour de plus amples informations, consultez Référence à des ressources en dehors de AWS Control Tower dans le Guide de l'utilisateur de AWS Control Tower .

**Autorisations minimales**

Pour créer une unité d'organisation au sein d'une racine de votre organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:CreateOrganizationalUnit`

## AWS Management Console

Pour créer une unité d'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez à la page Comptes AWS.

   La console affiche l'unité d'organisation racine et son contenu. La première fois que vous accédez à la racine, la console affiche l'ensemble de vos Comptes AWS dans cette vue de niveau supérieur. Si vous avez déjà créé des comptes OUs et y avez transféré des comptes, la console affiche uniquement les comptes de niveau supérieur OUs et les comptes que vous n'avez pas encore transférés dans une unité d'organisation.
3. (Facultatif) Si vous souhaitez créer une UO dans une UO existante, accédez à l'UO enfant en choisissant le nom (et non la case à cocher) de l'UO enfant, ou en choisissant le

   suivant OUs dans l'arborescence jusqu'à ce que vous voyiez celle que vous voulez, puis en choisissant son nom.
4. Lorsque vous avez sélectionné l'unité d'organisation parente correcte dans la hiérarchie, dans le menu Actions, sous Unité d'organisation, choisissez Créer
5. Dans la boîte de dialogue Créer une unité d'organisation, tapez le nom de l'unité d'organisation que vous voulez créer.
6. (Facultatif) Ajoutez une ou plusieurs balises en choisissant Ajouter une balise, puis entrez une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une UO.
7. Enfin, choisissez Créer une unité d'organisation.

Votre nouvelle unité d'organisation apparaît à l'intérieur de l'unité parente. Vous pouvez maintenant déplacer des comptes vers cette unité d'organisation ou lui attacher des stratégies.

## AWS CLI & AWS SDKs

Pour créer une UO

Les exemples de code suivants illustrent comment utiliser `CreateOrganizationalUnit`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };
```

```
            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
 {orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
 {response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateOrganizationalUnitàla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour créer une unité d'organisation dans une unité d'organisation racine ou parente

L'exemple suivant montre comment créer une unité d'organisation nommée AccountingOU :

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

La sortie inclut un objet organizationalUnit contenant des détails sur la nouvelle unité d'organisation :

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
```

```
                "Name": "AccountingOU"
        }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateOrganizationalUnitàla section Référence des AWS CLI commandes.

# Modification du nom d'une unité organisationnelle (UO) avec AWS Organizations

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez renommer une unité d'organisation. Pour ce faire, exécutez les étapes suivantes.

> **Autorisations minimales**
>
> Pour renommer une unité d'organisation au sein d'une racine dans votre organisation , vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
> - `organizations:UpdateOrganizationalUnit`

AWS Management Console

Pour renommer une unité d'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Comptes AWS, accédez à l'unité d'organisation (UO) que vous souhaitez renommer, puis effectuez l'une des étapes suivantes :

   - Cochez la case d'option

     en regard de l'unité d'organisation à renommer. Ensuite, dans le menu Actions, sous Unité d'organisation, choisissez Renommer.

- Choisissez le nom de l'unité d'organisation pour accéder à sa page de détails. En haut de la page, choisissez Renommer.

3. Dans la boîte de dialogue Renommer l'unité d'organisation, entrez un nouveau nom, puis choisissez Enregistrer les modifications.

AWS CLI & AWS SDKs

Pour renommer une unité d'organisation

Vous pouvez utiliser l'une des commandes suivantes pour renommer une unité d'organisation :

- AWS CLI: update-organizational-unit

  L'exemple suivant montre comment renommer une unité d'organisation.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU",
        "Path": "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
    }
}
```

- AWS SDKs: UpdateOrganizationalUnit

# Marquer une unité organisationnelle (UO) avec AWS Organizations

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les étiquettes attachées à une UO. Pour ce faire, exécutez les étapes suivantes.

> **Autorisations minimales**
>
> Pour modifier les balises attachées à une unité d'organisation au sein d'une racine dans votre organisation , vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:DescribeOrganizationalUnit` — requis uniquement si vous utilisez la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Pour modifier les balises attachées à une unité d'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Comptes AWS, accédez au nom de l'UO dont vous souhaitez modifier les étiquettes et choisissez ce nom.
3. Sur la page de détails de l'UO, choisissez l'onglet Tags (Étiquettes), puis Manage tags (Gérer les étiquettes).
4. Vous pouvez effectuer l'une des actions suivantes dans cet onglet :
   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé de la balise. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Supprimez une balise existante en choisissant Supprimer en regard de la balise à supprimer.
   - Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.
5. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

AWS CLI & AWS SDKs

Pour modifier les balises attachées à une unité d'organisation

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises attachées à une unité d'organisation :

- AWS CLI : tag-resource et untag-resource

  L'exemple suivant attache la balise `"Department"="12345"` à une unité d'organisation. Notez que les champs `Key` et `Value` sont sensibles à la casse.

  ```
  $ aws organizations tag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tags Key=Department,Value=12345
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

  L'exemple suivant supprime la balise `Department` d'une unité d'organisation.

  ```
  $ aws organizations untag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tag-keys Department
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS SDKs : TagResource et UntagResource

# Déplacement de comptes vers une unité organisationnelle (UO) ou entre la racine et OUs avec AWS Organizations

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez déplacer des comptes de votre organisation depuis la racine vers une unité d'organisation, entre des unités d'organisation et vers la racine depuis une unité d'organisation. Le fait de placer un compte dans une unité d'organisation le soumet à toutes les politiques associées à l'unité d'organisation parent et OUs à celles de la chaîne parent jusqu'à la racine. Si un compte n'est pas placé dans une unité d'organisation, il n'est soumis qu'aux politiques attachées directement à la racine et à celles attachées directement au compte. Pour déplacer des comptes, effectuez les opérations suivantes.

Autorisations minimales

Pour déplacer des comptes vers un nouvel emplacement dans la hiérarchie des unités d'organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:MoveAccount`

AWS Management Console

Pour déplacer des comptes vers une unité d'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, trouvez le ou les comptes à déplacer. Vous pouvez naviguer dans la hiérarchie des UO ou activer Afficher uniquement les Comptes AWS pour afficher une liste non hiérarchique des comptes sans la structure des unités d'organisation. Si vous disposez de nombreux comptes, vous devrez peut-être choisir Charger plus de comptes dans « nom-UO » au bas de la liste pour trouver tous ceux que vous souhaitez déplacer.
3. Cochez
   ☑
   en regard du nom de chaque compte à déplacer.
4. Dans le menu Actions, sous Compte AWS, choisissez Déplacer.
5. Dans la boîte de dialogue Déplacer des Compte AWS, trouvez et choisissez l'unité d'organisation ou la racine vers laquelle vous voulez déplacer le compte, puis choisissez Déplacer le Compte AWS.

AWS CLI & AWS SDKs

Pour déplacer des comptes vers une unité d'organisation

Vous pouvez utiliser l'une des commandes suivantes pour déplacer un compte :

- AWS CLI : move-account

L'exemple suivant déplace un Compte AWS de la racine vers une UO. Notez que vous devez spécifier IDs les conteneurs source et de destination.

```
$ aws organizations move-account \
    --account-id 111122223333 \
    --source-parent-id r-a1b2 \
    --destination-parent-id ou-a1b2-f6g7h111
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS SDKs: MoveAccount

## Afficher les détails de la racine avec AWS Organizations

Lorsque vous vous connectez au compte de gestion de l'organisation dans la AWS Organizations console, vous pouvez consulter les détails de la racine administrative.

> **Autorisations minimales**
>
> Pour afficher les détails de la racine, vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization` (console uniquement)
> - `organizations:ListRoots`

La racine est le conteneur le plus haut de la hiérarchie des unités organisationnelles (OUs) et se comporte généralement comme une unité d'organisation. Cependant, en tant que conteneur situé tout en haut de la hiérarchie, les modifications apportées à la racine affectent toutes les autres unités d'organisation et tous Compte AWS les membres de l'organisation.

AWS Management Console

Pour afficher les détails de la racine

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

2. Accédez à la page Comptes AWS, puis choisissez l'UO Racine (son nom, pas la case d'option).
3. La page de détails Racine apparaît et affiche les détails de la racine.

AWS CLI & AWS SDKs

Pour afficher les détails de la racine

Vous pouvez utiliser l'une des commandes suivantes pour afficher les détails d'une racine :

- AWS CLI : list-roots

  L'exemple suivant montre comment extraire les détails de la racine, notamment les types de politiques actuellement activés dans l'organisation :

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS SDKs: ListRoots

# Supprimer une unité organisationnelle (UO) avec AWS Organizations

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez supprimer tout OUs ce dont vous n'avez plus besoin.

Vous devez d'abord déplacer tous les comptes hors de l'unité d'organisation et tout enfant OUs, puis supprimer l'enfant OUs.

> **Autorisations minimales**
>
> Pour supprimer une unité d'organisation, vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
> - `organizations:DeleteOrganizationalUnit`

## AWS Management Console

Pour supprimer une unité d'organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la Comptes AWSpage, recherchez celle OUs que vous souhaitez supprimer et cochez la case à

   ☑

   côté du nom de chaque unité d'organisation.
3. Choisissez Actions, puis, sous Unité d'organisation, choisissez Supprimer.
4. Pour confirmer que vous souhaitez supprimer le OUs, entrez le nom de l'unité d'organisation (si vous avez choisi de n'en supprimer qu'une) ou le mot « supprimer » (si vous en avez choisi plusieurs), puis choisissez Supprimer.

   AWS Organizations les supprime OUs et les retire de la liste.

## AWS CLI & AWS SDKs

Pour supprimer une unité d'organisation

Les exemples de code suivants illustrent comment utiliser `DeleteOrganizationalUnit`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-00000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };

        var response = await client.DeleteOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteOrganizationalUnità la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour supprimer une unité d'organisation

L'exemple suivant montre comment supprimer une unité d'organisation. L'exemple suppose que vous avez précédemment supprimé tous les comptes et autres comptes OUs de l'unité d'organisation :

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Pour plus de détails sur l'API, reportez-vous DeleteOrganizationalUnità la section Référence des AWS CLI commandes.

# Gérer les politiques de l'organisation avec AWS Organizations

Les politiques vous AWS Organizations permettent d'appliquer des types de gestion supplémentaires au Comptes AWS sein de votre organisation. Vous pouvez utiliser des politiques lorsque toutes les fonctions sont activées dans votre organisation.

La AWS Organizations console affiche le statut activé ou désactivé pour chaque type de politique. Sous l'onglet Organiser les comptes, choisissez la racine (`Root`) dans le panneau de navigation de gauche. Le panneau de détails à droite de l'écran affiche tous les types de politiques disponibles. La liste indique ceux qui sont activés et ceux qui sont désactivés dans cette racine d'organisation. Si l'option Activer est présente pour un type, ce type est actuellement désactivé. Si l'option Désactiver est présente pour un type, ce type est actuellement activé.

Rubriques



## Types de politiques

Organizations propose des types de politiques dans les deux grandes catégories suivantes :

## Politiques d'autorisation

Les politiques d'autorisation vous aident à gérer de manière centralisée la sécurité Comptes AWS au sein d'une organisation.

- Les politiques de contrôle des services (SCPs) permettent de contrôler de manière centralisée les autorisations maximales disponibles pour les utilisateurs IAM et les rôles IAM dans une organisation.
- Les politiques de contrôle des ressources (RCPs) permettent de contrôler de manière centralisée les autorisations maximales disponibles pour les ressources d'une organisation.

## Politiques de gestion

Les politiques de gestion vous aident à configurer et à gérer Services AWS de manière centralisée leurs fonctionnalités au sein d'une organisation.

- Les politiques déclaratives vous permettent de déclarer et d'appliquer de manière centralisée les configurations souhaitées pour une donnée Service AWS à grande échelle au sein d'une organisation. Une fois connectée, la configuration est toujours maintenue lorsque le service ajoute de nouvelles fonctionnalités ou APIs.
- Les politiques de sauvegarde vous permettent de gérer et d'appliquer de manière centralisée des plans de sauvegarde aux AWS ressources des comptes d'une organisation.
- Les politiques relatives aux balises vous permettent de standardiser les balises associées aux AWS ressources dans les comptes d'une organisation.
- Les politiques relatives aux applications de chat vous permettent de contrôler l'accès aux comptes d'une organisation à partir d'applications de chat telles que Slack et Microsoft Teams.
- Les politiques de désabonnement aux services d'IA vous permettent de contrôler la collecte de données pour les services d' AWS IA pour tous les comptes d'une organisation.
- Les politiques du Security Hub vous permettent de combler les lacunes en matière de couverture de sécurité conformément aux exigences de sécurité de votre entreprise et de les appliquer de manière centralisée à l'ensemble de l'organisation.
- Les politiques Amazon Inspector vous permettent d'activer et de gérer Amazon Inspector de manière centralisée pour tous les comptes de votre AWS organisation.

- Les politiques d'Amazon Bedrock vous permettent d'appliquer automatiquement les mesures de protection configurées dans Amazon Bedrock Guardrails à tous les éléments de la structure de votre organisation pour tous les appels d'inférence de modèles adressés à Amazon Bedrock.
- Les politiques de déploiement des mises à niveau vous permettent de gérer de manière centralisée et d'échelonner les mises à niveau automatiques sur plusieurs AWS ressources et comptes de votre organisation.
- Les politiques Amazon S3 vous permettent de gérer de manière centralisée les configurations des ressources Amazon S3 à grande échelle sur l'ensemble des comptes d'une organisation.

Le tableau suivant résume certaines des caractéristiques de chaque type de politique. Pour des caractéristiques supplémentaires concernant ces types de politiques, consultez la rubrique Quotas et limites de service pour AWS Organizations.

| Type de politique | Catégorie de politique | Concerne le compte de gestion | Nombre maximal que vous pouvez attacher à une racine, une UO ou un compte | Taille maximum | Prend en charge l'affichage de la politique effective de l'unité d'organisation |
|---|---|---|---|---|---|
| SCP | Autorisation | ⊗ Non | 5 | 5 120 octets | ⊗ Non |
| RCP | Autorisation | ⊗ Non | 5 | 5 120 octets | ⊗ Non |
| Politique déclarative | Gestion | ⊘ Oui | 10 | 10 000 caractèr s | ⊘ Oui |
| Politique de sauvegarde | Gestion | ⊘ Oui | 10 | 10 000 caractèr s | ⊘ Oui |
| Politique de balises | Gestion | ⊘ Oui | 10 | 10 000 caractèr s | ⊘ Oui |
| Politique relative aux | Gestion | ⊘ Oui | 5 | 10 000 caractèr s | ⊘ Oui |

| Type de politique | Catégorie de politique | Concerne le compte de gestion | Nombre maximal que vous pouvez attacher à une racine, une UO ou un compte | Taille maximum | Prend en charge l'affichage de la politique effective de l'unité d'organisation |
|---|---|---|---|---|---|
| applications de chat | | | | | |
| Politique de désactivation des services IA | Gestion | ✓ Oui | 5 | 2 500 caractères | ✓ Oui |
| Politique du Security Hub | Gestion | ✓ Oui | 10 | 10 000 caractères | ✓ Oui |
| Politique d'Amazon Inspector | Gestion | ✓ Oui | 10 | 10 000 caractères | ✓ Oui |
| Politique d'Amazon Bedrock | Gestion | ✓ Oui | 10 | 10 000 caractères | ✓ Oui |
| Politique de déploiement des mises à niveau | Gestion | ✓ Oui | 10 | 10 000 caractères | ✓ Oui |
| Politique S3 | Gestion | ✓ Oui | 10 | 10 000 caractères | ✓ Oui |

# Politiques d'autorisation dans AWS Organizations

Les politiques d'autorisation vous AWS Organizations permettent de configurer et de gérer de manière centralisée l'accès des principaux et des ressources dans vos comptes membres. La manière dont ces politiques affectent les unités organisationnelles (OUs) et les comptes auxquels vous les appliquez dépend du type de politique d'autorisation que vous appliquez.

Il existe deux types de politiques d'autorisation AWS Organizations : les politiques de contrôle des services (SCPs) et les politiques de contrôle des ressources (RCPs).

Rubriques



## Différences entre SCPs et RCPs

SCPs sont des commandes centrées sur le principal. SCPs créez un garde-fou en matière d'autorisations, ou fixez des limites, aux autorisations maximales accordées aux principaux sur vos comptes de membres. Vous pouvez utiliser un SCP lorsque vous souhaitez appliquer de manière centralisée des contrôles d'accès cohérents aux principaux de votre organisation. Cela peut inclure la spécification des services auxquels vos utilisateurs et rôles IAM peuvent accéder, des ressources auxquelles ils peuvent accéder ou des conditions dans lesquelles ils peuvent faire des demandes (par exemple, depuis des régions ou des réseaux spécifiques).

RCPs sont des contrôles centrés sur les ressources. RCPs créez un garde-fou en matière d'autorisations, ou fixez des limites, aux autorisations maximales disponibles pour les ressources de vos comptes membres. Vous pouvez utiliser un RCP lorsque vous souhaitez appliquer de manière centralisée des contrôles d'accès cohérents à l'ensemble des ressources de votre organisation. Cela peut restreindre l'accès à vos ressources afin que seules les identités appartenant à votre organisation puissent y accéder, ou spécifier les conditions dans lesquelles des identités externes à votre organisation peuvent accéder à vos ressources.

Certaines commandes peuvent être appliquées de la même manière via SCPs et RCPs. Par exemple, vous souhaiterez peut-être empêcher vos utilisateurs de télécharger des objets non chiffrés

sur S3, qui peuvent être écrits sous forme de SCP afin de contrôler les actions que vos principaux responsables peuvent effectuer sur vos compartiments S3. Ce contrôle peut également être écrit sous forme de RCP pour exiger le chiffrement chaque fois qu'un principal télécharge des objets dans votre compartiment S3. La deuxième option peut être préférée si votre compartiment permet à des entités extérieures à votre organisation, telles que des fournisseurs tiers, de télécharger des objets dans votre compartiment S3. Cependant, certains contrôles ne peuvent être implémentés que dans un RCP, et certains contrôles ne peuvent être implémentés que dans un SCP. Pour de plus amples informations, veuillez consulter Cas d'utilisation généraux pour SCPs et RCPs.

## Utilisation SCPs et RCPs

SCPs et RCPs sont des commandes indépendantes. Vous pouvez choisir d'activer uniquement SCPs ou RCPs d'utiliser les deux types de politique ensemble. En utilisant les deux SCPs et RCPs, vous pouvez créer un périmètre de données autour de vos identités et de vos ressources.

SCPs offrent la possibilité de contrôler les ressources auxquelles vos identités peuvent accéder. Par exemple, vous pouvez autoriser vos identités à accéder aux ressources de votre AWS organisation. Toutefois, vous souhaiterez peut-être empêcher vos identités d'accéder à des ressources extérieures à votre organisation. Vous pouvez appliquer ce contrôle à l'aide de SCPs.

RCPs offrez la possibilité de contrôler quelles identités peuvent accéder à vos ressources. Par exemple, vous souhaiterez peut-être autoriser les identités de votre organisation à accéder aux ressources de votre organisation. Toutefois, vous souhaiterez peut-être empêcher les identités extérieures à votre organisation d'accéder à vos ressources. Vous pouvez appliquer ce contrôle à l'aide de RCPs. RCPs fournir la possibilité d'influencer les autorisations effectives pour les principaux externes à votre organisation qui accèdent à vos ressources. SCPs ne peut avoir d'impact que sur les autorisations effectives accordées aux directeurs au sein de votre AWS organisation.

### Cas d'utilisation généraux pour SCPs et RCPs

Le tableau suivant détaille les cas d'utilisation généraux d'un SCP et RCPs

| | | Répercussions | | | |
|---|---|---|---|---|---|
| Cas d'utilisation | Type de politique | Vos identités | Identités externes | Vos ressources | Ressources externes (cible de la demande) |

| | | Répercussions | | | |
|---|---|---|---|---|---|
| Limitez les services ou les actions que vos identités peuvent utiliser | SCP | X | | X | X |
| Limitez les ressources auxquelles vos identités peuvent accéder | SCP | X | | X | X |
| Appliquez les exigences relatives à la manière dont vos identités peuvent accéder aux ressources | SCP | X | | X | X |
| Limitez les identités autorisées à accéder à vos ressources | RCP | X | X | X | |
| Protégez les ressources sensibles de votre organisation | RCP | X | X | X | |

| | | Répercussions | | |
|---|---|---|---|---|
| Appliquez les exigences relatives à l'accès à vos ressources | RCP | X | X | X |

## Politiques de contrôle des services (SCPs)

Les politiques de contrôle des services (SCPs) sont un type de politique d'organisation que vous pouvez utiliser pour gérer les autorisations au sein de votre organisation. SCPs offrent un contrôle centralisé des autorisations maximales disponibles pour les utilisateurs IAM et les rôles IAM au sein de votre organisation. SCPs vous aider à garantir que vos comptes respectent les directives de contrôle d'accès de votre organisation. SCPsne sont disponibles que dans une organisation dont toutes les fonctionnalités sont activées. SCPs ne sont pas disponibles si votre organisation a activé uniquement les fonctionnalités de facturation consolidée. Pour obtenir des instructions sur l'activation SCPs, consultezDésactivation d'un type de politique.

SCPs n'accordez pas d'autorisations aux utilisateurs IAM et aux rôles IAM au sein de votre organisation. Aucune autorisation n'est accordée par une SCP. Un SCP définit une barrière d'autorisation, ou fixe des limites, aux actions que les utilisateurs IAM et les rôles IAM de votre organisation peuvent effectuer. Pour accorder des autorisations, l'administrateur doit associer des politiques pour contrôler l'accès, telles que des politiques basées sur l'identité associées aux utilisateurs IAM et aux rôles IAM, et des politiques basées sur les ressources associées aux ressources de vos comptes. Pour plus d'informations, consultez les sections Politiques basées sur l'identité et politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Les autorisations effectives sont l'intersection logique entre ce qui est autorisé par le SCP et les politiques de contrôle des ressources (RCPs) et ce qui est autorisé par les politiques basées sur l'identité et les ressources.

> ⚠ SCPs n'affectent pas les utilisateurs ou les rôles dans le compte de gestion
>
> SCPs n'affectent pas les utilisateurs ni les rôles dans le compte de gestion. Elles affectent uniquement les comptes membres de votre organisation. Cela signifie également que cela SCPs s'applique aux comptes de membres désignés comme administrateurs délégués.

Rubriques dans cette page



## Tester les effets de SCPs

AWS vous recommande vivement de ne pas vous attacher SCPs à la racine de votre organisation sans avoir testé de manière approfondie l'impact de la politique sur les comptes. À la place, créez une unité d'organisation dans laquelle vous pouvez déplacer vos comptes un par un, ou au moins en petits nombres, afin de veiller à ne pas accidentellement empêcher des utilisateurs d'accéder à des services clés. Pour déterminer si un service est utilisé par un compte, vous pouvez examiner les Dernières informations consultées relatives aux services dans IAM. Une autre méthode consiste AWS CloudTrail à enregistrer l'utilisation du service au niveau de l'API.

> **Note**
>
> Vous ne devez pas supprimer la AWSAccess politique complète à moins de la modifier ou de la remplacer par une politique distincte avec des actions autorisées, sinon toutes les AWS actions des comptes membres échoueront.

## Taille maximale de SCPs

Tous les caractères de votre SCP sont pris en compte dans le calcul de sa taille maximale. Les exemples de ce guide montrent les SCPs formats avec des espaces blancs supplémentaires pour améliorer leur lisibilité. Toutefois, pour économiser de l'espace si la taille de votre politique approche

de la taille maximale, vous pouvez supprimer les espaces, comme les espacements et les sauts de ligne qui ne figurent pas entre guillemets.

> **Tip**
>
> Utilisez l'éditeur visuel pour créer votre politique de contrôle des services. Il supprime automatiquement les espaces superflus.

## SCPs Attachement aux différents niveaux de l'organisation

Pour une explication détaillée du SCPs fonctionnement, voirÉvaluation du SCP.

## Effets des SCP sur les autorisations

SCPs sont similaires aux politiques Gestion des identités et des accès AWS d'autorisation et utilisent presque la même syntaxe. Toutefois, une politique de contrôle des services n'accorde jamais d'autorisations. SCPs Il s'agit plutôt de contrôles d'accès qui spécifient les autorisations maximales disponibles pour les utilisateurs IAM et les rôles IAM au sein de votre organisation. Pour de plus amples informations, consultez Logique d'évaluation des politiques dans le Guide de l'utilisateur IAM.

- SCPs concernent uniquement les utilisateurs et les rôles IAM gérés par des comptes faisant partie de l'organisation. SCPs n'affectent pas directement les politiques basées sur les ressources. Elles n'affectent pas les utilisateurs ni les rôles de comptes extérieurs à l'organisation. Par exemple, considérons un compartiment Amazon S3 détenu par le compte A d'une organisation. La politique du compartiment (politique basée sur une ressource) accorde l'accès aux utilisateurs du compte B qui est extérieur à l'organisation. Une politique SCP est attachée au compte A. Cette politique de contrôle des services ne s'applique pas aux utilisateurs externes du compte B. La politique de contrôle des services s'applique uniquement aux utilisateurs gérés par le compte A dans l'organisation.
- Une SCP limite les autorisations des utilisateurs et des rôles IAM dans les comptes membres, y compris l'utilisateur racine du compte membre. Chaque compte ne dispose que des autorisations octroyées par chaque parent au-dessus de lui. Si une autorisation est bloquée à n'importe quel niveau au-dessus du compte, implicitement (en n'étant pas incluse dans une instruction de politique `Allow`) ou explicitement (en étant incluse dans une instruction de politique `Deny`), un utilisateur ou un rôle figurant dans le compte concerné ne peut pas utiliser cette autorisation, même si l'administrateur du compte attache à l'utilisateur la politique IAM `AdministratorAccess` avec des autorisations */*.

- SCPs concernent uniquement les comptes des membres de l'organisation. Elles n'ont aucun effet sur les utilisateurs ou les rôles du compte de gestion. Cela signifie également que cela SCPs s'applique aux comptes de membres désignés comme administrateurs délégués. Pour de plus amples informations, veuillez consulter Bonnes pratiques relatives au compte de gestion.
- Les utilisateurs et les rôles doivent toujours se voir attribuer des autorisations avec les politiques d'autorisation IAM appropriées. Un utilisateur ne disposant d'aucune politique d'autorisation IAM n'a aucun accès, même si les règles applicables SCPs autorisent tous les services et toutes les actions.
- Si un utilisateur ou un rôle dispose d'une politique d'autorisation IAM qui accorde l'accès à une action également autorisée par l'autorité applicable SCPs, l'utilisateur ou le rôle peut effectuer cette action.
- Si un utilisateur ou un rôle dispose d'une politique d'autorisation IAM qui accorde l'accès à une action non autorisée ou explicitement refusée par l'autorité applicable SCPs, l'utilisateur ou le rôle ne peut pas effectuer cette action.
- SCPs affectent tous les utilisateurs et rôles des comptes attachés, y compris l'utilisateur root. Les seules exceptions sont celles décrites dans Tâches et entités non limitées par SCPs.
- SCPs n'affectent aucun rôle lié à un service. Les rôles liés aux services permettent Services AWS aux autres de s'intégrer AWS Organizations et ne peuvent pas être limités par. SCPs
- Lorsque vous désactivez le type de politique SCP dans une racine, toutes SCPs sont automatiquement détachées de toutes les AWS Organizations entités de cette racine. AWS Organizations les entités incluent les unités organisationnelles, les organisations et les comptes. Si vous le réactivez SCPs dans une racine, cette racine revient uniquement à la `FullAWSAccess` politique par défaut automatiquement attachée à toutes les entités de la racine. Toutes les pièces jointes d' AWS Organizations entités antérieures SCPs à la désactivation SCPs sont perdues et ne sont pas automatiquement récupérables, bien que vous puissiez les rattacher manuellement.
- Si une limite d'autorisations (une fonctionnalité IAM avancée) et une politique de contrôle des services sont présentes, la limite, la politique de contrôle des services et la politique basée sur l'identité doivent toutes autoriser l'action.

## Utiliser les données d'accès pour améliorer SCPs

Lorsque vous êtes connecté avec les informations d'identification du compte de gestion, vous pouvez consulter les données du dernier accès au service pour une AWS Organizations entité ou une politique dans la AWS Organizationssection de la console IAM. Vous pouvez également utiliser le

AWS Command Line Interface (AWS CLI) ou l' AWS API dans IAM pour récupérer les dernières données du service auxquelles vous avez accédé. Ces données incluent des informations sur les services autorisés auxquels les utilisateurs et les rôles IAM d'un AWS Organizations compte ont tenté d'accéder pour la dernière fois et à quel moment. Vous pouvez utiliser ces informations pour identifier les autorisations non utilisées afin d'affiner les SCPs vôtres afin de mieux respecter le principe du moindre privilège.

Par exemple, vous pouvez avoir une liste de refus SCP qui interdit l'accès à trois Services AWS d'entre eux. Tous les services qui ne sont pas répertoriés dans l'instruction `Deny` de la SCP sont autorisés. Les données du dernier accès au service dans IAM vous indiquent celles qui Services AWS sont autorisées par le SCP mais qui ne sont jamais utilisées. Ces informations vous permettent de mettre à jour la SCP pour refuser l'accès aux services dont vous n'avez pas besoin.

Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur IAM :

- Affichage des dernières informations relatives aux services pour Organizations
- Using Data to Refine Permissions for an Organizational Unit (Utilisation des données pour affiner les autorisations d'une unité d'organisation)

## Tâches et entités non limitées par SCPs

Vous ne pouvez pas utiliser SCPs pour restreindre les tâches suivantes :

- Toute action effectuée par le compte de gestion
- Toute action réalisée à l'aide des autorisations attachées à un rôle lié à un service.
- Enregistrement pour le plan Enterprise Support en tant qu'utilisateur racine
- Fournir des fonctionnalités de signature fiables pour le contenu CloudFront privé
- Configuration de DNS inverse pour un serveur de messagerie Amazon Lightsail et une instance Amazon EC2 en tant qu'utilisateur racine
- Tâches AWS relatives à certains services connexes :
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - API Amazon Product Marketing

# Évaluation du SCP

> **Note**
>
> Les informations contenues dans cette section ne s'appliquent pas aux types de politiques de gestion, y compris les politiques de sauvegarde, les politiques de balises, les politiques relatives aux applications de chat ou les politiques de désactivation des services d'intelligence artificielle. Pour de plus amples informations, veuillez consulter Fonctionnement de l'héritage des politiques de gestion.

Comme vous pouvez associer plusieurs politiques de contrôle des services (SCPs) à différents niveaux AWS Organizations, comprendre comment SCPs elles sont évaluées peut vous aider à rédiger des politiques SCPs qui donneront le bon résultat.

Rubriques

- Comment SCPs travailler avec Allow
- Comment SCPs travailler avec Deny
- Stratégie d'utilisation SCPs

## Comment SCPs travailler avec Allow

Pour qu'une autorisation soit accordée pour un compte spécifique, une instruction **`Allow`** explicite est nécessaire à chaque niveau, de la racine via chaque UO sur le chemin d'accès direct au compte (y compris le compte cible lui-même). C'est pourquoi, lorsque vous l'activez SCPs, AWS Organizations elle associe une politique SCP AWS gérée nommée Full AWSAccess qui autorise tous les services et actions. Si cette politique est supprimée et qu'elle n'est remplacée à aucun niveau de l'organisation, tous OUs les comptes inférieurs à ce niveau seront empêchés d'effectuer des actions.

Examinons le scénario des figures 1 et 2. Pour qu'une autorisation soit accordée ou qu'un service soit autorisé pour le compte B, une SCP accordant l'autorisation ou autorisant le service doit être attachée à la racine, à l'UO de production et au compte B.

L'évaluation du SCP suit un deny-by-default modèle, ce qui signifie que toutes les autorisations non explicitement autorisées dans le SCPs sont refusées. Si aucune instruction d'autorisation n'est présente dans aucun des niveaux tels que Root, Production OU ou Account B, l'accès est refusé. SCPs

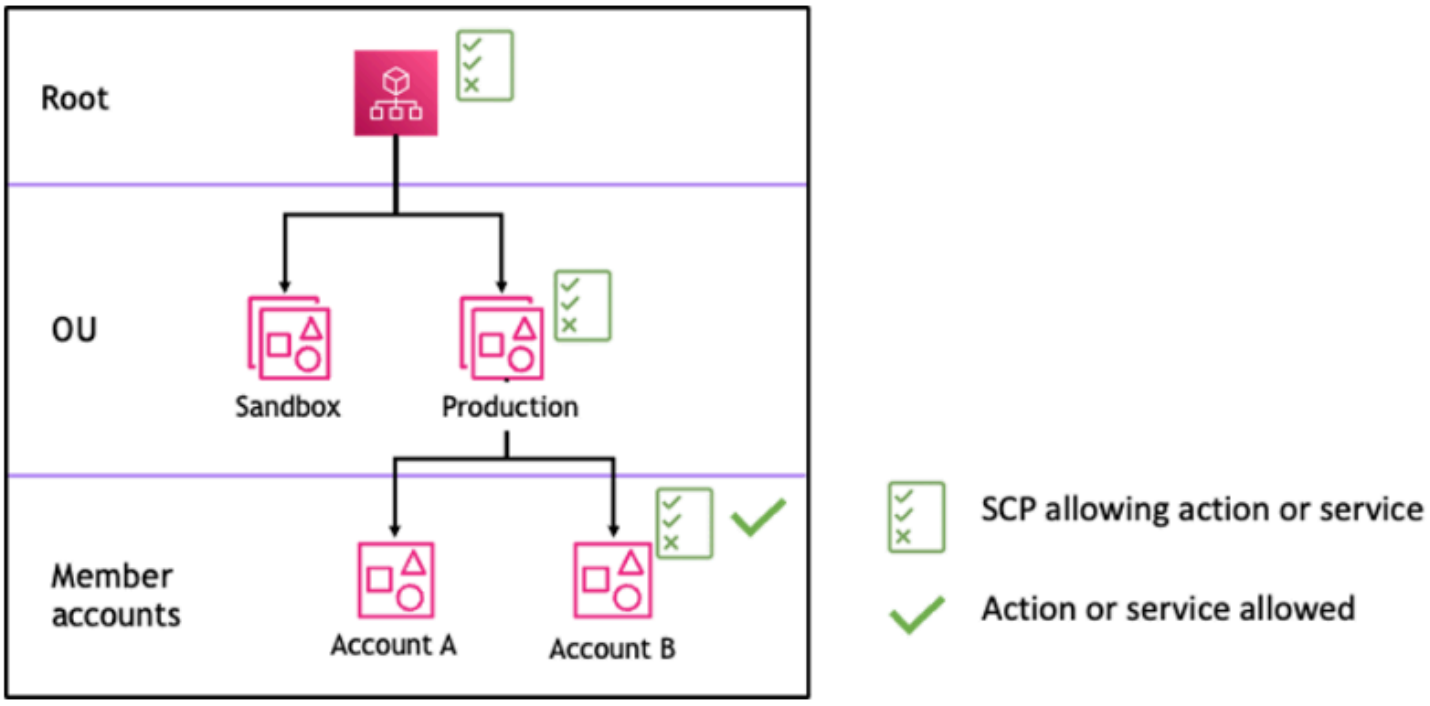



Figure 1 : exemple de structure organisationnelle avec une instruction *Allow* attachée à la racine, à l'UO de production et au compte B

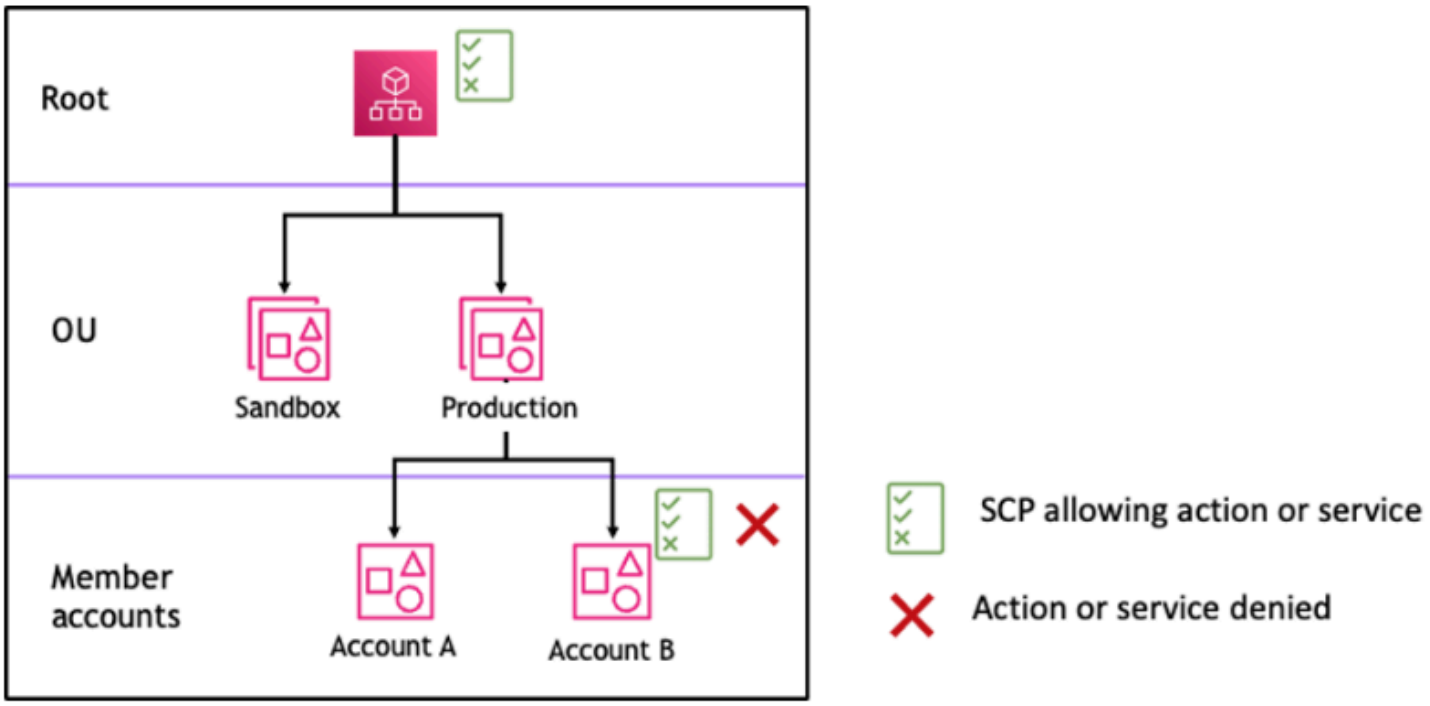



Figure 2 : exemple de structure organisationnelle avec une instruction *Allow* attachée à l'UO de production et impact sur le compte B

Comment SCPs travailler avec Deny

N'importe quelle SCP de la racine via chaque UO sur le chemin d'accès direct au compte (y compris le compte cible lui-même) peut refuser une autorisation pour un compte spécifique.

Supposons, par exemple, qu'une SCP attachée à l'UO de production comporte une instruction `Deny` explicite spécifiée pour un service donné. Une autre SCP attachée à la racine et au compte B autorise explicitement l'accès à ce même service, comme le montre la figure 3. Par conséquent, le compte A et le compte B se verront refuser l'accès au service, car une politique de refus attachée à tous les niveaux de l'organisation est évaluée pour tous les comptes OUs et membres sous-jacents.

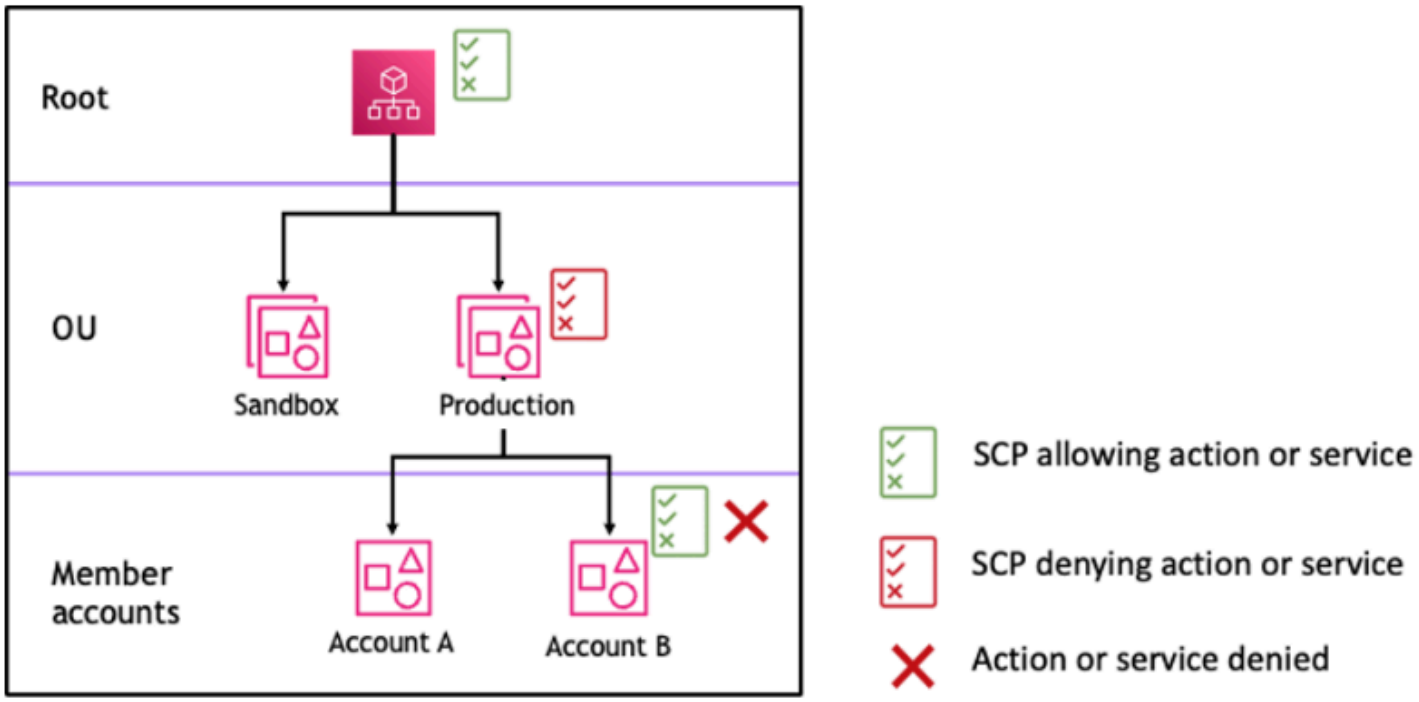



Figure 3 : exemple de structure organisationnelle avec une instruction *`Deny`* attachée à l'UO de production et impact sur le compte B

Stratégie d'utilisation SCPs

Lorsque SCPs vous rédigez, vous pouvez utiliser une combinaison de `Deny` déclarations `Allow` et de déclarations pour autoriser les actions et les services prévus dans votre organisation. `Deny`les déclarations constituent un moyen efficace de mettre en œuvre des restrictions qui devraient s'appliquer à une plus grande partie de votre organisation ou OUs parce que lorsqu'elles sont appliquées à la racine ou au niveau de l'unité d'organisation, elles affectent tous les comptes qui en dépendent.

> **Tip**
>
> Vous pouvez utiliser les données du dernier accès au service dans IAM pour les mettre à jour SCPs afin de restreindre l'accès aux seules données Services AWS dont vous avez besoin. Pour de plus amples informations, consultez Affichage des dernière informations consultées pour Organizations dans le Guide de l'utilisateur IAM.

AWS Organizations attache un SCP AWS géré nommé Full AWSAccess à chaque racine, unité d'organisation et compte lors de sa création. Cette politique autorise tous les services et actions. Vous pouvez AWSAccess remplacer Full par une politique n'autorisant qu'un ensemble de services, de sorte que les nouveaux services ne Services AWS sont pas autorisés, sauf s'ils sont explicitement autorisés par le biais d'une mise à jour SCPs. Par exemple, si votre organisation souhaite uniquement autoriser l'utilisation d'un sous-ensemble de services dans votre environnement, vous pouvez utiliser une instruction `Allow` pour n'autoriser que certains services. Vous pouvez choisir de remplacer Full AWSAccess à la racine ou à tous les niveaux. Si vous associez une liste d'autorisations (SCP) spécifique à un service à la racine, elle s'applique automatiquement à tous les comptes OUs et aux comptes situés en dessous, ce qui signifie qu'une seule politique au niveau de la racine détermine la liste d'autorisations de service effective dans l'ensemble de l'organisation, comme indiqué dans le scénario 7. Vous pouvez également supprimer et remplacer Full AWSAccess au niveau de chaque unité organisationnelle et de chaque compte, ce qui vous permet de mettre en œuvre des listes d'autorisation de service plus détaillées qui diffèrent selon les unités organisationnelles ou les comptes individuels.

Remarque : Le fait de s'appuyer uniquement sur les instructions d'autorisation et le deny-by-default modèle implicite peut entraîner un accès involontaire, car les instructions Allow plus larges ou qui se chevauchent peuvent remplacer les instructions plus restrictives.

JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
```

```
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

L'exemple suivant montre une politique combinant les deux instructions, ce qui empêche les comptes membres de quitter l'organisation et autorise l'utilisation des services AWS souhaités. L'administrateur de l'organisation peut détacher la AWSAccess politique complète et joindre celle-ci à la place.

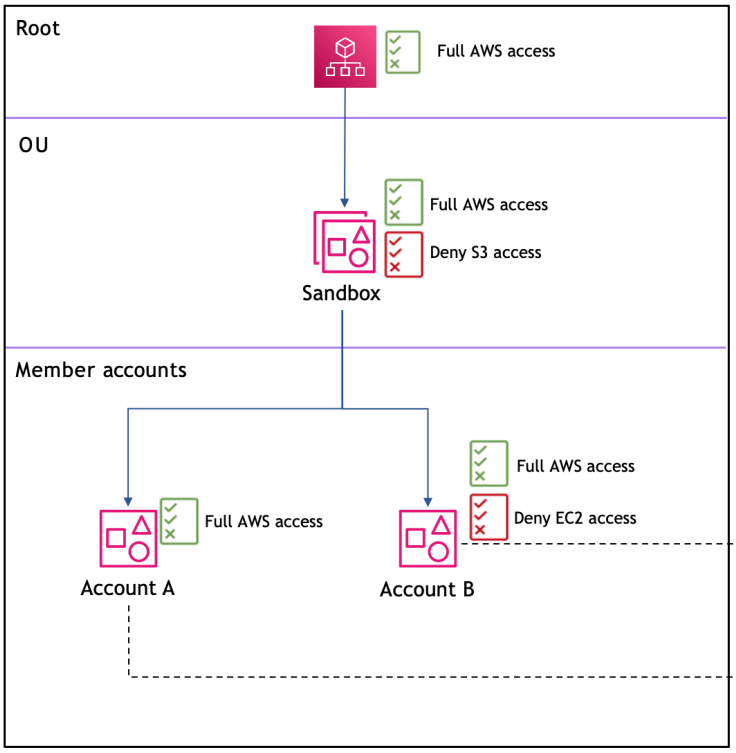
JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Pour démontrer comment plusieurs politiques de contrôle des services (SCPs) peuvent être appliquées dans une AWS organisation, considérez la structure organisationnelle et les scénarios suivants.

### Scénario 1 : Impact des politiques de refus

Ce scénario montre comment les politiques de refus appliquées aux niveaux supérieurs de l'organisation ont un impact sur tous les comptes ci-dessous. Lorsque l'unité d'organisation Sandbox possède à la fois des politiques « AWS accès complet » et « Refuser l'accès S3 », et que le compte B applique une politique « Refuser l'accès EC2 », le compte B ne peut pas accéder à S3 (depuis le refus au niveau de l'unité d'organisation) et à EC2 (depuis son refus au niveau du compte). Le compte A ne dispose pas d'un accès S3 (depuis le refus au niveau de l'unité d'organisation).

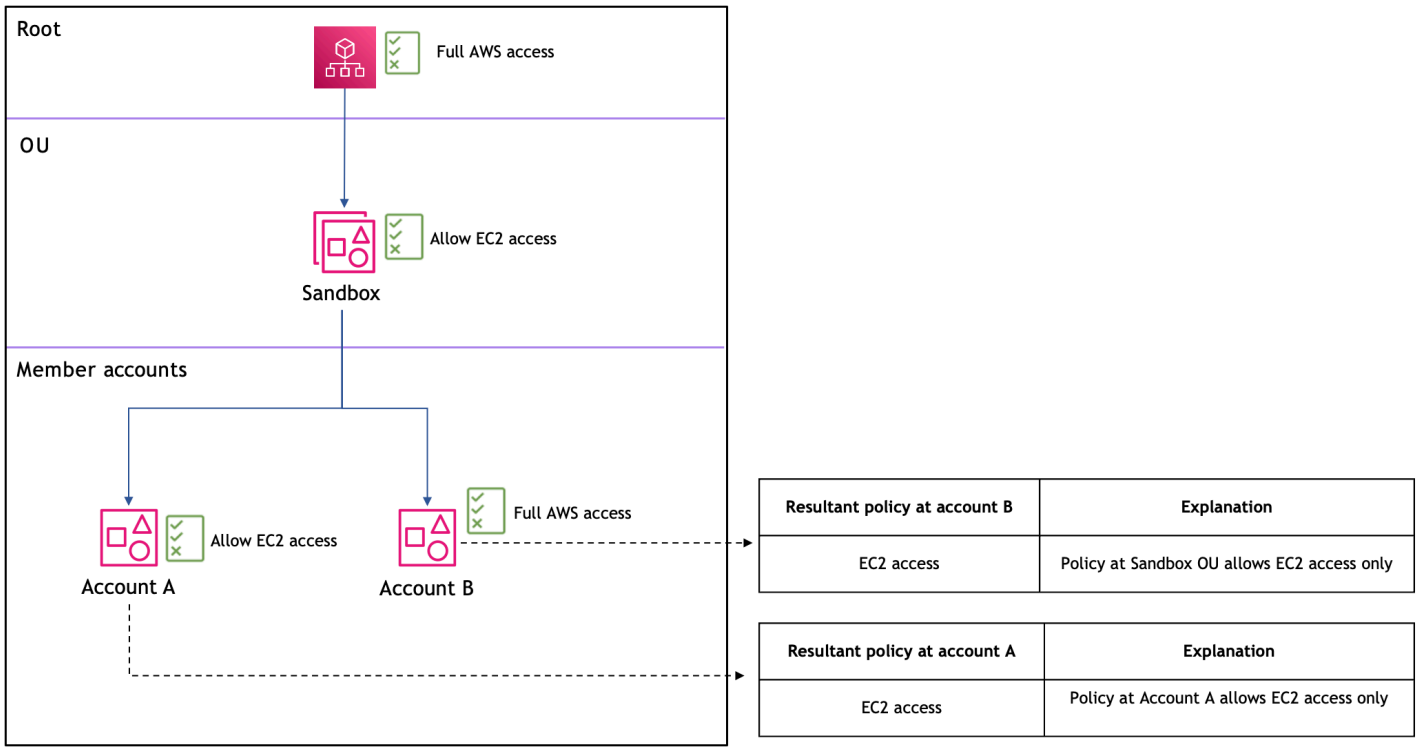



| Resultant policy at account B | Explanation |
|---|---|
| All service access except S3 and EC2 | S3 denial cascades down from Sandbox; EC2 denial from account level SCP |

| Resultant policy at account A | Explanation |
|---|---|
| All service access except S3 | S3 denial cascades down from Sandbox level |

### Scénario 2 : les politiques d'autorisation doivent exister à tous les niveaux

Ce scénario montre comment les politiques d'autorisation fonctionnent dans les SCP. Pour qu'un service soit accessible, il doit y avoir une autorisation explicite à tous les niveaux, depuis le root jusqu'au compte. Dans ce cas, étant donné que l'unité d'organisation Sandbox applique une politique « Autoriser l'accès EC2 », qui n'autorise explicitement que l'accès au service EC2, les comptes A et B auront uniquement accès à EC2.

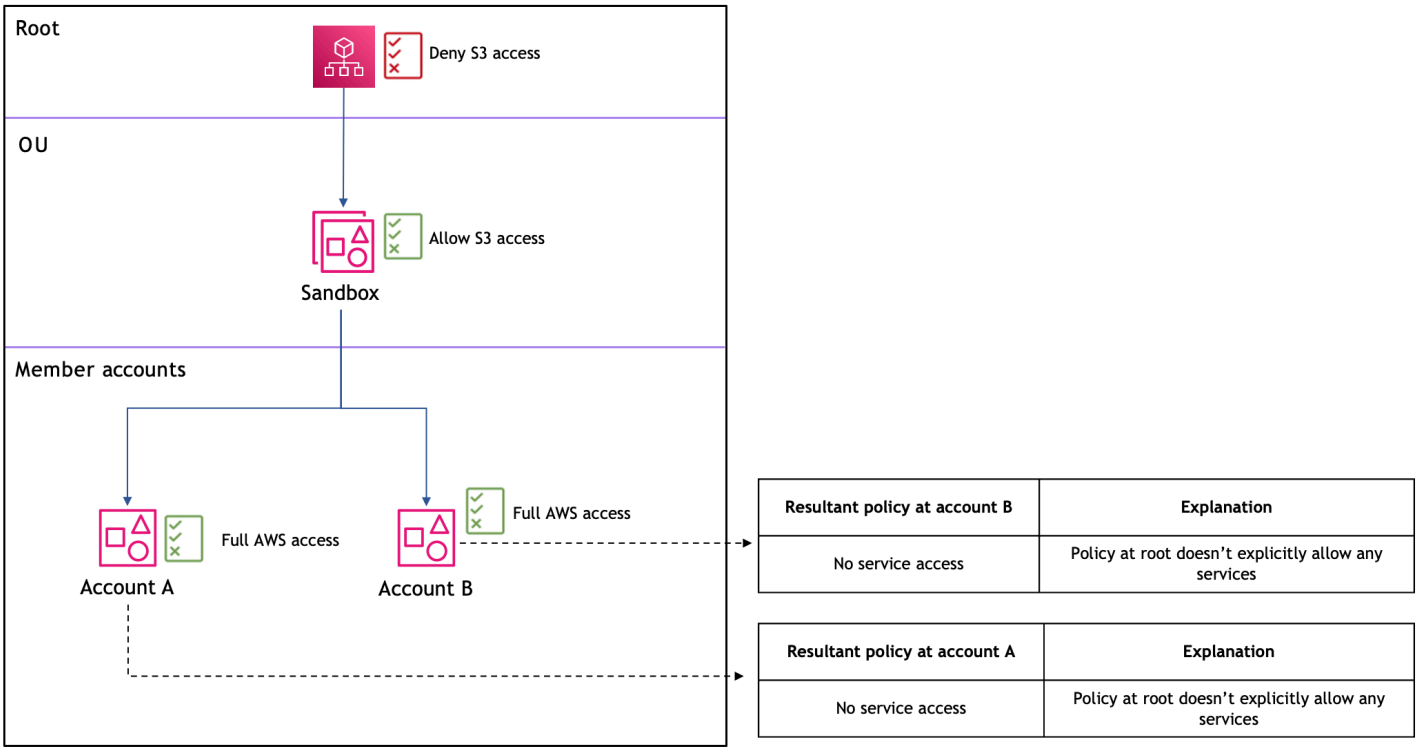



| Resultant policy at account B | Explanation |
|---|---|
| EC2 access | Policy at Sandbox OU allows EC2 access only |

| Resultant policy at account A | Explanation |
|---|---|
| EC2 access | Policy at Account A allows EC2 access only |

Scénario 3 : impact de l'absence d'une instruction Allow au niveau de la racine

L'absence d'une instruction « Autoriser » au niveau de la racine dans un SCP constitue une erreur de configuration critique qui bloquera efficacement tout accès aux AWS services et aux actions pour tous les comptes membres de votre organisation.

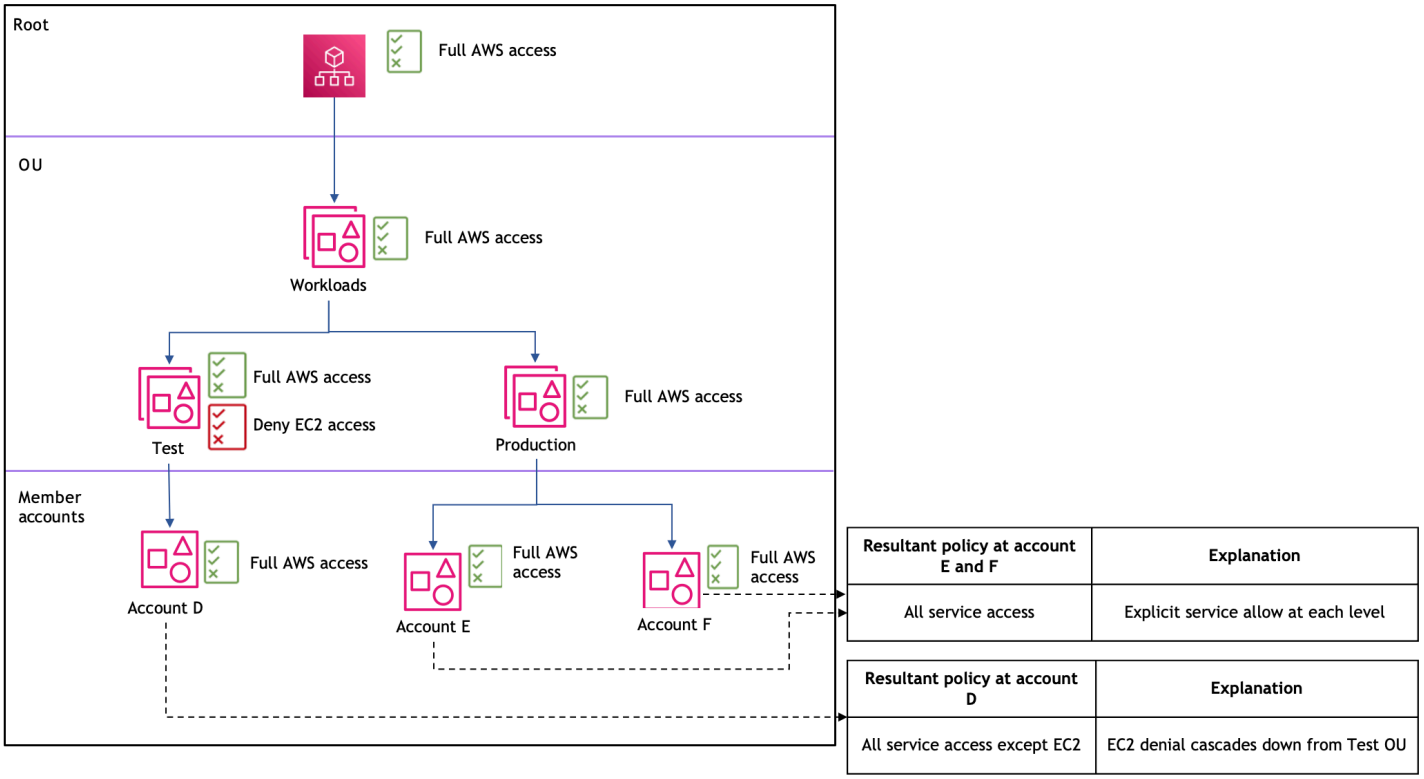



| Resultant policy at account B | Explanation |
|---|---|
| No service access | Policy at root doesn't explicitly allow any services |

| Resultant policy at account A | Explanation |
|---|---|
| No service access | Policy at root doesn't explicitly allow any services |

Scénario 4 : déclarations de refus en couches et autorisations qui en résultent

Ce scénario illustre une structure d'UO profonde à deux niveaux. L'unité d'organisation racine et l'unité d'organisation de charges de travail ont toutes deux un «  AWS  accès complet », l'unité d'organisation de test dispose d'un «  AWS  accès complet » avec « Refuser l'accès EC2 » et l'unité d'organisation de production dispose d'un «  AWS  accès complet ». Par conséquent, le compte D dispose de tous les accès aux services, à l'exception de l'EC2, et les comptes E et F ont tous les accès aux services.

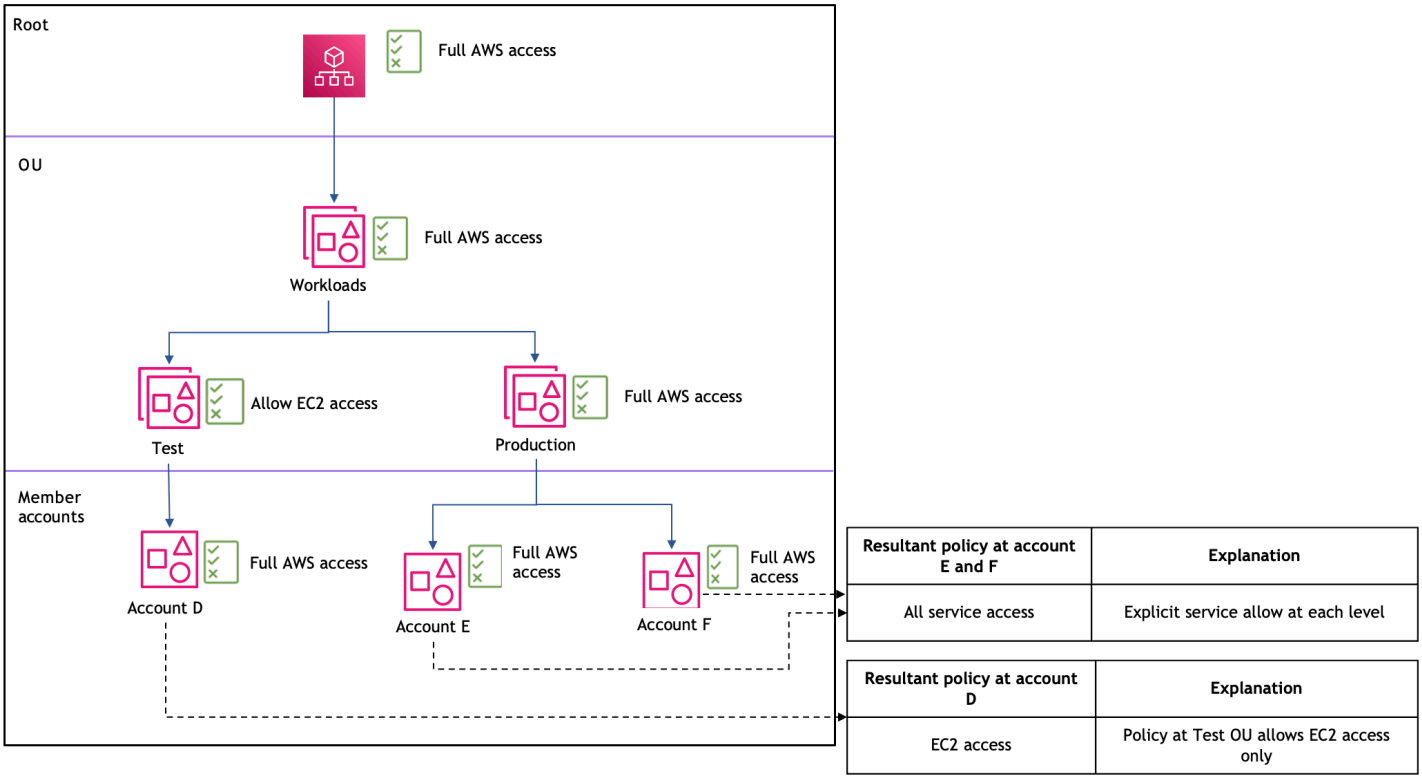



| Resultant policy at account E and F | Explanation |
|---|---|
| All service access | Explicit service allow at each level |

| Resultant policy at account D | Explanation |
|---|---|
| All service access except EC2 | EC2 denial cascades down from Test OU |

Scénario 5 : autoriser les politiques au niveau de l'unité d'organisation à restreindre l'accès aux services

Ce scénario montre comment les politiques d'autorisation peuvent être utilisées pour restreindre l'accès à des services spécifiques. L'UO de test applique une politique « Autoriser l'accès EC2 », ce qui signifie que seuls les services EC2 sont autorisés pour le compte D. L'UO de production maintient un «  AWS  accès complet », de sorte que les comptes E et F ont accès à tous les services. Cela montre comment des politiques d'autorisation plus restrictives peuvent être mises en œuvre au niveau de l'unité d'organisation tout en maintenant une autorisation plus large au niveau racine.

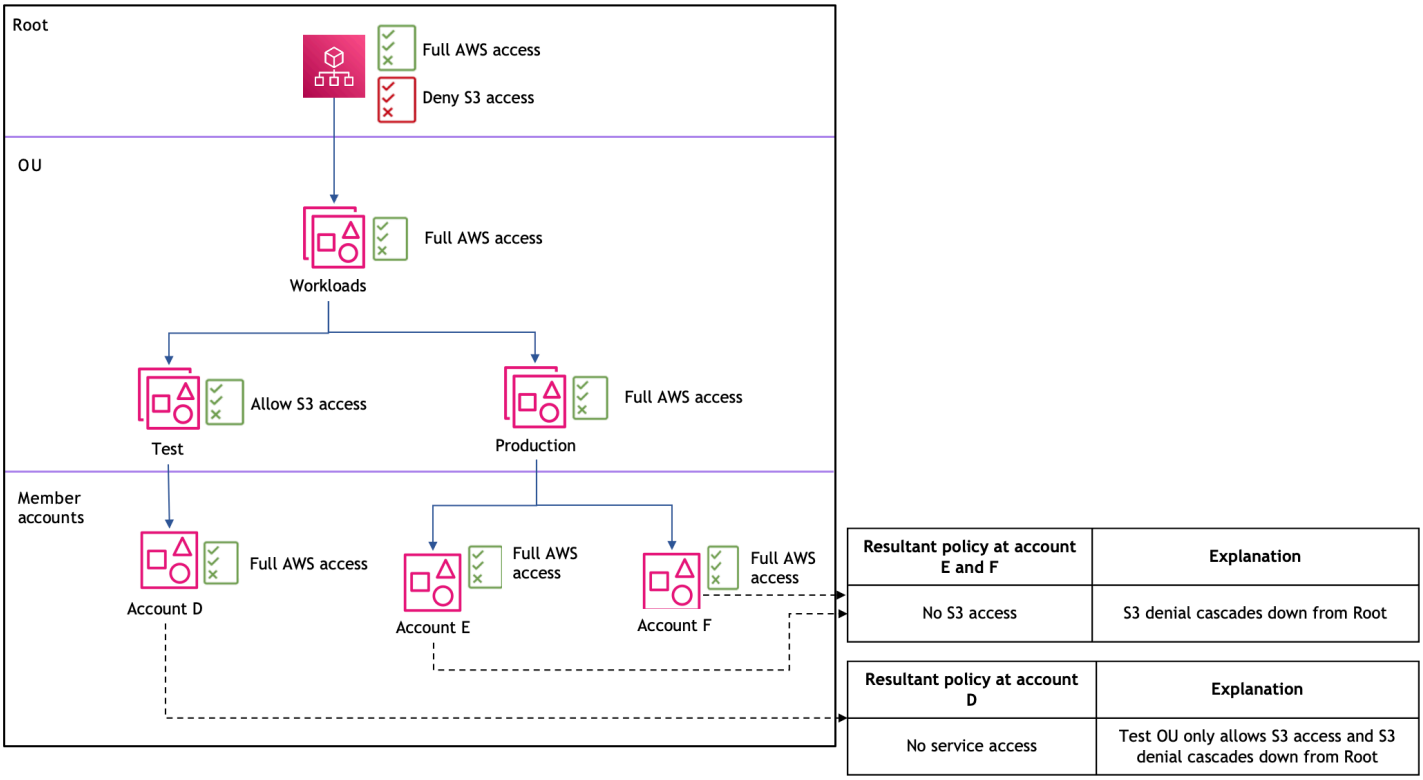



| Resultant policy at account E and F | Explanation |
|---|---|
| All service access | Explicit service allow at each level |

| Resultant policy at account D | Explanation |
|---|---|
| EC2 access | Policy at Test OU allows EC2 access only |

Scénario 6 : le refus au niveau root affecte tous les comptes, quelles que soient les autorisations de niveau inférieur

Ce scénario montre qu'une politique de refus au niveau racine affecte tous les comptes de l'organisation, quelles que soient les politiques d'autorisation aux niveaux inférieurs. La racine applique à la fois des politiques «  AWS  Accès complet » et « Refuser l'accès S3 ». Même si l'unité d'organisation de test applique une politique « Autoriser l'accès au S3 », le refus du S3 au niveau racine a la priorité. Le compte D n'a aucun accès au service car l'unité d'organisation de test autorise uniquement l'accès à S3, mais S3 est refusé au niveau racine. Les comptes E et F peuvent accéder à d'autres services à l'exception de S3 en raison du refus explicite au niveau de la racine.

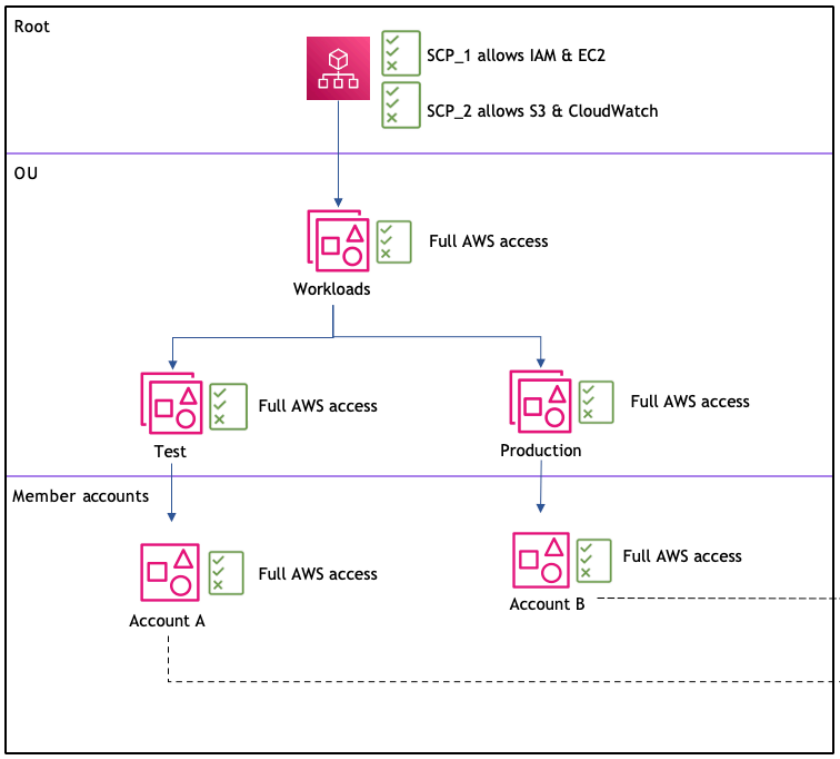



| Resultant policy at account E and F | Explanation |
|---|---|
| No S3 access | S3 denial cascades down from Root |

| Resultant policy at account D | Explanation |
|---|---|
| No service access | Test OU only allows S3 access and S3 denial cascades down from Root |

Scénario 7 : politiques d'autorisation personnalisées au niveau de la racine pour restreindre l'accès au niveau de l'unité d'organisation

Ce scénario montre comment, SCPs avec un service explicite, les listes d'autorisations fonctionnent lorsqu'elles sont appliquées au niveau de la racine dans un AWS Organizations. Au niveau de la racine de l'organisation, deux « Autorisations de service » personnalisées SCPs sont associées qui autorisent explicitement l'accès à un ensemble limité de AWS services : SCP_1 autorise IAM et Amazon EC2, SCP_2 autorise Amazon S3 et Amazon. CloudWatch Au niveau de l'unité organisationnelle (UO), la AWSAccess politique complète par défaut reste attachée. Cependant, en raison du comportement des intersections, les comptes A et B de ces UO ne peuvent accéder qu'aux services explicitement autorisés par le SCP de niveau racine. La politique racine la plus restrictive a la priorité, limitant efficacement l'accès aux seuls IAM, EC2, S3 et CloudWatch aux services, indépendamment des autorisations plus larges accordées aux niveaux organisationnels inférieurs.




| Resultant policy at account B | Explanation |
|---|---|
| Can access only IAM, EC2, S3, and CloudWatch services (SCP_1 + SCP_2) | Allow statements at the root only allow specific services. |

| Resultant policy at account A | Explanation |
|---|---|
| Can access only IAM, EC2, S3, and CloudWatch services (SCP_1 + SCP_2) | Allow statements at the root only allow specific services. |

## Syntaxe d'une stratégie de contrôle de service

Les politiques de contrôle des services (SCPs) utilisent une syntaxe similaire à celle utilisée par les politiques d'autorisation Gestion des identités et des accès AWS (IAM) et les politiques basées sur les ressources (comme les politiques relatives aux compartiments Amazon S3). Pour plus d'informations sur les politiques IAM et leur syntaxe, consultez Présentation des politiques IAM dans le Guide de l'utilisateur IAM.

Une politique SCP est un fichier texte brut qui est structuré conformément aux règles de JSON. Elle utilise les éléments qui sont décrits dans cette rubrique.

> **Note**
>
> Tous les caractères de votre SCP sont pris en compte dans le calcul de sa taille maximale. Les exemples présentés dans ce guide montrent les SCPs fichiers formatés avec des espaces blancs supplémentaires pour améliorer leur lisibilité. Toutefois, pour économiser de l'espace si la taille de votre politique approche de la taille maximale, vous pouvez supprimer les espaces, comme les espacements et les sauts de ligne qui ne figurent pas entre guillemets.

Pour des informations générales sur SCPs, voirPolitiques de contrôle des services (SCPs).

Récapitulatif des éléments

Le tableau suivant récapitule les éléments de stratégie que vous pouvez utiliser dans SCPs. Certains éléments de politique ne sont disponibles SCPs que dans les cas où les actions sont interdites. La colonne Effets pris en charge répertorie le type d'effet que vous pouvez utiliser avec chaque élément de politique SCPs.

| Element | Objectif | Effets pris en charge |
| --- | --- | --- |
| Action | Spécifie le AWS service et les actions que le SCP autorise ou refuse. | `Allow`, `Deny` |
| Effet | Définit si l'instruction SCP autorise ou refuse l'accès aux utilisateurs et rôles IAM d'un compte. | `Allow`, `Deny` |
| Instruction | Sert de conteneur pour les éléments | `Allow`, `Deny` |

| Element | Objectif | Effets pris en charge |
| --- | --- | --- |
| | de politique. Vous pouvez avoir plusieurs instructions dans SCPs. | |
| ID d'instruction (Sid) | (Facultatif) Fournit un nom simple pour l'instruction. | `Allow`, `Deny` |
| Version | Spécifie les règles de syntaxe du langage à utiliser pour le traitement de la politique. | `Allow`, `Deny` |

| Element | Objectif | Effets pris en charge |
| --- | --- | --- |
| Condition | Spécifie les conditions lorsque l'instruction est vigueur. | `Allow,Deny` |
| NotAction | Spécifie le AWS service et les actions exemptés du SCP. Utilisé au lieu de l'élément `Action`. | `Allow,Deny` |
| Ressource | Spécifie les AWS ressources auxquelles le SCP s'applique. | `Allow,Deny` |

| Element | Objectif | Effets pris en charge |
| --- | --- | --- |
| NotResource | Spécifie les AWS ressources exemptées du SCP. Utilisé au lieu de l'élément `Resource`. | `Allow`, `Deny` |

Les sections suivantes fournissent des informations supplémentaires et des exemples de la manière dont les éléments de politique sont utilisés dans SCPs.

Rubriques

- Éléments Action et NotAction
- Élément Condition
- Élément Effect
- Resourceet NotResource élément
- Élément Statement
- Élément ID d'instruction (Sid)
- Élément Version
- Élément non pris en charge

### Éléments **`Action`** et **`NotAction`**

La valeur de l'`NotAction`élément `Action` or est une liste (un tableau JSON) de chaînes identifiant les AWS services et les actions autorisés ou refusés par l'instruction.

Chaque chaîne est constituée de l'abréviation du service (par exemple, « s3 », « ec2 », « iam » ou « organizations »), en minuscules, suivie de deux points, puis d'une action de ce service. Les actions et les notactions ne font pas la distinction majuscules/majuscules. En général, ils sont tous saisis

avec chaque mot commençant par une lettre majuscule et le reste par une minuscule. Par exemple : `"s3:ListAllMyBuckets"`.

Vous pouvez également utiliser des caractères génériques comme un astérisque (*) ou un point d'interrogation (?) dans une SCP :

- Utilisez un astérisque (*) en tant que caractère générique pour faire correspondre plusieurs actions partageant une partie d'un nom. La valeur `"s3:*"` signifie toutes les actions dans le service Amazon S3. La valeur `"ec2:Describe*"` correspond uniquement aux actions EC2 commençant par « Describe ».
- Utilisez le caractère générique point d'interrogation (?) pour faire correspondre un seul caractère.

Pour obtenir une liste de tous les services et des actions qu'ils prennent en charge dans les politiques d'autorisation IAM AWS Organizations SCPs et dans les politiques d'autorisation IAM, consultez la section Actions, ressources et clés de condition pour les AWS services dans le guide de l'utilisateur IAM.

Pour plus d'informations, consultez les sections Éléments de stratégie IAM JSON : action et Éléments de stratégie IAM JSON : NotAction dans le guide de l'utilisateur IAM.

Exemple d'élément **`Action`**

L'exemple suivant montre une politique de contrôle des services dans une instruction qui permet aux administrateurs de compte de déléguer les autorisations décrire, démarrer, arrêter et résilier pour les instances EC2 dans le compte. Il s'agit d'un exemple de liste d'autorisations, qui est utile lorsque les politiques `Allow *` par défaut ne sont pas attachées afin que, par défaut, les autorisations soient implicitement refusées. Si la politique `Allow *` par défaut est encore attachée à la racine, à l'unité d'organisation ou au compte auquel la politique suivante est attachée, cette politique n'a aucun effet.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
```

```
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

L'exemple suivant montre comment vous pouvez refuser l'accès à des services qui ne doivent pas être utilisés dans les comptes attachés. Il suppose que les politiques de contrôle des services `"Allow *"` par défaut sont encore attachées à toutes les unités d'organisation et à la racine. Cet exemple de politique empêche les administrateurs de compte dans les comptes attachés de déléguer des autorisations pour les services IAM, Amazon EC2 et Amazon RDS. Les actions d'autres services peuvent être déléguées dans la mesure où aucune autre politique attachée ne les refuse :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Exemple d'élément **`NotAction`**

L'exemple suivant montre comment utiliser un `NotAction` élément pour exclure AWS des services de l'effet de la politique.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
```

```
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

Avec cette instruction, les comptes concernés sont limités à l'exécution des actions spécifiées Région AWS, sauf lorsqu'ils utilisent des actions IAM.

### Élément **`Condition`**

Vous pouvez spécifier un `Condition` élément dans les instructions d'autorisation et de refus d'un SCP.

L'exemple suivant montre comment utiliser un élément de condition avec une instruction allow dans un SCP pour autoriser des principaux spécifiques à accéder AWS aux services.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowServicesForSpecificPrincipal",
         "Effect":"Allow",
         "Action":[
            "ec2:*",
            "s3:*",
            "rds:*",
            "lambda:*",
            "cloudformation:*",
            "iam:*",
            "cloudwatch:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:PrincipalArn":[
                  "arn:aws:iam::123456789012:role/specific-role"
               ]
```

```
            }
         }
      }
   ]
}
```

L'exemple suivant montre comment utiliser un élément de condition avec une déclaration de refus dans un SCP pour restreindre l'accès à toutes les opérations en dehors des `eu-west-1` régions `eu-central-1` et, à l'exception des actions dans les services spécifiés.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez Éléments de politique JSON IAM : Condition dans le Guide de l'utilisateur IAM.

### Élément `Effect`

Chaque instruction doit contenir un élément `Effect`. La valeur peut être `Allow` ou `Deny`. Cet élément affecte toutes les actions répertoriées dans la même instruction.

Pour plus d'informations, consultez Éléments de politique JSON IAM : Effet dans le Guide de l'utilisateur IAM.

#### `"Effect": "Allow"`

L'exemple suivant montre une politique de contrôle des services avec une instruction qui contient un élément `Effect` avec une valeur `Allow` qui permet aux utilisateurs de compte d'effectuer des actions pour le service Amazon S3. Cet exemple est utile dans une organisation qui utilise la stratégie de liste d'autorisations (où les politiques `FullAWSAccess` par défaut sont toutes détachées, de sorte que les autorisations sont implicitement refusées par défaut). Le résultat est que l'instruction permet les autorisations Amazon S3 pour les comptes attachés :

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

Même si cette instruction utilise le même mot clé de valeur `Allow` qu'une politique d'autorisation IAM, dans une politique SCP, cela n'autorise pas réellement un utilisateur à effectuer une action. SCPs Agissez plutôt comme des filtres qui spécifient les autorisations maximales pour les comptes d'une organisation, d'une unité organisationnelle (UO) ou d'un compte. Dans l'exemple précédent, même si une politique gérée `AdministratorAccess` est attachée à un utilisateur du compte, la politique de contrôle des services limite tous les utilisateurs des comptes concernés aux seules actions Amazon S3.

#### `"Effect": "Deny"`

Dans une instruction dont la valeur de l'`Effect`élément est égale à`Deny`, vous pouvez également restreindre l'accès à des ressources spécifiques ou définir les conditions d'entrée en vigueur. SCPs

L'exemple suivant montre la façon d'utiliser une clé de condition dans une instruction de refus.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Cette instruction dans une politique de contrôle des services définit une protection pour empêcher les comptes concernés (dans lesquels la politique de contrôle des services est attachée au compte lui-même ou à la racine de l'organisation ou à l'unité d'organisation qui contient le compte), de lancer des instances Amazon EC2 si l'instance Amazon EC2 n'est pas définie sur `t2.micro`. Même si une politique IAM qui permet cette action est attachée au compte, la protection créée par la politique de contrôle des services empêche cette action.

**`Resource`**et **`NotResource`** élément

Dans les instructions où l'élément `Effect` a une valeur `Allow`, vous pouvez spécifier uniquement «* » dans l'élément `Resource` d'une politique de contrôle des services (SCP). Vous ne pouvez pas spécifier de ressource Amazon Resource Names (ARNs) individuelle.

Vous pouvez utiliser des caractères génériques tels que l'astérisque (*) ou le point d'interrogation (?) dans l'élément ressource :

- Utilisez un astérisque (*) en tant que caractère générique pour faire correspondre plusieurs actions partageant une partie d'un nom.
- Utilisez le caractère générique point d'interrogation (?) pour faire correspondre un seul caractère.

Dans les instructions où l'`Effect`élément a une valeur égale à`Deny`, vous pouvez spécifier un élément individuel ARNs, comme indiqué dans l'exemple suivant.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

Cette politique de contrôle des services empêche les utilisateurs et les rôles IAM des comptes concernés de modifier un rôle IAM d'administration commun créé dans tous les comptes de votre organisation.

L'exemple suivant montre comment utiliser un `NotResource` élément pour exclure des modèles Amazon Bedrock spécifiques de l'effet de la politique.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Statement1",
         "Effect":"Deny",
         "Action":[
```

```
            "bedrock:InvokeModel",
            "bedrock:InvokeModelWithResponseStream"
         ],
         "NotResource":[
            "arn:aws:bedrock:*::foundation-model/model-to-permit"
         ]
      }
   ]
}
```

Pour plus d'informations, consultez Éléments de politique JSON IAM : Ressource dans le Guide de l'utilisateur IAM.

### Élément **`Statement`**

Une politique de contrôle des services est constituée d'un ou plusieurs éléments `Statement`. Vous ne pouvez avoir qu'un mot clé `Statement` dans une politique, mais la valeur peut être un tableau d'instructions JSON (encadré par des caractères [ ]).

L'exemple suivant montre une instruction unique qui se compose d'éléments `Effect`, `Action` et `Resource` uniques.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

L'exemple suivant inclut deux instructions sous la forme d'un tableau à l'intérieur d'un élément `Statement`. La première instruction autorise toutes les actions, tandis que la deuxième refuse toutes les actions EC2. Le résultat est un qu'administrateur du compte peut déléguer n'importe quelle autorisation, à l'exception de celles provenant d'Amazon Elastic Compute Cloud (Amazon EC2).

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
```

```
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

Pour plus d'informations, consultez Éléments de politique JSON IAM : Instruction dans le Guide de l'utilisateur IAM.

Élément ID d'instruction (**`Sid`**)

L'élément `Sid` est un identifiant facultatif que vous pouvez fournir pour l'instruction de politique. Vous pouvez affecter une valeur `Sid` à chaque instruction d'un tableau d'instructions. L'exemple suivant de politique de contrôle des services présente un exemple d'instruction `Sid`.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

Pour plus d'informations, consultez Éléments de politique JSON IAM : Id dans le Guide de l'utilisateur IAM.

Élément **`Version`**

Chaque politique de contrôle des services doit inclure un élément `Version` avec la valeur `"2012-10-17"`. Il s'agit de la même valeur de version que la version la plus récente des politiques d'autorisation IAM.

Pour plus d'informations, consultez Éléments de politique JSON IAM : Version dans le Guide de l'utilisateur IAM.

Élément non pris en charge

Les éléments suivants ne sont pas pris en charge dans SCPs :

- `NotPrincipal`
- `Principal`

# Exemples de politiques de contrôle des services

Les exemples de politiques de contrôle des services (SCPs) présentés dans cette rubrique sont fournis à titre informatif uniquement.

**Avant d'utiliser ces exemples**

Avant d'utiliser ces exemples SCPs dans votre organisation, tenez compte des points suivants :

- Les politiques de contrôle des services (SCPs) sont destinées à être utilisées comme des barrières de sécurité grossières et n'accordent pas directement l'accès. L'administrateur doit toujours associer des politiques basées sur l'identité ou les ressources aux principaux IAM ou aux ressources de vos comptes pour réellement accorder des autorisations. Les autorisations effectives sont l'intersection logique entre la politique de policy/Resource contrôle des services et une politique d'identité ou entre la politique de policy/Resource contrôle des services et une politique des ressources. Vous pouvez obtenir plus de détails sur les effets du SCP sur les autorisations ici.
- Lorsqu'elle est associée à une organisation, à une unité organisationnelle ou à un compte, une politique de contrôle des services (SCP) permet de contrôler de manière centralisée les autorisations maximales disponibles pour tous les comptes de votre organisation, de votre unité organisationnelle ou d'un compte. Comme un SCP peut être appliqué à plusieurs niveaux dans une organisation, comprendre comment SCPs sont évalués peut vous aider à rédiger des articles SCPs qui donnent le bon résultat.
- Les politiques de contrôle des services de ce référentiel sont présentées à titre d'exemples. Vous ne devez pas joindre une SCPs pièce jointe sans avoir testé de manière approfondie l'impact de la politique sur les comptes. Une fois que vous avez une politique prête à mettre en œuvre, nous vous recommandons de la tester dans une organisation ou une unité d'organisation distincte pouvant représenter votre environnement de production. Une fois le test effectué, vous devez déployer les modifications de manière plus spécifique, OUs puis les déployer progressivement de manière plus large OUs au fil du temps.
- Les exemples de SCP de ce référentiel utilisent une stratégie de liste de refus, ce qui signifie que vous avez également besoin d'une AWSAccess politique complète ou d'une autre politique autorisant l'accès attaché aux entités de votre organisation pour autoriser les actions. Vous devez également accorder les autorisations appropriées à vos principaux en utilisant des politiques basées sur l'identité ou les ressources.

> **Tip**
>
> Vous pouvez utiliser les données du dernier accès au service dans IAM pour les mettre à jour SCPs afin de restreindre l'accès aux seules données Services AWS dont vous avez besoin. Pour de plus amples informations, consultez Affichage des dernière informations consultées pour Organizations dans le Guide de l'utilisateur IAM.

GitHub référentiel

- Exemples de politiques de contrôle des services - Ce GitHub référentiel contient des exemples de politiques pour démarrer ou affiner votre utilisation de AWS SCPs

## Résolution des problèmes liés aux politiques de contrôle des services (SCPs) avec AWS Organizations

Utilisez les informations fournies ici pour vous aider à diagnostiquer et à corriger les erreurs courantes détectées dans les politiques de contrôle des services (SCPs).

Les politiques de contrôle des services (SCPs) AWS Organizations sont similaires aux politiques IAM et partagent une syntaxe commune. Cette syntaxe commence par les règles de la notation d'JavaScript objet (JSON). JSON décrit un objet avec des paires nom-valeur qui constituent l'objet. La grammaire des politiques IAM s'appuie sur cela en définissant les noms et les valeurs qui ont une signification et sont compris par ceux Services AWS qui utilisent des politiques pour accorder des autorisations.

AWS Organizations utilise un sous-ensemble de la syntaxe et de la grammaire IAM. Pour en savoir plus, consultez Syntaxe d'une stratégie de contrôle de service.

Erreurs courantes dans les politiques

- Plus d'un objet de politique
- Plusieurs éléments d'instruction
- La taille du document de politique dépasse la taille maximale autorisée

Plus d'un objet de politique

Une politique SCP doit inclure un et un seul objet JSON. Vous désignez un objet en le plaçant entre accolades { }. S'il est possible d'imbriquer d'autres objets au sein d'un objet JSON en incorporant des

parenthèses { } supplémentaires dans la paire extérieure, une politique peut uniquement comporter une paire de parenthèses { } extérieure. L'exemple suivant est incorrect car il contient deux objets au niveau supérieur (appelés dans*red*) :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Toutefois, il est possible de réaliser ce que voulait faire l'exemple précédent en utilisant une grammaire correcte. Au lieu d'utiliser deux objets de politique complets, avec chacun son propre élément `Statement`, vous pouvez combiner les deux blocs en un seul élément `Statement`. La valeur de l'élément `Statement` est un tableau de deux objets, comme illustré dans l'exemple suivant :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*"
    }
  ]
}
```

Cet exemple ne peut pas être davantage compressé en une `Statement` ne comportant qu'un seul élément car les deux éléments ont des effets différents. En général, vous pouvez combiner des instructions uniquement lorsque les éléments `Effect` et `Resource` de chaque instruction sont identiques.

Plusieurs éléments d'instruction

Au premier abord, cette erreur peut sembler être une variante de l'erreur de la section précédente. Toutefois, d'un point de vue syntaxique, il s'agit d'un type d'erreur différent. L'exemple suivant comporte un seul objet de politique, comme indiqué par la paire de parenthèses { } unique au niveau supérieur. Toutefois, cet objet contient deux éléments `Statement`.

Une politique SCP ne peut comporter qu'un seul élément `Statement`, composé du nom (`Statement`) suivi de deux points, eux-mêmes suivis de sa valeur à droite. La valeur d'un élément `Statement` doit être un objet, indiqué par des accolades { }, contenant un élément `Effect`, un élément `Action` et un élément `Resource`. L'exemple suivant est incorrect car il contient deux éléments `Statement` dans l'objet de politique :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Dans la mesure où un objet de valeur peut être un tableau de plusieurs objets de valeur, vous pouvez résoudre ce problème en combinant les deux éléments `Statement` en un seul élément avec un tableau d'objets, comme illustré dans l'exemple suivant :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

La valeur de l'élément `Statement` est un tableau d'objets. Dans l'exemple, le tableau se compose de deux objets, chaque objet étant une valeur correcte pour un élément `Statement` Les objets du tableau sont séparés par des virgules.

La taille du document de politique dépasse la taille maximale autorisée

La taille maximale d'un document SCP est de 5 120 octets. Cette taille maximale inclut tous les caractères, y compris les espaces blancs. Pour réduire la taille de votre politique SCP, vous pouvez supprimer tous les espaces (comme les espacements et les sauts de ligne) qui ne figurent pas entre guillemets.

> **Note**
>
> Si vous enregistrez la politique en utilisant le AWS Management Console, les espaces blancs supplémentaires entre les éléments JSON et en dehors des guillemets sont supprimés et ne sont pas pris en compte. Si vous enregistrez la politique à l'aide d'une opération du SDK ou

du AWS CLI, elle est enregistrée exactement comme vous l'avez indiqué et aucun caractère n'est automatiquement supprimé.

## Politiques de contrôle des ressources (RCPs)

> **Note**
>
> Politiques de contrôle des services (SCPs) et politiques de contrôle des ressources (RCPs) Utilisez un SCP lorsque vous devez limiter les autorisations des principaux IAM sur les comptes membres de votre organisation.
> Utilisez un RCP lorsque vous devez empêcher les principaux IAM externes aux comptes de votre organisation de faire des demandes d'accès aux ressources des comptes membres de votre organisation.
> Pour plus d'informations, voir Comprendre SCPs et RCPs.

Les politiques de contrôle des ressources (RCPs) sont un type de politique d'organisation que vous pouvez utiliser pour gérer les autorisations au sein de votre organisation. RCPs offrent un contrôle centralisé sur le maximum d'autorisations disponibles pour les ressources de votre organisation. RCPs vous aider à garantir que les ressources de vos comptes respectent les directives de contrôle d'accès de votre organisation. RCPs ne sont disponibles que dans une organisation dont toutes les fonctionnalités sont activées. RCPs ne sont pas disponibles si votre organisation a activé uniquement les fonctionnalités de facturation consolidée. Pour obtenir des instructions sur l'activation RCPs, consultezDésactivation d'un type de politique.

RCPs ne suffisent pas à eux seuls à octroyer des autorisations aux ressources de votre organisation. Aucune autorisation n'est accordée par un RCP. Un RCP définit un garde-fou en matière d'autorisations, ou fixe des limites, aux actions que les identités peuvent effectuer sur les ressources de vos organisations. L'administrateur doit toujours associer des politiques basées sur l'identité aux utilisateurs ou aux rôles IAM, ou des politiques basées sur les ressources aux ressources de vos comptes pour réellement accorder des autorisations. Pour plus d'informations, consultez les sections Politiques basées sur l'identité et politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Les autorisations effectives sont l'intersection logique entre ce qui est autorisé par les RCPs politiques de contrôle des services (SCPs) et ce qui est autorisé par les politiques basées sur l'identité et les ressources.

⚠ RCPs n'affectent pas les ressources du compte de gestion

RCPs n'affectent pas les ressources du compte de gestion. Ils n'affectent que les ressources des comptes membres de votre organisation. Cela signifie également que cela RCPs s'applique aux comptes de membres désignés comme administrateurs délégués.

Rubriques dans cette page



## Liste de Services AWS ce support RCPs

RCPs s'appliquent aux actions suivantes Services AWS :

- Amazon S3
- AWS Security Token Service
- AWS Key Management Service
- Amazon SQS
- AWS Secrets Manager
- Amazon Cognito
- Amazon CloudWatch Logs
- Amazon DynamoDB
- Amazon Elastic Container Registry
- Amazon OpenSearch sans serveur

## Tester les effets de RCPs

AWS vous recommande vivement de ne pas vous rattacher RCPs à la racine de votre organisation sans avoir testé de manière approfondie l'impact de la politique sur les ressources de vos comptes. Vous pouvez commencer par les rattacher RCPs à des comptes de test individuels, les déplacer vers le OUs bas de la hiérarchie, puis gravir les échelons de la structure organisationnelle selon les besoins. L'un des moyens de déterminer l'impact consiste à examiner AWS CloudTrail les journaux pour détecter les erreurs d'accès refusé.

## Taille maximale de RCPs

Tous les caractères de votre RCP sont pris en compte dans sa taille maximale. Les exemples présentés dans ce guide montrent les RCPs fichiers formatés avec des espaces blancs supplémentaires pour améliorer leur lisibilité. Toutefois, pour économiser de l'espace si la taille de votre politique approche de la taille maximale, vous pouvez supprimer les espaces, comme les espacements et les sauts de ligne qui ne figurent pas entre guillemets.

> **Tip**
>
> Utilisez l'éditeur visuel pour créer votre RCP. Il supprime automatiquement les espaces superflus.

## RCPs Attachement aux différents niveaux de l'organisation

Vous pouvez les joindre RCPs directement à des comptes individuels ou à la racine de l'organisation. OUs Pour une explication détaillée du RCPs fonctionnement, voirÉvaluation du RCP.

## Effets du RCP sur les autorisations

RCPs sont un type de politique Gestion des identités et des accès AWS (IAM). Elles sont étroitement liées aux politiques basées sur les ressources. Cependant, un RCP n'accorde jamais d'autorisations. RCPs Il s'agit plutôt de contrôles d'accès qui spécifient les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Logique d'évaluation des politiques dans le Guide de l'utilisateur IAM.

- RCPs s'appliquent aux ressources d'un sous-ensemble de. Services AWS Pour de plus amples informations, veuillez consulter Liste de Services AWS ce support RCPs.

- RCPs affectent uniquement les ressources gérées par des comptes appartenant à l'organisation à laquelle le RCPs. Ils n'affectent pas les ressources provenant de comptes extérieurs à l'organisation. Prenons l'exemple d'un compartiment Amazon S3 appartenant au compte A d'une organisation. La politique de compartiment (une politique basée sur les ressources) accorde l'accès aux utilisateurs depuis le compte B en dehors de l'organisation. Un RCP est joint au compte A. Ce RCP s'applique au compartiment S3 du compte A même lorsque les utilisateurs y accèdent depuis le compte B. Cependant, ce RCP ne s'applique pas aux ressources du compte B lorsque les utilisateurs y accèdent depuis le compte A.
- Un RCP restreint les autorisations pour les ressources dans les comptes des membres. Toute ressource d'un compte possède uniquement les autorisations autorisées par chaque parent supérieur. Si une autorisation est bloquée à un niveau supérieur au compte, une ressource du compte concerné ne dispose pas de cette autorisation, même si le propriétaire de la ressource applique une politique basée sur les ressources qui autorise un accès complet à n'importe quel utilisateur.
- RCPs s'appliquent aux ressources autorisées dans le cadre d'une demande d'opération. Ces ressources se trouvent dans la colonne « Type de ressource » du tableau Action de la référence d'autorisation de service. Si une ressource est spécifiée dans la colonne « Type de ressource », les ressources RCPs du compte principal appelant sont appliquées. `s3:GetObject`Autorise, par exemple, la ressource de l'objet. Chaque fois qu'une `GetObject` demande est faite, un RCP applicable s'applique pour déterminer si le principal demandeur peut invoquer l'`GetObject`opération. Un RCP applicable est un RCP qui a été attaché à un compte, à une unité organisationnelle (UO) ou à la racine de l'organisation propriétaire de la ressource à laquelle vous accédez.
- RCPs affectent uniquement les ressources des comptes des membres de l'organisation. Ils n'ont aucun effet sur les ressources du compte de gestion. Cela signifie également que cela RCPs s'applique aux comptes de membres désignés comme administrateurs délégués. Pour de plus amples informations, veuillez consulter Bonnes pratiques relatives au compte de gestion.
- Lorsqu'un principal fait une demande pour accéder à une ressource d'un compte auquel est attaché un RCP (une ressource associée à un RCP applicable), le RCP est inclus dans la logique d'évaluation des politiques afin de déterminer si l'accès est autorisé ou refusé au principal.
- RCPs ont un impact sur les autorisations effectives des principaux qui tentent d'accéder aux ressources d'un compte membre avec un RCP applicable, que les principaux appartiennent ou non aux mêmes organisations. Cela inclut les utilisateurs root. L'exception est lorsque les principaux sont des rôles liés à un service, car ils ne s'appliquent RCPs pas aux appels effectués par des

rôles liés à un service. Les rôles liés à un service permettent Services AWS d'effectuer les actions nécessaires en votre nom et ne peuvent pas être limités par. RCPs

- Les utilisateurs et les rôles doivent toujours bénéficier d'autorisations conformément aux politiques d'autorisation IAM appropriées, y compris les politiques basées sur l'identité et les ressources. Un utilisateur ou un rôle sans politique d'autorisation IAM n'a aucun accès, même si un RCP applicable autorise tous les services, toutes les actions et toutes les ressources.

## Ressources et entités non limitées par RCPs

Vous ne pouvez pas utiliser RCPs pour restreindre les éléments suivants :

- Toute action sur les ressources du compte de gestion.
- RCPs n'ont aucune incidence sur les autorisations effectives d'un rôle lié à un service. Les rôles liés à un service sont un type unique de rôle IAM directement lié à un AWS service et comprenant toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom. Les autorisations des rôles liés à un service ne peuvent pas être limitées par. RCPs RCPs n'ont pas non plus d'impact sur AWS la capacité des services à assumer un rôle lié au service ; c'est-à-dire que la politique de confiance du rôle lié au service n'est pas non plus affectée par. RCPs
- RCPs ne postulez pas auprès Clés gérées par AWS de AWS Key Management Service. Clés gérées par AWS sont créés, gérés et utilisés en votre nom par un Service AWS. Vous ne pouvez pas modifier ou gérer leurs autorisations.
- RCPs n'ont aucune incidence sur les autorisations suivantes :

| Service | API | Ressources non autorisées par RCPs |
| --- | --- | --- |
| AWS Key Management Service | `kms:RetireGrant` | RCPs n'ont aucune incidence sur l'`kms:RetireGrant` autorisation. Pour plus d'informations sur la manière dont l'autorisation `kms:RetireGrant` est déterminée, consultez la section Retrait et révocation des subventions dans |

| Service | API | Ressources non autorisées par RCPs |
| --- | --- | --- |
| | | le Guide du AWS KMS développeur. |

## Évaluation du RCP

> **Note**
>
> Les informations contenues dans cette section ne s'appliquent pas aux types de politiques de gestion, notamment les politiques de sauvegarde, les politiques de balises, les politiques relatives aux applications de chat ou les politiques de désactivation des services d'intelligence artificielle. Pour de plus amples informations, veuillez consulter Fonctionnement de l'héritage des politiques de gestion.

Comme vous pouvez associer plusieurs politiques de contrôle des ressources (RCPs) à différents niveaux AWS Organizations, comprendre comment RCPs elles sont évaluées peut vous aider à rédiger des politiques RCPs qui donneront le bon résultat.

Stratégie d'utilisation RCPs

La `RCPFullAWSAccess` politique est une politique AWS gérée. Il est automatiquement attaché à la racine de l'organisation, à chaque unité d'organisation et à chaque compte de votre organisation lorsque vous activez les politiques de contrôle des ressources (RCPs). Vous ne pouvez pas dissocier cette politique. Ce RCP par défaut permet à tous les principaux et à toutes les actions de passer par une évaluation RCP, ce qui signifie que jusqu'à ce que vous commenciez à créer et à joindre RCPs, toutes vos autorisations IAM existantes continuent de fonctionner comme elles le faisaient. Cette politique AWS gérée n'accorde pas d'accès.

Vous pouvez utiliser des `Deny` instructions pour bloquer l'accès aux ressources de votre organisation. Lorsqu'une autorisation est refusée pour une ressource d'un compte spécifique, tout RCP partant de la racine et passant par chaque unité d'organisation située sur le chemin direct vers le compte (y compris le compte cible lui-même) peut refuser cette autorisation.

`Deny`les déclarations constituent un moyen efficace de mettre en œuvre des restrictions qui devraient s'appliquer à une plus grande partie de votre organisation. Par exemple, vous pouvez joindre une

politique pour empêcher les identités externes à votre organisation d'accéder au niveau racine de vos ressources. Cette politique sera effective pour tous les comptes de l'organisation. AWS vous recommande vivement de ne pas vous rattacher RCPs à la racine de votre organisation sans avoir testé de manière approfondie l'impact de la politique sur les ressources de vos comptes. Pour de plus amples informations, veuillez consulter Tester les effets de RCPs.

Dans la figure 1, un RCP rattaché à l'unité d'organisation de production possède une `Deny` instruction explicite spécifiée pour un service donné. Par conséquent, le compte A et le compte B se verront refuser l'accès au service car une politique de refus attachée à tous les niveaux de l'organisation est évaluée pour tous les comptes OUs et membres sous-jacents.

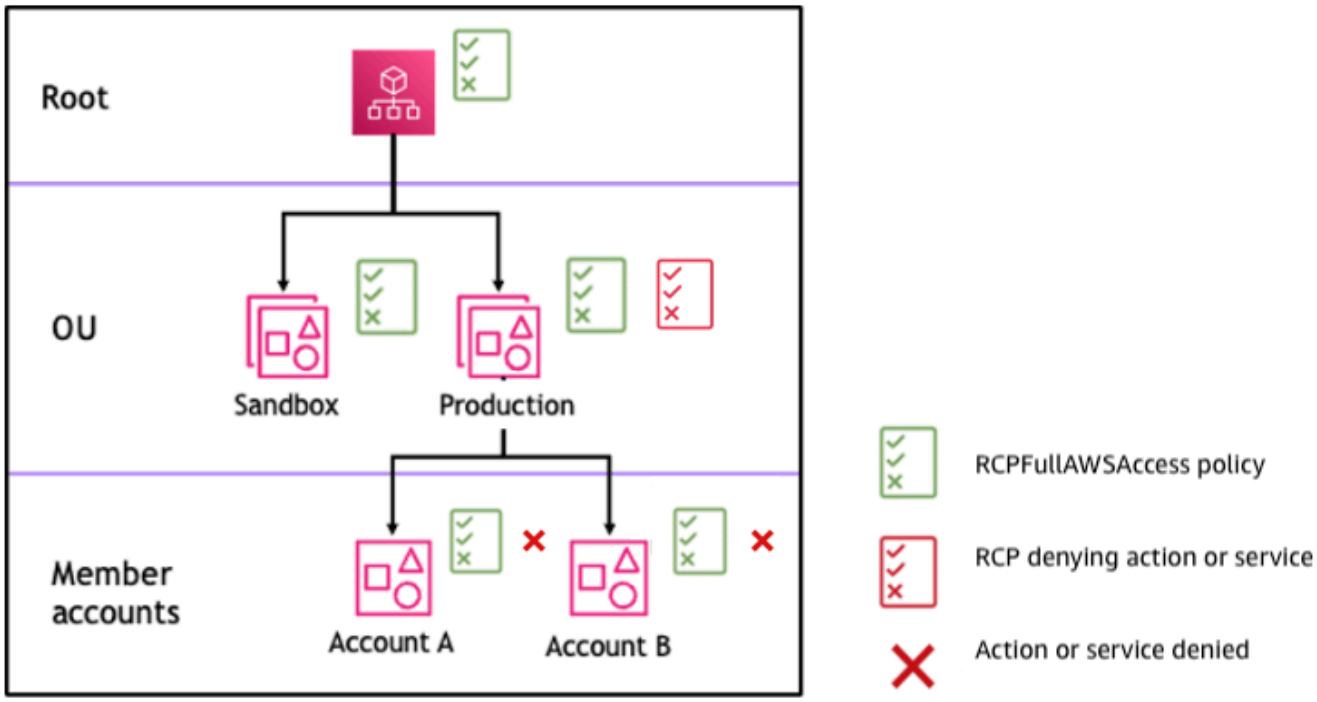



Figure 1 : Exemple de structure organisationnelle avec une *Deny* déclaration jointe à l'unité de production et son impact sur le compte A et le compte B

## Syntaxe d'une RCP

Les politiques de contrôle des ressources (RCPs) utilisent une syntaxe similaire à celle utilisée par les politiques basées sur les ressources. Pour plus d'informations sur les politiques IAM et leur syntaxe, consultez Présentation des politiques IAM dans le Guide de l'utilisateur IAM.

Un RCP est structuré selon les règles du JSON. Elle utilise les éléments qui sont décrits dans cette rubrique.

> **Note**
>
> Tous les caractères de votre RCP sont pris en compte dans sa taille maximale. Les exemples présentés dans ce guide montrent les RCPs fichiers formatés avec des espaces blancs supplémentaires pour améliorer leur lisibilité. Toutefois, pour économiser de l'espace si la taille de votre politique approche de la taille maximale, vous pouvez supprimer les espaces, comme les espacements et les sauts de ligne qui ne figurent pas entre guillemets.

Pour des informations générales sur RCPs, voirPolitiques de contrôle des ressources (RCPs).

Récapitulatif des éléments

Le tableau suivant récapitule les éléments de stratégie que vous pouvez utiliser dans RCPs.

> **Note**
>
> L'effet de n'**`Allow`**est pris en charge que pour la **`RCPFullAWSAccess`** politique
> L'effet de n'`Allow`est pris en charge que pour la `RCPFullAWSAccess` politique. Cette politique est automatiquement attachée à la racine de l'organisation, à chaque unité d'organisation et à chaque compte de votre organisation lorsque vous activez les politiques de contrôle des ressources (RCPs). Vous ne pouvez pas dissocier cette politique. Ce RCP par défaut permet à tous les principaux et à toutes les actions de passer par une évaluation RCP, ce qui signifie que jusqu'à ce que vous commenciez à créer et à joindre RCPs, toutes vos autorisations IAM existantes continuent de fonctionner comme elles le faisaient. Cela n'autorise pas l'accès.

| Element | Objectif | |
|---|---|---|
| Version | Spécifie les règles de syntaxe du langage à utiliser pour le traitement de la politique. | |
| Instruction | Sert de conteneur pour les éléments | |

| Element | Objectif |
| --- | --- |
| | de politique. Vous pouvez avoir plusieurs instructions dans RCPs. |
| ID d'instruction (Sid) | (Facultatif) Fournit un nom simple pour l'instruction. |
| Effet | Définit si l'instruction RCP refuse l'accès aux ressources d'un compte. |
| Principal | Spécifie le principal auquel l'accès aux ressources d'un compte est autorisé ou refusé. |
| Action | Spécifie le AWS service et les actions que le RCP autorise ou refuse. |
| Ressource | Spécifie les AWS ressources auxquelles le RCP s'applique. |

| Element | Objectif |
| --- | --- |
| NotResource | Spécifie les AWS ressources exemptées du RCP. Utilisé au lieu de l'élément `Resource`. |
| Condition | Spécifie les conditions lorsque l'instruction est vigueur. |

Rubriques

- Élément Version
- Élément Statement
- Élément ID d'instruction (Sid)
- Élément Effect
- Élément Principal
- Élément Action
- Éléments Resource et NotResource
- Élément Condition
- Élément non pris en charge

### Élément **`Version`**

Chaque RCP doit inclure un `Version` élément avec la valeur**`"2012-10-17"`**. Il s'agit de la même valeur de version que la version la plus récente des politiques d'autorisation IAM.

Pour plus d'informations, consultez Éléments de politique JSON IAM : Version dans le Guide de l'utilisateur IAM.

### Élément **`Statement`**

Un RCP est composé d'un ou de plusieurs `Statement` éléments. Vous ne pouvez avoir qu'un mot clé `Statement` dans une politique, mais la valeur peut être un tableau d'instructions JSON (encadré par des caractères [ ]).

L'exemple suivant montre une instruction unique composée d'`Resource`éléments simples `Effect` `Principal``Action`,, et.

```
 {
    "Statement": {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutBucketPublicAccessBlock",
        "Resource": "*"
    }
}
```

Pour plus d'informations, consultez Éléments de politique JSON IAM : Instruction dans le Guide de l'utilisateur IAM.

### Élément ID d'instruction (**`Sid`**)

L'élément `Sid` est un identifiant facultatif que vous pouvez fournir pour l'instruction de politique. Vous pouvez affecter une valeur `Sid` à chaque instruction d'un tableau d'instructions. L'exemple de RCP suivant montre un exemple d'`Sid`instruction.

```
{
    "Statement": {
        "Sid": "DenyBPAConfigurations",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutBucketPublicAccessBlock",
        "Resource": "*"
    }
}
```

Pour plus d'informations, consultez IAM JSON Policy Elements : Sid dans le guide de l'utilisateur IAM.

### Élément **`Effect`**

Chaque instruction doit contenir un élément `Effect`. En utilisant la valeur de `Deny` dans l'`Effect`élément, vous pouvez restreindre l'accès à des ressources spécifiques ou définir les conditions d'entrée en vigueur. RCPs Pour RCPs que vous puissiez créer cela, la valeur doit êtreDeny. Pour plus d'informations, consultez Évaluation du RCP la section Eléments de politique JSON IAM : effet dans le guide de l'utilisateur IAM.

### Élément **`Principal`**

Chaque déclaration doit contenir l'`Principal`élément. Vous ne pouvez spécifier « * » que dans l'`Principal`élément d'un RCP. Utilisez l'`Conditions`élément pour restreindre des principes spécifiques.

Pour plus d'informations, voir IAM JSON Policy Elements : Principal dans le guide de l'utilisateur IAM.

### Élément **`Action`**

Chaque déclaration doit contenir l'`Action`élément.

La valeur de l'`Action`élément est une chaîne ou une liste (un tableau JSON) de chaînes identifiant les AWS services et les actions autorisés ou refusés par l'instruction.

Chaque chaîne est composée de l'abréviation du service (telle que « s3 », « sqs » ou « sts »), en minuscules, suivie de deux points, puis d'une action de ce service. En général, ils sont tous saisis avec chaque mot commençant par une lettre majuscule et le reste par une minuscule. Par exemple : `"s3:ListAllMyBuckets"`.

Vous pouvez également utiliser des caractères génériques tels que l'astérisque (*) ou le point d'interrogation (?) dans un RCP :

- Utilisez un astérisque (*) en tant que caractère générique pour faire correspondre plusieurs actions partageant une partie d'un nom. La valeur `"s3:*"` signifie toutes les actions dans le service Amazon S3. La valeur `"sts:Get*"` correspond uniquement aux AWS STS actions qui commencent par « Obtenir ».
- Utilisez le caractère générique point d'interrogation (?) pour faire correspondre un seul caractère.

> **Note**
>
> Caractères génériques (*) et points d'interrogation (?) peut être utilisé n'importe où dans le nom de l'action
> Vous ne pouvez pas utiliser « * » dans l'élément Action d'un RCP géré par le client et vous devez spécifier l'abréviation du service (tel que « s3 », « sqs » ou « sts ») auquel vous souhaitez restreindre l'accès.

Pour obtenir la liste des services pris en charge RCPs, consultezListe de Services AWS ce support RCPs. Pour obtenir la liste des actions prises en Service AWS charge, consultez la section Actions, ressources et clés de condition pour les AWS services dans la référence d'autorisation des services.

Pour plus d'informations, consultez Éléments de politique JSON IAM : Action dans le Guide de l'utilisateur IAM.

Éléments **`Resource`** et **`NotResource`**

Chaque instruction doit contenir l'`NotResource`élément `Resource` or.

Vous pouvez utiliser des caractères génériques tels que l'astérisque (*) ou le point d'interrogation (?) dans l'élément ressource :

- Utilisez un astérisque (*) comme caractère générique pour faire correspondre plusieurs ressources qui partagent une partie du même nom.
- Utilisez le caractère générique point d'interrogation (?) pour faire correspondre un seul caractère.

Pour plus d'informations, consultez IAM JSON Policy Elements : Resource et IAM JSON Policy Elements : NotResource dans le guide de l'utilisateur IAM.

Élément **`Condition`**

Vous pouvez spécifier un `Condition` élément dans les instructions de refus d'un RCP.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Ce RCP refuse l'accès aux opérations et aux ressources d'Amazon S3 sauf si la demande est envoyée via un transport sécurisé (la demande a été envoyée via TLS).

Pour plus d'informations, consultez Éléments de politique JSON IAM : Condition dans le Guide de l'utilisateur IAM.

Élément non pris en charge

Les éléments suivants ne sont pas pris en charge dans RCPs :

- `NotPrincipal`
- `NotAction`

## Exemples de politiques de contrôle des ressources

Les exemples de politiques de contrôle des ressources (RCPs) présentés dans cette rubrique sont fournis à titre informatif uniquement.

> **Avant d'utiliser ces exemples**
>
> Avant d'utiliser ces exemples RCPs dans votre organisation, tenez compte des points suivants :
>
> - Les politiques de contrôle des ressources (RCPs) sont destinées à être utilisées comme des contrôles préventifs grossiers et n'accordent pas d'accès. Vous devez toujours associer des politiques basées sur l'identité ou les ressources aux principaux IAM ou aux ressources de vos comptes pour accorder réellement des autorisations. Les autorisations

effectives sont l'intersection logique entre SCP/RCP et une politique d'identité ou une politique de ressources. SCP/RCP Vous pouvez obtenir plus de détails sur les effets du RCP sur les autorisations ici.

- Les politiques de contrôle des ressources de ce référentiel sont présentées à titre d'exemples. Vous ne devez pas joindre une RCPs pièce jointe sans avoir testé de manière approfondie l'impact de la politique sur les ressources de vos comptes. Une fois que vous avez une politique prête à mettre en œuvre, nous vous recommandons de la tester dans une organisation ou une unité d'organisation distincte pouvant représenter votre environnement de production. Une fois le test effectué, vous devez déployer les modifications à tester, OUs puis les déployer progressivement sur un ensemble plus large de données OUs au fil du temps.
- La RCPFullAWSAccesspolitique est automatiquement attachée à la racine de l'organisation, à chaque unité d'organisation et à chaque compte de votre organisation lorsque vous activez les politiques de contrôle des ressources (RCPs). Ce RCP par défaut permet à tous les principaux et à tous les accès aux actions de passer par une évaluation RCP. Vous pouvez utiliser les instructions Deny pour restreindre l'accès aux ressources de votre organisation. Vous devez également accorder les autorisations appropriées à vos principaux en utilisant des politiques basées sur l'identité ou les ressources.
- Lorsqu'elle est attachée à une racine d'organisation, à une unité organisationnelle ou à un compte, une politique de contrôle des ressources (RCP) permet de contrôler de manière centralisée les autorisations maximales disponibles pour les ressources de votre organisation, de votre unité organisationnelle ou d'un compte. Comme un RCP peut être appliqué à plusieurs niveaux dans une organisation, comprendre comment RCPs sont évalués peut vous aider à rédiger des informations RCPs qui produiront les résultats attendus.

Les exemples de politiques présentés dans cette section illustrent la mise en œuvre et l'utilisation de RCPs. Ils ne sont pas destinés à être interprétés comme des recommandations ou des bonnes pratiques AWS officielles à mettre en œuvre exactement comme indiqué. Il est de votre responsabilité de tester soigneusement toute politique afin de déterminer si elle répond aux exigences commerciales de votre environnement. Les politiques de contrôle des ressources basées sur le refus peuvent involontairement limiter ou bloquer votre utilisation des AWS services, sauf si vous ajoutez les exceptions nécessaires à la politique.

> **Tip**
>
> Avant la mise en œuvre RCPs, outre l'examen AWS CloudTrail des journaux, l'évaluation des résultats d'accès externe d'IAM Access Analyzer peut aider à comprendre quelles ressources sont actuellement publiques ou partagées en externe.

GitHub référentiel

- Exemples de politiques de contrôle des ressources - Ce GitHub référentiel contient des exemples de politiques pour démarrer ou affiner votre utilisation de AWS RCPs

# Politiques de gestion dans AWS Organizations

Les politiques de gestion vous permettent de configurer et de gérer Services AWS leurs fonctionnalités de manière centralisée. L'impact de ces politiques sur les comptes OUs et les comptes qui en héritent dépend du type de stratégie de gestion que vous appliquez. AWS Organizations Consultez les rubriques de cette section pour comprendre les termes et concepts pertinents relatifs aux politiques de gestion.

Rubriques

- Conditions préalables et autorisations pour les politiques de gestion pour AWS Organizations
- Fonctionnement de l'héritage des politiques de gestion
- Afficher les politiques de gestion efficaces
- À propos des alertes de politique efficaces non valides
- Politiques déclaratives
- Politiques de sauvegarde
- Politiques de balises
- Politiques relatives aux applications de chat
- Politiques de désactivation des services IA
- Politiques du Security Hub
- Politiques d'Amazon Bedrock
- Politiques d'Amazon Inspector

- Mettre à niveau les politiques de déploiement
- Politiques Amazon S3
- AWS Shield Politiques du directeur de la sécurité réseau

# Conditions préalables et autorisations pour les politiques de gestion pour AWS Organizations

Cette page décrit les prérequis et les autorisations requises pour les politiques de gestion pour AWS Organizations.

Rubriques

- Conditions requises pour les politiques de gestion
- Autorisations pour les politiques de gestion

## Conditions requises pour les politiques de gestion

L'utilisation de politiques de gestion pour une organisation nécessite les éléments suivants :

- Toutes les fonctions doivent être activées pour votre organisation.
- Vous devez être connecté au compte de gestion de votre organisation ou être un administrateur délégué.
- Votre utilisateur ou rôle Gestion des identités et des accès AWS (IAM) doit disposer des autorisations répertoriées dans la section suivante.

## Autorisations pour les politiques de gestion

L'exemple de politique IAM suivant fournit des autorisations pour utiliser tous les aspects des politiques de gestion dans une organisation.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPolicies",
```

```
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur les politiques et les autorisations IAM, consultez le Guide de l'utilisateur IAM.

## Fonctionnement de l'héritage des politiques de gestion

> **Important**
>
> Les informations de cette section ne s'appliquent pas aux politiques d'autorisation : politiques de contrôle des services (SCPs) et politiques de contrôle des ressources (RCPs).

Pour plus d'informations sur le fonctionnement SCPs et le RCPs fonctionnement d'une AWS Organizations hiérarchie, reportez-vous Évaluation du SCP aux sections etÉvaluation du RCP.

Vous pouvez attacher des politiques de gestion à n'importe quelle entité de votre organisation (racine, unité d'organisation [UO] ou compte) :

- Lorsque vous attachez une stratégie de gestion à la racine de l'organisation, tous OUs les comptes de l'organisation héritent de cette politique.
- Lorsque vous attachez une politique de gestion à une UO spécifique, les comptes sous-jacents à cette UO ou à une UO enfant héritent de cette politique.
- Lorsque vous attachez une politique de gestion à un compte spécifique, elle affecte uniquement ce compte.

Étant donné que vous pouvez attacher des politiques de gestion à plusieurs niveaux de l'organisation, les comptes peuvent hériter de plusieurs politiques.

Les rubriques suivantes expliquent comment les politiques relatives aux parents et aux enfants sont intégrées à la politique effective d'un compte.

Rubriques



## Terminologie de l'héritage

Cette rubrique utilise les termes suivants en ce qui concerne l'héritage des politiques de gestion.

Héritage de politique

Interaction des politiques à différents niveaux d'une organisation, allant de la racine supérieure de l'organisation, en passant par la hiérarchie des unités d'organisation (UO) jusqu'aux comptes individuels.

Vous pouvez associer des politiques à la racine de l'organisation OUs, à des comptes individuels et à n'importe quelle combinaison de ces entités d'organisation. L'héritage de politique désigne les politiques attachées à la racine de l'organisation ou à une UO. Tous les comptes membres de la racine de l'organisation ou de l'UO à laquelle une politique de gestion est attachée héritent de cette politique.

Par exemple, lorsque des politiques de gestion sont attachées à la racine de l'organisation, tous les comptes de l'organisation héritent de cette politique. En effet, tous les comptes d'une organisation se trouvent toujours sous la racine de l'organisation. Lorsque vous attachez une politique à une unité d'organisation spécifique, les comptes qui se trouvent directement sous cette unité d'organisation ou sous une unité d'organisation enfant héritent de cette politique. Étant donné que vous pouvez attacher des politiques à plusieurs niveaux de l'organisation, les comptes peuvent hériter de plusieurs documents de politique pour un même type de politique.

Politiques parentes

Politiques attachées plus haut dans l'arborescence de l'organisation que les politiques attachées à des entités plus bas dans l'arborescence.

Par exemple, si vous attachez la politique de gestion A à la racine de l'organisation, il s'agit simplement d'une politique. Si vous attachez également la politique B à une unité d'organisation sous cette racine, la politique A devient la politique parente de la politique B. La politique B est la politique enfant de la politique A. La politique A et la politique B fusionnent pour créer la politique effective pour les comptes de l'unité d'organisation.

Politiques enfants

Politiques attachées à un niveau plus bas dans l'arborescence de l'organisation que la politique parente.

Politiques effectives

Document de politique unique final qui spécifie les règles qui s'appliquent à un compte. La politique effective correspond à l'agrégation de toutes les politiques héritées par le compte, ainsi que des politiques directement attachées au compte. Pour de plus amples informations, veuillez consulter Afficher les politiques de gestion efficaces.

Opérateurs d'héritage

Opérateurs qui contrôlent la façon dont les politiques héritées fusionnent en une seule politique effective. Ces opérateurs sont considérés comme une fonction avancée. Les auteurs de politiques expérimentés peuvent les utiliser pour limiter les modifications qu'une politique enfant peut

apporter et la manière dont les paramètres des politiques fusionnent. Pour de plus amples informations, veuillez consulter Opérateurs d'héritage.

## Syntaxe des politiques et héritage pour les types de politiques de gestion

La manière exacte dont les politiques affectent les comptes OUs et qui en héritent dépend du type de stratégie de gestion que vous choisissez. Les types de politiques de gestion sont les suivants :

- Politiques déclaratives
- Stratégies de sauvegarde
- Stratégies de balises
- Politiques relatives aux applications de chat
- Politiques de désabonnement aux services d'IA
- Politiques du Security Hub
- Politiques de Bedrock
- Politiques relatives aux inspecteurs
- Mettre à niveau les politiques de déploiement
- Politiques S3
- AWS Shield Politiques du directeur de la sécurité réseau

La syntaxe des types de politique de gestion inclut Opérateurs d'héritageles éléments suivants : ils vous permettent de spécifier avec une fine granularité quels éléments des politiques parentes sont appliqués et quels éléments peuvent être remplacés ou modifiés en cas d'héritage par un enfant OUs ou un compte.

La politique efficace est l'ensemble des règles héritées de la racine de l'organisation OUs et associées à celles directement associées au compte. La politique effective spécifie l'ensemble final des règles qui s'appliquent au compte. Vous pouvez afficher la politique effective pour un compte, qui inclut l'effet de tous les opérateurs d'héritage dans les politiques appliquées. Pour de plus amples informations, veuillez consulter Afficher les politiques de gestion efficaces.

## Opérateurs d'héritage

Les opérateurs d'héritage contrôlent la façon dont les politiques héritées et les politiques attachées à un compte fusionnent pour former la politique effective de ce compte. Ces opérateurs comprennent les opérateurs de définition de valeurs et les opérateurs de contrôle enfants.

Lorsque vous utilisez l'éditeur visuel de la AWS Organizations console, vous ne pouvez utiliser que l'`@@assign`opérateur. Les autres opérateurs sont considérés comme une fonction avancée. Pour utiliser les autres opérateurs, vous devez créer la politique JSON manuellement. Les auteurs de politiques expérimentés peuvent utiliser les opérateurs d'héritage pour contrôler les valeurs appliquées à la politique effective et limiter les modifications que les politiques enfants peuvent apporter.

Pour plus d'informations sur le fonctionnement de l'héritage des politiques dans une organisation, consultezExemples d'héritages.

Opérateurs de définition de valeurs

Vous pouvez utiliser les opérateurs de définition de valeurs suivants pour contrôler la façon dont votre politique interagit avec ses politiques parentes :

- `@@assign` : remplace tous les paramètres de politique hérités par les paramètres spécifiés. Si le paramètre spécifié n'est pas hérité, cet opérateur l'ajoute à la politique effective. Cet opérateur peut s'appliquer à n'importe quel paramètre de politique de n'importe quel type.
  - Pour les paramètres à valeur unique, cet opérateur remplace la valeur héritée par la valeur spécifiée.
  - Pour les paramètres à valeurs multiples (tableaux JSON), cet opérateur supprime toutes les valeurs héritées et les remplace par les valeurs spécifiées par cette politique.
- `@@append` : ajoute les paramètres spécifiés (sans en supprimer) aux paramètres hérités. Si le paramètre spécifié n'est pas hérité, cet opérateur l'ajoute à la politique effective. Vous pouvez utiliser cet opérateur avec des paramètres à valeurs multiples uniquement.
  - Cet opérateur ajoute les valeurs spécifiées à toutes les valeurs du tableau hérité.
- `@@remove` : supprime les paramètres hérités spécifiés de la politique effective, s'ils existent. Vous pouvez utiliser cet opérateur avec des paramètres à valeurs multiples uniquement.
  - Cet opérateur supprime uniquement les valeurs spécifiées du tableau de valeurs héritées des politiques parentes. D'autres valeurs peuvent continuer à exister dans le tableau et peuvent être héritées par les politiques enfants.

Opérateurs de contrôle enfants

L'utilisation d'opérateurs de contrôle enfants est facultative. Vous pouvez utiliser l'opérateur `@@operators_allowed_for_child_policies` pour contrôler les opérateurs de définition de valeurs que les politiques enfants peuvent utiliser. Vous pouvez autoriser tous les opérateurs,

certains opérateurs spécifiques, ou aucun opérateur. Par défaut, tous les opérateurs (`@@all`) sont autorisés.

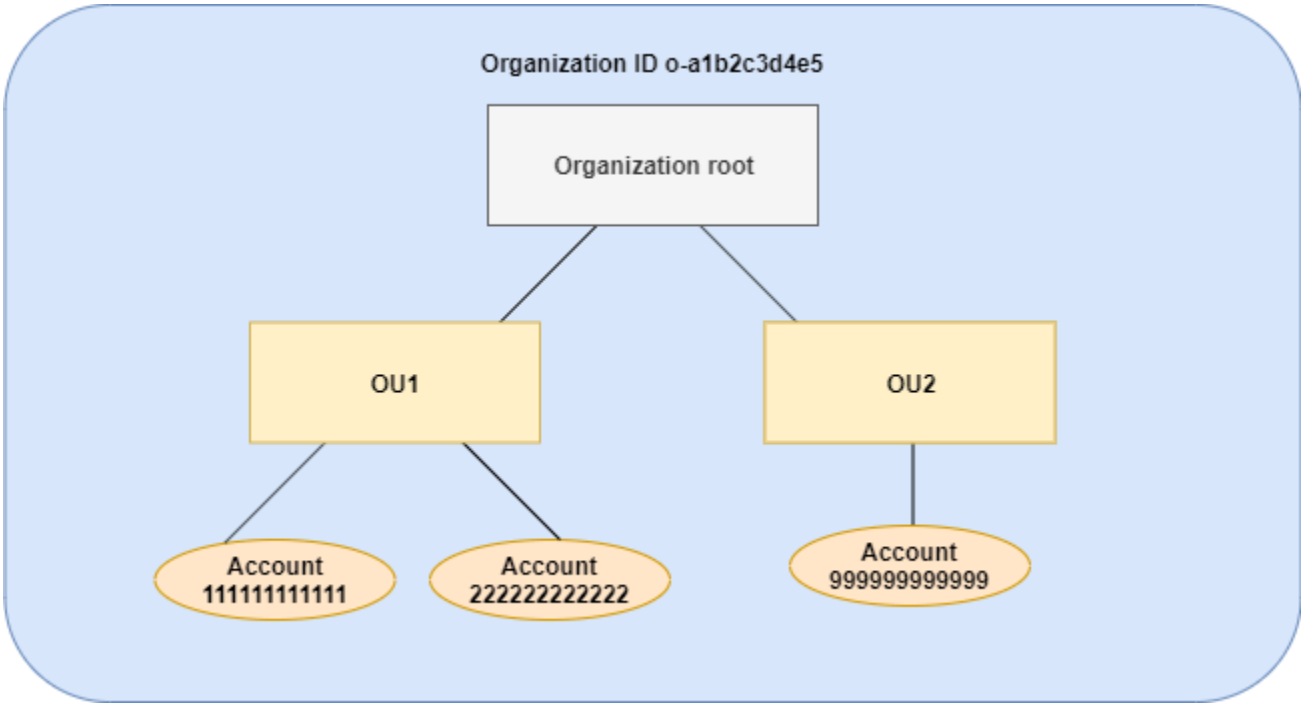
- `"@@operators_allowed_for_child_policies": ["@@all"]` — L'enfant OUs et les comptes peuvent utiliser n'importe quel opérateur dans les politiques. Par défaut, tous les opérateurs sont autorisés dans les politiques enfants.
- `"@@operators_allowed_for_child_policies": ["@@assign", "@@append", "@@remove"]` — L'enfant OUs et les comptes ne peuvent utiliser que les opérateurs spécifiés dans les politiques relatives aux enfants. Vous pouvez spécifier un ou plusieurs opérateurs de définition de valeurs dans cet opérateur de contrôle enfant.
- `"@@operators_allowed_for_child_policies": ["@@none"]` — L'enfant OUs et les comptes ne peuvent pas utiliser d'opérateurs dans les politiques. Vous pouvez utiliser cet opérateur pour verrouiller efficacement les valeurs définies dans une politique parente afin que les politiques enfants ne puissent pas ajouter, compléter ou supprimer ces valeurs.

> **Note**
>
> Si un opérateur de contrôle enfant hérité limite l'utilisation d'un opérateur, vous ne pouvez pas inverser cette règle dans une politique enfant. Si vous incluez des opérateurs de contrôle enfants dans une politique parente, ils limitent les opérateurs de définition de valeurs dans toutes les politiques enfants.

## Exemples d'héritages

Ces exemples illustrent le fonctionnement de l'héritage de politiques. Ils indiquent comment les politiques de balises parentes et enfants sont fusionnées en une politique de balises effective pour un compte.

Les exemples supposent que vous disposez de la structure d'organisation présentée dans le diagramme suivant.




Exemples

- Exemple 1 : Autoriser les stratégies enfants à remplacer uniquement les valeurs de balise
- Exemple 2 : Ajouter de nouvelles valeurs aux balises héritées
- Exemple 3 : Supprimer des valeurs de balises héritées
- Exemple 4 : Restreindre les modifications dans les politiques enfants
- Exemple 5 : Conflits avec les opérateurs de contrôle enfants
- Exemple 6 : Conflits liés à l'ajout de valeurs au même niveau de hiérarchie

Exemple 1 : Autoriser les stratégies enfants à remplacer uniquement les valeurs de balise

La politique de balises suivante définit la clé de balise `CostCenter` et deux valeurs admises : `Development` et `Support`. Si vous l'attachez à la racine de l'organisation, la politique de balises s'applique à tous les comptes de l'organisation.

Politique A : politique d'identifications attachée à la racine de l'organisation

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
```

```
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Supposons que vous souhaitiez que les OU1 utilisateurs utilisent une valeur de balise différente pour une clé et que vous souhaitiez appliquer la politique de balise pour des types de ressources spécifiques. Étant donné que la politique A ne spécifie pas les opérateurs de contrôle enfants qui sont autorisés, tous les opérateurs sont autorisés. Vous pouvez utiliser l'`@@assign`opérateur et créer une politique de balises telle que la suivante à laquelle vous pouvez vous associer OU1.

Stratégie B — politique des OU1 balises

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

La spécification de l'opérateur `@@assign` pour la balise entraîne le résultat suivant lorsque la politique A et la politique B fusionnent pour constituer la politique de balises effective d'un compte :

- La politique B remplace les deux valeurs de balise spécifiées dans la politique parente (la politique A). Le résultat est que `Sandbox` est la seule valeur conforme pour la clé de balise `CostCenter`.
- L'ajout de `enforced_for` indique que la balise `CostCenter` doit être la valeur de balise spécifiée sur toutes les ressources Amazon Redshift et les tables Amazon DynamoDB.

Comme le montre le diagramme, OU1 inclut deux comptes : 111111111111 et 222222222222.

Stratégie de balise effective obtenue pour les comptes 111111111111 et 222222222222

> **Note**
>
> Vous ne pouvez pas utiliser directement le contenu d'une politique effective affichée comme contenu d'une nouvelle politique. La syntaxe n'inclut pas les opérateurs nécessaires pour contrôler la fusion avec d'autres politiques enfants et parentes. L'affichage d'une politique effective n'a pour but que de comprendre les résultats de la fusion.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Exemple 2 : Ajouter de nouvelles valeurs aux balises héritées

Dans certains cas, vous souhaitez que tous les comptes de votre organisation spécifient une clé de balise avec une courte liste de valeurs admises. Pour les comptes d'une unité d'organisation, vous souhaiterez peut-être autoriser une valeur supplémentaire que seuls ces comptes peuvent spécifier

lors de la création de ressources. Cet exemple spécifie la procédure à suivre à l'aide de l'opérateur `@@append`. L'opérateur `@@append` est une fonction avancée.

Comme pour l'exemple 1, cet exemple commence par la politique A comme politique de balises attachée à la racine de l'organisation.

Politique A : politique d'identifications attachée à la racine de l'organisation

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Pour cet exemple, attachez la politique C à OU2. La différence dans cet exemple est que l'utilisation de l'opérateur `@@append` dans la politique C ajoute des valeurs à la liste des valeurs admises ainsi que la règle `enforced_for` plutôt que d'écraser la liste.

Stratégie C — politique de OU2 balises pour l'ajout de valeurs

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
```

```
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

L'association de la politique C à OU2 a les effets suivants lorsque la politique A et la politique C fusionnent pour former la politique de balises effective pour un compte :

- Étant donné que la politique C inclut l'opérateur `@@append`, elle permet d'ajouter des valeurs à la liste des valeurs de balise admises spécifiées dans la politique A (plutôt que d'écraser la liste).
- Comme dans la politique B, l'ajout de `enforced_for` indique que la balise `CostCenter` doit être utilisée comme valeur de balise spécifiée sur toutes les ressources Amazon Redshift et les tables Amazon DynamoDB. L'écrasement (`@@assign`) et l'ajout (`@@append`) ont le même effet si la politique parente n'inclut pas d'opérateur de contrôle enfant qui limite les valeurs qu'une politique enfant peut spécifier.

Comme le montre le schéma, OU2 inclut un compte : 999999999999. La politique A et la politique C fusionnent pour créer la politique de balises effective du compte 999999999999.

Stratégie de balise effective pour le compte 999999999999

> **Note**
>
> Vous ne pouvez pas utiliser directement le contenu d'une politique effective affichée comme contenu d'une nouvelle politique. La syntaxe n'inclut pas les opérateurs nécessaires pour contrôler la fusion avec d'autres politiques enfants et parentes. L'affichage d'une politique effective n'a pour but que de comprendre les résultats de la fusion.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
```

```
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Exemple 3 : Supprimer des valeurs de balises héritées

Dans certains cas, la politique de balises attachée à l'organisation peut définir plus de valeurs de balise que vous ne souhaitez qu'un compte en utilise. Cet exemple décrit comment réviser une politique de balise à l'aide de l'opérateur `@@remove`. `@@remove` est une fonction avancée.

Comme pour les autres exemples, cet exemple commence par la politique A comme politique de balises attachée à la racine de l'organisation.

Politique A : politique d'identifications attachée à la racine de l'organisation

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Pour cet exemple, attachez la politique D au compte 999999999999.

Politique D : politique d'identifications attachée au compte 999999999999 pour supprimer des valeurs

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

L'attachement de la politique D au compte 999999999999 a les effets suivants lorsque la politique A, la politique C et la politique D fusionnent pour constituer la politique de balises effective :

- En supposant que vous ayez suivi tous les exemples précédents, les politiques B, C et C sont des politiques secondaires de A. La politique B est uniquement attachée à OU1, elle n'a donc aucun effet sur le compte 9999999999999.
- Pour le compte 9999999999999, la seule valeur admise pour la clé de balise `CostCenter` est `Support`.
- La conformité n'est pas appliquée pour la clé de balise `CostCenter`.

Nouvelle stratégie de balise effective pour le compte 999999999999

> **Note**
>
> Vous ne pouvez pas utiliser directement le contenu d'une politique effective affichée comme contenu d'une nouvelle politique. La syntaxe n'inclut pas les opérateurs nécessaires pour contrôler la fusion avec d'autres politiques enfants et parentes. L'affichage d'une politique effective n'a pour but que de comprendre les résultats de la fusion.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Si vous ajoutez ultérieurement d'autres comptes OU2, leurs politiques en matière de balises en vigueur seront différentes de celles du compte 999999999999. En effet, la politique D plus restrictive n'est attachée qu'au niveau du compte et pas à l'unité d'organisation.

Exemple 4 : Restreindre les modifications dans les politiques enfants

Vous souhaiterez peut-être, dans certains cas, restreindre les modifications apportées dans les politiques enfants. Cet exemple décrit la procédure à suivre à l'aide d'opérateurs de contrôle enfants.

Cet exemple commence par une nouvelle politique de balises attachée à la racine de l'organisation et suppose que les politiques de balises ne sont pas encore attachées aux entités d'organisation.

Politique E : politique de balises attachée à la racine de l'organisation pour restreindre les modifications apportées dans les politiques enfants

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
```

```
}
```

Lorsque vous attachez la politique E à la racine de l'organisation, elle empêche les politiques enfants de modifier la clé de balise `Project`. Les politiques enfants peuvent cependant remplacer ou ajouter des valeurs de balise.

Supposons que vous attachez ensuite la politique F suivante à une unité d'organisation.

Politique F : politique d'identifications attachée à une unité organisationnelle

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

La fusion de la politique E et de la politique F a les effets suivants sur les comptes de l'unité d'organisation :

- La politique F est une politique enfant de la politique E.
- La politique F tente de modifier le traitement de la casse, mais elle ne le peut pas. En effet, la politique E inclut l'opérateur `"@@operators_allowed_for_child_policies": ["@@none"]` pour la clé de balise.
- La politique F peut cependant ajouter des valeurs de balises pour la clé. En effet, la politique E inclut `"@@operators_allowed_for_child_policies": ["@@append"]` comme valeur de balise.

Stratégie effective pour les comptes de l'unité organisationnelle

> **Note**
>
> Vous ne pouvez pas utiliser directement le contenu d'une politique effective affichée comme contenu d'une nouvelle politique. La syntaxe n'inclut pas les opérateurs nécessaires pour contrôler la fusion avec d'autres politiques enfants et parentes. L'affichage d'une politique effective n'a pour but que de comprendre les résultats de la fusion.

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Exemple 5 : Conflits avec les opérateurs de contrôle enfants

Des opérateurs de contrôle enfants peuvent figurer dans des politiques de balises attachées au même niveau dans la hiérarchie de l'organisation. Dans ce cas, l'intersection des opérateurs autorisés est utilisée lorsque les politiques fusionnent pour constituer la politique effective des comptes.

Supposons que la politique G et la politique H sont attachées à la racine de l'organisation.

Politique G : politique d'identifications 1 attachée à la racine de l'organisation

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
```

```
        }
    }
}
```

Politique H : politique d'identifications 2 attachée à la racine de l'organisation

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

Dans cet exemple, une politique attachée à la racine de l'organisation définit que les valeurs de la clé de balise peuvent uniquement être complétées. L'autre politique attachée à la racine de l'organisation permet aux politiques enfants d'ajouter et de supprimer des valeurs. L'intersection de ces deux autorisations est utilisée pour les politiques enfants. Le résultat est que les politiques enfants peuvent ajouter des valeurs, mais pas les supprimer. Par conséquent, la politique enfant peut ajouter une valeur à la liste des valeurs de balise, mais ne peut pas supprimer la valeur `Maintenance`.

Exemple 6 : Conflits liés à l'ajout de valeurs au même niveau de hiérarchie

Vous pouvez attacher plusieurs politiques de balises à chaque entité d'organisation. Lorsque vous effectuez cette opération, les politiques de balises attachées à la même entité d'organisation peuvent inclure des informations conflictuelles. Ces politiques sont évaluées en fonction de l'ordre dans lequel elles ont été attachées à l'entité d'organisation. Pour changer l'ordre d'évaluation des politiques, vous pouvez détacher une politique, puis la rattacher.

Supposons que la politique J est attachée à la racine de l'organisation en premier, puis que la politique K est attachée à la racine de l'organisation.

PolitiqueJ : première politique d'identifications attachée à la racine de l'organisation

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
```

```
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

Politique K : deuxième politique d'identifications attachée à la racine de l'organisation

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

Dans cet exemple, la clé de balise `PROJECT` est utilisée dans la politique de balises effective car la politique qui l'a définie a été attachée à la racine de l'organisation en premier.

Politique JK : politique d'identifications effective du compte

La politique effective du compte est la suivante.

> **Note**
>
> Vous ne pouvez pas utiliser directement le contenu d'une politique effective affichée comme contenu d'une nouvelle politique. La syntaxe n'inclut pas les opérateurs nécessaires pour contrôler la fusion avec d'autres politiques enfants et parentes. L'affichage d'une politique effective n'a pour but que de comprendre les résultats de la fusion.

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
```

```
            ]
        }
    }
}
```

# Afficher les politiques de gestion efficaces

Déterminez la politique de gestion efficace pour un compte au sein de votre organisation.

## Qu'est-ce qu'une politique de gestion efficace ?

La politique effective spécifie les règles finales qui s'appliquent à et Compte AWS pour un type de stratégie de gestion. Il s'agit de l'agrégation d'une politique de gestion dont le compte hérite, ainsi que de toutes les politiques relatives à ce type de stratégie de gestion directement associées au compte. Lorsque vous associez une politique de gestion à la racine de l'organisation, elle s'applique à tous les comptes de votre organisation. Lorsque vous associez une politique de gestion à une unité organisationnelle (UO), elle s'applique à tous OUs les comptes appartenant à l'UO. Lorsque vous associez une politique de gestion directement à un compte, elle ne s'applique qu'à celui-ci Compte AWS.

Pour de plus amples informations sur la façon dont les politiques de désactivation des services IA se combinent pour former politique effective finale, consultez Fonctionnement de l'héritage des politiques de gestion.

### Exemple de politique de sauvegarde

La politique de sauvegarde attachée à la racine de l'organisation peut spécifier que tous les comptes de l'organisation sauvegardent toutes les tables Amazon DynamoDB avec une fréquence de sauvegarde par défaut d'une fois par semaine. Une politique de sauvegarde séparée directement attachée à un compte membre contenant des informations critiques dans une table peut remplacer la fréquence par une valeur d'une fois par jour. La combinaison de ces politiques de sauvegarde constitue la politique de sauvegarde effective. Cette politique de sauvegarde effective est déterminée individuellement pour chaque compte de l'organisation. Le résultat de cet exemple est que tous les comptes de l'organisation sauvegardent leurs tables DynamoDB une fois par semaine, à l'exception d'un compte qui les sauvegarde chaque jour.

### Exemple de politique en matière de balises

La politique de balises attachée à la racine de l'organisation peut définir une `CostCenter` balise avec quatre valeurs conformes. Une autre politique de balises attachée au compte peut limiter la clé

`CostCenter` à seulement deux des quatre valeurs conformes. La combinaison de ces politiques de balises constitue la politique de balises effective. Au final, seules deux des quatre valeurs de balise conformes définies dans la politique de balises attachée à la racine de l'organisation sont conformes pour le compte.

Exemple de politique d'applications de chat

Amazon Q Developer dans les applications de chat réévaluera tout développeur Amazon Q créé précédemment dans les configurations d'applications de chat par rapport aux politiques d'applications de chat en vigueur et refusera toute action précédemment autorisée si elle est conforme aux paramètres autorisés et aux garde-fous de la politique effective. La politique en vigueur pour un compte membre définit les paramètres et les garde-fous autorisés. Par exemple, si une politique d'applications de chat interdisant l'accès aux chaînes publiques Slack est appliquée à un compte membre, le développeur Amazon Q existant dans les configurations d'applications de chat pour les chaînes publiques Slack du compte membre sera désactivé. Amazon Q Developer dans les applications de chat n'enverra pas de notifications et les membres de la chaîne ne pourront exécuter aucune tâche dans le canal bloqué. Dans la console des applications de chat Amazon Q Developer, les canaux concernés seront marqués comme désactivés avec un message d'erreur approprié à côté.

Exemple de désabonnement aux services d'IA

La politique de désactivation des services d'intelligence artificielle attachée à la racine de l'organisation peut spécifier que tous les comptes de l'organisation refusent l'utilisation du contenu par tous les services d'apprentissage AWS automatique. Une politique distincte de désactivation des services IA attachée directement à un compte membre spécifie qu'il accepte l'utilisation du contenu uniquement pour Amazon Rekognition. La combinaison de ces politiques de désactivation des services IA constitue la politique effective de désactivation des services IA. Par conséquent, tous les comptes de l'organisation sont désactivés Services AWS, à l'exception d'un compte qui souscrit à Amazon Rekognition.

## Comment consulter la politique de gestion efficace

Vous pouvez consulter la politique effective d'un type de politique de gestion pour un compte à partir de l' AWS Management Console AWS API ou AWS Command Line Interface.

> **Autorisations minimales**
>
> Pour consulter la politique effective d'un type de stratégie de gestion pour un compte, vous devez être autorisé à exécuter les actions suivantes :

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations

### AWS Management Console

Pour consulter la politique effective d'un type de politique de gestion pour un compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la Comptes AWSpage, choisissez le nom du compte pour lequel vous souhaitez consulter la politique effective. Vous devrez peut-être développer OUs (choisir le ) pour trouver le compte que vous souhaitez.
3. Dans l'onglet Stratégies, choisissez le type de stratégie de gestion pour lequel vous souhaitez afficher la politique effective.
4. Choisissez Afficher la politique effective pour cela Compte AWS.

   La console affiche la politique effective appliquée au compte spécifié.

   > **Note**
   >
   > Vous ne pouvez pas copier-coller une politique efficace et l'utiliser comme JSON pour une autre politique sans modifications importantes. Les documents de politique doivent inclure les opérateurs d'héritage qui spécifient comment chaque paramètre est fusionné dans la politique effective finale.

### AWS CLI & AWS SDKs

Pour consulter la politique effective d'un type de politique de gestion pour un compte

Vous pouvez utiliser l'une des méthodes suivantes pour afficher la politique effective :

- AWS CLI: describe-effective-policy

L'exemple suivant illustre la politique effective de désactivation des services IA pour un compte.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

Pour plus d'informations sur les situations dans lesquelles une politique efficace peut devenir non valide, consultez la section Affichage des alertes de stratégie non valides.

## À propos des alertes de politique efficaces non valides

Les alertes de politique non valides vous informent des politiques efficaces non valides et fournissent des mécanismes (APIs) pour identifier les comptes dont les politiques ne sont pas valides. AWS Organizations vous avertit de manière asynchrone lorsque la politique effective de l'un de vos comptes n'est pas valide. La notification apparaît sous forme de bannière sur la page de AWS Organizations console et est enregistrée en tant qu' AWS CloudTrail événement.

### Détectez les politiques de gestion efficaces non valides dans votre organisation

Vous pouvez consulter les politiques de gestion efficaces non valides de votre organisation de plusieurs manières : depuis la console de AWS gestion, l' AWS API, l'interface de ligne de AWS commande (CLI) ou sous forme d' AWS CloudTrail événement.

> **Autorisations minimales**
>
> Pour trouver les informations relatives aux politiques efficaces non valides d'un type de stratégie de gestion dans votre organisation, vous devez être autorisé à exécuter les actions suivantes :

- `organizations:ListAccountsWithInvalidEffectivePolicy`
- `organizations:ListEffectivePolicyValidationErrors`
- `organizations:ListRoots`- obligatoire uniquement lors de l'utilisation de la console Organizations

AWS Management Console

Pour afficher les politiques de gestion efficaces non valides depuis la console

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la Comptes AWSpage de page, si les politiques en vigueur de votre organisation ne sont pas valides, une bannière d'avertissement s'affiche en haut de la page.
3. Dans la bannière, cliquez sur Afficher les problèmes détectés pour afficher la liste de tous les comptes de votre organisation dont les politiques en vigueur ne sont pas valides.
4. Pour chaque compte de la liste, sélectionnez Afficher les problèmes pour obtenir plus d'informations sur les erreurs associées à chaque compte figurant dans les sections Problèmes de politique efficaces de cette page.

AWS CLI & AWS SDKs

Pour consulter la politique effective d'un type de politique de gestion pour un compte

Les commandes suivantes vous permettent d'afficher les comptes dont les politiques efficaces ne sont pas valides.

- AWS CLI: list-accounts-with-invalid-politique efficace
- AWS SDKs: ListAccountsWithInvalidEffectivePolicy

Les commandes suivantes vous aident à visualiser les erreurs de politique effectives sur un compte.

- AWS CLI: list-effective-policy-validation-erreurs
- AWS SDKs: ListEffectivePolicyValidationErrors

AWS CloudTrail

Vous pouvez utiliser les AWS CloudTrail événements pour surveiller les cas où les comptes de votre organisation sont dotés de politiques de gestion efficaces non valides et lorsque ces politiques sont corrigées. Pour plus d'informations, consultez la section Exemples de politiques efficaces dans Comprendre les entrées des fichiers AWS Organizations journaux.

Si vous recevez une notification de politique effective non valide, vous pouvez naviguer dans la AWS Organizations console ou les appeler APIs depuis votre compte de gestion ou d'administrateur délégué pour obtenir plus de détails sur le statut de comptes et de politiques spécifiques :

- `ListAccountsWithInvalidEffectivePolicy`— Renvoie une liste des comptes de l'organisation dont les politiques effectives d'un type spécifié ne sont pas valides.
- `ListEffectivePolicyValidationErrors`— Renvoie la liste des erreurs de validation pour un compte et un type de politique de gestion spécifiés. Les erreurs de validation contiennent des détails, notamment le code d'erreur, la description de l'erreur et les politiques contributives qui ont rendu la politique effective invalide.

## Quand une politique de gestion efficace peut être considérée comme non valide

Les politiques efficaces d'un compte peuvent devenir invalides si elles enfreignent les contraintes définies pour le type de politique en question. Par exemple, il se peut qu'il manque un paramètre obligatoire dans la politique effective finale ou qu'il dépasse certains quotas définis pour le type de stratégie.

Exemple de politique de sauvegarde

Supposons que vous créiez une politique de sauvegarde comportant neuf règles de sauvegarde et que vous l'associiez à la racine de votre organisation. Plus tard, vous créez une autre politique de sauvegarde pour le même plan de sauvegarde (avec deux règles supplémentaires) et vous l'associez à n'importe quel compte de l'organisation. Dans ce cas, il existe une politique en vigueur non valide sur le compte. Elle n'est pas valide car l'agrégation des deux politiques définit 11 règles pour le plan de sauvegarde. La limite est de 10 règles de sauvegarde par plan.

> **Warning**
>
> Si un compte de l'organisation possède une politique effective non valide, ce compte ne recevra pas de mises à jour de politique effectives pour le type de politique en question.

Elle se poursuit avec la dernière politique valide appliquée pour le compte, sauf si toutes les erreurs sont corrigées.

Exemples d'erreurs possibles pour des politiques efficaces

- `ELEMENTS_TOO_MANY`— Se produit lorsqu'un attribut spécifique d'une politique effective dépasse la limite autorisée, par exemple lorsque plus de 10 règles sont définies pour un plan de sauvegarde.
- `ELEMENTS_TOO_FEW`— Se produit lorsqu'un attribut particulier d'une politique efficace n'atteint pas la limite minimale, par exemple lorsqu'aucune région n'est définie pour un plan de sauvegarde.
- `KEY_REQUIRED`— Se produit lorsqu'une configuration requise est absente de la politique effective, par exemple lorsqu'une règle de sauvegarde est absente d'un plan de sauvegarde.

AWS Organizations valide les politiques efficaces avant de les appliquer aux comptes de votre organisation. Ce processus d'audit est particulièrement utile si votre structure organisationnelle est importante et si les politiques de votre organisation sont gérées par plusieurs équipes.

## Politiques déclaratives

Les politiques déclaratives vous permettent de déclarer et d'appliquer de manière centralisée la configuration souhaitée pour une donnée Service AWS à grande échelle au sein d'une organisation. Une fois connectée, la configuration est toujours maintenue lorsque le service ajoute de nouvelles fonctionnalités ou APIs. Utilisez des politiques déclaratives pour empêcher les actions non conformes. Par exemple, vous pouvez bloquer l'accès public à Internet aux ressources Amazon VPC au sein de votre organisation.

Les principaux avantages de l'utilisation de politiques déclaratives sont les suivants :

- Facilité d'utilisation : vous pouvez appliquer la configuration de base pour un Service AWS avec quelques sélections dans les AWS Control Tower consoles AWS Organizations et ou avec quelques commandes à l'aide du AWS CLI & AWS SDKs.
- Définissez une fois et oubliez : la configuration de base d'un Service AWS est toujours maintenue, même lorsque le service introduit de nouvelles fonctionnalités ou APIs. La configuration de base est également maintenue lorsque de nouveaux comptes sont ajoutés à une organisation ou lorsque de nouveaux directeurs et ressources sont créés.

- Transparence : le rapport sur l'état du compte vous permet de consulter l'état actuel de tous les attributs pris en charge par les politiques déclaratives applicables aux comptes concernés. Vous pouvez également créer des messages d'erreur personnalisables, qui peuvent aider les administrateurs à rediriger les utilisateurs finaux vers des pages wiki internes ou fournir un message descriptif qui peut aider les utilisateurs finaux à comprendre pourquoi une action a échoué.

Pour obtenir la liste complète des attributs Services AWS et des attributs pris en charge, consultezSupporté Services AWS et attributs.

Rubriques



## Comment fonctionnent les politiques déclaratives

Les politiques déclaratives sont appliquées dans le plan de contrôle du service, ce qui constitue une distinction importante par rapport aux politiques d'autorisation telles que les politiques de contrôle des services (SCPs) et les politiques de contrôle des ressources (RCPs). Alors que les politiques d'autorisation réglementent l'accès APIs, les politiques déclaratives sont appliquées directement au niveau du service pour faire respecter une intention durable. Cela garantit que la configuration de base est toujours appliquée, même lorsque de nouvelles fonctionnalités APIs sont introduites par le service.

Le tableau suivant permet d'illustrer cette distinction et fournit quelques cas d'utilisation.

| | Politiques de contrôle des services | Politiques de contrôle des ressources | Politiques déclaratives | | |
|---|---|---|---|---|---|
| Pourquoi ? | Définir et appliquer de manière centralisée des contrôles d'accès cohérents sur les principaux acteurs (tels que les utilisateurs IAM et les rôles IAM) à grande échelle. | Pour définir et appliquer de manière centralisée des contrôles d'accès cohérents sur les ressources à grande échelle | Définir et appliquer de manière centralisée la configuration de base pour les AWS services à grande échelle. | | |
| Comment ? | En contrôlant les autorisations d'accès maximales disponibles pour les principaux au niveau de l'API. | En contrôlant les autorisations d'accès maximales disponibles pour les ressources au niveau de l'API. | En appliquant la configuration souhaitée d'un Service AWS sans utiliser d'actions d'API. | | |
| Gère les rôles liés aux services ? | Non | Non | Oui | | |
| Mécanisme de feedback | Erreur SCP refusée à un accès non | Erreur RCP refusée à un accès non | Message d'erreur personnal | | |

| | Politiques de contrôle des services | Politiques de contrôle des ressources | Politiques déclaratives | | |
|---|---|---|---|---|---|
| | personnal isable. | personnal isable. | isable. Pour de plus amples informati ons, veuillez consulter Messages d'erreur personnal isés pour les politiques déclaratives. | | |
| Exemple de stratégie | Empêcher les comptes des membres de quitter l'organisation | Limitez l'accès à vos ressources aux seules connexions HTTPS | Paramètres des images autorisées | | |

Une fois que vous avez créé et joint une politique déclarative, celle-ci est appliquée et appliquée dans l'ensemble de votre organisation. Les politiques déclaratives peuvent être appliquées à l'ensemble d'une organisation, à des unités organisationnelles (OUs) ou à des comptes. Les comptes rejoignant une organisation hériteront automatiquement de la politique déclarative de l'organisation. Pour de plus amples informations, veuillez consulter Fonctionnement de l'héritage des politiques de gestion.

La politique efficace est l'ensemble des règles héritées de la racine de l'organisation OUs et associées à celles directement associées au compte. La politique effective spécifie l'ensemble final des règles qui s'appliquent au compte. Pour de plus amples informations, veuillez consulter Afficher les politiques de gestion efficaces.

Si une politique déclarative est détachée, l'état de l'attribut revient à son état précédent avant que la politique déclarative ne soit attachée.

## Messages d'erreur personnalisés pour les politiques déclaratives

Les politiques déclaratives vous permettent de créer des messages d'erreur personnalisés. Par exemple, si une opération d'API échoue en raison d'une politique déclarative, vous pouvez définir le message d'erreur ou fournir une URL personnalisée, telle qu'un lien vers un wiki interne ou un lien vers un message décrivant l'échec. Si vous ne spécifiez pas de message d'erreur personnalisé, AWS Organizations fournit le message d'erreur par défaut suivant :`Example: This action is denied due to an organizational policy in effect`.

Vous pouvez également auditer le processus de création de politiques déclaratives, de mise à jour des politiques déclaratives et de suppression de politiques déclaratives avec. AWS CloudTrail CloudTrail peut signaler les défaillances des opérations d'API dues à des politiques déclaratives. Pour plus d'informations, consultez la section Journalisation et surveillance.

> **Important**
>
> N'incluez pas d'informations personnelles identifiables (PII) ou d'autres informations sensibles dans un message d'erreur personnalisé. Les informations personnelles incluent des informations générales qui peuvent être utilisées pour identifier ou localiser une personne. Il couvre des dossiers tels que les dossiers financiers, médicaux, éducatifs ou liés à l'emploi. Les exemples d'informations personnelles incluent les adresses, les numéros de compte bancaire et les numéros de téléphone.

## Rapport sur l'état du compte pour les politiques déclaratives

Le rapport sur l'état du compte vous permet de consulter l'état actuel de tous les attributs pris en charge par les politiques déclaratives applicables aux comptes concernés. Vous pouvez choisir les comptes et les unités organisationnelles (OUs) à inclure dans le champ d'application du rapport, ou choisir une organisation entière en sélectionnant la racine.

Ce rapport vous aide à évaluer le niveau de préparation en fournissant une ventilation par région et en indiquant si l'état actuel d'un attribut est uniforme sur tous les comptes (par le biais du`numberOfMatchedAccounts`) ou incohérent (par le`numberOfUnmatchedAccounts`). Vous pouvez également voir la valeur la plus fréquente, qui est la valeur de configuration la plus fréquemment observée pour l'attribut.

Dans la figure 1, un rapport d'état des comptes généré montre l'uniformité entre les comptes pour les attributs suivants : VPC Block Public Access et Image Block Public Access. Cela signifie que, pour chaque attribut, tous les comptes concernés ont la même configuration pour cet attribut.

Le rapport d'état des comptes généré indique des comptes incohérents pour les attributs suivants : paramètres d'images autorisés, valeurs par défaut des métadonnées d'instance, accès à la console série et accès public par blocage des instantanés. Dans cet exemple, chaque attribut présentant un compte incohérent est dû à l'existence d'un compte avec une valeur de configuration différente.

Si une valeur est la plus fréquente, elle est affichée dans la colonne correspondante. Pour des informations plus détaillées sur ce que contrôle chaque attribut, consultez Syntaxe de politique déclarative et exemples de politiques.

Vous pouvez également développer un attribut pour voir la répartition par région. Dans cet exemple, l'accès public au bloc d'images est étendu et, dans chaque région, vous pouvez constater qu'il existe également une uniformité entre les comptes.

Le choix d'associer une politique déclarative pour appliquer une configuration de base dépend de votre cas d'utilisation spécifique. Utilisez le rapport sur l'état du compte pour vous aider à évaluer votre niveau de préparation avant de joindre une politique déclarative.

Pour plus d'informations, consultez la section Génération du rapport sur l'état du compte.

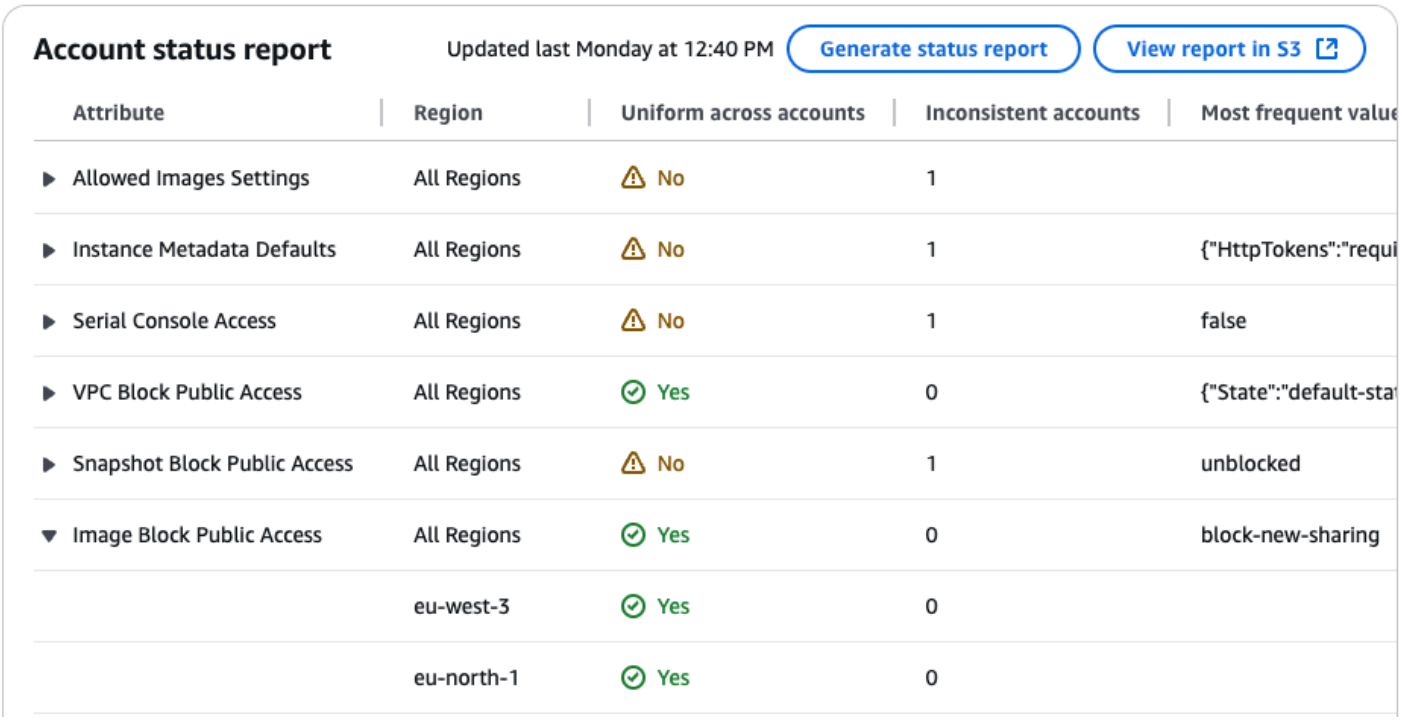


Figure 1 : Exemple de rapport sur l'état du compte avec uniformité entre les comptes pour l'accès public par bloc VPC et pour l'accès public par bloc d'images.

## Supporté Services AWS et attributs

Attributs pris en charge pour les politiques déclaratives pour EC2

Le tableau suivant présente les attributs pris en charge pour les services liés à Amazon EC2.

Politiques déclaratives pour EC2

| AWS service | Attribut | Effet de la politique | Contenu de la politique | En savoir plus |
|---|---|---|---|---|
| Amazon VPC | Accès public aux blocs VPC | Contrôle si les ressources d'Amazon VPCs et des sous-réseaux peuvent accéder à Internet via des passerelles Internet ()IGWs. | Afficher la politique | Pour plus d'informations, consultez Bloquer l'accès public aux sous-réseaux VPCs et aux sous-réseaux dans le guide de l'utilisateur Amazon VPC. |
| Amazon EC2 | Accès à la console série | Contrôle si la console série EC2 est accessible. | Afficher la politique | Pour plus d'informations, consultez Configurer l'accès à la console série EC2 dans le guide de l'utilisateur Amazon Elastic Compute Cloud. |

| AWS service | Attribut | Effet de la politique | Contenu de la politique | En savoir plus |
|---|---|---|---|---|
| | Accès public au bloc d'images | Contrôle si Amazon Machine Images (AMIs) est partageable publiquement. | Afficher la politique | Pour plus d'informations, consultez Comprendre le blocage de l'accès public AMIs dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud. |
| | Paramètres des images autorisées | Contrôle la découverte et l'utilisation d'Amazon Machine Images (AMI) dans Amazon EC2 avec Allowed. AMIs | Afficher la politique | Pour plus d'informations, consultez Amazon Machine Images (AMIs) dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud. |

| AWS service | Attribut | Effet de la politique | Contenu de la politique | En savoir plus |
|---|---|---|---|---|
| | Valeurs par défaut des métadonnées de l'instance | Contrôle les paramètres IMDS par défaut pour tous les lancements de nouvelles instances EC2. | Afficher la politique | Pour plus d'informations, consultez Configurer les options de métadonnées d'instance pour les nouvelles instances dans le guide de l'utilisateur Amazon Elastic Compute Cloud. |
| Amazon EBS | Accès public à Snapshot Block | Contrôle si les instantanés Amazon EBS sont accessibles au public. | Afficher la politique | Pour plus d'informations, consultez Bloquer l'accès public aux instantanés Amazon EBS dans le guide de l'utilisateur d'Amazon Elastic Block Store. |

## Commencer à utiliser les politiques déclaratives

Suivez ces étapes pour commencer à utiliser les politiques déclaratives.

1. Découvrez les autorisations dont vous devez disposer pour effectuer des tâches de politique déclarative.
2. Activez les politiques déclaratives pour votre organisation.

> **Note**
>
> L'activation de l'accès sécurisé est requise
> Vous devez activer l'accès sécurisé pour le service où la politique déclarative appliquera une configuration de base. Cela crée un rôle lié à un service en lecture seule qui est utilisé pour générer le rapport d'état du compte indiquant la configuration existante pour les comptes de votre organisation.
> Utilisation de la console
> Si vous utilisez la console Organizations, cette étape fait partie du processus d'activation des politiques déclaratives.
> À l'aide du AWS CLI
> Si vous utilisez le AWS CLI, il en existe deux distincts APIs :
>
> - EnablePolicyType, que vous utilisez pour activer les politiques déclaratives.
> - Activez AWSService Access, que vous utilisez pour activer un accès sécurisé.
>
> Pour plus d'informations sur la façon d'activer l'accès sécurisé pour un service spécifique à l'aide de la AWS CLI section, Services AWS que vous pouvez utiliser avec AWS Organizations.

3. Exécutez le rapport sur l'état du compte.
4. Créez une politique déclarative.
5. Associez la politique déclarative à la racine, à l'unité d'organisation ou au compte de votre organisation.
6. Consultez la politique déclarative effective combinée qui s'applique à un compte.

Pour effectuer toutes ces étapes, vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

Autres informations

- Apprenez la syntaxe des politiques déclaratives et consultez des exemples de politiques

## Bonnes pratiques d'utilisation des politiques déclaratives

AWS recommande les meilleures pratiques suivantes pour l'utilisation des politiques déclaratives.

Tirez parti des évaluations de préparation

Utilisez le rapport d'état des comptes de politique déclarative pour évaluer l'état actuel de tous les attributs pris en charge par les politiques déclaratives pour les comptes concernés. Vous pouvez choisir les comptes et les unités organisationnelles (OUs) à inclure dans le champ d'application du rapport, ou choisir une organisation entière en sélectionnant la racine.

Ce rapport vous aide à évaluer le niveau de préparation en fournissant une ventilation par région et en indiquant si l'état actuel d'un attribut est uniforme sur tous les comptes (par le biais du`numberOfMatchedAccounts`) ou incohérent (par le`numberOfUnmatchedAccounts`). Vous pouvez également voir la valeur la plus fréquente, qui est la valeur de configuration la plus fréquemment observée pour l'attribut.

Le choix d'associer une politique déclarative pour appliquer une configuration de base dépend de votre cas d'utilisation spécifique.

Pour plus d'informations et un exemple illustratif, voirRapport sur l'état du compte pour les politiques déclaratives.

Commencez petit, puis agrandissez

Pour simplifier le débogage, commencez par une politique de test. Validez le comportement et l'impact de chaque modification avant d'effectuer la suivante. Cette approche réduit le nombre de variables à prendre en compte en cas d'erreur ou de résultat inattendu.

Par exemple, vous pouvez commencer par une politique de test attachée à un compte unique dans un environnement de test non critique. Une fois que vous avez confirmé qu'elle fonctionne conformément à vos spécifications, vous pouvez déplacer progressivement la politique vers le haut de la structure de l'organisation pour inclure davantage de comptes et d'unités organisationnelles (OUs).

Mettre en place des processus de révision

Mettez en œuvre des processus pour surveiller les nouveaux attributs déclaratifs, évaluer les exceptions aux politiques et apporter des ajustements afin de maintenir l'alignement sur les exigences opérationnelles et de sécurité de votre organisation.

Validez les modifications en utilisant **`DescribeEffectivePolicy`**

Après avoir modifié une politique déclarative, vérifiez les politiques en vigueur pour les comptes représentatifs inférieurs au niveau auquel vous avez apporté la modification. Vous pouvez consulter

la politique effective à l'aide de l'opération DescribeEffectivePolicyAPI AWS Management Console, de l'une de ses variantes AWS CLI ou du AWS SDK. Assurez-vous que la modification que vous avez apportée a eu l'impact escompté sur la politique effective.

Communiquez et entraînez-vous

Assurez-vous que vos organisations comprennent l'objectif et l'impact de vos politiques déclaratives. Fournissez des conseils clairs sur les comportements attendus et sur la manière de gérer les défaillances dues à l'application des politiques.

## Génération du rapport sur l'état du compte pour les politiques déclaratives

Le rapport sur l'état du compte vous permet de consulter l'état actuel de tous les attributs pris en charge par les politiques déclaratives applicables aux comptes concernés. Vous pouvez choisir les comptes et les unités organisationnelles (OUs) à inclure dans le champ d'application du rapport, ou choisir une organisation entière en sélectionnant la racine.

Ce rapport vous aide à évaluer le niveau de préparation en fournissant une ventilation par région et en indiquant si l'état actuel d'un attribut est uniforme sur tous les comptes (par le biais du`numberOfMatchedAccounts`) ou incohérent (par le`numberOfUnmatchedAccounts`). Vous pouvez également voir la valeur la plus fréquente, qui est la valeur de configuration la plus fréquemment observée pour l'attribut.

Le choix d'associer une politique déclarative pour appliquer une configuration de base dépend de votre cas d'utilisation spécifique.

Pour plus d'informations et un exemple illustratif, voirRapport sur l'état du compte pour les politiques déclaratives.

Conditions préalables

Avant de pouvoir générer un rapport sur l'état du compte, vous devez effectuer les étapes suivantes

1. L'`StartDeclarativePoliciesReport`API ne peut être appelée que par le compte de gestion ou les administrateurs délégués d'une organisation.
2. Vous devez disposer d'un compartiment S3 avant de générer le rapport (en créer un nouveau ou en utiliser un existant), il doit se trouver dans la même région que celle dans laquelle la demande est faite et il doit disposer d'une politique de compartiment S3 appropriée. Pour un exemple de politique S3, consultez Exemple de politique Amazon S3 sous Exemples dans le manuel Amazon EC2 API Reference

3. Vous devez activer l'accès sécurisé pour le service où la politique déclarative appliquera une configuration de base. Cela crée un rôle lié à un service en lecture seule qui est utilisé pour générer le rapport d'état du compte indiquant la configuration existante pour les comptes de votre organisation.

   Utilisation de la console

   Pour la console Organizations, cette étape fait partie du processus d'activation des politiques déclaratives.

   À l'aide du AWS CLI

   Pour ce faire AWS CLI, utilisez l'API Enable AWSService Access.

   Pour plus d'informations sur la façon d'activer l'accès sécurisé pour un service spécifique à l'aide de la AWS CLI section, Services AWS que vous pouvez utiliser avec AWS Organizations.
4. Un seul rapport par organisation peut être généré à la fois. Toute tentative de génération d'un rapport alors qu'un autre est en cours d'élaboration entraînera une erreur.

Accédez au rapport sur l'état de conformité

> **Autorisations minimales**
>
> Pour générer un rapport sur l'état de conformité, vous devez être autorisé à exécuter les actions suivantes :
>
> - `ec2:StartDeclarativePoliciesReport`
> - `ec2:DescribeDeclarativePoliciesReports`
> - `ec2:GetDeclarativePoliciesReportSummary`
> - `ec2:CancelDeclarativePoliciesReport`
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization`
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:ListAccounts`
> - `organizations:ListDelegatedAdministrators`
> - `organizations:ListAWSServiceAccessForOrganization`

- `s3:PutObject`

> **Note**
>
> Si votre compartiment Amazon S3 utilise le chiffrement SSE-KMS, vous devez également inclure l'`kms:GenerateDataKey`autorisation dans la politique.

### AWS Management Console

Utilisez la procédure suivante pour générer un rapport sur l'état du compte.

Pour générer un rapport sur l'état du compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques, choisissez Politiques déclaratives pour EC2.
3. Sur la page Politiques déclaratives pour EC2, choisissez Afficher le rapport d'état du compte dans le menu déroulant Actions.
4. Sur la page Afficher le rapport d'état du compte, choisissez Générer un rapport d'état.
5. Dans le widget Structure organisationnelle, spécifiez les unités organisationnelles (OUs) que vous souhaitez inclure dans le rapport.
6. Sélectionnez Soumettre.

### AWS CLI & AWS SDKs

Pour générer un rapport sur l'état du compte

Utilisez les opérations suivantes pour générer un rapport sur l'état de conformité, vérifier son état et consulter le rapport :

- `ec2:start-declarative-policies-report`: Génère un rapport sur l'état du compte. Le rapport est généré de manière asynchrone et son élaboration peut prendre plusieurs heures. Pour plus d'informations, consultez StartDeclarativePoliciesReportle manuel Amazon EC2 API Reference.

- `ec2:describe-declarative-policies-report`: décrit les métadonnées d'un rapport sur l'état d'un compte, y compris l'état du rapport. Pour plus d'informations, consultez DescribeDeclarativePoliciesReportsle manuel Amazon EC2 API Reference.
- `ec2:get-declarative-policies-report-summary`: Récupère un résumé du rapport sur l'état du compte. Pour plus d'informations, consultez GetDeclarativePoliciesReportSummaryle manuel Amazon EC2 API Reference.
- `ec2:cancel-declarative-policies-report`: annule la génération d'un rapport sur l'état du compte. Pour plus d'informations, consultez CancelDeclarativePoliciesReportle manuel Amazon EC2 API Reference.

Avant de générer un rapport, accordez aux politiques déclaratives EC2 un accès principal au compartiment Amazon S3 dans lequel le rapport sera stocké. Pour ce faire, associez la politique suivante au bucket. `amzn-s3-demo-bucket`Remplacez-le par le nom réel de votre compartiment Amazon S3 et `identity_`ARN par l'identité IAM utilisée pour appeler l'`StartDeclarativePoliciesReport`API.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DeclarativePoliciesReportDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "organizations.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

## Syntaxe de politique déclarative et exemples

Cette page décrit la syntaxe de la politique déclarative et fournit des exemples.

### Considérations

- Lorsque vous configurez un attribut de service à l'aide d'une politique déclarative, cela peut avoir un impact sur plusieurs APIs. Toute action non conforme échouera.
- Les administrateurs de compte ne seront pas en mesure de modifier la valeur de l'attribut de service au niveau du compte individuel.

### Syntaxe des politiques déclaratives

Une politique déclarative est un fichier en texte brut structuré selon les règles du JSON. La syntaxe des politiques déclaratives suit celle de tous les types de politiques de gestion. Pour une analyse complète de cette syntaxe, consultez Syntaxe et héritage des politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques du type de politique déclarative.

L'exemple suivant montre la syntaxe de base de la politique déclarative :

```
{
  "ec2_attributes": {
    "exception_message": {
      "@@assign": "Your custom error message.https://myURL"
    }
  }
}
```

- Le nom de clé du champ `ec2_attributes`. Les politiques déclaratives commencent toujours par un nom de clé fixe pour le donné Service AWS. Il s'agit de la ligne du haut dans l'exemple de politique ci-dessus. Actuellement, les politiques déclaratives ne prenaient en charge que les services liés à Amazon EC2.
- Sous`ec2_attributes`, vous pouvez l'utiliser `exception_message` pour définir un message d'erreur personnalisé. Pour plus d'informations, consultez la section Messages d'erreur personnalisés pour les politiques déclaratives.

- Sous`ec2_attributes`, vous pouvez insérer une ou plusieurs politiques déclaratives prises en charge. Pour ces schémas, voirPolitiques déclaratives prises en charge.

### Politiques déclaratives prises en charge

Les attributs Services AWS et pris en charge par les politiques déclaratives sont les suivants. Dans certains des exemples suivants, la mise en forme des espaces JSON peut être compressée pour économiser de l'espace.

- Accès public aux blocs VPC
- Accès à la console série
- Accès public au bloc d'images
- Paramètres des images autorisées
- Métadonnées de l'instance
- Accès public à Snapshot Block

#### VPC Block Public Access

##### Effet de la politique

Contrôle si les ressources d'Amazon VPCs et des sous-réseaux peuvent accéder à Internet via des passerelles Internet ()IGWs. Pour plus d'informations, consultez la section Configuration de l'accès à Internet dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

##### Contenu de la politique

```
{
  "ec2_attributes": {
    "vpc_block_public_access": {
      "internet_gateway_block": {
        "mode": {
          "@@assign": "block_ingress"
        },
        "exclusions_allowed": {
          "@@assign": "enabled"
        }
      }
    }
```

```
  }
}
```

Les champs disponibles pour cet attribut sont les suivants :

- `"internet_gateway"`:
  - `"mode"`:
    - `"off"`: le VPC BPA n'est pas activé.
    - `"block_ingress"`: Tout le trafic Internet vers le VPCs (à l'exception VPCs des sous-réseaux exclus) est bloqué. Seul le trafic à destination et en provenance des passerelles NAT et des passerelles Internet de sortie uniquement est autorisé, car ces passerelles autorisent uniquement l'établissement de connexions sortantes.
    - `"block_bidirectional"`: Tout le trafic à destination et en provenance des passerelles Internet et des passerelles Internet de sortie uniquement (à l'exception des réseaux exclus VPCs et des sous-réseaux) est bloqué.
- `"exclusions_allowed"`: Une exclusion est un mode qui peut être appliqué à un seul VPC ou sous-réseau pour l'exempter du mode BPA VPC du compte et autoriser un accès bidirectionnel ou de sortie uniquement.
  - `"enabled"`: Les exclusions peuvent être créées par le compte.
  - `"disabled"`: Les exclusions ne peuvent pas être créées par le compte.

> **Note**
>
> Vous pouvez utiliser l'attribut pour configurer si les exclusions sont autorisées, mais vous ne pouvez pas créer d'exclusions avec cet attribut lui-même. Pour créer des exclusions, vous devez les créer dans le compte propriétaire du VPC. Pour plus d'informations sur la création d'exclusions BPA pour VPC, consultez la section Créer et supprimer des exclusions dans le guide de l'utilisateur Amazon VPC.

Considérations

Si vous utilisez cet attribut dans une politique déclarative, vous ne pouvez pas utiliser les opérations suivantes pour modifier la configuration appliquée aux comptes concernés. Cette liste n'est pas exhaustive :

- `ModifyVpcBlockPublicAccessOptions`

- `CreateVpcBlockPublicAccessExclusion`
- `ModifyVpcBlockPublicAccessExclusion`

### Serial Console Access

#### Effet de la politique

Contrôle si la console série EC2 est accessible. Pour plus d'informations sur la console série EC2, consultez la section Console série EC2 dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

#### Contenu de la politique

```
{
  "ec2_attributes": {
    "serial_console_access": {
      "status": {
        "@@assign": "enabled"
      }
    }
  }
}
```

Les champs disponibles pour cet attribut sont les suivants :

- `"status"`:
  - `"enabled"`: l'accès à la console série EC2 est autorisé.
  - `"disabled"`: l'accès à la console série EC2 est bloqué.

#### Considérations

Si vous utilisez cet attribut dans une politique déclarative, vous ne pouvez pas utiliser les opérations suivantes pour modifier la configuration appliquée aux comptes concernés. Cette liste n'est pas exhaustive :

- `EnableSerialConsoleAccess`
- `DisableSerialConsoleAccess`

### Image Block Public Access

#### Effet de la politique

Contrôle si Amazon Machine Images (AMIs) est partageable publiquement. Pour plus d'informations AMIs, consultez Amazon Machine Images (AMIs) dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

#### Contenu de la politique

```
{
  "ec2_attributes": {
    "image_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```

Les champs disponibles pour cet attribut sont les suivants :

- `"state"`:
  - `"unblocked"`: Aucune restriction quant au partage public de AMIs.
  - `"block_new_sharing"`: Bloque le nouveau partage public de AMIs. AMIs qui ont déjà été partagés publiquement restent accessibles au public.

#### Considérations

Si vous utilisez cet attribut dans une politique déclarative, vous ne pouvez pas utiliser les opérations suivantes pour modifier la configuration appliquée aux comptes concernés. Cette liste n'est pas exhaustive :

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`

### Allowed Images Settings

#### Effet de la politique

Contrôle la découverte et l'utilisation d'Amazon Machine Images (AMI) dans Amazon EC2 avec Allowed. AMIs Pour plus d'informations AMIs, consultez la section Contrôler la découverte et l'utilisation des AMI dans Amazon EC2 avec Autorisé AMIs dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

Contenu de la politique

Les champs disponibles pour cet attribut sont les suivants :

```
{
  "ec2_attributes": {
    "allowed_images_settings": {
      "state": {
        "@@assign": "enabled"
      },
      "image_criteria": {
        "criteria_1": {
          "allowed_image_providers": {
            "@@append": [
              "amazon"
            ]
          }
        }
      }
    }
  }
}
```

- `"state"`:
  - `"enabled"`: L'attribut est actif et appliqué.
  - `"disabled"`: L'attribut est inactif et n'est pas appliqué.
  - `"audit_mode"`: L'attribut est en mode audit. Cela signifie qu'il identifiera les images non conformes mais ne bloquera pas leur utilisation.
- `"image_criteria"`: liste de critères. Support d'un maximum de 10 critères dont le nom est compris entre criteria_1 et criteria_10
  - `"allowed_image_providers"`: liste séparée par des virgules d'alias de compte IDs ou de propriétaire à 12 chiffres pour Amazon, aws_marketplace, aws_backup_vault.
  - `"image_names"`: noms des images autorisées. Les noms peuvent inclure des caractères génériques (? et *). Longueur : 1 à 128 caractères Avec ? , le minimum est de 3 caractères.

- `"marketplace_product_codes"`: Les codes de produit AWS Marketplace pour les images autorisées. Longueur : 1 à 25 caractères Caractères valides : lettres (A—Z, a—z) et chiffres (0—9)
- `"creation_date_condition"`: âge maximum pour les images autorisées.
  - `"maximum_days_since_created"`: nombre maximal de jours écoulés depuis la création de l'image. Plage valide : Valeur minimum de 0. Valeur maximale de 2147483647.
- `"deprecation_time_condition"`: période maximale depuis la dépréciation pour les images autorisées.
  - `"maximum_days_since_deprecated"`: nombre maximal de jours écoulés depuis que l'image est devenue obsolète. Plage valide : Valeur minimum de 0. Valeur maximale de 2147483647.

#### Considérations

Si vous utilisez cet attribut dans une politique déclarative, vous ne pouvez pas utiliser les opérations suivantes pour modifier la configuration appliquée aux comptes concernés. Cette liste n'est pas exhaustive :

- `EnableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`
- `DisableAllowedImagesSettings`

### Instance Metadata

#### Effet de la politique

Contrôle les paramètres IMDS par défaut et l'application de l'IMDSv2 pour tous les nouveaux lancements d'instances EC2. Pour plus d'informations sur les paramètres par défaut et leur IMDSv2 mise en œuvre, consultez la section Utiliser les métadonnées d'instance pour gérer votre instance EC2 dans le guide de l'utilisateur Amazon EC2.

#### Contenu de la politique

Les champs disponibles pour cet attribut sont les suivants :

```
{
```

```
  "ec2_attributes": {
    "instance_metadata_defaults": {
      "http_tokens": {
        "@@assign": "required"
      },
      "http_put_response_hop_limit": {
        "@@assign": "4"
      },
      "http_endpoint": {
        "@@assign": "enabled"
      },
      "instance_metadata_tags": {
        "@@assign": "enabled"
      },
      "http_tokens_enforced": {
        "@@assign": "enabled"
      }
    }
  }
}
```

- `"http_tokens"`:
  - `"no_preference"`: Les autres valeurs par défaut s'appliquent. Par exemple, les paramètres par défaut de l'AMI, le cas échéant.
  - `"required"`: IMDSv2 doit être utilisé. IMDSv1 n'est pas autorisé.
  - `"optional"`: Les deux IMDSv1 IMDSv2 sont autorisés.

  > **Note**
  >
  > Version des métadonnées
  > Avant `http_tokens` de définir sur `required` (IMDSv2 doit être utilisé), assurez-vous qu'aucune de vos instances ne passe d' IMDSv1 appel. Pour plus d'informations, consultez Étape 1 : Identifier les instances avec IMDSv2 =optional et auditer IMDSv1 l'utilisation dans le guide de l'utilisateur Amazon EC2.

- `"http_put_response_hop_limit"`:
  - `"Integer"`: valeur entière comprise entre -1 et 64, représentant le nombre maximal de sauts que le jeton de métadonnées peut effectuer. Pour n'indiquer aucune préférence, spécifiez -1.

> **Note**
>
> Limite de sauts
> Si `http_tokens` cette valeur est définie sur`required`, il est recommandé de `http_put_response_hop_limit` définir une valeur minimale de 2. Pour plus d'informations, consultez la section Considérations relatives à l'accès aux métadonnées des instances dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

- `"http_endpoint"`:
  - `"no_preference"`: Les autres valeurs par défaut s'appliquent. Par exemple, les paramètres par défaut de l'AMI, le cas échéant.
  - `"enabled"`: le point de terminaison du service de métadonnées de l'instance est accessible.
  - `"disabled"`: le point de terminaison du service de métadonnées de l'instance n'est pas accessible.
- `"instance_metadata_tags"`:
  - `"no_preference"`: Les autres valeurs par défaut s'appliquent. Par exemple, les paramètres par défaut de l'AMI, le cas échéant.
  - `"enabled"`: Les balises d'instance sont accessibles à partir des métadonnées de l'instance.
  - `"disabled"`: Les balises d'instance ne sont pas accessibles à partir des métadonnées de l'instance.
- `"http_tokens_enforced":`
  - `"no_preference"`: Les autres valeurs par défaut s'appliquent. Par exemple, les paramètres par défaut de l'AMI, le cas échéant.
  - `"enabled"`: IMDSv2 doit être utilisé. Les tentatives de lancement d'une IMDSv1 instance ou d'activation IMDSv1 sur des instances existantes échoueront.
  - `"disabled"`: Les deux IMDSv1 IMDSv2 sont autorisés.

> **Warning**
>
> IMDSv2 mise en application
> IMDSv2 L'activation de l'application tout en autorisant IMDSv1 et IMDSv2 (jeton facultatif) entraînera des échecs de lancement, sauf si elle IMDSv1 est explicitement désactivée, soit par le biais des paramètres de lancement, soit par le biais des paramètres de lancement ou des paramètres par défaut de l'AMI. Pour plus

d'informations, consultez la section Échec du lancement d'une instance IMDSv1 activée dans le guide de l'utilisateur Amazon EC2.

### Snapshot Block Public Access

#### Effet de la politique

Contrôle si les instantanés Amazon EBS sont accessibles au public. Pour plus d'informations sur les instantanés EBS, consultez les instantanés Amazon EBS dans le guide de l'utilisateur d'Amazon Elastic Block Store.

#### Contenu de la politique

```
{
  "ec2_attributes": {
    "snapshot_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```

Les champs disponibles pour cet attribut sont les suivants :

- `"state"`:
  - `"block_all_sharing"`: bloque tout partage public d'instantanés. Les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
  - `"block_new_sharing"`: bloque le nouveau partage public d'instantanés. Les instantanés déjà partagés publiquement restent accessibles au public.
  - `"unblocked"`: Aucune restriction quant au partage public des instantanés.

#### Considérations

Si vous utilisez cet attribut dans une politique déclarative, vous ne pouvez pas utiliser les opérations suivantes pour modifier la configuration appliquée aux comptes concernés. Cette liste n'est pas exhaustive :

- `EnableSnapshotBlockPublicAccess`

- `DisableSnapshotBlockPublicAccess`

## Politiques de sauvegarde

Les politiques de sauvegarde vous permettent de gérer et d'appliquer de manière centralisée des plans de sauvegarde aux AWS ressources des comptes d'une organisation.

AWS Backupvous permet de créer des plans de sauvegarde qui définissent le mode de sauvegarde de vos AWS ressources. Les règles du plan incluent divers paramètres, tels que la fréquence des sauvegardes, la période pendant laquelle la sauvegarde a lieu, Région AWS le contenu des ressources à sauvegarder et le coffre-fort dans lequel stocker la sauvegarde. Vous pouvez ensuite appliquer un plan de sauvegarde aux groupes de AWS ressources identifiés à l'aide de balises. Vous devez également identifier un rôle Gestion des identités et des accès AWS (IAM) qui AWS Backup autorise l'exécution de l'opération de sauvegarde en votre nom.

Les politiques de sauvegarde AWS Organizations combinent tous ces éléments dans des documents texte JSON. Vous pouvez associer une politique de sauvegarde à tous les éléments de la structure de votre organisation, tels que la racine, les unités organisationnelles (OUs) et les comptes individuels. Organizations applique des règles d'héritage pour combiner les politiques établies à la racine de l'organisation, celles de n'importe quel parent OUs ou celles associées au compte. Il en résulte une politique de sauvegarde effective pour chaque compte. Cette politique efficace indique AWS Backup comment sauvegarder automatiquement vos AWS ressources.

### Comment fonctionnent les politiques de sauvegarde

Les politiques de sauvegarde vous procurent un contrôle granulaire sur la sauvegarde de vos ressources, quel que soit le niveau requis par votre organisation. Vous pouvez par exemple spécifier dans une politique attachée à la racine de l'organisation que toutes les tables Amazon DynamoDB doivent être sauvegardées. Cette politique peut inclure une fréquence de sauvegarde par défaut. Vous pouvez ensuite y associer une politique de sauvegarde OUs qui remplace la fréquence de sauvegarde en fonction des exigences de chaque unité d'organisation. Par exemple, l'UO `Developers` peut spécifier une fréquence de sauvegarde d'une fois par semaine, tandis que l'UO `Production` spécifie une fois par jour.

Vous pouvez créer des politiques de sauvegarde partielle qui incluent individuellement une partie seulement des informations requises pour sauvegarder correctement vos ressources. Vous pouvez associer ces politiques à différentes parties de l'arborescence organisationnelle, telles que la racine ou une unité d'organisation parent, dans le but que ces politiques partielles soient héritées par

les comptes OUs et les niveaux inférieurs. Lorsque Organizations combine toutes les politiques d'un compte à l'aide de règles d'héritage, la politique effective obtenue doit posséder tous les éléments requis. Dans le cas contraire, AWS Backup considère que la politique n'est pas valide et ne sauvegarde pas les ressources concernées.

> **Important**
>
> AWS Backup ne peut effectuer une sauvegarde réussie que lorsqu'elle est invoquée par une politique efficace complète comportant tous les éléments requis.
> Bien qu'une stratégie de politique partielle comme celle décrite plus haut puisse fonctionner, si une politique effective pour un compte est incomplète, elle provoque des erreurs ou ne sauvegarde pas correctement certaines ressources. Une autre stratégie consisterait à exiger que toutes les politiques de sauvegarde soient complètes et valables par elles-mêmes. Utilisez les valeurs par défaut fournies par les politiques attachées dans les niveaux supérieurs de la hiérarchie et remplacez-les si nécessaire dans les politiques enfants, en incluant des opérateurs de contrôle enfants d'héritage.

Le plan de sauvegarde effectif pour chaque membre Compte AWS de l'organisation apparaît dans la AWS Backup console sous la forme d'un plan immuable pour ce compte. Vous pouvez le voir, mais pas le modifier. Vous pouvez toutefois ajouter ou supprimer des balises de plan de sauvegarde à l'aide de TagResourceet UntagResource APIs.

Lorsque AWS Backup commence une sauvegarde basée sur un plan de sauvegarde créé par des règles, vous pouvez voir l'état de la tâche de sauvegarde dans la AWS Backup console. Un utilisateur d'un compte membre peut voir l'état et les erreurs éventuelles des tâches de sauvegarde de ce compte membre. Si vous activez également l'accès aux services sécurisés avec AWS Backup, un utilisateur du compte de gestion de l'organisation peut voir le statut et les erreurs de toutes les tâches de sauvegarde de l'organisation. Pour de plus amples informations, consultez Activation de la gestion intercompte dans le Guide du développeur AWS Backup .

## Mise en route avec les politiques de sauvegarde

Suivez ces étapes pour commencer à utiliser des politiques de sauvegarde.

1. Découvrez les autorisations dont vous devez disposer pour effectuer des tâches de politique de sauvegarde

2. Découvrez les bonnes pratiques que nous recommandons lors de l'utilisation de politiques de sauvegarde.
3. Activez des politiques de sauvegarde pour votre organisation.
4. Créez une politique de sauvegarde.
5. Attachez la politique de sauvegarde à la racine, une UO ou un compte de votre organisation.
6. Affichez la politique de sauvegarde effective combinée qui s'applique à un compte.

Pour effectuer toutes ces étapes, vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

Autres informations

- Découvrez la syntaxe des stratégies de sauvegarde et consultez des exemples de stratégies

## Bonnes pratiques pour l'utilisation des politiques de sauvegarde

AWS recommande les meilleures pratiques suivantes pour l'utilisation des politiques de sauvegarde.

Décider d'une stratégie de politique de sauvegarde

Vous pouvez créer des politiques de sauvegarde en parties incomplètes qui sont héritées et fusionnées pour composer une politique complète pour chaque compte membre. Ce faisant, vous risquez d'obtenir une police effective incomplète si vous effectuez une modification à un niveau sans tenir compte de l'impact de cette dernière sur tous les comptes inférieurs à ce niveau. Pour éviter cela, nous vous recommandons de vous assurer que les politiques de sauvegarde que vous mettez en œuvre à tous les niveaux sont complètes en elles-mêmes. Traitez les politiques parentes comme des politiques par défaut qui peuvent être remplacées par des paramètres spécifiés dans les politiques enfants. De cette façon, même si une politique enfant n'existe pas, la politique héritée est complète et utilise les valeurs par défaut. Vous pouvez décider quels paramètres peuvent être ajoutés, modifiés ou supprimés par les stratégies enfants à l'aide des opérateurs de contrôle d'héritage enfants.

Validez les modifications apportées à vos politiques de sauvegarde à l'aide de **`GetEffectivePolicy`**

Après avoir apporté une modification à une politique de sauvegarde, vérifiez les politiques effectives pour des comptes représentatifs inférieurs au niveau où la modification a été appliquée. Vous pouvez

consulter la politique effective à l'aide de l'opération GetEffectivePolicyAPI AWS Management Console, de l'une de ses variantes AWS CLI ou du AWS SDK. Assurez-vous que la modification que vous avez apportée a eu l'impact escompté sur la politique effective.

Commencez simplement en réalisant de petites modifications

Pour simplifier le débogage, commencez par des politiques simples et apportez des modifications à un élément à la fois. Validez le comportement et l'impact de chaque modification avant d'effectuer la suivante. Vous réduisez ainsi le nombre de variables dont vous devez tenir compte lorsqu'une erreur ou un résultat inattendu se produit.

Stockez des copies de vos sauvegardes dans d'autres comptes Régions AWS et dans d'autres comptes de votre organisation

Pour améliorer votre position de reprise après sinistre, vous pouvez stocker des copies de vos sauvegardes.

- Une autre région : si vous stockez des copies de la sauvegarde en plus Régions AWS, vous contribuez à protéger la sauvegarde contre toute corruption ou suppression accidentelle dans la région d'origine. Utilisez la section `copy_actions` de la politique pour spécifier un coffre-fort dans une ou plusieurs régions du même compte dans lequel le plan de sauvegarde s'exécute. Pour ce faire, identifiez le compte à l'aide de la variable `$account` lorsque vous spécifiez l'ARN du coffre-fort de sauvegarde dans lequel stocker la copie de la sauvegarde. La variable `$account` est automatiquement remplacée au moment de l'exécution par l'ID du compte dans lequel la politique de sauvegarde est exécutée.
- Un autre compte — Si vous stockez des copies de la sauvegarde en plus Comptes AWS, vous ajoutez une barrière de sécurité qui aide à vous protéger contre un acteur malveillant qui compromettrait l'un de vos comptes. Utilisez la section `copy_actions` de la politique pour spécifier un coffre-fort dans un ou plusieurs comptes de votre organisation, séparément du compte dans lequel le plan de sauvegarde s'exécute. Pour ce faire, identifiez le compte à l'aide de son numéro ID réel lorsque vous spécifiez l'ARN du coffre-fort de sauvegarde dans lequel stocker la copie de la sauvegarde.

Limitez le nombre de plans par politique

Les politiques qui contiennent plusieurs plans sont plus compliquées à dépanner en raison du plus grand nombre de sorties qui doivent toutes être validées. Au lieu de cela, faites en sorte que chaque politique contienne un seul et unique plan de sauvegarde, pour simplifier le débogage et le

dépannage. Vous pouvez ensuite ajouter des politiques supplémentaires avec d'autres plans pour satisfaire d'autres exigences. Cela permet de limiter à une seule politique les problèmes liés à un plan et d'éviter que ces problèmes compliquent la résolution des problèmes liés à d'autres politiques et à leurs plans.

Utilisez des ensembles de piles pour créer les coffres-forts de sauvegarde et les rôles IAM requis

Utilisez l'intégration des ensembles de AWS CloudFormation piles avec Organizations pour créer automatiquement les coffres-forts de sauvegarde et les rôles Gestion des identités et des accès AWS (IAM) requis dans chacun des comptes membres de votre organisation. Vous pouvez créer un ensemble de ressources qui inclut les ressources que vous souhaitez voir automatiquement disponibles Compte AWS dans tous les membres de votre organisation. Vous pouvez ainsi exécuter vos plans de sauvegarde avec la garantie que les dépendances sont déjà respectées. Pour de plus amples informations, consultez Créer un ensemble de piles avec des autorisations autogérées dans le Guide de l'utilisateur AWS CloudFormation .

Vérifiez vos résultats en examinant la première sauvegarde créée dans chaque compte

Lorsque vous modifiez une politique, vérifiez la sauvegarde suivante créée après cette modification pour vous assurer qu'elle a eu l'impact souhaité. Cette étape va au-delà de l'examen de la politique efficace et garantit l' AWS Backup interprétation de vos politiques et la mise en œuvre des plans de sauvegarde comme vous le souhaitiez.

## Utilisation d' AWS CloudTrail événements pour surveiller les politiques de sauvegarde au sein de votre entreprise

Vous pouvez utiliser les AWS CloudTrail événements pour surveiller le moment où des politiques de sauvegarde sont créées, mises à jour ou supprimées de n'importe quel compte de votre organisation, ou lorsqu'un plan de sauvegarde organisationnel n'est pas valide. Pour plus d'informations, consultez la rubrique Journalisation des événements de gestion inter-comptes du Guide du développeur AWS Backup .

## Syntaxe et exemples d'une politique de sauvegarde

Cette page décrit la syntaxe d'une politique de sauvegarde et fournit des exemples.

Syntaxe des politiques de sauvegarde

Une politique de sauvegarde est un fichier texte brut qui est structuré conformément aux règles de JSON. La syntaxe des politiques de sauvegarde suit celle de tous les types de politiques de

gestion. Pour plus d'informations, voir Syntaxe des politiques et héritage pour les types de politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques du type de politique de sauvegarde.

Pour plus d'informations sur AWS Backup les forfaits, consultez CreateBackupPlanle guide du AWS Backup développeur.

Considérations

Syntaxe des politiques

Les noms de clé dupliqués seront rejetés en JSON.

Les politiques doivent spécifier les ressources Régions AWS et les ressources à sauvegarder.

Les politiques doivent spécifier le rôle IAM assumé AWS Backup .

`@@assign`L'utilisation d'un opérateur au même niveau peut remplacer les paramètres existants. Pour plus d'informations, voir Une politique relative aux enfants remplace les paramètres d'une politique parentale.

Les opérateurs d'héritage contrôlent la façon dont les politiques héritées et les politiques attachées à un compte fusionnent pour former la politique effective de ce compte. Ces opérateurs comprennent les opérateurs de définition de valeurs et les opérateurs de contrôle enfants.

Pour plus d'informations, consultez les sections Opérateurs d'héritage et Exemples de politiques de sauvegarde.

Rôles IAM

Le rôle IAM doit exister lors de la première création d'un plan de sauvegarde.

Le rôle IAM doit être autorisé à accéder aux ressources identifiées par une requête de balise.

Le rôle IAM doit être autorisé à effectuer la sauvegarde.

Coffres-forts de sauvegarde

Des coffres-forts doivent exister dans chaque unité spécifiée pour Régions AWS qu'un plan de sauvegarde puisse être exécuté.

Des coffres-forts doivent exister pour chaque AWS compte bénéficiant de la politique effective. Pour plus d'informations, consultez la section Création et suppression d'un coffre de sauvegarde dans le Guide du AWS Backup développeur.

Nous vous recommandons d'utiliser des ensembles de AWS CloudFormation piles et de les intégrer à Organizations pour créer et configurer automatiquement des coffres-forts de sauvegarde et des rôles IAM pour chaque compte membre de l'organisation. Pour de plus amples informations, consultez Créer un ensemble de piles avec des autorisations autogérées dans le Guide de l'utilisateur AWS CloudFormation .

Quotas

Pour une liste des quotas, voir « AWS Backup quotas » dans le Guide du AWS Backup développeur.

Syntaxe de sauvegarde : présentation

La syntaxe d'une politique de sauvegarde inclut les composants suivants :

```
{
    "plans": {
        "PlanName": {
            "rules": { ... },
            "regions": { ... },
            "selections": { ... },
            "advanced_backup_settings": { ... },
            "backup_plan_tags": { ... },
            "scan_settings": { ... }
        }
    }
}
```

Éléments de la politique de sauvegarde

| Element | Description | Obligatoire |
| --- | --- | --- |
| règles | Liste des règles de sauvegarde. Chaque règle définit le moment où les sauvegard es démarrent et la fenêtre d'exécution des ressources spécifiées dans les `selections` éléments `regions` et. | Oui |
| régions | Liste des domaines Régions AWS dans lesquels une politique de sauvegarde peut protéger les ressources. | Oui |

| Element | Description | Obligatoire |
| --- | --- | --- |
| sélections | Un ou plusieurs types de ressources dans les limites spécifiées `regions` que la sauvegarde `rules` protège. | Oui |
| paramètres_de_sauvegarde avancés | Options de configuration pour des scénarios de sauvegarde spécifiques.<br><br>Actuellement, le seul paramètre de sauvegarde avancé pris en charge consiste à activer les sauvegardes Microsoft Volume Shadow Copy Service (VSS) pour Windows ou SQL Server exécutées sur une instance Amazon EC2. | Non |
| backup_plan_tags | Tags que vous souhaitez associer à un plan de sauvegarde. Chaque balise est une étiquette composée d'une clé définie par l'utilisateur et d'une valeur.<br><br>Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer vos plans de sauvegarde. | Non |
| paramètres de numérisation | Options de configuration pour les paramètres de numérisation. Actuellement, le seul paramètre de scan pris en charge est d'activer Amazon GuardDuty Malware Protection pour AWS Backup. | Non |

Syntaxe de sauvegarde : règles

La clé `rules` de stratégie spécifie les tâches de sauvegarde planifiées qui AWS Backup s'exécutent sur les ressources sélectionnées.

Éléments de règles de sauvegarde

| Element | Description | Obligatoire |
| --- | --- | --- |
| `schedule_expression` | Expression Cron en UTC qui indique à quel moment une AWS Backup tâche de sauvegarde est lancée.<br><br>Pour plus d'informations sur les expressions cron, consultez la section Utilisation des expressions cron et rate pour planifier des règles dans le guide de EventBridge l'utilisateur Amazon. | Oui |
| `target_backup_vault_name` | Coffre-fort de sauvegarde dans lequel les sauvegardes sont stockées.<br><br>Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à l' Région AWS endroit où ils ont été créés. | Oui |
| `target_logically_air_gapped_backup_vault_arn` | ARN du coffre-fort logiquement espacé dans lequel les sauvegardes sont stockées.<br><br>Si elles sont fournies, les ressources entièrement gérées prises en charge sont sauvegardées directement dans un coffre-fort à espacement logique, tandis que les autres ressources prises en charge créent un instantané temporaire (facturable) dans le coffre-fort de sauvegarde, puis le copient dans un coffre-fort à espacement logique. Les ressources non prises en charge ne sont sauvegardées que dans le coffre de sauvegarde spécifié.<br><br>L'ARN doit utiliser les espaces réservés spéciaux `$region` et`$account`. Par exemple, pour un coffre nommé, `AirGappedVault` | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | la valeur correcte est`arn:aws:backup:$region:$account:backup-vault:AirGappedVault` . | |
| `start_backup_window_minutes` | Le nombre de minutes à attendre avant d'annuler une tâche de sauvegarde sera annulé si elle ne démarre pas correctement.<br><br>Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs. | Non |
| `complete_backup_window_minutes` | Nombre de minutes après le démarrage réussi d'une tâche de sauvegarde avant qu'elle ne doive être terminée, faute de quoi elle sera annulée par AWS Backup. | Non |
| `enable_continuous_backup` | Spécifie s'il AWS Backup crée des sauvegardes continues.<br><br>`True`provoque AWS Backup la création de sauvegardes continues capables de point-in-time restauration (PITR). `False`(ou non spécifiée) provoque AWS Backup la création de sauvegardes instantanées.<br><br>Pour plus d'informations sur les sauvegardes continues, consultez P oint-in-time recovery dans le Guide du AWS Backup développeur.<br><br>Remarque : les sauvegardes compatibles PITR ont une durée de conservation maximale de 35 jours. | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| `lifecycle` | Spécifie à AWS Backup quel moment une sauvegarde passe en stockage à froid et à quel moment elle expire.<br><br>Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource Disponibilité des fonctionnalités par ressource du Guide du AWS Backup développeur.<br><br>Chaque cycle de vie contient les éléments suivants :<br><br>• `move_to_cold_storage_after_days` : Nombre de jours après la sauvegarde avant le transfert du AWS Backup point de restauration vers un stockage à froid.<br>• `delete_after_days` : nombre de jours après l'exécution d'une sauvegarde avant la AWS Backup suppression du point de restauration.<br>• `opt_in_to_archive_for_supported_resources` : si cette valeur est attribuée à`true`, un plan de sauvegarde fait passer les ressources prises en charge au niveau de stockage d'archivage (froid) conformément à vos paramètres de cycle de vie.<br><br>Remarque : Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | Cela signifie que le délai `delete_after_days` doit être supérieur de 90 jours à `move_to_cold_storage_after_days` . | |

| Element | Description | Obligatoire |
| --- | --- | --- |
| `copy_actions` | Spécifie si une sauvegarde est AWS Backup copiée vers un ou plusieurs emplacements supplémentaires.<br><br>Chaque action de copie contient les éléments suivants :<br><br>• `target_backup_vault_arn` : coffre-fort AWS Backup dans lequel est stockée une copie supplémentaire de la sauvegarde.<br>  • À utiliser `$account` pour les copies du même compte<br>  • Utiliser l'identifiant de compte réel pour les copies entre comptes<br>• `lifecycle` : Spécifie à AWS Backup quel moment une sauvegarde passe en stockage à froid et à quel moment elle expire.<br><br>  Chaque cycle de vie contient les éléments suivants :<br>  • `move_to_cold_storage_after_days` : Nombre de jours après la sauvegarde avant le transfert du AWS Backup point de restauration vers un stockage à froid.<br>  • `delete_after_days` : Nombre de jours après qu'une sauvegarde a été effectuée avant la AWS Backup suppression du point de restauration.<br><br>Remarque : Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | Cela signifie que le délai `delete_after_days` doit être supérieur de 90 jours à `move_to_cold_storage_after_days` . | |
| `recovery_point_tags` | Tags que vous souhaitez attribuer aux ressources restaurées à partir d'une sauvegarde.<br><br>Chaque balise contient les éléments suivants :<br><br>• `tag_key`:Ce champ est obligatoire dans ce bloc. Nom du tag (sensible aux majuscules et minuscules)<br>• `tag_value` :Ce champ est obligatoire dans ce bloc. Valeur du tag (sensible aux majuscules et minuscules) | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| `index_actions` | Spécifie s'il AWS Backup crée un index de sauvegarde de vos instantanés Amazon EBS et des sauvegardes and/or Amazon S3. Des index de sauvegarde sont créés afin de recherche r les métadonnées de vos sauvegardes. Pour plus d'informations sur la création d'index de sauvegarde et la recherche de sauvegarde, consultez la section Recherche de sauvegarde.<br><br>Remarque : des autorisations de rôle IAM supplémentaires sont requises pour créer un index de sauvegarde instantanée Amazon EBS.<br><br>Chaque action d'indexation contient l'élément suivant : les types `resource_types` de ressources pris en charge pour l'indexation sont Amazon EBS et Amazon S3. Ce paramètre indique le type de ressource qui sera sélection né pour l'indexation. | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| `scan_actions` | Spécifie si une action d'analyse est activée pour une règle donnée. Vous devez spécifier un`ScanMode`. Vous devez utiliser `scan_settings` les éléments de politique de sauvegarde conjointement avec pour que `scan_actions` les tâches de numérisation démarrent correctement. Vérifiez également que vous disposez des autorisations de rôle IAM appropriées.<br>• `ScanMode`: Cela indiquera le type de scan que vous souhaitez exécuter selon la fréquence de votre règle de plan de sauvegarde. Vous avez le choix entre `INCREMENTAL_SCAN` et `FULL_SCAN` . | Non |

Syntaxe de sauvegarde : régions

La clé de `regions` stratégie Régions AWS indique laquelle AWS Backup recherche les ressources qui répondent aux conditions de la `selections` clé.

Éléments des régions de sauvegarde

| Element | Description | Obligatoire |
| --- | --- | --- |
| `regions` | Spécifie les Région AWS codes. Par exemple : `["us-east-1", "eu-north-1"]` . | Oui |

Syntaxe de sauvegarde : sélections

La clé `selections` de stratégie spécifie les ressources qui sont sauvegardées par les règles d'une stratégie de sauvegarde.

Il existe deux éléments qui s'excluent mutuellement : `tags` et`resources`. Pour être valide, une politique efficace doit être `resources` inscrite dans des balises `have` ou dans la sélection.

Si vous souhaitez une sélection comportant à la fois des conditions de balise et des conditions de ressources, utilisez les `resources` clés.

Éléments de sélection de sauvegarde : Tags

| Element | Description | Obligatoire |
| --- | --- | --- |
| `iam_role_arn` | Rôle IAM qui AWS Backup suppose d'interroger, de découvrir et de sauvegarder des ressources dans les régions spécifiées.<br><br>Le rôle doit disposer d'autorisations suffisantes pour interroger les ressources en fonction des conditions des balises et effectuer des opérations de sauvegarde sur les ressources correspondantes. | Oui |
| `tag_key` | Nom de la clé de balise à rechercher. | Oui |
| `tag_value` | Valeur qui doit être associée au tag_key correspondant.<br><br>AWS Backup inclut la ressource uniquement si tag_key et tag_value correspondent (distinction majuscules/minuscules). | Oui |
| `conditions` | Étiquetez les clés et les valeurs que vous souhaitez inclure ou exclure<br><br>Utilisez string_equals ou string_not_equals pour inclure ou exclure les balises correspondant exactement à une correspondance.<br><br>Utilisez string_like et string_not_like pour inclure ou exclure les balises contenant ou ne contenant pas de caractères spécifiques<br><br>Remarque : Limité à 30 conditions pour chaque sélection. | Non |

Éléments de sélection de sauvegarde : Ressources

| Element | Description | Obligatoire |
| --- | --- | --- |
| `iam_role_arn` | Rôle IAM qui AWS Backup suppose d'interroger, de découvrir et de sauvegarder des ressources dans les régions spécifiées.<br><br>Le rôle doit disposer d'autorisations suffisantes pour interroger les ressources en fonction des conditions des balises et effectuer des opérations de sauvegarde sur les ressources correspondantes.<br><br>Remarque : Dans AWS GovCloud (US) Regions, vous devez ajouter le nom de la partition à l'ARN.<br><br>Par exemple, « `arn:aws:ec2:*:*:volume/*` » doit être « `arn:aws-us-gov:ec2:*:*:volume/*` ». | Oui |
| `resource_types` | Types de ressources à inclure dans un plan de sauvegarde. | Oui |
| `not_resource_types` | Types de ressources à exclure d'un plan de sauvegarde. | Non |
| `conditions` | Étiquetez les clés et les valeurs que vous souhaitez inclure ou exclure<br><br>Utilisez string_equals ou string_not_equals pour inclure ou exclure les balises correspondant exactement à une correspondance.<br><br>Utilisez string_like et string_not_like pour inclure ou exclure les balises contenant ou ne contenant pas de caractères spécifiques | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | Remarque : Limité à 30 conditions pour chaque sélection. | |

Types de ressources pris en charge

Organizations prend en charge les types de ressources suivants pour les `not_resource_types` éléments `resource_types` et :

- AWS Backup gateway machines virtuelles : `"arn:aws:backup-gateway:*:*:vm/*"`
- AWS CloudFormation piles : `"arn:aws:cloudformation:*:*:stack/*"`
- Tables Amazon DynamoDB : `"arn:aws:dynamodb:*:*:table/*"`
- Instances Amazon EC2 : `"arn:aws:ec2:*:*:instance/*"`
- Volumes Amazon EBS : `"arn:aws:ec2:*:*:volume/*"`
- Systèmes de fichiers Amazon EFS : `"arn:aws:elasticfilesystem:*:*:file-system/*"`
- Clusters Amazon Aurora/Amazon DocumentDB/Amazon Neptune : `"arn:aws:rds:*:*:cluster:*"`
- Bases de données Amazon RDS : `"arn:aws:rds:*:*:db:*"`
- Clusters Amazon Redshift : `"arn:aws:redshift:*:*:cluster:*"`
- Amazon S3 : `"arn:aws:s3:::*"`
- Gestionnaire de systèmes AWS pour SAP Bases de données HANA : `"arn:aws:ssm-sap:*:*:HANA/*"`
- AWS Storage Gateway passerelles : `"arn:aws:storagegateway:*:*:gateway/*"`
- Bases de données Amazon Timestream : `"arn:aws:timestream:*:*:database/*"`
- Systèmes de FSx fichiers Amazon : `"arn:aws:fsx:*:*:file-system/*"`
- FSx Volumes Amazon : `"arn:aws:fsx:*:*:volume/*"`
- Volumes Amazon Elastic Kubernetes Service : `"arn:aws:eks:*:*:cluster/*"`

Exemples de code

Pour plus d'informations, consultez les sections Spécification des ressources à l'aide du bloc de balises et Spécification des ressources à l'aide du bloc de ressources.

Syntaxe de sauvegarde : paramètres de sauvegarde avancés

La `advanced_backup_settings` clé spécifie les options de configuration pour des scénarios de sauvegarde spécifiques. Chaque paramètre contient les éléments suivants :

Éléments de paramètres de sauvegarde avancés

| Element | Description | Obligatoire |
| --- | --- | --- |
| `advanced_backup_settings` | Spécifie les paramètres pour des scénarios de sauvegarde spécifiques. Cette clé contient un ou plusieurs paramètres. Chaque paramètre est une chaîne d'objet JSON avec les éléments suivants :<br><br>Actuellement, le seul paramètre de sauvegarde avancé pris en charge consiste à activer les sauvegardes Microsoft Volume Shadow Copy Service (VSS) pour Windows ou SQL Server exécutées sur une instance Amazon EC2.<br><br>Chaque sauvegarde avancée définit les éléments suivants :<br><br>• `Object key name`: chaîne qui indique le type de ressource auquel s'appliquent les paramètres avancés suivants.<br><br>Le nom de clé doit être le type de `"ec2"` ressource | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | • `Object value`: chaîne contenant un ou plusieurs paramètres de sauvegarde spécifiques au type de ressource associé.<br><br>La valeur indique que le `"windows_vss"` support concerne `enabled` ou concerne `disabled` les sauvegardes effectuées sur les instances Amazon EC2. | |

Exemple :

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
},
```

Syntaxe de sauvegarde : balises du plan de sauvegarde

La clé de `backup_plan_tags` stratégie spécifie les balises associées au plan de sauvegarde lui-même. Cela n'a aucun impact sur les balises spécifiées pour `rules` ou`selections`.

Éléments des balises du plan de sauvegarde

| Element | Description | Obligatoire |
| --- | --- | --- |
| `backup_plan_tags` | Chaque balise est une étiquette composée d'une clé et d'une valeur définies par l'utilisateur : | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | • `tag_key`: nom de la clé de balise à rechercher. Ce champ est obligatoire dans ce bloc. La valeur est sensible à la casse.<br>• `tag_value` : valeur attachée au plan de sauvegarde et associée au`tag_key`. Ce champ est obligatoire dans ce bloc. La valeur est sensible à la casse. | |

Syntaxe de sauvegarde : paramètres de numérisation

La clé `scan_settings` de politique spécifie la configuration pour l'analyse des programmes malveillants à l'aide d'Amazon GuardDuty Malware Protection for AWS Backup. Vous devez les utiliser `scan_settings` conjointement avec vos règles `scan_actions` de sauvegarde pour que les tâches de numérisation démarrent correctement.

Éléments des paramètres de numérisation

| Element | Description | Obligatoire |
| --- | --- | --- |
| `scan_settings` | Options de configuration pour les paramètre s de numérisation. Actuellement, les seuls paramètres de scan pris en charge sont l'activat ion d'Amazon GuardDuty Malware Protectio n pour AWS Backup. Vous devez spécifier le `ResourceTypes` et`ScannerRoleArn` .<br>• `ResourceTypes` : Cela filtrera l'analyse des programmes malveillants en fonction des critères de sélection des ressources que vous avez choisis. Vous pouvez utiliser `EBS`, `EC2`, `S3` ou `ALL`.<br>• `ScannerRoleArn` : Ce rôle est transmis AWS Backup à Amazon GuardDuty lorsqu'une analyse est lancée, ce qui permet d'accéder aux sauvegardes. Consultez l'accès à la protection contre les programme | Non |

| Element | Description | Obligatoire |
| --- | --- | --- |
| | s malveillants pour consulter la liste complète des autorisations requises. | |

Exemple :

Ce qui suit explique comment configurer `scan_actions` dans une règle de sauvegarde et `scan_settings` au niveau du plan pour activer l'analyse Amazon GuardDuty Malware Protection.

`scan_actions`dans une règle :

```
"scan_actions": {
    "GUARDDUTY": {
        "scan_mode": {
            "@@assign": "INCREMENTAL_SCAN"
        }
    }
}
```

`scan_settings`au niveau du plan :

```
"scan_settings": {
    "GUARDDUTY": {
        "resource_types": {
            "@@assign": ["EBS"]
        },
        "scanner_role_arn": {
            "@@assign": "arn:aws:iam::$account:role/MyGuardDutyScannerRole"
        }
    }
}
```

Exemples de politiques de sauvegarde

Les exemples de politiques de sauvegarde qui suivent sont fournis à titre informatif uniquement. Dans certains des exemples suivants, la mise en forme des espaces JSON peut être compressée pour économiser de l'espace.

- Exemple 1 : Politique attribuée à un nœud parent
- Exemple 2 : une politique parent est fusionnée avec une politique enfant

- Exemple 3 : Une politique parentale empêche toute modification par une politique enfant
- Exemple 4 : Une politique parent empêche la modification d'un plan de sauvegarde par une politique enfant
- Exemple 5 : une politique relative aux enfants remplace les paramètres d'une politique parentale
- Exemple 6 : Spécification des ressources à l'aide du bloc de balises
- Exemple 7 : Spécification des ressources avec le bloc de ressources
- Exemple 8 : plan de sauvegarde avec analyse Amazon GuardDuty Malware Protection

Exemple 1 : Politique affectée à un nœud parent

L'exemple suivant montre une politique de sauvegarde affectée à l'un des nœuds parents d'un compte.

Politique parente : cette politique peut être attachée à la racine de l'organisation ou à une UO parente de tous les comptes prévus.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
```

```
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@assign": "false"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "target_logically_air_gapped_backup_vault_arn": {
                        "@@assign": "arn:aws:backup:$region:$account:backup-
vault:AirGappedVault"
                    },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
```

```
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": {
                                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                            },
                            "tag_key": {
                                "@@assign": "dataType"
                            },
                            "tag_value": {
                                "@@assign": [
                                    "PII",
                                    "RED"
                                ]
                            }
                        }
                    }
                },
                "advanced_backup_settings": {
                    "ec2": {
                        "windows_vss": {
                            "@@assign": "enabled"
                        }
                    }
                }
```

```
        }
    }
}
```

Si aucune autre politique n'est héritée ou attachée aux comptes, la politique effective affichée dans chaque cas applicable Compte AWS ressemble à l'exemple suivant. L'expression CRON provoque l'exécution de la sauvegarde une fois par heure à l'heure pile. L'ID de compte 123456789012 sera l'ID de compte réel de chaque compte.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "target_logically_air_gapped_backup_vault_arn": "arn:aws:backup:
$region:$account:backup-vault:AirGappedVault",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
```

```
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

Exemple 2 : Une politique parente est fusionnée avec une politique enfant

Dans l'exemple suivant, une politique parent héritée et une politique enfant héritées ou directement associées à une Compte AWS fusion pour former la politique effective.

Politique parente : cette politique peut être attachée à la racine de l'organisation ou à une UO parente.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "delete_after_days": { "@@assign": "180" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "delete_after_days": { "@@assign": "180" },
```

```
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Politique enfant : cette politique peut être attachée directement au compte ou à une UO dans n'importe quel niveau inférieur à celui auquel la politique parente est attachée.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {
```

```
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "delete_after_days": { "@@assign": "365" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "MonthlyDatatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                            "tag_key": { "@@assign": "BackupType" },
                            "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                        }
                    }
                }
            }
        }
}
```

Politique effective résultante : la politique effective appliquée aux comptes contient deux plans, chacun avec son propre ensemble de règles et son ensemble de ressources auquel appliquer les règles.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "index_actions": {
                        "resource_types": {
```

```
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
```

```
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "delete_after_days": "365",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

Exemple 3 : Une politique parente empêche toute modification par une politique enfant

Dans l'exemple suivant, une politique parente héritée utilise les opérateurs de contrôle enfants pour appliquer tous les paramètres et empêche leur modification ou remplacement par une politique enfant.

Politique parente : cette politique peut être attachée à la racine de l'organisation ou à une UO parente. La présence de `"@@operators_allowed_for_child_policies": ["@@none"]` à chaque nœud de la politique signifie qu'une politique enfant ne peut apporter aucune modification au plan. Une politique enfant ne peut pas non plus ajouter des plans supplémentaires à la politique effective. Cette politique devient la politique effective pour chaque UO et chaque compte sous l'UO à laquelle elle est rattachée.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "index_actions": {
                       "@@operators_allowed_for_child_policies": ["@@none"],
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
```

```
                        }
                     },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "false"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                },
                                 "opt_in_to_archive_for_supported_resources": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "false"
                                }
```

```
                            }
                        }
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

Politique effective résultante : si des politiques de sauvegarde enfants existent, elles sont ignorées et la politique parente devient la politique effective.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "delete_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
```

```
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

Exemple 4 : Une politique parente empêche les modifications d'un plan de sauvegarde par une politique enfant

Dans l'exemple suivant, une politique parente héritée utilise les opérateurs de contrôle enfants pour appliquer les paramètres d'un plan unique et les empêche d'être modifiés ou remplacés par une politique enfant. La politique enfant peut encore ajouter des plans supplémentaires.

Politique parente : cette politique peut être attachée à la racine de l'organisation ou à une UO parente. Cet exemple est similaire au précédent où tous les opérateurs d'héritage enfants sont bloqués, sauf au niveau supérieur `plans`. Le paramètre `@@append` à ce niveau permet aux politiques enfants d'ajouter d'autres plans à l'ensemble dans la politique effective. Toutes les modifications du plan hérité sont toujours bloquées.

Les sections du plan sont tronquées pour plus de clarté.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Politique enfant : cette politique peut être attachée directement au compte ou à une UO dans n'importe quel niveau inférieur à celui auquel la politique parente est attachée. Cette politique enfant définit un nouveau plan.

Les sections du plan sont tronquées pour plus de clarté.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Politique effective résultante : la politique effective inclut les deux plans.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Exemple 5 : Une politique enfant remplace les paramètres d'une politique parente

Dans l'exemple suivant, une politique enfant utilise des opérateurs de définition de valeur pour remplacer certains des paramètres hérités d'une politique parente.

Politique parente : cette politique peut être attachée à la racine de l'organisation ou à une UO parente. Tous les paramètres peuvent être remplacés par une politique enfant, car le comportement par défaut, en l'absence d'un opérateur de contrôle enfant qui l'empêche, est d'autoriser la politique

enfant à `@@assign`, `@@append` ou `@@remove`. La politique parente contient tous les éléments requis pour un plan de sauvegarde valable, de sorte qu'elle sauvegarde vos ressources correctement si elles sont héritées en l'état.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "delete_after_days": {"@@assign": "180"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
```

```
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Politique enfant : la politique enfant inclut uniquement les paramètres qui doivent être différents de ceux de la politique parente héritée. Il doit y avoir une politique parente héritée qui fournit les autres paramètres requis lors de la fusion dans une politique effective. Sinon, la politique de sauvegarde effective contient un plan de sauvegarde non valable qui ne sauvegarde pas vos ressources comme prévu.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
```

```
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "delete_after_days": {"@@assign": "365"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    }
                }
            }
        }
    }
}
```

Politique effective résultante : la politique effective inclut les paramètres des deux politiques, ceux fournis par la politique enfant remplaçant les paramètres hérités de la politique parente. Dans cet exemple, les modifications suivantes se produisent :

- La liste des régions est remplacée par une liste complètement différente. Si vous souhaitez ajouter une région à la liste héritée, utilisez `@@append` au lieu de `@@assign` dans la politique enfant.
- AWS Backup se produit toutes les deux heures au lieu d'une heure.
- AWS Backup accorde 80 minutes pour démarrer la sauvegarde au lieu de 60 minutes.
- AWS Backup utilise le `Default` coffre au lieu de`FortKnox`.
- Le cycle de vie est prolongé pour le transfert vers le stockage à froid et la suppression à terme de la sauvegarde.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                     "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
```

```
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": "false"

                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Exemple 6 : Spécification des ressources avec le **`tags`** bloc

L'exemple suivant inclut toutes les ressources avec les `tag_key` symboles = "`env`" et `tag_value` = "`prod`" ou"`gamma`". Cet exemple exclut les ressources avec le `tag_key` = "`backup`" et le `tag_value` ="`false`".

```
...
"selections":{
    "tags":{
        "selection_name":{
            "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "tag_key":{"@@assign": "env"},
            "tag_value":{"@@assign": ["prod", "gamma"]},
            "conditions":{
                "string_not_equals":{
                    "condition_name1":{
                        "condition_key": { "@@assign": "aws:ResourceTag/backup"  },
                        "condition_value": {  "@@assign": "false" }
                    }
                }
            }
        }
    }
},
...
```

Exemple 7 : Spécification des ressources avec le **`resources`** bloc

Voici des exemples d'utilisation du `resources` bloc pour spécifier des ressources.

Example: Select all resources in my account

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Le `"resource_types"` bloc utilise un booléen `AND` pour combiner les types de ressources.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
```

```
            ]
        }
    }
},
...
```

Example: Select all resources in my account, but exclude Amazon EBS volumes

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Les `"not_resource_types"` blocs `"resource_types"` et utilisent un booléen `AND` pour combiner les types de ressources.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Les `"not_resource_types"` blocs `"resource_types"` et utilisent un booléen `AND` pour combiner les types de ressources. Le `"conditions"` bloc utilise un `AND` booléen.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
```

```
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key": { "@@assign":"aws:ResourceTag/backup"},
                    "condition_value": {  "@@assign":"true" }
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Le `"resource_types"` bloc utilise un booléen AND pour combiner les types de ressources. Le `"conditions"` bloc utilise un booléen AND pour combiner les types de ressources et les conditions des balises.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
```

```
                },
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"prod"}
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Le `"resource_types"` bloc utilise un booléen `AND` pour combiner les types de ressources. Le `"conditions"` bloc utilise un booléen `AND` pour combiner les types de ressources et les conditions des balises.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                  }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"test"}
                }
            }
        }
```

```
    }
},
...
```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Le `"resource_types"` bloc utilise un booléen AND pour combiner les types de ressources. Le `"conditions"` bloc utilise un booléen AND pour combiner les types de ressources et les conditions des balises.

Dans cet exemple, notez l'utilisation du caractère générique (`*`) dans `include**exclude*`, et`arn:aws:rds:*:*:db:*`. Vous pouvez utiliser le caractère générique (`*`) au début, à la fin et au milieu d'une chaîne.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "conditions":{
            "string_like":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key1"},
                    "condition_value":{"@@assign":"include*"}
                }
            },
            "string_not_like":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key2"},
                    "condition_value":{"@@assign":"*exclude*"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

La logique booléenne est similaire à celle que vous pouvez utiliser dans les politiques IAM. Les `"not_resource_types"` blocs `"resource_types"` et utilisent un booléen `AND` pour combiner les types de ressources. Le `"conditions"` bloc utilise un booléen `AND` pour combiner les types de ressources et les conditions des balises.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "resource_types":{
                "@@assign": [
                    "*"
                ]
            },
            "not_resource_types":{
                "@@assign":[
                    "arn:aws:fsx:*:*:file-system/*",
                    "arn:aws:rds:*:*:db:*"
                ]
            },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                }
            }
        }
    }
},
...
```

Exemple 8 : plan de sauvegarde avec analyse Amazon GuardDuty Malware Protection

L'exemple suivant montre une politique de sauvegarde qui permet à Amazon GuardDuty Malware Protection de scanner les points de restauration des sauvegardes. La politique utilise `scan_actions` la règle pour activer le scan et `scan_settings` au niveau du plan pour configurer le scanner.

Pour utiliser cette fonctionnalité, vous devez disposer des autorisations de rôle IAM appropriées. Pour plus d'informations, consultez Access dans le guide du AWS Backup développeur.

```
{
    "plans": {
        "Malware_Scan_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-east-1",
                    "us-west-2"
                ]
            },
            "rules": {
                "Daily_With_Incremental_Scan": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@assign": "Default"
                    },
                    "lifecycle": {
                        "delete_after_days": {
                            "@@assign": "35"
                        }
                    },
                    "scan_actions": {
                        "GUARDDUTY": {
                            "scan_mode": {
                                "@@assign": "INCREMENTAL_SCAN"
                            }
                        }
                    }
                },
                "Monthly_With_Full_Scan": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5 1 * ? *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "60"
                    },
```

```
                "target_backup_vault_name": {
                    "@@assign": "Default"
                },
                "lifecycle": {
                    "delete_after_days": {
                        "@@assign": "365"
                    }
                },
                "scan_actions": {
                    "GUARDDUTY": {
                        "scan_mode": {
                            "@@assign": "FULL_SCAN"
                        }
                    }
                }
            }
        },
        "selections": {
            "tags": {
                "scan_selection": {
                    "iam_role_arn": {
                        "@@assign": "arn:aws:iam::$account:role/MyBackupRole"
                    },
                    "tag_key": {
                        "@@assign": "backup"
                    },
                    "tag_value": {
                        "@@assign": [
                            "true"
                        ]
                    }
                }
            }
        },
        "scan_settings": {
            "GUARDDUTY": {
                "resource_types": {
                    "@@assign": [
                        "EBS"
                    ]
                },
                "scanner_role_arn": {
                    "@@assign": "arn:aws:iam::$account:role/MyGuardDutyScannerRole"
                }
```

```
                }
            }
        }
    }
}
```

Les points clés de cet exemple sont les suivants :

- `scan_actions`est spécifié dans chaque règle. Le nom du scanner `GUARDDUTY` est utilisé comme clé. Les utilisations des règles quotidiennes `INCREMENTAL_SCAN` et les utilisations des règles mensuelles`FULL_SCAN`.
- `scan_settings`est spécifié au niveau du plan (et non dans une règle). Il configure le rôle du scanner et les types de ressources à scanner.
- Ils `scanner_role_arn` doivent faire référence à un rôle IAM auquel est attachée la politique `AWSBackupGuardDutyRolePolicyForScans` gérée et à une politique de confiance qui permet au principal du `malware-protection.guardduty.amazonaws.com` service d'assumer le rôle.

## Politiques de balises

Les politiques relatives aux balises vous permettent de standardiser les balises associées aux AWS ressources dans les comptes de votre organisation.

Vous pouvez utiliser des politiques de balises pour maintenir la cohérence des balises, notamment le traitement préférentiel de la casse des clés et des valeurs de balise.

### Qu'est-ce qu'une balise ?

Les balises sont des étiquettes d'attributs personnalisées que vous attribuez ou que vous AWS attribuez à AWS des ressources. Chaque balise se compose de deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Les clés de balises sont sensibles à la casse.
- Un champ facultatif appelé valeur de balise (par exemple, `111122223333` ou `Production`). Si la valeur de balise est identique à l'utilisation d'une chaîne vide. Les valeurs de balise sont sensibles à la casse, tout comme les clés de balise.

La suite de cette page décrit les politiques de balises. Pour de plus amples informations sur les balises, consultez les sources suivantes :

- Pour obtenir des informations générales sur le balisage, notamment les conventions de dénomination et d'utilisation, consultez le Guide de l'utilisateur AWS des ressources de balisage.
- Pour obtenir la liste des services qui prennent en charge l'utilisation de balises, consultez Resource Groups Tagging API Reference.
- Pour plus d'informations sur l'utilisation de balises pour classer les ressources, consultez le livre blanc sur les meilleures pratiques en matière de balisage AWS des ressources.
- Pour de plus amples informations sur le balisage des ressources Organizations, consultez Ressources de balisage AWS Organizations.
- Pour plus d'informations sur le balisage des ressources dans d'autres services Services AWS, consultez la documentation de ce service.

## En quoi consistent les politiques de balises ?

Les politiques de balises sont un type de politique qui peut vous aider à standardiser les balises entre les ressources des comptes de votre organisation. Dans une politique de balises, vous spécifiez les règles de balisage applicables aux ressources lorsqu'elles sont balisées.

Par exemple, une politique de balises peut spécifier que lorsque la balise `CostCenter` est attachée à une ressource, elle doit utiliser le traitement de la casse et les valeurs de balise définis par la politique de balises. Une politique de balises peut également spécifier que des opérations de balisage non conformes sur certains types de ressources sont appliquées. En d'autres termes, les demandes de balisage non conformes sur des types de ressources spécifiés ne peuvent pas aboutir. Les ressources non balisées ou les balises qui ne sont pas définies dans la politique de balises ne sont pas soumises à une évaluation de conformité à la politique de balises.

L'utilisation de politiques de balises implique de travailler avec plusieurs Services AWS :

- Utilisez AWS Organizations pour gérer les politiques de balises. Lorsque vous êtes connecté au compte de gestion de l'organisation, vous utilisez Organizations pour activer la fonction des politiques de balises. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation. Vous pouvez ensuite créer des politiques de balises et les attacher aux entités de l'organisation pour appliquer ces règles de balisage.
- Utilisez Groupes de ressources AWS pour gérer la conformité aux politiques de balises. Lorsque vous êtes connecté à un compte de votre organisation, vous utilisez Resource Groups pour rechercher des balises non conformes sur les ressources du compte. Vous pouvez corriger les

balises non conformes dans le AWS service dans lequel vous avez créé la ressource. Vous pouvez également utiliser l'éditeur de balises et l'API de balisage Resource Groups pour étiqueter et dissocier les ressources de plusieurs services.

Si vous vous connectez au compte de gestion de votre organisation, vous pouvez afficher les informations de conformité pour tous les comptes de l'organisation.

Les politiques de balises sont disponibles uniquement dans une organisation où toutes les fonctions sont activées. Pour de plus amples informations sur les exigences d'utilisation des politiques de balises, consultez Conditions préalables et autorisations pour les politiques de gestion pour AWS Organizations.

> **Important**
>
> Pour commencer à utiliser les politiques de balises, il AWS est vivement recommandé de suivre l'exemple de flux de travail décrit dans Mise en route avec les politiques de balises avant de passer à des politiques de balises plus avancées. Il est préférable de comprendre les effets de l'attachement d'une politique de balises simple à un seul compte avant d'étendre les politiques de balises à l'ensemble d'une unité d'organisation ou d'une organisation. Il est particulièrement important de comprendre les effets d'une politique de balises avant d'appliquer la conformité à toute politique de balises. Les tableaux de la page Mise en route avec les politiques de balises comportent également des liens vers des instructions pour des tâches plus avancées liées aux politiques.

## Bonnes pratiques pour l'utilisation de politiques de balises

AWS recommande les meilleures pratiques suivantes pour l'utilisation des politiques relatives aux balises.

Décider d'une stratégie de capitalisation des balises

Déterminez comment utiliser les majuscules dans les balises et implémentez cette stratégie de manière systématique pour tous les types de ressources. Par exemple, décidez si vous souhaitez utiliser `Costcenter`, `costcenter` ou `CostCenter`, et utilisez la même convention pour toutes les balises. Pour obtenir des résultats cohérents dans les rapports de conformité, évitez d'utiliser des balises similaires avec un traitement de la casse incohérent. Cette stratégie vous aidera à définir des politiques de balises pour votre organisation.

Utiliser le flux de travail recommandé

Commencez petit en créant une politique de balises simple. Attachez-la ensuite à un compte membre que vous pouvez utiliser à des fins de test. Utilisez les flux de travail décrits sous la rubrique Mise en route avec les politiques de balises.

Déterminer des règles de balisage

Cela varie selon les besoins de votre organisation. Par exemple, vous souhaiterez peut-être spécifier que lorsqu'une `CostCenter` balise est attachée à des AWS Secrets Manager secrets, elle doit utiliser le traitement au cas par cas spécifié. Créez des politiques de balises qui définissent des balises conformes et attachez-les aux entités de l'organisation où vous souhaitez appliquer ces règles de balisage.

Former les administrateurs de compte

Lorsque vous êtes prêt à étendre votre utilisation des politiques de balises, formez les administrateurs de compte comme suit :

- Communiquez votre politique de balisage.
- Soulignez le fait que les administrateurs doivent utiliser des balises sur des types de ressources spécifiques.

  Cette étape est importante car les ressources non balisées ne s'affichent pas comme non conformes dans les résultats de conformité.
- Donnez des conseils sur la vérification de la conformité aux politiques de balises. Demandez aux administrateurs de rechercher et de corriger les balises non conformes sur les ressources de leur compte en suivant la procédure décrite dans la section Évaluation de la conformité d'un compte dans le Guide de l'utilisateur  AWS des ressources de balisage. Indiquez la fréquence à laquelle vous souhaitez qu'ils vérifient la conformité.

Soyez vigilant lors de l'application de la conformité.

L'application de la conformité risque d'empêcher les utilisateurs des comptes de votre organisation de baliser les ressources dont ils ont besoin. Prenez connaissance des informations de la rubrique Renforcez la cohérence du balisage. Consultez également les flux de travail décrits sous Mise en route avec les politiques de balises.

Soyez conscient des limites de marquage

AWS les services ont généralement une limite de 50 balises définies par l'utilisateur qui ne peuvent pas être modifiées. Lorsque vous utilisez des fonctionnalités telles que les balises requises pour signaler, assurez-vous que les politiques efficaces de votre organisation ne dépassent pas 50 balises requises pour un type de ressource donné. Le dépassement de cette limite peut entraîner deux problèmes : les ressources peuvent ne pas être en mesure d'atteindre le statut de conformité indiqué dans les résumés de conformité, et les plateformes d'infrastructure en tant que code (IaC) peuvent ne pas créer de ressources lorsque plus de 50 balises sont définies comme requis.

Envisagez de créer une politique de contrôle des services (SCP) pour définir des garde-fous autour des demandes de création de ressources

Les ressources auxquelles des balises n'ont jamais été associées ne s'affichent pas comme non conformes dans les rapports. Les administrateurs de compte peuvent toujours créer des ressources non balisées. Dans certains cas, vous pouvez utiliser une politique de contrôle des services (SCP) pour définir des barrières de sécurité autour des demandes de création de ressources.

Pour savoir si un AWS service prend en charge le contrôle d'accès à l'aide de balises, voir Services AWS That Work with IAM dans le guide de l'utilisateur IAM. Recherchez les services dont la valeur est « Oui » dans la colonne ABAC (autorisation basée sur les balises). Choisissez le nom du service pour afficher la documentation sur l'autorisation et le contrôle d'accès de ce service.

## Mise en route avec les politiques de balises

L'utilisation de politiques relatives aux balises implique de travailler avec plusieurs Services AWS. Pour commencer, consultez les pages suivantes. Suivez ensuite les flux de travail de cette page pour vous familiariser avec les politiques de balises et leurs effets.

- Conditions préalables et autorisations pour les politiques de gestion pour AWS Organizations
- Bonnes pratiques pour l'utilisation de politiques de balises

Utilisation des politiques de balises pour la première fois

Suivez ces étapes pour commencer à utiliser les politiques de balises pour la première fois.

| Sous-tâche | Compte auquel vous connecter | AWS console de service à utiliser |
| --- | --- | --- |
| Étape 1 : Activer les politiques de balises pour votre organisation. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Étape 2 : Créer une politique de balises.<br><br>Votre première politique de balises doit rester simple. Entrez une clé de balise dans le traitement de la casse que vous souhaitez utiliser et conservez les valeurs par défaut de toutes les autres options. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Étape 3 : Attacher une politique de balises à un seul compte membre que vous pouvez utiliser à des fins de test.<br><br>Vous devrez vous connecter à ce compte à l'étape suivante. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Étape 4 : Créer des ressources avec des balises conformes et d'autres ressources avec des balises non conformes. | Le compte membre que vous utilisez à des fins de test. | Tout AWS service avec lequel vous êtes à l'aise. Par exemple, vous pouvez utiliser AWS Secrets Manager et suivre la procédure présentée dans Création d'un secret basique pour créer des secrets conformes et non conformes. |

| Sous-tâche | Compte auquel vous connecter | AWS console de service à utiliser |
| --- | --- | --- |
| Étape 5 : Afficher la politique de balises effective et évaluer le statut de conformité du compte. | Le compte membre que vous utilisez à des fins de test. | Resource Groups et AWS service dans lequel la ressource a été créée.<br><br>Si vous avez créé des ressources avec des balises conformes et non conformes , vous devriez voir les balises non conformes dans les résultats. |
| Étape 6 : Répéter le processus de recherche et de correction des problèmes de conformité jusqu'à ce que les ressources du compte de test soient conformes à votre politique de balises. | Le compte membre que vous utilisez à des fins de test. | Resource Groups et AWS service dans lequel la ressource a été créée. |
| Vous pouvez évaluer la conformité à l'échelle de l'organisation à tout moment. | Le compte de gestion de l'organisation.[1] | Groupes de ressources |

[1] Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

Extension de l'utilisation des politiques de balises

Vous pouvez effectuer les tâches suivantes dans n'importe quel ordre pour étendre votre utilisation des politiques de balises.

| Tâche avancée | Compte auquel vous connecter | AWS console de service à utiliser |
| --- | --- | --- |
| Créez des politiques de balises plus avancées.<br><br>Suivez le même processus que pour les utilisateurs débutants, en essayant d'autres tâches. Par exemple, définissez des clés ou des valeurs supplémentaires ou spécifiez un traitement de la casse différent pour une clé de balise.<br><br>Vous pouvez utiliser les informations des rubriques Fonctionnement de l'héritage des politiques de gestion et Syntaxe des politiques de balises pour créer des politiques de balises plus détaillées. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Attachez des politiques en matière de balises à des comptes supplémentaires ou OUs.<br><br>Vérifiez la politique de balises effective d'un compte après avoir attaché d'autres politiques à ce compte ou à toute unité d'organisation dont il est membre. | Le compte de gestion de l'organisation.[1] | AWS Organizations |

| Tâche avancée | Compte auquel vous connecter | AWS console de service à utiliser |
| --- | --- | --- |
| Créez une SCP pour exiger des balises lorsque quelqu'un crée de nouvelles ressources. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Continuez à évaluer le statut de conformité du compte par rapport à la politique de balises effective à mesure de son évolution. Corrigez les balises non conformes. | Un compte membre avec une politique de balises effective. | Resource Groups et AWS service dans lequel la ressource a été créée. |
| Évaluez la conformité à l'échelle de l'organisation. | Le compte de gestion de l'organisation.[1] | Groupes de ressources |

[1] Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

Application des politiques de balises pour la première fois

Pour appliquer des politiques de balises pour la première fois, suivez un flux de travail similaire à l'utilisation des politiques de balises pour la première fois et utilisez un compte de test.

> **Warning**
>
> Soyez vigilant lors de l'application de la conformité. Assurez-vous de bien comprendre les effets de l'utilisation des politiques de balises et de suivre le flux de travail recommandé. Testez le fonctionnement de l'application sur un compte de test avant de l'étendre à d'autres comptes. Sinon, vous risquez d'empêcher des utilisateurs de comptes de votre organisation de baliser les ressources dont ils ont besoin. Pour de plus amples informations, consultez Renforcez la cohérence du balisage.

| Tâches d'application | Compte auquel vous connecter | AWS console de service à utiliser |
| --- | --- | --- |
| Étape 1 : Créez une politique de balises.<br><br>Votre première politique de balises appliquée doit rester simple. Entrez une clé de balise dans le traitement de la casse que vous souhaitez utiliser, puis choisissez l'option Empêcher les opérations non conformes pour cette balise. Spécifiez ensuite un type de ressource sur lequel l'appliquer. Dans le cas de l'exemple précédent, vous pouvez choisir de l'appliquer sur des secrets de Secrets Manager. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Étape 2 : Attachez une politique de balises à un seul compte de test. | Le compte de gestion de l'organisation.[1] | AWS Organizations |
| Étape 3 : Essayez de créer des ressources avec des balises conformes et d'autres avec des balises non conformes. Vous ne devriez pas être autorisé à créer une balise sur une ressource du type spécifié dans la politique de balises avec une balise non conforme. | Le compte membre que vous utilisez à des fins de test. | Tout AWS service avec lequel vous êtes à l'aise. Par exemple, vous pouvez utiliser AWS Secrets Manager et suivre la procédure présentée dans Création d'un secret basique pour créer des secrets conformes et non conformes. |

| Tâches d'application | Compte auquel vous connecter | AWS console de service à utiliser |
| --- | --- | --- |
| Étape 4 : Évaluez le statut de conformité du compte par rapport à la politique de balises effective et corrigez les balises non conformes. | Le compte membre que vous utilisez à des fins de test. | Resource Groups et AWS service dans lequel la ressource a été créée. |
| Étape 5 : Répétez le processus de recherche et de correction des problèmes de conformité jusqu'à ce que les ressources du compte de test soient conformes à votre politique de balises. | Le compte membre que vous utilisez à des fins de test. | Resource Groups et AWS service dans lequel la ressource a été créée. |
| Vous pouvez évaluer la conformité à l'échelle de l'organisation à tout moment. | Le compte de gestion de l'organisation.[1] | Groupes de ressources |

[1] Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

## Conformité du balisage des rapports

Les politiques de balises fournissent un mode de rapport pour les « règles de conformité de base » et la « clé de balise requise ». Vous pouvez utiliser ce mode pour évaluer la conformité d'un compte de votre organisation à sa politique en matière de balises en vigueur. Le rapport généré inclut uniquement les ressources qui ont eu au moins une balise définie par l'utilisateur à un moment quelconque de leur cycle de vie.

> **Important**
>
> Les ressources non balisées n'apparaissent pas comme non conformes dans les résultats. Pour rechercher des ressources non balisées dans votre compte, utilisez l'Explorateur de AWS ressources avec une requête qui utilise`tag:none`. Pour plus d'informations, consultez

la section Rechercher des ressources non balisées dans le guide de l'utilisateur de AWS Resource Explorer.

Rubriques

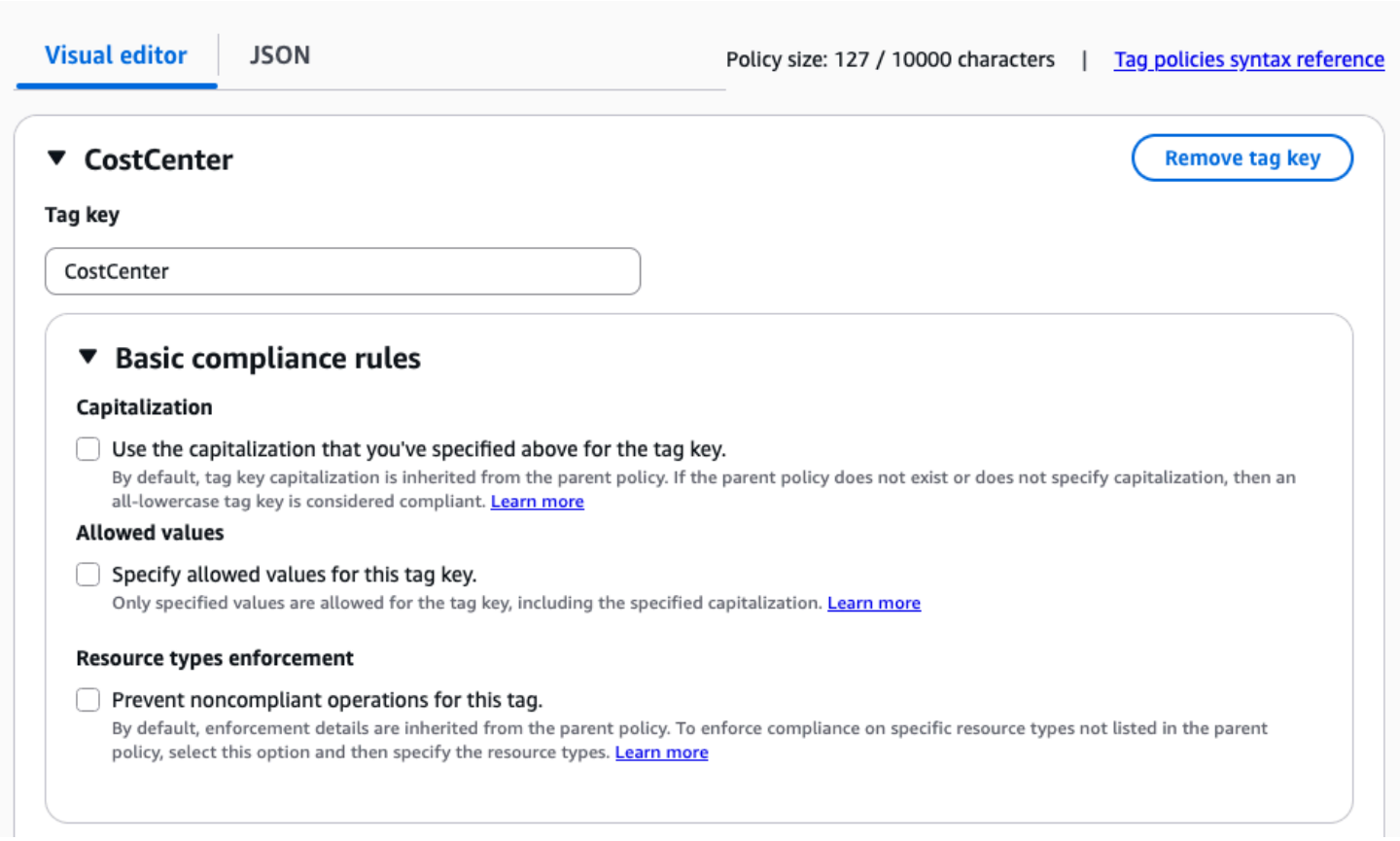
- Rapports pour les « règles de conformité de base »
- Signaler une « clé de balise requise »
- Génération d'un rapport de conformité à l'échelle de l'organisation

Rapports pour les « règles de conformité de base »

Grâce aux rapports relatifs aux règles de conformité de base, vous pouvez générer un rapport de conformité en matière de balisage qui vérifie la conformité par rapport à la capitalisation et aux valeurs de balise autorisées.

Pour signaler,

Dans l'onglet Éditeur visuel, entrez la valeur de la clé de balise par rapport à laquelle vous souhaitez signaler la conformité. La capture d'écran ci-dessous montre un rapport de conformité client pour la clé de balise CostCenter « ». Dans cet exemple, le rapport mettra en évidence une ressource étiquetée comme étant conforme si elle ne correspond qu'à une valeur minuscule de la clé de balise « CostCenter », ce qui signifie que la chaîne est égale à « costcenter ».

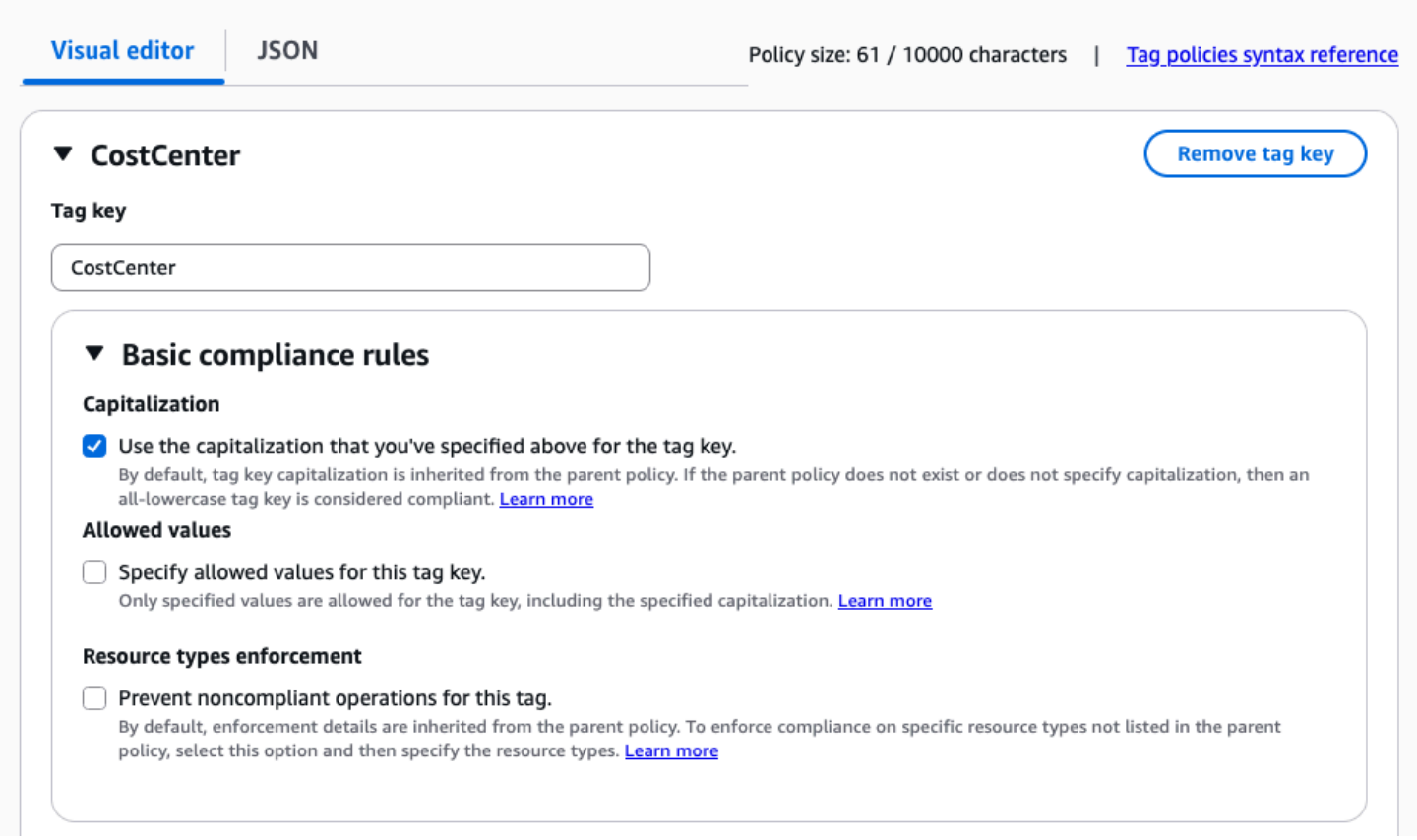



Le JSON ci-dessous génère un rapport de conformité pour les ressources par rapport à une valeur minuscule de la clé de balise « CostCenter ».

```
{
    "tags": {
        "CostCenter": {}
    }
}
```

Pour rendre compte de la capitalisation,

Dans l'onglet Éditeur visuel, entrez la valeur de la clé de balise par rapport à laquelle vous souhaitez signaler la conformité, puis sélectionnez l'option Capitalisation. La capture d'écran ci-dessous montre un rapport de conformité client pour la clé de balise CostCenter « » avec majuscule. Dans cet exemple, le rapport mettra en évidence une ressource balisée comme étant conforme si sa chaîne correspond exactement à la clé de balise CostCenter « ».



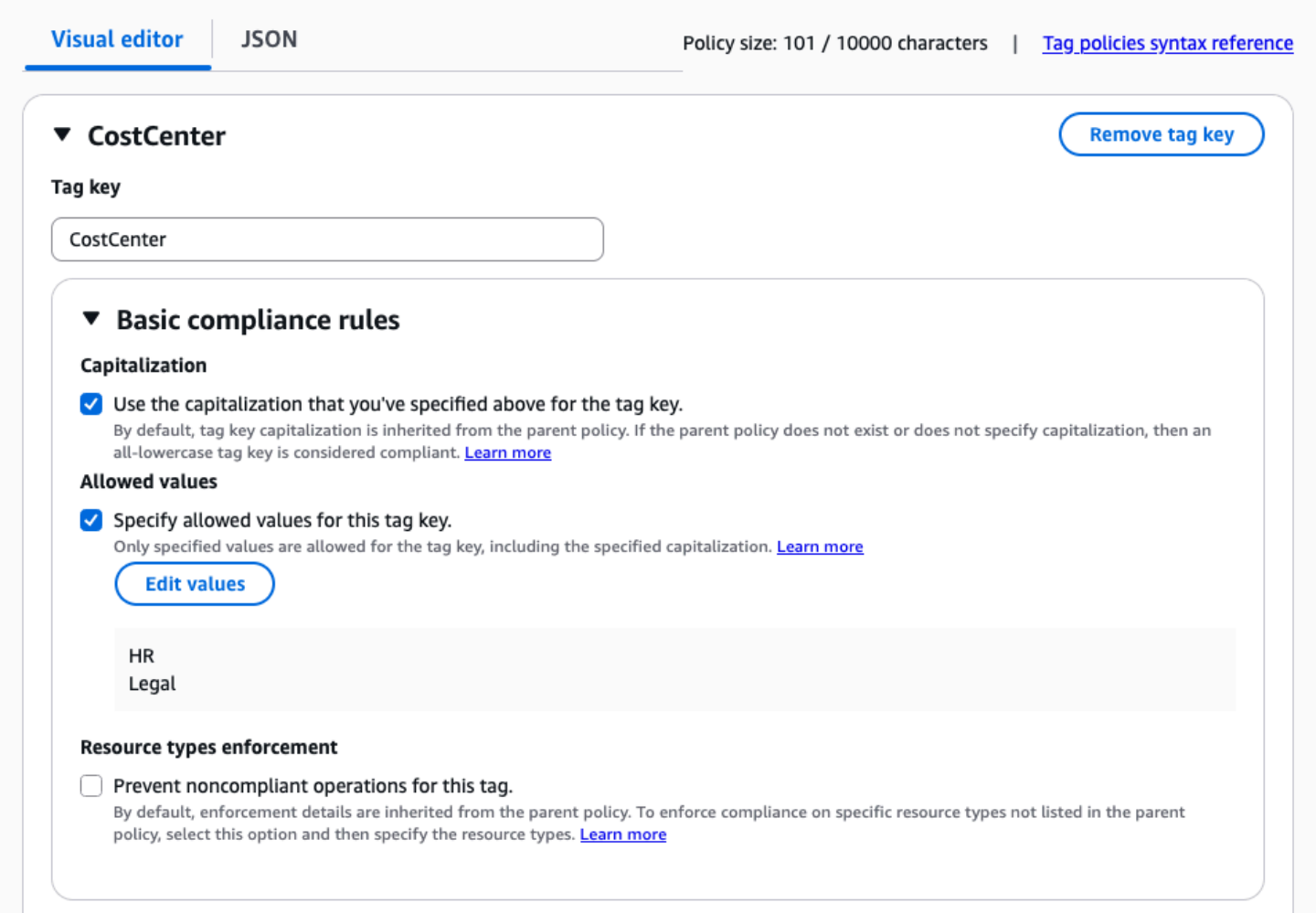

Le JSON ci-dessous génère un rapport de conformité des ressources par rapport à la clé de balise CostCenter « » avec une majuscule.

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            }
        }
    }
}
```

Pour établir un rapport sur les valeurs de balises autorisées en majuscules,

Dans l'onglet Éditeur visuel, entrez la valeur de la clé de balise par rapport à laquelle vous souhaitez signaler la conformité, sélectionnez l'option Valeurs autorisées et entrez des valeurs pour les valeurs de balise autorisées. La capture d'écran ci-dessous montre un rapport de conformité client pour la clé de balise CostCenter « » avec les majuscules et les valeurs de balise autorisées. Dans cet exemple,

le rapport indiquera qu'une ressource balisée est conforme s'il s'agit d'une chaîne correspondant exactement à la clé de balise CostCenter « » et si la valeur de la balise est « HR » ou « Legal ».




Le JSON ci-dessous génère un rapport de conformité des ressources par rapport à la clé de balise CostCenter « » avec une majuscule et les valeurs de balise autorisées « HR » et « Legal ».

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "HR",
                    "Legal"
                ]
            }
```

```
        }
    }
}
```

Signaler une « clé de balise requise »

> **Warning**
>
> La console AWS Resource Groups ne prend actuellement pas en charge la création de rapports sur les clés de balise requises lors de l'évaluation de la conformité d'un compte. Les ressources non conformes auxquelles il manque une clé de balise requise n'apparaîtront pas dans la section Ressources contenant des balises non conformes et ne marqueront pas le compte comme non conforme. Utilisez plutôt un rapport de conformité à l'échelle de l'entreprise pour rechercher les ressources non conformes auxquelles il manque une clé de balise requise.

Grâce aux rapports sur les clés de balise requises, vous pouvez évaluer si votre opération de création de ressources ne contient pas de clés de balise obligatoires ou obligatoires. Exécutez la commande suivante dans votre CLI pour répertorier les clés de balise requises définies dans la politique de balise effective du compte. Vous pouvez utiliser ces informations pour vérifier manuellement que vous créez une ressource avec toutes les balises requises telles que définies par l'administrateur de votre compte.

```
$ aws resourcegroupstaggingapi list-required-tags
```

Pour signaler les clés de tag requises,

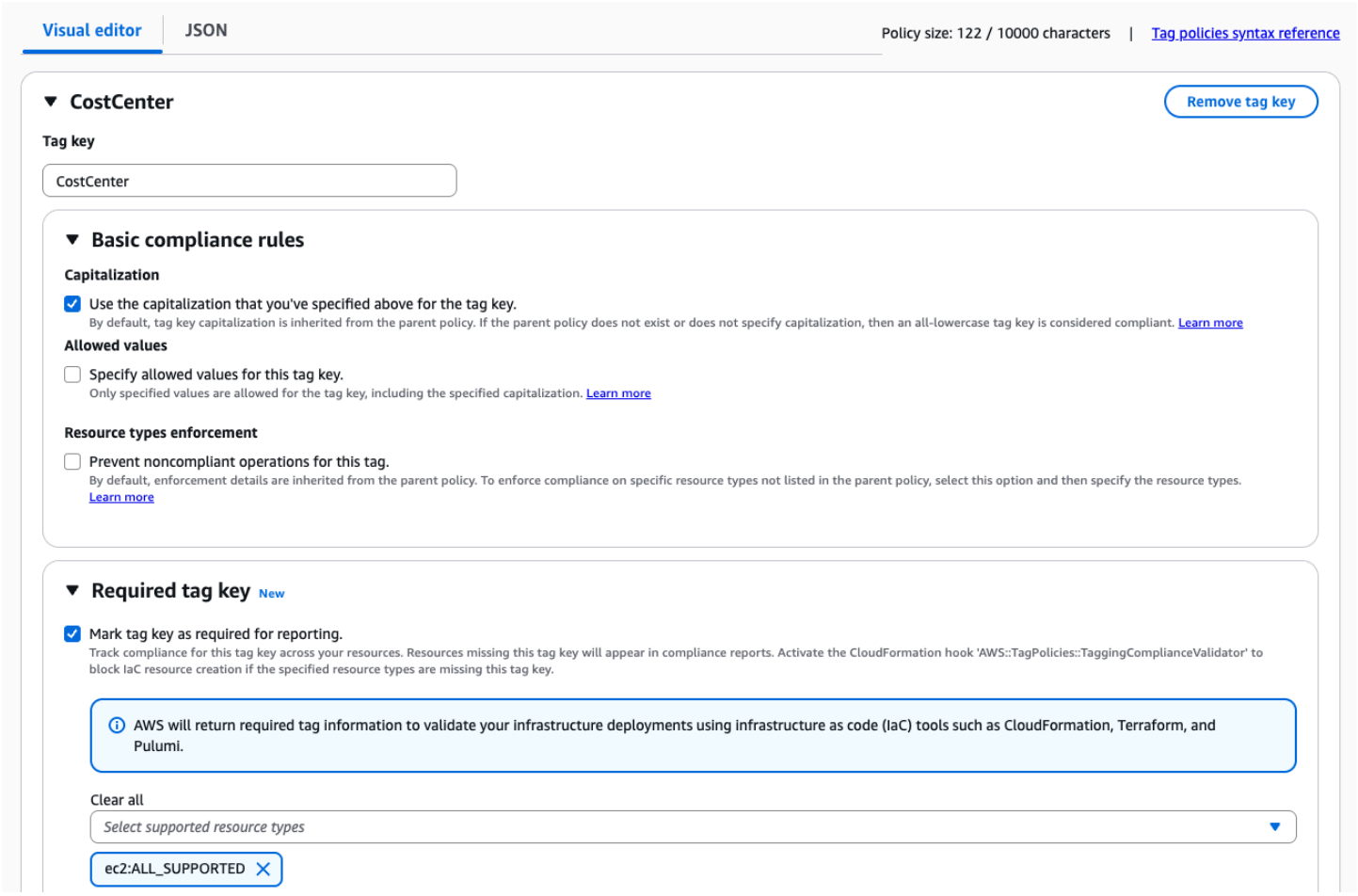
Dans l'onglet Éditeur visuel, entrez la valeur de la clé de balise par rapport à laquelle vous souhaitez signaler la conformité, puis sélectionnez l'option Marquer la balise comme requise pour le rapport. La capture d'écran ci-dessous montre un rapport de conformité client pour la clé de balise CostCenter « » avec une capitalisation et un rapport pour la clé de balise requise. Dans cet exemple, le rapport mettra en évidence une ressource balisée comme étant conforme si elle contient la chaîne exacte « CostCenter » comme clé de balise.

> **Important**
>
> Vous devez sélectionner à la fois les balises Capitalisation et Marque selon les besoins pour les options de reporting afin de générer un rapport des types de ressources sélectionnés pour

lesquels les balises requises sont manquantes. Par exemple, vous utiliserez ces deux options lorsque vous tenterez de vérifier la correspondance exacte avec la clé de balise CostCenter « ».

Vous pouvez uniquement sélectionner l'option Marquer les balises comme requises pour les rapports afin de générer un rapport sur les types de ressources sélectionnés pour lesquels les balises requises sont manquantes. Dans ce scénario, le rapport généré marquera les ressources comme conformes si elles présentent des variantes « », CostCenter « CostCenter », « Costcenter », « costcenter » ou toute autre variante similaire. Cette fonctionnalité vous permet de générer des rapports de conformité pour certains types de ressources, au lieu de toutes les ressources étiquetées de votre compte.

Si vous sélectionnez uniquement la mise en majuscules, un rapport sera généré pour TOUTES les ressources étiquetées et marquera ces ressources comme non conformes si la clé de balise ne correspond pas exactement à une chaîne.



Le JSON ci-dessous génère un rapport de conformité pour les ressources par rapport à la clé de balise CostCenter « » avec une majuscule et une balise mark, comme requis pour le reporting.

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "report_required_tag_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED"
                ]
            }
        }
    }
}
```

Pour faire appliquer,

Vous pouvez utiliser les rapports à l'aide d'outils IaC tels que CloudFormation Terraform et Pulumi pour avertir vos développeurs ou bloquer les déploiements dont les balises requises sont manquantes. Vous pouvez désormais utiliser une politique de balises efficace qui fonctionne entre CloudFormation Terraform et Pulumi. Voir Appliquer la « clé de balise requise » avec iAc pour plus de détails.

Génération d'un rapport de conformité à l'échelle de l'organisation

À tout moment, vous pouvez générer un rapport répertoriant toutes les ressources balisées de votre organisation. Comptes AWS Le rapport indique si chaque ressource est conforme à la politique de balises effective. Notez que l'affichage des modifications apportées à une politique de balises ou à des ressources dans le rapport de conformité à l'échelle de l'organisation peut prendre jusqu'à 48 heures. Par exemple, si vous avez une politique de balises qui définit une nouvelle balise standardisée pour un type de ressource, les ressources de ce type qui ne possèdent pas cette balise sont indiquées comme conformes dans le rapport pendant 48 heures au maximum.

Vous pouvez générer le rapport à partir du compte de gestion de votre organisation dans la région `us-east-1`, à condition qu'elle ait accès à un compartiment Amazon S3. Une politique de compartiment doit être attachée au compartiment, comme indiqué sous la rubrique Amazon S3 Bucket Policy for Storing Report. Pour générer le rapport, exécutez la commande suivante :

```
$ aws resourcegroupstaggingapi start-report-creation --region us-east-1
```

Vous pouvez générer un rapport à la fois.

La création de ce rapport peut prendre un certain temps. Vous pouvez vérifier son statut en exécutant la commande suivante :

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Une fois que la commande ci-dessus renvoie `SUCCEEDED`, vous pouvez ouvrir le rapport à partir du compartiment Amazon S3.

## Renforcez la cohérence du balisage

Les politiques de balises fournissent deux fonctionnalités pour vous aider à renforcer la cohérence du balisage dans vos AWS environnements : « Règles de conformité de base » et « Clé de balise requise ». Vous pouvez utiliser ces fonctionnalités avec deux modes de politique de balises : application et reporting. Cette section met en évidence le mode d'application pour les deux fonctionnalités. Pour plus de détails sur le mode de création de rapports pour les deux fonctionnalités, voir « Signaler la conformité en matière de balisage ».

Rubriques

- Appliquer les « règles de conformité de base »
- Bonnes pratiques
- Appliquer la « clé de balise requise » avec IaC
- Syntaxe des politiques de balises et exemples

### Appliquer les « règles de conformité de base »

En appliquant les règles de conformité de base, vous pouvez empêcher la création de ressources avec des valeurs de balises qui ne répondent pas aux exigences spécifiées dans votre politique de balises. Par exemple, vous pouvez définir une politique qui bloque les opérations de EC2 création d'Amazon si la clé de balise CostCenter « » fournie n'a pas de valeur de balise « Business » ou « Legal ». Les règles de conformité de base vous permettent également d'appliquer les règles

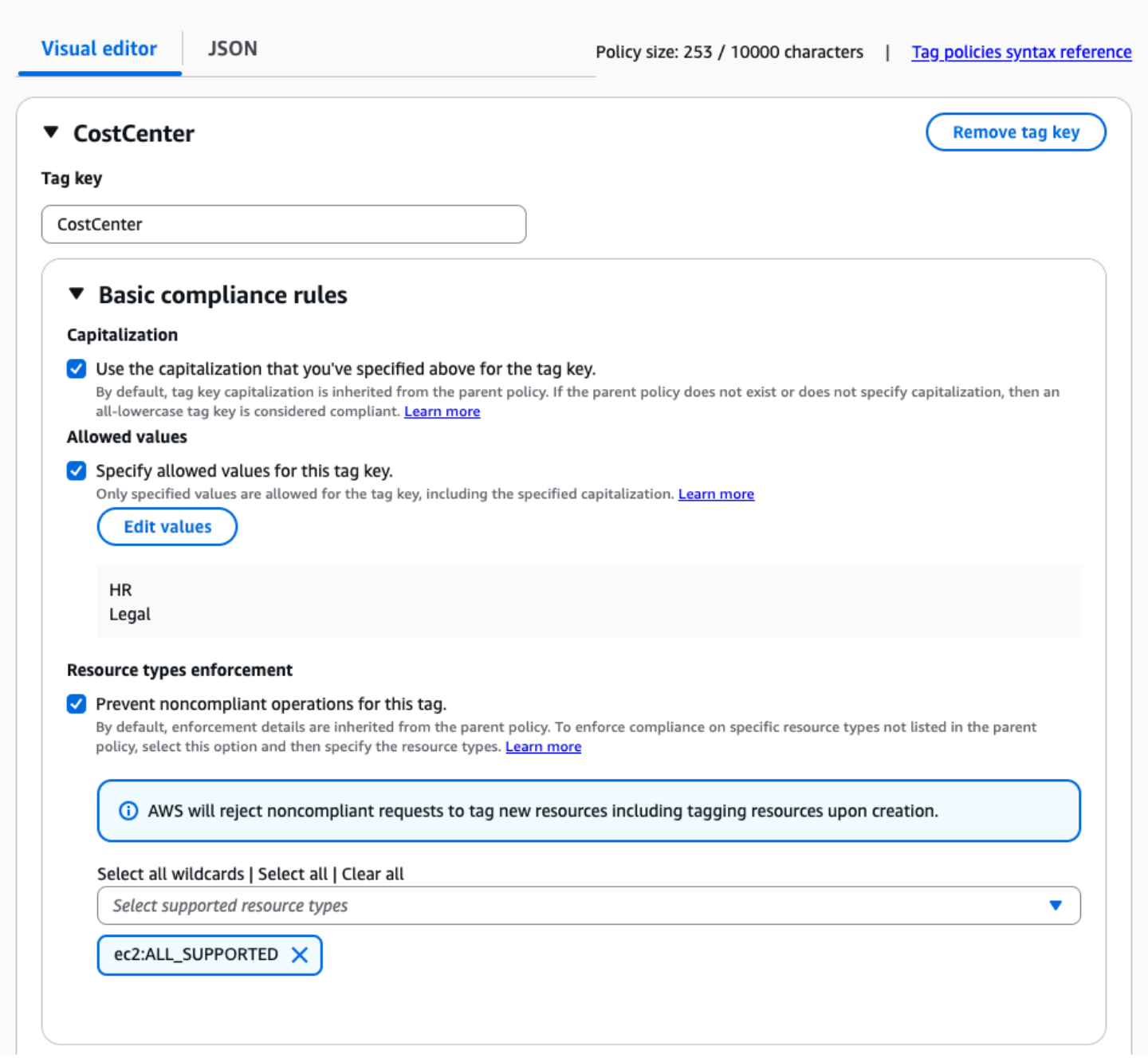
en fonction de la capitalisation des clés de balise. L'activation de la capitalisation garantit que les clés des balises correspondent exactement aux chaînes de caractères. La mise en majuscule traite CostCenter « », « CostCenter » et « Costcenter » comme des clés de balise uniques, ce qui signifie que l'application des clés de balise distingue les majuscules et minuscules. L'application des majuscules empêche les équipes de créer accidentellement des variations de tags. La cohérence du balisage est essentielle à la fois à la précision du suivi des coûts et aux politiques de sécurité du contrôle d'accès basé sur les attributs (ABAC) qui reposent sur une correspondance précise des balises pour accorder ou refuser l'accès aux ressources.

> **Important**
>
> Les règles de conformité de base n'appliquent pas la conformité aux balises sur les ressources créées sans balises. Cette fonctionnalité n'impose pas l'absence de clés de balise. Vous ne pouvez pas utiliser cette fonctionnalité pour garantir que les clés de balise requises ou obligatoires sont configurées lors de la création de la ressource. Utilisez le mode reporting dans « Clés de balise requises » pour appliquer les clés de balise requises pour les ressources créées par des outils IaC tels que CloudFormation Terraform et Pulumi. SCPs À utiliser pour empêcher les utilisateurs et les rôles IAM dans les comptes cibles de créer certains types de ressources si la demande n'inclut pas les balises spécifiées.

Pour appliquer les règles de conformité de base aux politiques de balises, effectuez l'une des opérations suivantes lorsque vous créez une politique de balises :

- Dans l'onglet Éditeur visuel, sélectionnez l'option Empêcher les opérations non conformes pour cette balise. Consultez la section Création d'une politique de balises pour savoir comment créer et joindre une politique de balises.
- Dans l'onglet JSON, utilisez le champ `enforced_for`. Pour de plus amples informations sur la syntaxe des politiques de balises, consultez Syntaxe des politiques de balises et exemples.

L'image ci-dessous montre l'expérience de console de l'onglet Visual editor. Dans cet exemple, le client définit une politique de balises qui appliquera la validation de la valeur des balises uniquement pour les types de EC2 ressources Amazon pris en charge par les politiques de balises. Cette politique vérifiera si la valeur de la balise est « Legal » ou « HR » lorsque la clé de balise fournie est « CostCenter » pour les types de EC2 ressources Amazon. Cette politique applique également la capitalisation, ce qui signifie qu'elle recherche une chaîne correspondant exactement à la clé de balise « CostCenter ».




Le JSON ci-dessous est la politique de balises générée à partir de l'exemple « CostCenter » ci-dessus.

> **Important**
>
> Nous vous recommandons d'utiliser l'éditeur visuel lorsque vous définissez votre politique de balises pour la première fois. L'éditeur visuel garantit la validité de la syntaxe de votre politique de balises, sans étapes supplémentaires, et vous offre une expérience cliquable

simplifiée pour définir votre politique de balises. Vous pouvez utiliser l'éditeur visuel ou l'onglet JSON pour définir votre politique en matière de balises.

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "HR",
                    "Legal"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED"
                ]
            }
        }
    }
}
```

Bonnes pratiques

Suivez ces bonnes pratiques en matière d'application avec les « Règles de conformité de base » et les « Clés de balise requises pour iAc » avec les politiques de balises :

- Faites preuve de prudence lors de l'application de la conformité : assurez-vous de comprendre les effets de l'utilisation de politiques en matière de balises et de suivre les flux de travail recommandés décrits dansMise en route avec les politiques de balises. Testez le fonctionnement de l'application sur un compte test avant de l'étendre à d'autres comptes ou unités organisationnelles. Sinon, vous risquez d'empêcher des utilisateurs de comptes de votre organisation de créer les ressources dont ils ont besoin.
- Soyez conscient des types de ressource que vous pouvez appliquer. Vous pouvez uniquement appliquer la conformité aux politiques de balise sur les types de ressources pris en charge. Les types de ressources prenant en charge l'application de la conformité sont répertoriés lorsque vous utilisez l'éditeur visuel pour créer une politique de balises.

- Comprenez les interactions avec certains services : certains Services AWS proposent des groupements de ressources semblables à des conteneurs qui créent automatiquement des ressources pour vous et propagent les balises d'une ressource d'un service à l'autre. Par exemple, les balises des EC2 groupes Amazon et des clusters Amazon EMR peuvent se propager automatiquement aux instances Amazon contenues. EC2 Vous avez peut-être des politiques en matière de balises pour Amazon EC2 plus strictes que pour les groupes ou les clusters Amazon EMR. Si vous activez l'application, la politique de balises empêche les ressources d'être balisées et peut bloquer le dimensionnement et le provisionnement dynamiques.

Les sections suivantes montrent comment trouver des ressources non conformes et les corriger pour qu'elles soient conformes.

- Identifiez et corrigez les incohérences en matière de balisage

Appliquer la « clé de balise requise » avec IaC

Les politiques de balises vous aident à maintenir un balisage cohérent dans l'ensemble de vos déploiements d'infrastructure sous forme de code (IaC). Avec les « clés de balise requises », vous pouvez vous assurer que toutes les ressources créées via des outils IaC tels CloudFormation que Terraform et Pulumi incluent les balises obligatoires définies par votre organisation.

Cette fonctionnalité vérifie vos déploiements iAc par rapport aux politiques de tag de votre organisation avant de créer des ressources. Lorsqu'un déploiement ne contient pas les balises requises, vous pouvez configurer vos paramètres iAc pour avertir vos équipes de développement ou empêcher complètement le déploiement. Cette approche proactive garantit la conformité du balisage dès la création des ressources, au lieu de nécessiter une correction manuelle ultérieure. L'application fonctionne sur plusieurs outils IaC à l'aide d'une seule définition de politique de balises, ce qui élimine le besoin de configurer des règles de balisage distinctes pour chaque outil utilisé par votre organisation.

Rubriques

- Renforcez avec CloudFormation
- Appliquer avec Terraform
- Renforcez avec Pulumi

Renforcez avec CloudFormation

> **Note**
>
> Pour appliquer les clés de balise requises CloudFormation, vous devez spécifier les balises requises pour votre type de ressource dans les politiques de balises. Pour en savoir plus, consultez la section the section called “Signaler une « clé de balise requise »”.

Configurer le rôle d'exécution pour le TaggingComplianceValidator crochet AWS : TagPolicies : : :

Avant d'activer le `AWS::TagPolicies::TaggingComplianceValidator` hook, vous devez créer un rôle d'exécution que le hook utilise pour accéder aux AWS services. Le rôle doit être associé à la politique de confiance suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "resources.cloudformation.amazonaws.com",
                    "hooks.cloudformation.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

Le rôle d'exécution doit également disposer d'une politique de rôle avec au moins les autorisations suivantes :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "tag:ListRequiredTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur la configuration des rôles d'exécution pour les extensions publiques, voir Configurer un rôle d'exécution avec des autorisations IAM et une politique de confiance pour l'accès aux extensions publiques dans le Guide de l' CloudFormation utilisateur.

Activez le TaggingComplianceValidator crochet AWS TagPolicies : : :

> **Important**
>
> Avant de continuer, vérifiez que vous disposez des autorisations requises pour utiliser les Hooks et consulter les contrôles proactifs depuis la CloudFormation console. Pour plus d'informations, consultez la section Accorder des autorisations IAM pour les CloudFormation Hooks.

Après avoir mis à jour votre politique en matière de balises, vous devez activer le `AWS::TagPolicies::TaggingComplianceValidator` hook dans tous les AWS comptes et régions où vous souhaitez faire respecter les exigences en matière de balisage.

Ce hook AWS géré peut être configuré selon deux modes :

- Mode d'avertissement : autorise les déploiements mais génère des avertissements lorsque les balises requises sont manquantes
- Mode échec : bloque les déploiements auxquels il manque les balises requises

Pour activer le hook à l'aide de la AWS CLI :

```
aws cloudformation activate-type \
    --type HOOK \
    --type-name AWS::TagPolicies::TaggingComplianceValidator \
    --execution-role-arn arn:aws:iam::123456789012:role/MyHookExecutionRole \
    --publisher-id aws-hooks \
    --region us-east-1
```

```
aws cloudformation set-type-configuration \
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":
{"HookInvocationStatus": "ENABLED", "FailureMode": "WARN", "TargetOperations":
 ["STACK"], "Properties":{}}}}' \
  --type-arn "arn:aws:cloudformation:us-east-1:123456789012:type/hook/AWS-TagPolicies-
TaggingComplianceValidator" \
  --region us-east-1
```

`region`Remplacez-le par votre AWS région cible et passez `"FailureMode":"FAIL"` au mode d'avertissement `"FailureMode":"WARN"` si vous préférez.

Activez le lien AWS TagPolicies : : : TaggingComplianceValidator : sur plusieurs comptes et régions avec CloudFormation StackSets

Pour les organisations possédant plusieurs AWS comptes, vous pouvez AWS CloudFormation StackSets activer le crochet de conformité en matière de balisage pour tous vos comptes et régions simultanément.

CloudFormation StackSets vous permettent de déployer le même CloudFormation modèle sur plusieurs comptes et régions en une seule opération. Cette approche garantit une application cohérente du balisage dans AWS l'ensemble de votre organisation sans nécessiter de configuration manuelle pour chaque compte.

À utiliser CloudFormation StackSets à cette fin :

1. Créez un CloudFormation modèle qui active le crochet de conformité en matière de balisage
2. Déployez le modèle en utilisant CloudFormation StackSets pour cibler vos unités organisationnelles ou des comptes spécifiques
3. Spécifiez toutes les régions dans lesquelles vous souhaitez activer l'application

Le CloudFormation StackSets déploiement gérera automatiquement le processus d'activation pour tous les comptes et régions spécifiés, garantissant ainsi une conformité uniforme en matière de balisage dans l'ensemble de votre organisation. Pour savoir comment déployer des CloudFormation Hooks dans une organisation avec un service géré CloudFormation StackSets, consultez ce AWS blog.

Déployez le CloudFormation modèle ci-dessous en utilisant CloudFormation StackSets pour activer le AWS : TagPolicies : : TaggingComplianceValidator Hook pour les comptes de votre organisation.

> **Important**
>
> Ce crochet ne fonctionne que comme un StackHook. Il n'a aucun effet lorsqu'il est utilisé comme crochet de ressources.

```
Resources:
  # Activate the AWS-managed hook type
  HookTypeActivation:
    Type: AWS::CloudFormation::TypeActivation
    Properties:
        AutoUpdate: True
        PublisherId: "AWS"
        TypeName: "AWS::TagPolicies::TaggingComplianceValidator"

  # Configure the hook
  HookTypeConfiguration:
    Type: AWS::CloudFormation::HookTypeConfig
    DependsOn: HookTypeActivation
    Properties:
      TypeName: "AWS::TagPolicies::TaggingComplianceValidator"
      TypeArn: !GetAtt HookTypeActivation.Arn
      Configuration: !Sub |
        {
          "CloudFormationConfiguration": {
            "HookConfiguration": {
              "TargetStacks": "ALL",
              "TargetOperations": ["STACK"],
              "Properties": {},
              "FailureMode": "Warn",
              "TargetFilters": {
                "Actions": [
                    "CREATE",
                    "UPDATE"
                ]}
            }
          }
        }
```

> **Note**
>
> Pour plus d'informations sur l'utilisation CloudFormation des hooks, voir Activer un hook basé sur le contrôle proactif dans votre compte.

### Appliquer avec Terraform

Pour appliquer les clés de balise requises avec Terraform, vous devez mettre à jour votre AWS fournisseur Terraform vers la version 6.22.0 ou supérieure et activer la validation des politiques de balises dans la configuration de votre fournisseur. Pour plus de détails sur la mise en œuvre et des exemples de configuration, consultez la documentation du AWS fournisseur Terraform sur l'application de la politique en matière de balises.

### Renforcez avec Pulumi

Pour appliquer les clés de balise requises avec Pulumi, vous devez activer le pack de politiques Tag Policy Reporting dans Pulumi Cloud et configurer votre rôle IAM avec des autorisations de lecture des politiques de balises. Pour plus de détails sur la mise en œuvre et des exemples de configuration, consultez la documentation de Pulumi sur l'application de la politique en matière de balises.

## Syntaxe des politiques de balises et exemples

Cette page décrit la syntaxe des politiques de balises et fournit des exemples.

### Rubriques

### Syntaxe des politiques de balises

Une politique de balises est un fichier texte brut qui est structuré conformément aux règles de JSON. La syntaxe des politiques de balises suit la syntaxe des types de politiques de gestion. Pour une présentation complète de cette syntaxe, consultez Fonctionnement de l'héritage des politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques du type de politique de balises.

La politique de balises suivante présente une syntaxe de base :

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200",
                    "300*"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:ALL_SUPPORTED"
                ]
            }
        }
    }
}
```

La syntaxe d'une politique de balises inclut les composants suivants :

- Le nom de clé du champ `tags`. Les politiques de balises commencent toujours par ce nom de clé fixe. Il s'agit de la ligne du haut dans l'exemple de politique ci-dessus.
- Une clé de politique qui identifie de manière unique l'instruction de politique. Elle doit correspondre à la valeur de la clé de balise, sauf pour le traitement de la casse. La valeur de la politique distingue les majuscules et minuscules.

  Dans cet exemple, `costcenter` est la clé de politique.

- Au moins une clé de balise qui spécifie la clé de balise autorisée avec l'utilisation des majuscules avec laquelle vous souhaitez que les ressources soient conformes. Si le traitement de la casse n'est pas défini, les clés de balise utilisent des minuscules par défaut. La valeur de la clé de balise doit correspondre à celle de la clé de politique. Toutefois, étant donné que la valeur de la clé de politique n'est pas sensible à la casse, l'usage de la casse peut être différent.

  Dans cet exemple, `CostCenter` est la clé de balise. Il s'agit du traitement de casse requis pour la conformité à la politique de balises. Les ressources qui utilisent un autre traitement de la casse pour cette clé de balise ne sont pas conformes à la politique de balises.

  Vous pouvez définir plusieurs clés de balise dans une politique de balises.

- (Facultatif) Une liste d'une ou plusieurs valeurs de balise acceptables pour la clé de balise. Si la politique de balises ne spécifie pas de valeur de balise pour une clé de balise, toutes les valeurs (y compris aucune valeur) sont considérées comme conformes.

  Dans cet exemple, les valeurs acceptables pour la clé de `CostCenter` balise sont `100200`, et`300*`.

- (Facultatif) Une option `enforced_for` qui indique s'il convient d'empêcher toute opération de balisage non conforme sur les services et ressources spécifiés. Dans la console, il s'agit de l'option Empêcher les opérations non conformes pour cette balise dans l'éditeur visuel permettant de créer des politiques de balises. La valeur par défaut de cette option est null.

  L'exemple de politique de balise indique que la `CostCenter` balise appliquée à toutes les AWS Secrets Manager ressources doit être conforme à cette politique.

  > **Warning**
  >
  > Vous ne devez modifier cette option par défaut que si vous êtes familiarisé avec l'utilisation de politiques de balises. Sinon, vous risquez d'empêcher des utilisateurs de comptes de votre organisation de créer les ressources dont ils ont besoin.

- Des opérateurs qui spécifient la manière dont la politique de balises fusionne avec les autres politiques de balises dans l'arborescence de l'organisation pour créer la politique de balises effective d'un compte. Dans cet exemple, `@@assign` est utilisé pour affecter des chaînes à `tag_key`, `tag_value` et `enforced_for`. Pour plus d'informations sur les opérateurs, consultez Opérateurs d'héritage.

- Vous pouvez utiliser le * caractère générique dans les valeurs des balises.

- Vous pouvez utiliser un caractère générique par valeur de balise. Par exemple, `*@example.com` est autorisé, contrairement à `*@*.com`.
- Vous pouvez utiliser le `ALL_SUPPORTED` caractère générique `enforced_for` sur le terrain pour certains services afin de permettre l'application de toutes les ressources prises en charge pour ce service. Pour obtenir la liste des services et des types de ressources qui prennent en charge `enforced_for`, consultez Services et types de ressource prenant en charge l'application.
- Vous ne pouvez pas utiliser un caractère générique pour spécifier tous les services ou pour spécifier une ressource pour tous les services.

### Exemples de politiques de balises

Les exemples de politiques de balises qui suivent sont fournis à titre informatif uniquement.

> **Note**
>
> Avant de tenter d'utiliser ces exemples de politiques de balises dans votre organisation, notez les éléments suivants :
>
> - Assurez-vous d'avoir suivi le flux de travail recommandé pour commencer à utiliser les politiques de balises.
> - Vous devez vérifier attentivement et personnaliser ces politiques de balises en fonction de vos exigences uniques.
> - Tous les caractères de votre politique de balises sont soumis à une taille maximale. Les exemples présentés dans ce manuel illustrent des politiques de balises formatées avec des espaces supplémentaires pour une meilleure lisibilité. Toutefois, pour gagner de l'espace si la taille de votre politique approche la limite maximale, vous pouvez supprimer tous les espaces. Les espacements et les sauts de ligne à l'extérieur des guillemets sont des exemples d'espaces.
> - Les ressources non balisées n'apparaissent pas dans les résultats comme étant non conformes.

#### Exemple 1 : Définition d'une casse de clé de balise à l'échelle de l'organisation

L'exemple suivant illustre une politique de balises qui définit uniquement deux clés de balise et la casse selon laquelle vous souhaitez standardiser les comptes de votre organisation.

Politique A : politique de balise attachée à la racine de l'organisation

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Cette politique de balises définit deux clés de balise : `CostCenter` et `Project`. L'attachement de cette politique de balises à la racine de l'organisation a les effets suivants :

- Tous les comptes de votre organisation héritent de cette politique de balises.
- Tous les comptes de votre organisation doivent utiliser le traitement de casse défini pour assurer la conformité. Les ressources avec des balises `CostCenter` et `Project` sont conformes. Les ressources avec un usage de la casse différent pour la clé de balise (par exemple `costcenter`, `Costcenter`, ou `COSTCENTER`) ne sont pas conformes.
- Les lignes `@@operators_allowed_for_child_policies": ["@@none"]` « verrouillent » les clés de balise. Les politiques de balises attachées plus bas dans l'arborescence de l'organisation (politiques enfants) ne peuvent pas utiliser les opérateurs de définition de valeur pour modifier la clé de balise, y compris son traitement de la casse.
- Comme avec toutes les politiques de balises, les ressources non balisées ou les balises qui ne sont pas définies dans la politique de balises ne sont pas soumises à une évaluation de leur conformité à la politique de balises.

AWS vous recommande d'utiliser cet exemple comme guide pour créer une politique de balise similaire pour les clés de balise que vous souhaitez utiliser. Attachez-la à la racine de l'organisation. Créez ensuite une politique de balises similaire à l'exemple suivant, qui définit uniquement les valeurs admises pour les clés de balise définies.

Étape suivante : Définir des valeurs

Supposons que vous avez attaché la politique de balises précédente à la racine de l'organisation. Vous pouvez ensuite créer une politique de balises comme suit, puis l'attacher à un compte. Cette politique définit les valeurs admises pour les clés de balise `CostCenter` et `Project`.

Politique B : politique de balise attachée à un compte

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Si vous attachez la politique A à la racine de l'organisation et la politique B à un compte, les politiques se combinent pour créer la politique de balises effective suivante pour le compte :

Stratégie A + stratégie B = stratégie de balise effective pour le compte

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
```

```
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Pour plus d'informations sur l'héritage des politiques, notamment des exemples de fonctionnement des opérateurs d'héritage et des exemples de politiques de balises efficaces, consultezFonctionnement de l'héritage des politiques de gestion.

Exemple 2 : Empêcher l'utilisation d'une clé de balise

Pour empêcher l'utilisation d'une clé de balise, vous pouvez attacher une politique de balises telle que la suivante à une entité d'organisation.

Cet exemple de politique spécifie qu'aucune valeur n'est acceptable pour la clé de balise `Color`. Il spécifie également qu'aucun opérateur n'est autorisé dans les politiques de balises enfants. Par conséquent, toutes les balises `Color` sur les ressources des comptes concernés sont considérées comme non conformes. Toutefois, l'option `enforced_for` empêche effectivement les comptes concernés de baliser uniquement les tables Amazon DynamoDB avec la balise `Color`.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
```

```
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Exemple 3 : Spécifier une politique de balises pour tous les types de ressources pris en charge par un AWS service spécifique

Pour définir une politique de balises pour tous les types de ressources pris en charge par un AWS service spécifique, vous utilisez le `ALL_SUPPORTED` caractère générique.

Cette politique utilise le `ALL_SUPPORTED` caractère générique pour spécifier que toutes les instances Amazon EC2 dotées de la `Environment` clé de balise ne peuvent avoir qu'une valeur `Prod` de balise égale à ou. `Non-prod` Ce joker constitue une alternative efficace sur une seule ligne à la liste individuelle de chaque instance Amazon EC2. Pour obtenir la liste des services et des types de ressources compatibles avec le `ALL_SUPPORTED` caractère générique, consultezServices et types de ressource prenant en charge l'application.

```
{
    "tags": {
        "Environment": {
            "tag_key": {
                "@@assign": "Environment",
                "@@operators_allowed_for_child_policies": ["@@none"]
            },
            "tag_value": {
                "@@assign": [
                    "Prod",
                    "Non-prod"
                ],
                "@@operators_allowed_for_child_policies": ["@@none"]
            },
            "enforced_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED"
                ]
            }
        }
    }
```

```
}
```

Exemple 4 : appliquer les clés de balise requises pour garantir la conformité

Cet exemple montre comment définir une politique de balises qui exige que toutes les ressources incluent des balises de conformité obligatoires. Organisations utilisent généralement ce modèle pour garantir une allocation des coûts, un suivi de propriété et une identification de l'environnement appropriés.

```
{
    "tags": {
        "CostCenter": {
            "report_required_tag_for": {
                "@@assign": [
                    "ec2:instance",
                    "s3:bucket",
                    "rds:db",
                    "lambda:function"
                ]
            },
            "tag_key": {
                "@@assign": "CostCenter"
            }
        },
        "Environment": {
            "report_required_tag_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED",
                    "rds:ALL_SUPPORTED",
                    "s3:ALL_SUPPORTED"
                ]
            },
            "tag_key": {
                "@@assign": "Environment"
            },
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Staging",
                    "Development",
                    "Test"
                ]
            }
```

```
        },
        "Owner": {
            "report_required_tag_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED"
                ]
            },
            "tag_key": {
                "@@assign": "Owner"
            }
        }
    }
}
```

Lorsque vous appliquez cette politique et configurez votre outil IaC avec l'application de la politique de balises :

- CostCenter: obligatoire pour les instances EC2, les compartiments S3, les bases de données RDS et les fonctions Lambda
- Environnement : obligatoire pour toutes les ressources EC2, RDS et S3, les valeurs autorisées étant limitées à la production, à la préparation, au développement ou aux tests
- Propriétaire : obligatoire pour toutes les ressources EC2 de votre organisation

Exemple de code d'infrastructure conforme à cette politique :

```
EC2Instance:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: ami-0c02fb55956c7d316
      InstanceType: t2.micro
      Tags:
        - Key: CostCenter
          Value: CC-12345
        - Key: Environment
          Value: Test
        - Key: Owner
          Value: john.doe@company.com
```

Si vous tentez de créer une ressource sans les balises requises, votre déploiement iAc échouera ou générera un avertissement pendant la phase de planification, en fonction de votre configuration.

Lorsqu'il est configuré en mode échec, le déploiement est bloqué avant la création de toute ressource. Lorsqu'il est configuré en mode avertissement, le déploiement se poursuit mais avertit votre équipe des balises manquantes. Le message d'erreur de validation identifie exactement les balises requises manquantes et les ressources qui en ont besoin.

Pour des instructions de configuration spécifiques à votre outil IaC :

- CloudFormation: Voir the section called "Renforcez avec CloudFormation" pour activer le crochet de conformité au balisage
- Terraform : voir the section called "Appliquer avec Terraform" pour activer la validation des politiques de balises dans le fournisseur AWS
- Remarque : Voir the section called "Renforcez avec Pulumi" pour activer le pack de politiques Tag Policy Reporting

## Identifiez et corrigez les incohérences en matière de balisage

Après avoir mis en œuvre des politiques relatives aux balises dans votre organisation, vous pouvez identifier les ressources présentant des balises non conformes et y remédier afin de garantir la cohérence au sein de votre AWS environnement. Cette section fournit des conseils pour détecter et corriger les incohérences en matière de balisage.

Rubriques

- Trouver des ressources non étiquetées ou mal étiquetées pour votre organisation avec Resource Explorer
- Correction des balises non conformes dans les ressources
- Utiliser Amazon EventBridge pour surveiller les tags non conformes

### Trouver des ressources non étiquetées ou mal étiquetées pour votre organisation avec Resource Explorer

Pour rechercher des ressources non balisées dans votre compte, utilisez-les Explorateur de ressources AWS avec une requête qui utilise`tag:none`. Resource Explorer fournit des fonctionnalités de recherche complètes pour identifier les ressources qui ne sont pas correctement étiquetées ou dont les valeurs de balise sont incohérentes au sein de votre organisation.

Pour obtenir des instructions détaillées sur l'utilisation de l'Explorateur de ressources pour rechercher des ressources non balisées ou mal étiquetées, voir Rechercher des ressources non balisées dans le guide de l'utilisateur.Explorateur de ressources AWS

Correction des balises non conformes dans les ressources

Après avoir trouvé des balises non conformes, apportez des corrections en utilisant l'une des méthodes suivantes. Vous devez être connecté au compte qui possède la ressource comportant des balises non conformes :

- Utilisez la console ou les opérations d'API de balisage du AWS service qui a créé les ressources non conformes.
- Utilisez les UntagResourcesopérations Groupes de ressources AWS TagResourceset pour ajouter des balises conformes à la politique en vigueur ou pour supprimer des balises non conformes.

Utiliser Amazon EventBridge pour surveiller les tags non conformes

Vous pouvez utiliser Amazon EventBridge, anciennement Amazon CloudWatch Events, pour surveiller l'introduction de balises non conformes. Dans l'exemple d'événement suivant, la valeur `"false"` de `tag-policy-compliant` indique qu'une nouvelle balise n'est pas conforme à la politique de balises effective.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
```

```
}
```

Vous pouvez vous abonner à des événements et spécifier des chaînes ou des modèles à surveiller. Pour plus d'informations EventBridge, consultez le guide de EventBridge l'utilisateur Amazon.

## Services et types de ressource prenant en charge l'application

Les services et types de ressources suivants prennent en charge l'application avec des politiques de balises :

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Amplify UI Builder [amplifyu ibuilder] | ampli build heme | • AWS: ifyU der: e | Yes | No | No | No |
| | ampli build pp/ envir nment, com ponen | • AWS: ifyU der: oner | Yes | Yes | No | No |
| | ampli build ompon | • AWS: ifyU der: oner | Yes | No | No | No |
| | ampli build | • N/ A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | LL_SU TED | | | | | |
| AWS Amplify [amplify] | ampli pps | • AWS: ify: | Yes | No | Yes | Yes |
| AWS App Mesh [appmesh] | appme esh | • AWS: esh: | Yes | Yes | Yes | Yes |
| | appme esh/ virtu algat / gatew oute | • AWS: esh: wayF | Yes | Yes | Yes | Yes |
| | appme esh/ virtu algat | • AWS: esh: ualG y | Yes | Yes | Yes | Yes |
| | appme esh/ virtu alnod | • AWS: esh: ualN | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | appme esh/ virtu alrou route | • AWS: esh: e | Yes | Yes | Yes | Yes |
| | appme esh/ virtu alser | • AWS: esh: ualS e | Yes | Yes | Yes | Yes |
| | appme esh/ virtu alrou | • AWS: esh: ualF | Yes | Yes | Yes | Yes |
| | appme LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| AWS App Runner [apprunne r] | appru :auto ingco uratio | • AWS: unne toSc Conf tior | Yes | No | Yes | Yes |
| | appru :serv | • AWS: unne rvic | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | appru :conn on | • N/ A | Yes | No | No | No |
| | appru :vpci ssconn ion | • AWS: unne cInc onne | Yes | No | Yes | Yes |
| | appru :obse ility igura | • AWS: unne serv tyCc rati | Yes | No | Yes | Yes |
| | appru :vpcc ctor | • AWS: unne cCor r | Yes | No | Yes | Yes |
| AWS AppConfig [appconfi g] | appco :appl ion/ envir onmen | • AWS: onfi virc | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | appco :envi ent | • AWS: onfi virc | Yes | No | No | No |
| | appco :conf ation | • N/ A | Yes | No | No | No |
| | appco :exte n | • AWS: onfi tens | Yes | No | Yes | Yes |
| | appco :appl ion | • AWS: onfi plic | Yes | Yes | Yes | Yes |
| | appco :exte nasso ion | • AWS: onfi tens soci | Yes | No | Yes | Yes |
| | appco :appl ion/ confi gurat rofil | • AWS: onfi nfig onPr | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | appco :appl ion/ envir onmen de ploym | • AWS: onfi ploy | Yes | Yes | No | No |
| | appco :depl ntstr y | • AWS: onfi ploy trat | Yes | Yes | Yes | Yes |
| AWS AppFabric [appfabric] | appfal :appb e/ inges on | • N/ A | Yes | No | No | No |
| | appfal :appb e | • N/ A | Yes | No | No | No |
| | appfal :appb e/ appau oriza | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS AppSync [appsync] | appsy omain s | • AWS: ync: inNa | Yes | No | No | No |
| | appsy pis | • AWS: ync: hQL/ | Yes | No | No | No |
| | appsy pis | • AWS: ync: | Yes | No | No | No |
| AWS Applicati on Auto Scaling [applicat ion-autos caling] | appli on- autos aling lable tar get | • AWS: icat toSc ::Sc eTa | Yes | No | No | No |
| AWS Applicati on Migration Service [mgn] | mgn:s e- serve | • N/ A | Yes | No | No | No |
| | mgn:c ctor | • N/ A | Yes | No | No | No |
| | mgn:a catio | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | mgn:w | • N/A | Yes | No | No | No |
| | mgn:l h- confi ratio te mplat | • N/A | Yes | No | No | No |
| | mgn:r catio co nfigu on- templ te | • N/A | Yes | No | No | No |
| | mgn:j | • N/A | Yes | No | No | No |
| | mgn:i t | • N/A | Yes | No | No | No |
| | mgn:v er- clien | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | mgn:e t | • N/ A | Yes | No | No | No |
| AWS Audit Manager [auditman ager] | auditı ger:a sment | • AWS: tMar :Ass nt | Yes | Yes | Yes | Yes |
| | auditı ger:c ol | • N/ A | Yes | Yes | No | No |
| | auditı ger:a sment ework | • N/ A | Yes | Yes | No | No |
| | auditı ger:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS B2B Data Interchan ge [b2bi] | b2bi: ile | • AWS: ::Pı | Yes | No | Yes | Yes |
| | b2bi: nersh | • AWS: ::Pa shi | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | b2bi: sform | • AWS: ::Tr rmer | Yes | No | Yes | Yes |
| | b2bi: bilit | • AWS: ::Ca ity | Yes | No | Yes | Yes |
| AWS Backup Gateway [backup-g ateway] | backu ga teway | • N/ A | Yes | Yes | No | No |
| | backu ga teway ervis | • AWS: upGa ::Hy sor | Yes | Yes | Yes | Yes |
| | backu ga teway eway | • N/ A | Yes | Yes | No | No |
| | backu ga teway _SUPP D | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Backup [backup-s earch] | backu se arch: ch- expor - job | • N/ A | Yes | No | No | No |
| | backu se arch: ch- job | • N/ A | Yes | No | No | No |
| AWS Backup [backup] | backu gal- hold | • N/ A | Yes | No | No | No |
| | backu ering con figur n | • N/ A | Yes | No | No | No |
| | backu port- plan | • AWS: up:: tPla | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | backu ckup- vaul t | • AWS: up:: ally ppec pVau<br>• AWS: up:: pVau | Yes | Yes | No | No |
| | backu store tes ting- plan | • AWS: up:: reTe Plar | Yes | No | Yes | Yes |
| | backu amewo | • AWS: up:: work | Yes | No | Yes | Yes |
| | backu ckup- plan | • AWS: up:: pPla | Yes | Yes | Yes | Yes |
| | backu cover po int | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | backu L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| AWS Batch [batch] | batch vice- envi ronme | • AWS: h::S eEnv ent | Yes | No | No | No |
| | batch - defin on | • AWS: h::J init | Yes | Yes | Yes | Yes |
| | batch eduli p olicy | • AWS: h::S ling y | Yes | No | Yes | Yes |
| | batch sumab r esour | • AWS: h::C able rce | Yes | No | Yes | Yes |
| | batch vice- job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | batch pute- envi ronme | • AWS: h::C eEnv ent | Yes | No | Yes | Yes |
| | batch | • N/ A | Yes | Yes | No | No |
| | batch - queue | • AWS: h::J ue | Yes | Yes | Yes | Yes |
| | batch _SUPP D | • N/ A | No | Yes | Yes | Yes |
| AWS Billing And Cost Managemen t Data Exports [bcm-data -exports] | bcm- data- expor xport | • AWS: ataE s::E | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Billing And Cost Managemen t Pricing Calculato r [bcm-pricing-calcu lator] | bcm-prici ng-calcu ator:v load-esti mate | • N/A | Yes | No | No | No |
| | bcm-prici ng-calcu ator:l - estim | • N/A | Yes | No | No | No |
| | bcm-prici ng-calcu ator:l - scena | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Billing Conductor [billingc onductor] | billi nduct illin up | • AWS: ingC tor: ingC | Yes | No | No | No |
| | billi nduct ricin n | • AWS: ingC tor: ingF | Yes | No | No | No |
| | billi nduct ustom item | • AWS: ingC tor: omLi m | Yes | No | No | No |
| | billi nduct ricin e | • AWS: ingC tor: ingF | Yes | No | No | No |
| AWS Billing [billing] | billi illin w | • AWS: ing: ingV | Yes | No | No | No |
| AWS Budget Service [budgets] | budge udget | • AWS: ets: et | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | budge udget, act ion | • AWS: ets: etsA | Yes | No | Yes | Yes |
| AWS BugBust [bugbust] | bugbu vent | • N/ A | Yes | Yes | No | No |
| | bugbu LL_SU TED | • N/ A | No | Yes | No | No |
| AWS Certifica te Manager [acm] | acm:c ficat | • AWS: ific nage rtif | Yes | Yes | Yes | Yes |
| | acm:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS Chatbot [chatbot] | chatb ustom act ion | • AWS: bot: omAc | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | chatb hat-confi gurat micro - teams ch annel | • AWS: bot: kCha onfi ion<br>• AWS: bot: osof sCha onfi ion | Yes | No | No | No |
| | chatb hat-confi gurat slack cha nnel | • AWS: bot: kCha onfi ion<br>• AWS: bot: osof sCha onfi ion | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | chatb hat-confi gurat chime web hook | • AWS: bot: kCha onfi ion<br>• AWS: bot: osof sCha onfi ion | Yes | No | No | No |
| AWS Clean Rooms ML [cleanroo ms-ml] | clean s-ml:co igure mo del-algor ithm | • N/ A | Yes | No | No | No |
| | clean s-ml:tr ned-model | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | clean s-ml:me ershi tr ained mod el | • N/ A | Yes | No | No | No |
| | clean s-ml:co igure mo del- algor ithm- asso ciati | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | clean s-ml:me ershi co nfigu model alg orith as socia | • N/A | Yes | No | No | No |
| | clean s-ml:me ershi tr ained mod el-infer nce-job | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | clean s-ml:tr ned-model -infer e-job | • N/A | Yes | No | No | No |
| | clean s-ml:au ence-mode l | • N/A | Yes | No | No | No |
| | clean s-ml:au ence-gene ratio job | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | clean s-ml:tr ning-data set | • AWS: nRoc :Tra Data | Yes | No | Yes | Yes |
| | clean s-ml:co igure au dienc mo del | • N/ A | Yes | No | No | No |
| AWS Clean Rooms [cleanroo ms] | clean s:col ratio | • AWS: nRoc olla ion | Yes | Yes | No | No |
| | clean s:mem hip/ priva cybud empla | • AWS: nRoc riva getT te | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | clean s:mem hip/ confi gured easso ion | • AWS: nRoc onfi Tabl ciat | Yes | Yes | No | No |
| | clean s:con redta | • AWS: nRoc onfi Tabl | Yes | Yes | Yes | Yes |
| | clean s:mem hip/ analy siste te | • AWS: nRoc naly mpla | Yes | No | No | No |
| | clean s:mem hip/ confi gured encem assoc on | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | clean s:mem hip | • AWS: nRoc embe | Yes | Yes | No | No |
| | clean s:mem hip/ idmap pingt | • AWS: nRoc dMap able | Yes | No | No | No |
| | clean s:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| AWS Cloud Map [serviced iscovery] | servi scove amesp | • AWS: iceD ery: Name<br>• AWS: iceD ery: ateD espa | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | servi scove ervic | • AWS: iceD ery: ice | Yes | No | Yes | Yes |
| AWS Cloud9 [cloud9] | cloud viron | • AWS: d9:: onme | Yes | Yes | No | No |
| | cloud L_SUP ED | • N/ A | No | Yes | No | No |
| AWS CloudForm ation [cloudfor mation] | cloud ation ck | • AWS: dFor n::S | Yes | No | Yes | Yes |
| | cloud ation ckset | • AWS: dFor n::S et | Yes | No | Yes | Yes |
| AWS CloudHSM [cloudhsm ] | cloud backu | • N/ A | Yes | No | No | No |
| | cloud clust | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS CloudTrail [cloudtrail] | cloud l:cha | • AWS: dTra hanr | Yes | No | Yes | Yes |
| | cloud l:eve tasto | • AWS: dTra vent tore | Yes | No | Yes | Yes |
| | cloud l:tra | • AWS: dTra rail | Yes | Yes | Yes | Yes |
| | cloud l:das rd | • AWS: dTra ashb | Yes | No | Yes | Yes |
| | cloud l:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| AWS CloudWatch RUM [rum] | rum:a nitor | • AWS: :App or | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS CodeArtifact [codeartifact] | codeart:r itory | • AWS: Arti :Rep ry | Yes | No | Yes | Yes |
| | codeart:d n | • AWS: Arti :Dom | Yes | No | Yes | Yes |
| | codeart:p ge-group | • AWS: Arti :Pac roup | Yes | No | No | No |
| AWS CodeBuild [codebuild] | codebu :proj | • AWS: Buil ojec | Yes | Yes | Yes | Yes |
| | codebu :flee | • AWS: Buil eet | Yes | No | No | No |
| | codebu :repo g roup | • AWS: Buil port | Yes | No | Yes | Yes |
| | codebu :ALL_ ORTED | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS CodeCommit [codecommit] | codec t:rep ory | • AWS: Comm epos | Yes | Yes | Yes | Yes |
| | codec t:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| AWS CodeConnections [codeconnections] | codec ction st | • N/ A | Yes | No | No | No |
| | codec ction nnect | • AWS: Conn ns:: ctic | Yes | No | Yes | Yes |
| | codec ction posit link | • N/ A | Yes | No | No | No |
| AWS CodeDeploy [codedeploy] | coded y:dep entco | • AWS: Depl eplc Conf | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | coded y:app tion | • AWS: Depl ppli n | Yes | No | Yes | Yes |
| | coded y:dep entgr | • AWS: Depl eplc Grou | Yes | No | No | No |
| | coded y:ins e | • N/ A | Yes | No | No | No |
| AWS CodePipeline [codepipeline] | codep ine:w ok | • AWS: Pipe :Web | Yes | Yes | Yes | Yes |
| | codep ine:p ine | • AWS: Pipe :Pip | Yes | Yes | Yes | Yes |
| | codep ine:a ntype | • AWS: Pipe :Cus tion | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | codep ine:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS CodeStar Connectio ns [codestar -connecti ons] | codes conne ns:co tion | • AWS: Sta ctic onne | Yes | Yes | Yes | Yes |
| | codes conne ns:ho | • N/ A | Yes | Yes | No | No |
| | codes conne ns:re tory- link | • AWS: Sta ctic epos Link | Yes | No | Yes | Yes |
| | codes conne ns:AL PPORT | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS CodeStar Notifications [codestar-notifications] | codes notif ions:r ficat ule | • AWS: Star icat :Not tior | Yes | No | Yes | Yes |
| AWS CodeStar [codestar] | codes proje | • AWS: Star HubR tory | Yes | No | No | No |
| AWS Config [config] | confi grega - autho ation | • AWS: ig:: gati hori n | Yes | Yes | Yes | Yes |
| | confi ganiz n- confi rule | • AWS: ig:: izat nfig | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | confi ganiz n- confo ance- pack | • AWS: ig:: izat nfor Pack | Yes | No | No | No |
| | confi nfig- rule | • AWS: ig:: gRul | Yes | Yes | Yes | Yes |
| | confi nfigu on- recor er | • AWS: ig:: gura ecor | Yes | No | No | No |
| | confi ored- quer y | • AWS: ig:: dQue | Yes | No | Yes | Yes |
| | confi nfig- aggr egato | • AWS: ig:: gura ggre | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | confi nform - pack | • AWS: ig:: rmar k | Yes | No | Yes | Yes |
| | confi L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| AWS Control Tower [controlt ower] | contr wer:l ngzon | • AWS: roll :Lar one | Yes | No | No | No |
| | contr wer:e edcon | • AWS: roll :Ena ontr | Yes | No | No | No |
| | contr wer:e edbas e | • AWS: roll :Ena asel | Yes | No | No | No |
| AWS Cost Explorer Service [ce] | ce:an ysubs tion | • AWS: Anom bscr n | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ce:co tegor | • AWS: Cost ory | Yes | No | Yes | Yes |
| | ce:an ymoni | • AWS: Anom nitc | Yes | No | Yes | Yes |
| AWS Cost and Usage Report [cur] | cur:d ition | • AWS: :Rep fini | Yes | No | Yes | Yes |
| AWS Data Exchange [dataexch ange] | datae nge:e led- revis ions | • N/ A | Yes | No | No | No |
| | datae nge:e - actio | • N/ A | Yes | No | No | No |
| | datae nge:e led- data- sets | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | datae nge:d grant | • N/ A | Yes | No | No | No |
| | datae nge:d sets | • N/ A | Yes | No | No | No |
| AWS Data Pipeline [datapipe line] | datap ine:p ine | • AWS: Pipe :Pip | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS DataSync [datasync ] | datas locat | • AWS: Sync atic<br>• AWS: Sync atic<br>• AWS: Sync atic ustı<br>• AWS: Sync atic<br>• AWS: Sync atic NTAF<br>• AWS: Sync atic ctSt<br>• AWS: Sync atic penz | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | | • AWS: Sync atic<br>• AWS: Sync atic indc<br>• AWS: Sync atic eBlc<br>• AWS: Sync atic | | | | |
| | datas task | • AWS: Sync k | Yes | No | Yes | Yes |
| | datas task/ exec ution | • N/ A | Yes | No | No | No |
| | datas agent | • AWS: Sync nt | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | datas syste job | • N/ A | Yes | No | No | No |
| | datas syste | • N/ A | Yes | No | No | No |
| AWS Database Migration Service [dms] | dms:a sment run | • N/ A | Yes | No | No | No |
| | dms:s p | • AWS: :Rep ionS Grou | Yes | Yes | Yes | Yes |
| | dms:e | • AWS: :Eve scri | Yes | Yes | Yes | Yes |
| | dms:r catio co nfig | • AWS: :Rep ionC | Yes | No | Yes | Yes |
| | dms:c | • AWS: :Cer ate | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | dms:r | • AWS: :Rep ionI ce | Yes | Yes | Yes | Yes |
| | dms:i nce- profi le | • AWS: :Ins Prof | Yes | No | Yes | Yes |
| | dms:t | • AWS: :Rep ionI | Yes | Yes | Yes | Yes |
| | dms:e int | • AWS: :Enc | Yes | Yes | Yes | Yes |
| | dms:d migra | • AWS: :Dat atic | Yes | No | No | No |
| | dms:d provi | • AWS: :Dat ider | Yes | No | Yes | Yes |
| | dms:m tion- proj ect | • AWS: :Mig nPro | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | dms:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS Deadline Cloud [deadline ] | deadl licen e ndpoi | • AWS: line ense int | Yes | No | Yes | Yes |
| | deadl farm | • AWS: line m | Yes | No | Yes | Yes |
| | deadl monit | • AWS: line itor | Yes | No | No | No |
| AWS DeepCompo ser [deepcomp oser] | deepc ser:c sitio | • N/ A | Yes | No | No | No |
| | deepc ser:m | • N/ A | Yes | No | No | No |
| AWS DeepRacer [deeprace r] | deepr :lead ard_e ation | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | deepr :lead ard | • N/ A | Yes | No | No | No |
| | deepr :mode | • N/ A | Yes | No | No | No |
| | deepr :trai _job | • N/ A | Yes | No | No | No |
| | deepr :eval on_jo | • N/ A | Yes | No | No | No |
| | deepr :car | • N/ A | Yes | No | No | No |
| AWS Device Farm [devicefa rm] | devic m:dev | • N/ A | Yes | No | No | No |
| | devic m:tes d- proje | • AWS: ceFa estC ojec | Yes | No | Yes | Yes |
| | devic m:dev nstan | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | devic m:dev ool | • AWS: ceFa evic | Yes | No | No | No |
| | devic m:pro | • AWS: ceFa roje | Yes | No | Yes | Yes |
| | devic m:tes d- sessi | • N/ A | Yes | No | No | No |
| | devic m:ses | • N/ A | Yes | No | No | No |
| | devic m:ins eprof | • AWS: ceFa nsta ofil | Yes | No | Yes | Yes |
| | devic m:net profi | • AWS: ceFa etwo file | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | devic m:vpc figur n | • AWS: ceFa PCE( urat | Yes | No | No | No |
| | devic m:run | • N/ A | Yes | No | No | No |
| AWS Diode Messaging [diode-me ssaging] | diode mes sagin spond flow | • N/ A | Yes | No | No | No |
| | diode mes sagin pping | • N/ A | Yes | Yes | No | No |
| | diode mes sagin quest flow | • N/ A | Yes | No | No | No |
| AWS Diode [diode] | diode nsfer | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | diode ount-mapp ing | • N/A | Yes | No | No | No |
| AWS Direct Connect [directco nnect] | direc nect:( f | • N/A | Yes | Yes | No | No |
| | direc nect:( g | • N/A | Yes | Yes | No | No |
| | direc nect:( n | • N/A | Yes | Yes | No | No |
| | direc nect:( g atewa | • N/A | Yes | No | No | No |
| | direc nect:/ SUPPO | • N/A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Directory Service [ds] | ds:di ory | • AWS: ctor ice: osof<br>• AWS: ctor ice: leAD | Yes | No | No | No |
| AWS Elastic Beanstalk [elasticb eanstalk] | elast anst latfo | • N/A | Yes | Yes | No | No |
| | elast anst onfig ionte te | • AWS: ticE alk: igur Temp | Yes | Yes | Yes | Yes |
| | elast anst pplic n | • AWS: ticE alk: icat | Yes | Yes | Yes | Yes |
| | elast anst nviro t | • AWS: ticE alk: ronm | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | elast anst pplic nvers | • AWS: ticE alk: icat rsic | Yes | Yes | Yes | Yes |
| | elast anst LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| AWS Elastic Disaster Recovery [drs] | drs:j | • N/ A | Yes | No | No | No |
| | drs:s e- netwo | • N/ A | Yes | No | No | No |
| | drs:r catio co nfigu on- templ te | • N/ A | Yes | No | No | No |
| | drs:s e- serve | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | drs:l h- confi ratio te mplat | • N/ A | Yes | No | No | No |
| | drs:r ery- insta nce | • N/ A | Yes | No | No | No |
| AWS Elastic Load Balancing [elasticl oadbalanc ing] | elast adbal ng:lo lance | • AWS: ticL lanc ::Lc ance | Yes | Yes | Yes | Yes |
| | elast adbal ng:ta group | • AWS: ticL lanc ::Ta roup | Yes | Yes | Yes | Yes |
| | elast adbal ng:lo lance | • AWS: ticL lanc Loac cer | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | elast adbal ng:li er | • AWS: ticL lanc ::Li r | Yes | Yes | Yes | Yes |
| | elast adbal ng:tr tore | • AWS: ticL lanc ::Tı ore | Yes | No | Yes | Yes |
| | elast adbal ng:li er- rule | • AWS: ticL lanc ::Li rRul | Yes | Yes | Yes | Yes |
| AWS Elemental Appliance s and Software [elementa l-applian ces-softw are] | eleme - appli es- softw re:qu | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Elemental MediaConnect [mediaconnect] | media ect:r routp | • AWS: aCor :Rou tput | Yes | No | No | No |
| | media ect:s e | • AWS: aCor :Flc ce | Yes | No | Yes | Yes |
| | media ect:o t | • AWS: aCor :Flc ut | Yes | No | Yes | Yes |
| | media ect:e lemen | • AWS: aCor :Flc tlem | Yes | No | Yes | Yes |
| | media ect:f | • AWS: aCor :Flc | Yes | No | Yes | Yes |
| | media ect:r rnetw nterf | • AWS: aCor :Rou two rfac | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | media ect:f vpcin ace | • AWS: aCor :Flo nte | Yes | No | No | No |
| | media ect:r rinpu | • AWS: aCor :Rou put | Yes | No | No | No |
| AWS Elemental MediaConv ert [mediacon vert] | media ert:q s | • AWS: aCor :Que | Yes | No | Yes | Yes |
| | media ert:p ts | • AWS: aCor :Pre | Yes | No | Yes | Yes |
| | media ert:j mplat | • AWS: aCor :Job ate | Yes | No | No | No |
| | media ert:j | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Elemental MediaLive [medialive] | media :node | • N/ A | Yes | No | No | No |
| | media :sdis e | • AWS: aLiv iSou | Yes | No | Yes | Yes |
| | media :rese ion | • N/ A | Yes | No | No | No |
| | media :sign map | • AWS: aLiv gnal | Yes | No | Yes | Yes |
| | media :netw | • AWS: aLiv twor | Yes | No | Yes | Yes |
| | media :clou ch- alarm templ | • AWS: aLiv oudW larm ate | Yes | No | Yes | Yes |
| | media :even dge- rule- templ | • AWS: aLiv entB Rule ate | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | media :mult x | • AWS: aLiv ltip | Yes | No | Yes | Yes |
| | media :clou ch- alarm templ group | • AWS: aLiv oudW larm ateG | Yes | No | Yes | Yes |
| | media :even dge- rule- templ group | • AWS: aLiv entB Rule ateG | Yes | No | Yes | Yes |
| | media :chan | • AWS: aLiv anne | Yes | No | No | No |
| | media :chan lacem roup | • AWS: aLiv anne emer p | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | media :inpu urity p | • AWS: aLiv putS tyGr | Yes | No | Yes | Yes |
| | media :inpu | • AWS: aLiv put | Yes | No | No | No |
| | media :inpu ice | • N/ A | Yes | No | No | No |
| AWS Elemental MediaPack age V2 [mediapac kagev2] | media agev2 nnelG / chann origi point | • AWS: aPac 2::C Endp | Yes | No | Yes | Yes |
| | media agev2 nnelg / chann origi point | • AWS: aPac 2::C Endp | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | media agev2 nnelg | • AWS: aPac 2::C lGrc | Yes | No | Yes | Yes |
| | media agev2 nnelG / chann | • AWS: aPac 2::C l | Yes | No | Yes | Yes |
| | media agev2 nnelg / chann | • AWS: aPac 2::C l | Yes | No | Yes | Yes |
| AWS Elemental MediaPack age [mediapac kage-vod] | media age- vod:p ackag confi tions | • AWS: aPac :Pac gCor atic | Yes | No | Yes | Yes |
| | media age- vod:a ssets | • AWS: aPac :Ass | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | media age-vod:p ackag group | • AWS: aPac :Pac gGrc | Yes | No | Yes | Yes |
| AWS Elemental MediaPack age [mediapac kage] | media age:c els | • AWS: aPac :Cha | Yes | No | Yes | Yes |
| | media age:o n_end ts | • AWS: aPac :Ori dpoi | Yes | No | Yes | Yes |
| AWS Elemental MediaStor e [mediasto re] | media e:fol | • N/ A | Yes | No | No | No |
| | media e:con er | • AWS: aSto onta | Yes | Yes | No | No |
| | media e:obj | • N/ A | Yes | No | No | No |
| | media e:ALL PORTE | • N/ A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Elemental MediaTail or [mediatai lor] | media or:pl ckcon ratio | • AWS: aTai Play onfi ion | Yes | No | Yes | Yes |
| | media or:so locat | • AWS: aTai Sou atic | Yes | No | Yes | Yes |
| | media or:li urce | • AWS: aTai Live e | Yes | No | Yes | Yes |
| | media or:vo rce | • AWS: aTai Vod | Yes | No | Yes | Yes |
| | media or:ch l | • AWS: aTai Char | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Elemental Support Cases [elemental-support-cases] | eleme - suppo cases e | • N/A | Yes | No | No | No |
| AWS End User Messaging Social [social-messaging] | socia me ssagi aba | • N/A | Yes | No | No | No |
| | socia me ssagi hone- numb er- id | • N/A | Yes | No | No | No |
| AWS Entity Resolution [entityresolution] | entit olutio chema ing | • AWS: tyRe ion: maMa | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | entit olutio atchi rkflo | • AWS: tyRe ion: hing low | Yes | Yes | Yes | Yes |
| | entit olutio dname e | • AWS: tyRe ion: mesp | Yes | No | Yes | Yes |
| | entit olutio dmapp orkfl | • AWS: tyRe ion: ppir flow | Yes | No | Yes | Yes |
| | entit olutio LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| AWS Fault Injection Service [fis] | fis:a n | • N/ A | Yes | No | No | No |
| | fis:e iment tem plate | • AWS: :Exp ntTe e | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | fis:e iment | • N/ A | Yes | No | No | No |
| AWS Firewall Manager [fms] | fms:a catio l ist | • N/ A | Yes | No | No | No |
| | fms:p cols- list | • N/ A | Yes | No | No | No |
| | fms:p y | • AWS: :Pol | Yes | No | No | No |
| | fms:r rce- set | • AWS: :Res Set | Yes | No | No | No |
| AWS Global Accelerat or [globalac celerator ] | globa elera accel or | • AWS: alAc ato ele | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | globa elera attac t | • AWS: alAc ator ssAc Atta t | Yes | No | Yes | Yes |
| AWS Glue DataBrew [databrew ] | datab job | • AWS: Brev | Yes | No | Yes | Yes |
| | datab recip | • AWS: Brev ipe | Yes | No | Yes | Yes |
| | datab sched | • AWS: Brev edul | Yes | No | Yes | Yes |
| | datab proje | • AWS: Brev ject | Yes | No | Yes | Yes |
| | datab rules | • AWS: Brev eset | Yes | No | Yes | Yes |
| | datab datas | • AWS: Brev aset | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Glue [glue] | glue:v flow | • AWS: ::Wo w | Yes | No | No | No |
| | glue: grati sourc perty | • AWS: ::Ir tior rceP ty | Yes | No | No | No |
| | glue: grati | • AWS: ::Ir tior | Yes | No | No | No |
| | glue:I print | • N/ A | Yes | No | No | No |
| | glue: letio | • N/ A | Yes | No | No | No |
| | glue: eprof | • AWS: ::Us ofil | Yes | No | Yes | Yes |
| | glue: | • AWS: ::Jo | Yes | No | Yes | Yes |
| | glue: ion | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | glue: ger | • AWS: ::Tr | Yes | No | Yes | Yes |
| | glue: log | • N/ A | Yes | No | No | No |
| | glue: ndpoi | • AWS: ::De oint | Yes | No | No | No |
| | glue: quali leset | • AWS: ::Da lity et | Yes | No | Yes | Yes |
| | glue:r ansfo | • AWS: ::ML form | Yes | No | Yes | Yes |
| | glue: ectio | • AWS: ::Co ion | Yes | No | Yes | Yes |
| | glue: ler | • AWS: ::Cr | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | glue: stry | • AWS: ::Re y | Yes | No | Yes | Yes |
| | glue: ma | • AWS: ::Sc | Yes | No | Yes | Yes |
| | glue: oment ype | • AWS: ::Cu ntit | Yes | No | Yes | Yes |
| | glue: base | • AWS: ::Da e | Yes | No | Yes | Yes |
| AWS Ground Station [groundst ation] | groun tion: act | • N/ A | Yes | No | No | No |
| | groun tion: ion- profi le | • AWS: ndSt ::Mi Prof | Yes | No | Yes | Yes |
| | groun tion: meris | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | groun tion: llite | • N/ A | Yes | No | No | No |
| | groun tion: ig | • AWS: ndSt ::Cc | Yes | No | Yes | Yes |
| | groun tion: flow- endp oint- grou p | • AWS: ndSt ::Da wEnc Grou | Yes | No | Yes | Yes |
| AWS HealthIma ging [medical- imaging] | medic i magin tasto | • AWS: thIm ::Da re | Yes | No | Yes | Yes |
| | medic i magin tasto i mages | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS HealthLake [healthlake] | healt e:dat re | • AWS: thLa HIRD ore | Yes | Yes | Yes | Yes |
| | healt e:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| AWS HealthOmics [omics] | omics otati ore | • AWS: s::A tior | Yes | Yes | No | No |
| | omics uence e/ reads | • N/ A | Yes | Yes | No | No |
| | omics erenc re/ refer nce | • N/ A | Yes | Yes | No | No |
| | omics | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | omics cache | • N/ A | Yes | No | No | No |
| | omics uence e | • AWS: s::S ceSt | Yes | Yes | Yes | Yes |
| | omics iants | • AWS: s::V tSto | Yes | Yes | No | No |
| | omics group | • AWS: s::F up | Yes | Yes | Yes | Yes |
| | omics kflow | • AWS: s::W ow | Yes | Yes | Yes | Yes |
| | omics erenc re | • AWS: s::F nceS | Yes | Yes | Yes | Yes |
| | omics otati ore/ versi on | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | omics kflow ver sion | • AWS: s::W owVe | Yes | No | No | No |
| | omics _SUPP D | • N/ A | No | Yes | Yes | Yes |
| AWS IAM Access Analyzer [access-a nalyzer] | acces an alyze alyze | • AWS: ssAr r::A er | Yes | No | Yes | Yes |
| AWS IAM Identity Center [sso] | sso:p ssion | • AWS: :Per onSe | Yes | No | No | No |
| | sso:a catio | • AWS: :App ion | Yes | No | No | No |
| | sso:i nce | • AWS: :Ins | Yes | No | No | No |
| | sso:t edtok suer | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Identity and Access Managemen t (IAM) [iam] | iam:m | • AWS: :Vir FADe | Yes | Yes | Yes | Yes |
| | iam:s r- certi cate | • AWS: :Ser rtif | Yes | Yes | Yes | Yes |
| | iam:s provi | • AWS: :SAM ider | Yes | Yes | Yes | Yes |
| | iam:o provi | • AWS: :OID ider | Yes | Yes | Yes | Yes |
| | iam:p y | • AWS: :Mar olic<br>• AWS: :Pol | Yes | Yes | No | No |
| | iam:r | • AWS: :Rol | Yes | No | Yes | Yes |
| | iam:u | • AWS: :Use | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iam:i nce- profi le | • AWS: :Ins Prof | Yes | Yes | Yes | Yes |
| | iam:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS Identity and Access Managemen t Roles Anywhere [nile] | nile: t- ancho | • AWS: sAny ::Tr chor | Yes | No | No | No |
| | nile: | • AWS: sAny ::CF | Yes | No | No | No |
| | nile: ect | • N/ A | Yes | No | No | No |
| | nile: ile | • AWS: sAny ::Pr | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Invoicing Service [invoicing] | invoi :proc ent-porta l-prefe nce | • N/A | Yes | No | No | No |
| | invoi :invo unit | • AWS: icir voic | Yes | No | Yes | Yes |
| AWS IoT Analytics [iotanalytics] | iotan ics:c el | • AWS: naly :Cha | Yes | Yes | No | No |
| | iotan ics:d et | • AWS: naly :Dat | Yes | Yes | No | No |
| | iotan ics:d tore | • AWS: naly :Dat e | Yes | Yes | No | No |
| | iotan ics:p ine | • AWS: naly :Pip | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotan ics:A UPPOR | • N/ A | No | Yes | No | No |
| AWS IoT Core Device Advisor [iotdevic eadvisor] | iotde advis uiter | • N/ A | Yes | No | No | No |
| | iotde advis uited ition | • AWS: oreD Advi Suit niti | Yes | No | Yes | Yes |
| AWS IoT Events [iotevent s] | iotev :dete model | • AWS: vent tect el | Yes | Yes | No | No |
| | iotev :inpu | • AWS: vent put | Yes | Yes | No | No |
| | iotev :alar el | • AWS: vent armM | Yes | No | No | No |
| | iotev :ALL_ ORTED | • N/ A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS IoT Fleet Hub for Device Managemen t [iotfleet hub] | iotfl ub:ap ation | • AWS: leet Appl on | Yes | Yes | Yes | Yes |
| | iotfl ub:AL PPORT | • N/ A | No | Yes | Yes | Yes |
| AWS IoT FleetWise [iotfleet wise] | iotfl ise:m - manif | • AWS: leet :Moc ifes | Yes | No | Yes | Yes |
| | iotfl ise:v le | • AWS: leet :Veh | Yes | No | Yes | Yes |
| | iotfl ise:d er- manif st | • AWS: leet :Dec anif | Yes | No | Yes | Yes |
| | iotfl ise:s - templ | • AWS: leet :Sta plat | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotfl ise:f | • AWS: leet :Fle | Yes | No | Yes | Yes |
| | iotfl ise:s l- catal | • AWS: leet :Sig talc | Yes | No | Yes | Yes |
| | iotfl ise:c ign | • AWS: leet :Cam | Yes | No | Yes | Yes |
| AWS IoT Greengras s [greengra ss] | green s:cor finit | • AWS: ngra oreD tior | Yes | Yes | Yes | Yes |
| | green s:com nts:v ons | • AWS: ngra :Com tVer | Yes | No | No | No |
| | green s:dev defin n | • AWS: ngra evic niti | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | green s:con orsde tion | • AWS: ngra onne efir | Yes | Yes | Yes | Yes |
| | green s:dep ents | • N/ A | Yes | No | No | No |
| | green s:fun nsdef ion | • AWS: ngra unct fini | Yes | Yes | Yes | Yes |
| | green s:bul | • N/ A | Yes | Yes | No | No |
| | green s:res esdef ion | • AWS: ngra esou fini | Yes | Yes | Yes | Yes |
| | green s:com nts | • N/ A | Yes | No | No | No |
| | green s:gro | • AWS: ngra roup | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | green s:log defin n | • AWS: ngra ogge niti | Yes | Yes | Yes | Yes |
| | green s:cor ices | • N/ A | Yes | No | No | No |
| | green s:sub ption initi | • AWS: ngra ubsc onDe ion | Yes | Yes | Yes | Yes |
| | green s:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| AWS IoT Managed Integrati ons [iotmanag edintegra tions] | iotma dinte ions: task | • N/ A | Yes | No | No | No |
| | iotma dinte ions: ged- thing | • AWS: anag egra ::Ma Thir | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotma dinte ions: d- conne or | • N/ A | Yes | No | No | No |
| | iotma dinte ions: unt- assoc iatio | • N/ A | Yes | No | No | No |
| | iotma dinte ions: ision profi | • AWS: anag egra ::Pr onir ile | Yes | No | No | No |
| | iotma dinte ions: entia lo cker | • AWS: anag egra ::Cr iall | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS IoT SiteWise [iotsitew ise] | iotsi se:po | • AWS: iteW Port | Yes | No | Yes | Yes |
| | iotsi se:da ard | • AWS: iteW Dash | Yes | No | Yes | Yes |
| | iotsi se:pr t | • AWS: iteW Proj | Yes | No | Yes | Yes |
| | iotsi se:as | • AWS: iteW Asse | Yes | Yes | Yes | Yes |
| | iotsi se:da t | • AWS: iteW Data | Yes | No | Yes | Yes |
| | iotsi se:ti s eries | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotsi se:co ation mod el | • AWS: iteW Comp onMo | Yes | No | No | No |
| | iotsi se:as model | • AWS: iteW Asse l | Yes | Yes | Yes | Yes |
| | iotsi se:ga y | • AWS: iteW Gate | Yes | No | Yes | Yes |
| | iotsi se:ac - polic | • AWS: iteW Acce icy | Yes | No | Yes | Yes |
| | iotsi se:AL PPORT | • N/ A | No | Yes | Yes | Yes |
| AWS IoT TwinMaker [iotdigit altwin] | iotdi ltwin kspac | • AWS: winM :Wor e | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotdi ltwin kspac co mpone t ype | • AWS: winM :Com tTyp | Yes | No | No | No |
| | iotdi ltwin kspac sc ene | • AWS: winM :Sce | Yes | No | No | No |
| | iotdi ltwin kspac sy nc- job | • AWS: winM :Syn | Yes | No | No | No |
| | iotdi ltwin ity | • AWS: winM :Ent | Yes | No | No | No |
| AWS IoT Wireless [iotwirel ess] | iotwi ss:si lkacc | • AWS: irel Part cour | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotwi ss:ne kanal confi tion | • AWS: irel Netw alyz figu n | Yes | No | Yes | Yes |
| | iotwi ss:se eprof | • AWS: irel Serv ofil | Yes | No | Yes | Yes |
| | iotwi ss:mu astgr | • AWS: irel Mult Grou | Yes | No | Yes | Yes |
| | iotwi ss:wi ssgat | • AWS: irel Wire atev | Yes | No | Yes | Yes |
| | iotwi ss:wi ssdev | • AWS: irel Wire evic | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iotwi ss:de ation | • AWS: irel Dest on | Yes | No | Yes | Yes |
| | iotwi ss:fu ask | • AWS: irel Fuot | Yes | No | Yes | Yes |
| | iotwi ss:im task | • AWS: irel Wire evic rtTa | Yes | No | Yes | Yes |
| | iotwi ss:wi ssgat taskd ition | • AWS: irel Task itic | Yes | No | Yes | Yes |
| | iotwi ss:de profi | • AWS: irel Devi file | Yes | No | Yes | Yes |
| AWS IoT [iot] | iot:p ge | • AWS: :Sof Pack | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iot:a rizer | • AWS: :Aut er | Yes | No | Yes | Yes |
| | iot:p ge/ versi n | • AWS: :Sof Pack rsic | Yes | No | No | No |
| | iot:f metri | • AWS: :Fle ric | Yes | No | Yes | Yes |
| | iot:j mplat | • AWS: :Job ate | Yes | No | Yes | Yes |
| | iot:b nggro | • AWS: :Bil roup | Yes | No | Yes | Yes |
| | iot:p sioni mplat | • AWS: :Pro ning ate | Yes | No | Yes | Yes |
| | iot:t type | • AWS: :Thi e | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iot:t group | • AWS: :Thi up | Yes | No | Yes | Yes |
| | iot:c ficat vider | • AWS: :Cer ateF er | Yes | No | Yes | Yes |
| | iot:r lias | • AWS: :Rol s | Yes | No | Yes | Yes |
| | iot:c t | • AWS: :CAC icat | Yes | No | Yes | Yes |
| | iot:c mmetr | • AWS: :Cus tric | Yes | No | Yes | Yes |
| | iot:d nconf ation | • AWS: :Dom nfig on | Yes | No | No | No |
| | iot:p y | • AWS: :Pol | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iot:m ation on | • AWS: :Mit onAc | Yes | No | Yes | Yes |
| | iot:s itypr e | • AWS: :Sec Prof | Yes | No | Yes | Yes |
| | iot:r | • AWS: :Top e | Yes | No | Yes | Yes |
| | iot:s uleda | • AWS: :Sch dAuc | Yes | No | Yes | Yes |
| | iot:t l | • N/ A | Yes | No | No | No |
| | iot:s m | • N/ A | Yes | No | No | No |
| | iot:j | • N/ A | Yes | No | No | No |
| | iot:o date | • N/ A | Yes | No | No | No |
| | iot:c nd | • AWS: :Com | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | iot:d sion | • AWS: :Dim n | Yes | No | Yes | Yes |
| AWS Key Managemen t Service [kms] | kms:k | • AWS: :Key | Yes | Yes | Yes | Yes |
| | kms:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS Lambda [lambda] | lambd yer/ versi on | • AWS: da:: Vers | Yes | No | No | No |
| | lambd yerve n | • AWS: da:: Vers | Yes | No | No | No |
| | lambd yer | • N/ A | Yes | No | No | No |
| | lambd nctio | • AWS: da:: ion | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | lambd ent- sourc e- mappi | • AWS: da:: Sou ping | Yes | No | Yes | Yes |
| | lambd de- signi g- confi | • AWS: da:: igni fig | Yes | No | Yes | Yes |
| | lambd L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| AWS Launch Wizard [launchwi zard] | launc ard:d yment | • AWS: chWi :Dep nt | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS License Manager Linux Subscript ions Manager [license- manager-l inux-subs criptions ] | licen m anage li nux- subsc ripti subsc ion- provi der | • N/ A | Yes | No | No | No |
| AWS License Manager User Subscript ions [license- manager-u ser-subsc riptions] | licen m anage us er- subsc iptio roduc su bscri n | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | licen m anage us er- subsc iptio denti p rovid | • N/ A | Yes | No | No | No |
| | licen m anage us er- subsc iptio nstan u ser | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | licen m anage us er- subsc iptio icens se rver- endp oint | • N/ A | Yes | No | No | No |
| AWS License Manager [license-manager] | licen m anage cense ass et- group | • N/ A | Yes | No | No | No |
| | licen m anage cense | • AWS: nseM r::l e | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | licen m anage cense ass et-rules t | • N/ A | Yes | No | No | No |
| | licen m anage cense con figur n | • N/ A | Yes | No | No | No |
| | licen m anage port- gene rator | • N/ A | Yes | No | No | No |
| | licen m anage ant | • AWS: nseM r::( | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS MWAA Serverles s [airflow-serverles s] | airfl s erver :work | • N/ A | Yes | No | No | No |
| AWS Mainframe Moderniza tion Applicati on Testing [apptest] | appte estsu | • N/ A | Yes | No | No | No |
| | appte estco urati | • N/ A | Yes | No | No | No |
| | appte estca | • AWS: est: Case | Yes | No | Yes | Yes |
| | appte estru | • N/ A | Yes | No | No | No |
| AWS Mainframe Moderniza tion Service [m2] | m2:ap | • AWS: Appl on | Yes | No | No | No |
| | m2:en | • AWS: Envi nt | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Marketpla ce Vendor Insights [vendor-i nsights] | vendo in sight curit pr ofile | • N/ A | Yes | No | No | No |
| | vendo in sight ta- sourc | • N/ A | Yes | No | No | No |
| AWS Marketpla ce [aws- mark etplace] | aws- marke tplac ploym arame | • N/ A | Yes | No | No | No |
| | aws- marke tplac anges | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Migration Hub Orchestrator [migrationhub-orchestrator] | migra hub- orche strat orkfl | • N/A | Yes | No | No | No |
| | migra hub- orche strat empla | • N/A | Yes | No | No | No |
| AWS Migration Hub Refactor Spaces [refactor-spaces] | refac space viron / appli ion | • AWS: ctor s::A atic | Yes | No | Yes | Yes |
| | refac space viron / appli ion/ servi ce | • AWS: ctor s::S e | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | refac space viron | • AWS: ctor s::E nmer | Yes | No | Yes | Yes |
| | refac space viron / appli ion/ route | • AWS: ctor s::F | Yes | No | Yes | Yes |
| AWS Network Firewall [network-firewall] | netwo f irewa tatel ruleg | • AWS: orkF ll:: roup | Yes | Yes | Yes | Yes |
| | netwo f irewa pc- endpo nt- assoc ation | • AWS: orkF ll:: dpoi ocia | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | netwo f irewa irewa | • AWS: orkF ll:: all | Yes | Yes | Yes | Yes |
| | netwo f irewa tatef r ulegr | • AWS: orkF ll:: roup | Yes | Yes | No | No |
| | netwo f irewa irewa p olicy | • AWS: orkF ll:: allF | Yes | Yes | Yes | Yes |
| | netwo f irewa LL_SU TED | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Network Manager [networkm anager] | netwo nager ring | • AWS: orkM r::T tGat eeri | Yes | No | No | No |
| | netwo nager bal- netwo rk | • AWS: orkM r::G Netw | Yes | No | Yes | Yes |
| | netwo nager k | • AWS: orkM r::L | Yes | No | Yes | Yes |
| | netwo nager e- netwo | • AWS: orkM r::G twor | Yes | No | Yes | Yes |
| | netwo nager ice | • AWS: orkM r::D | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | netwo nager nect- peer | • AWS: orkM r::( tPee | Yes | No | Yes | Yes |
| | netwo nager achme | • AWS: orkM r::\ achm<br>• AWS: orkM r::( tAtt nt | Yes | No | No | No |
| | netwo nager e | • AWS: orkM r::S | Yes | No | Yes | Yes |
| | netwo nager necti | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS OpsWorks Configura tion Managemen t [opsworks -cm] | opswo cm:se | • N/ A | Yes | No | No | No |
| | opswo cm:ba | • N/ A | Yes | No | No | No |
| AWS OpsWorks [opsworks ] | opswo instar | • AWS: orks tanc | Yes | No | No | No |
| | opswo stack | • AWS: orks ck | Yes | No | No | No |
| | opswo layer | • AWS: orks er | Yes | No | No | No |
| AWS Organizat ions [organiza tions] | organ ions: unt | • AWS: niza ::Ac | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | organ ions:( | • AWS: niza ::Or atic it | Yes | Yes | Yes | Yes |
| | organ ions:: urcep y | • AWS: niza ::Re ePol | Yes | No | Yes | Yes |
| | organ ions:: | • N/ A | Yes | Yes | No | No |
| | organ ions:p cy | • AWS: niza ::Pc | Yes | Yes | No | No |
| | organ ions:A SUPPO | • N/ A | No | Yes | Yes | Yes |
| AWS Outposts [outposts ] | outpo site | • N/ A | Yes | No | No | No |
| | outpo outpo | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Panorama [panorama ] | panor packa | • AWS: rama kage | Yes | No | Yes | Yes |
| | panor appli onins e | • AWS: rama lica nsta | Yes | No | No | No |
| | panor devic | • N/ A | Yes | No | No | No |
| AWS Parallel Computing Service [pcs] | pcs:c er | • AWS: :Clu | Yes | No | No | No |
| | pcs:q | • AWS: :Que | Yes | No | No | No |
| | pcs:c tenod up | • AWS: :Com odeC | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Partner Central Selling [partnerc entral] | partn ntral ortun | • N/ A | Yes | No | No | No |
| | partn ntral ageme by- accep ng- invit tion- task | • N/ A | Yes | No | No | No |
| | partn ntral ageme f rom- oppor tunit ta sk | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Payment Cryptography [payment-cryptography] | payme c rypto hy:ke | • AWS: entC grap ey | Yes | No | Yes | Yes |
| AWS Payments [payments] | payme payme i nstru | • N/ A | Yes | No | No | No |
| AWS Performance Insights [pi] | pi:pe r eport | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Private CA Connector for Active Directory [pca-connector-ad] | pca-connector-ad:connect | • AWS: onne D::C tor | Yes | No | No | No |
| | pca-connector-ad:connect templ | • AWS: onne D::T te | Yes | No | No | No |
| | pca-connector-ad:direct regis ion | • AWS: onne D::D oryF rati | Yes | No | No | No |
| AWS Private CA Connector for SCEP [pca-connector-scep] | pca-connector-scep :conn r | • AWS: onne CEP: ecto | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Private Certifica te Authority [acm-pca] | acm-pca:c ertif e-autho ty | • AWS: CA:: fica hori | Yes | Yes | Yes | Yes |
| | acm-pca:A LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| AWS Proton [proton] | proto viron - templ | • AWS: on:: onme plat | Yes | No | Yes | Yes |
| | proto viron | • N/ A | Yes | No | No | No |
| | proto rvice, ser vice- inst ance | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | proto posit | • N/A | Yes | No | No | No |
| | proto mpone | • N/A | Yes | No | No | No |
| | proto viron - accou conne n | • AWS: on:: onme ount ctio | Yes | No | Yes | Yes |
| | proto rvice | • N/A | Yes | No | No | No |
| | proto ploym | • N/A | Yes | No | No | No |
| | proto rvice tem plate | • AWS: on:: ceTe e | Yes | No | Yes | Yes |
| AWS Purchase Orders Console [purchase -orders] | purch order rchas or der | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS RTB Fabric [rtbfabric] | rtbfal :requ rgate | • AWS: abri ques tewa | Yes | No | No | No |
| | rtbfal :resp rgate | • AWS: abri spor tewa | Yes | No | No | No |
| AWS Recycle Bin [rbin] | rbin:: | • AWS: ::Ru | Yes | Yes | Yes | Yes |
| | rbin:/ SUPPO | • N/ A | No | Yes | Yes | Yes |
| AWS Resilienc e Hub [resilien cehub] | resil ehub: asses t | • N/ A | Yes | No | No | No |
| | resil ehub: lienc po licy | • AWS: lier ::Re ncyF | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | resil ehub: mmend n- templ e | • N/ A | Yes | No | No | No |
| | resil ehub: | • AWS: lier ::Ap | Yes | No | Yes | Yes |
| AWS Resource Access Manager (RAM) [ram] | ram:r rce- share | • AWS: :Res Shar | Yes | Yes | Yes | Yes |
| | ram:r rcesh nvita | • N/ A | Yes | No | No | No |
| | ram:p ssion | • N/ A | Yes | No | No | No |
| | ram:A UPPOR | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Resource Groups [resource -groups] | resou group oup | • AWS: urce s::( | Yes | Yes | Yes | Yes |
| | resou group L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| AWS RoboMaker [robomake r] | robom :worl ge nerat job | • N/ A | Yes | No | No | No |
| | robom :worl ge nerat jobs | • N/ A | Yes | No | No | No |
| | robom :simu on- job- ba tch | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | robom :simu on-job | • N/A | Yes | No | No | No |
| | robom :worl te mplat | • N/A | Yes | No | No | No |
| | robom :robo | • AWS: Make bot | Yes | No | No | No |
| | robom :worl ex port-job | • N/A | Yes | No | No | No |
| | robom :simu on-appli ation | • AWS: Make mula ppli n | Yes | No | No | No |
| | robom :depl nt-job | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | robom :robo ap plica | • AWS: Make botA atic | Yes | No | Yes | Yes |
| | robom :depl nt- fleet | • AWS: Make eet | Yes | No | No | No |
| | robom :worl | • N/ A | Yes | No | No | No |
| AWS SQL Workbench [sqlworkb ench] | sqlwo nch:q | • N/ A | Yes | No | No | No |
| | sqlwo nch:n ook | • N/ A | Yes | No | No | No |
| | sqlwo nch:c | • N/ A | Yes | No | No | No |
| | sqlwo nch:c ction | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Savings Plans [savingsplans] | savin ans:s gspla | • N/A | Yes | No | No | No |
| AWS Secrets Manager [secretsmanager] | secre nager ret | • AWS: etsM r::S | Yes | Yes | Yes | Yes |
| | secre nager _SUPP D | • N/A | No | Yes | Yes | Yes |
| AWS Security Hub [securityhub] | secur ub:co torv2 | • N/A | Yes | No | No | No |
| | secur ub:au tion- rule v2 | • AWS: rity Autc nRul | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | secur ub:au tion- rule | • AWS: rity Autc nRul | Yes | No | No | No |
| | secur ub:ag atorv | • AWS: rity Aggr rV2 | Yes | No | No | No |
| | secur ub:hul | • AWS: rity Hub\ | Yes | No | Yes | Yes |
| | secur ub:pr t- subsc ption | • AWS: rity Proc bscr n | Yes | No | No | No |
| | secur ub:hul | • AWS: rity Hub | Yes | No | No | No |
| | secur ub:co urati p olicy | • AWS: rity Conf tior y | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Service - Oracle Database@ AWS [odb] | odb:c - vm- clust er | • AWS: :Clc lust | Yes | No | No | No |
| | odb:c - exada infra cture | • AWS: :Clc data stru | Yes | No | No | No |
| | odb:d no de | • N/ A | Yes | No | No | No |
| | odb:c - auton us- vm- clu ster | • AWS: :Clc onom Clus | Yes | No | No | No |
| | odb:o p eerin co nnect | • AWS: :Odb ngCc ion | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | odb:o n etwor | • AWS: :Odb rk | Yes | No | No | No |
| AWS Service Catalog [catalog] | catal ortfo | • AWS: ice( g::F lio | Yes | Yes | Yes | Yes |
| | catal roduc | • AWS: ice( g::( orma rovi dPrc | Yes | Yes | No | No |
| | catal LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| AWS Service Catalog [servicec atalog] | servi talog ribut gr oups | • AWS: ice( gApp try: ibut p | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | servi talog licat | • AWS: iceC gApp try: icat | Yes | Yes | Yes | Yes |
| | servi talog _SUPP D | • N/ A | No | Yes | Yes | Yes |
| AWS Shield [shield] | shiel otect | • AWS: ld:: ctic | Yes | No | No | No |
| | shiel otect group | • AWS: ld:: ctic p | Yes | No | No | No |
| AWS Signer [signer] | signe gning pro files | • AWS: er:: ngPr | Yes | No | Yes | Yes |
| AWS SimSpace Weaver [simspace weaver] | simsp eaver ulati | • AWS: pace r::S tior | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Snow Device Managemen t [snow-device-manag ement] | snow-devi ce-manag ement:* | • N/A | Yes | No | No | No |
| | snow-devi ce-manag ement:m ged-devic e | • N/A | Yes | No | No | No |
| AWS Step Functions [states] | state ecuti | • N/A | Yes | No | No | No |
| | state tivit | • AWS: Func ::Ac y | Yes | Yes | Yes | Yes |
| | state atema e | • AWS: Func ::St chir | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | state L_SUP ED | • N/A | No | Yes | Yes | Yes |
| AWS Storage Gateway [storageg ateway] | stora teway epool | • N/A | Yes | No | No | No |
| | stora teway assoc on | • N/A | Yes | No | No | No |
| | stora teway e | • N/A | Yes | Yes | No | No |
| | stora teway eway | • N/A | Yes | Yes | No | No |
| | stora teway eway/ volu me | • N/A | Yes | Yes | No | No |
| | stora teway re | • N/A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS Supply Chain [scn] | scn:i nce | • N/ A | Yes | No | No | No |
| | scn:b fmate simpo b | • N/ A | Yes | No | No | No |
| AWS Systems Manager Incident Manager Contacts [ssm-cont acts] | ssm- conta cts:c ct | • AWS: onta Cont | Yes | Yes | No | No |
| | ssm- conta cts:r ion | • AWS: onta Rota | Yes | No | No | No |
| | ssm- conta cts:A UPPOR | • N/ A | No | Yes | No | No |
| AWS Systems Manager Incident Manager [ssm-inci dents] | ssm- incid ents: dent- reco rd | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ssm-incid ents:: icati set | • AWS: ncic :Rep ionS | Yes | No | Yes | Yes |
| | ssm-incid ents:: onse- plan | • AWS: ncic :Res Plar | Yes | No | Yes | Yes |
| AWS Systems Manager Quick Setup [ssm-quic ksetup] | ssm-quick setup figur n- manag | • AWS: uick ::Cc rati ager | Yes | No | No | No |
| AWS Systems Manager [ssm] | ssm:m ed- insta ce | • N/ A | Yes | Yes | No | No |
| | ssm:d ent | • AWS: :Doc | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ssm:a ation def initi | • N/ A | Yes | No | No | No |
| | ssm:p eter | • AWS: :Pa r | Yes | No | Yes | Yes |
| | ssm:a ation exe cutio | • N/ A | Yes | Yes | No | No |
| | ssm:o em | • N/ A | Yes | Yes | No | No |
| | ssm:p basel | • AWS: :Pat elir | Yes | Yes | Yes | Yes |
| | ssm:s on | • N/ A | Yes | Yes | No | No |
| | ssm:a iatio | • AWS: :Ass ion | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ssm:m enanc dow | • AWS: :Mai nceW | Yes | Yes | Yes | Yes |
| | ssm:o tadat | • N/ A | Yes | No | No | No |
| | ssm:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| AWS Systems Manager for SAP [ssm-sap] | ssm-sap:h ana/ db | • N/ A | Yes | No | No | No |
| | ssm-sap:h ana | • AWS: emsM rSAP lica | Yes | No | No | No |
| AWS Telco Network Builder [tnb] | tnb:n rk- insta ce | • N/ A | Yes | No | No | No |
| | tnb:f ion- insta nce | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | tnb:f ion- packa ge | • N/ A | Yes | No | No | No |
| | tnb:n rk- packa e | • N/ A | Yes | No | No | No |
| | tnb:n rk- opera ion | • N/ A | Yes | No | No | No |
| AWS Transfer Family [transfer ] | trans conne | • AWS: sfer nect | Yes | No | Yes | Yes |
| | trans user | • AWS: sfer r | Yes | Yes | Yes | Yes |
| | trans workf | • AWS: sfer kflc | Yes | Yes | Yes | Yes |
| | trans webap | • AWS: sfer App | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | trans agree | • AWS: sfer eeme | Yes | No | Yes | Yes |
| | trans host- key | • N/ A | Yes | No | No | No |
| | trans serve | • AWS: sfer ver | Yes | Yes | Yes | Yes |
| | trans certi te | • AWS: sfer tifi | Yes | No | Yes | Yes |
| | trans profi | • AWS: sfer file | Yes | No | Yes | Yes |
| | trans ALL_S RTED | • N/ A | No | Yes | Yes | Yes |
| AWS Transform [transfor m] | trans :conn r | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| AWS User Notificat ions Contacts [notifica tions-con tacts] | notif ions- cont acts: lcont | • AWS: fica Cont :Ema tact | Yes | No | Yes | Yes |
| AWS User Notificat ions [notifica tions] | notif ions: igura | • AWS: fica ::Nc atic igu | Yes | No | No | No |
| AWS WAF Regional [waf-regi onal] | waf- regio nal:r | • AWS: egic Rule | Yes | No | No | No |
| | waf- regio nal:r roup | • N/ A | Yes | No | No | No |
| | waf- regio nal:r asedr | • AWS: egic Rate Rule | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | waf-regio nal:w l | • AWS: egic WebA | Yes | No | No | No |
| AWS WAF [waf] | waf:r roup | • N/ A | Yes | No | No | No |
| | waf:w l | • AWS: :Web | Yes | No | No | No |
| | waf:r asedr | • N/ A | Yes | No | No | No |
| | waf:r | • AWS: :Rul | Yes | No | No | No |
| AWS Well-Arch itected Tool [wellarch itected] | wella tecte ns | • N/ A | Yes | No | No | No |
| | wella tecte view-temp late | • N/ A | Yes | No | No | No |
| | wella tecte rkloa | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | wella tecte ofile | • N/ A | Yes | No | No | No |
| | wella tecte L_SUP ED | • N/ A | No | Yes | No | No |
| AWS Wickr [wickr] | wickr work | • N/ A | Yes | Yes | No | No |
| | wickr _SUPP D | • N/ A | No | Yes | No | No |
| AWS WorkSpace s Managed Instances [workspac es-instan ces] | works s- insta es:wo acein ce | • AWS: spac tanc orks nsta | Yes | No | No | No |
| AWS X-Ray [xray] | xray: ling- rule | • AWS: ::Sa gRul | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | xray:g p | • AWS: ::Gr | Yes | No | Yes | Yes |
| AWS rePost Private [repostsp ace] | repos ce:sp | • N/ A | Yes | No | No | No |
| AWS service providing managed private networks [private-networks] | priva n etwor etwor si te | • N/ A | Yes | No | No | No |
| | priva n etwor rder | • N/ A | Yes | No | No | No |
| | priva n etwor etwor | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | priva n etwor etwor re sourc | • N/ A | Yes | No | No | No |
| | priva n etwor evice ide ntifi | • N/ A | Yes | No | No | No |
| Alexa for Business [a4b] | a4b:p le | • N/ A | Yes | No | No | No |
| | a4b:a ss- book | • N/ A | Yes | No | No | No |
| | a4b:n rk- profi e | • N/ A | Yes | No | No | No |
| | a4b:u | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | a4b:c rence pro vider | • N/ A | Yes | No | No | No |
| | a4b:s - group | • N/ A | Yes | No | No | No |
| | a4b:r | • N/ A | Yes | No | No | No |
| | a4b:g ay- group | • N/ A | Yes | No | No | No |
| | a4b:s ule | • N/ A | Yes | No | No | No |
| | a4b:c ct | • N/ A | Yes | No | No | No |
| | a4b:d e | • N/ A | Yes | No | No | No |
| Amazon AI Operation s [aiops] | aiops estig n- group | • AWS: s::I igat oup | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon API Gateway Managemen t [apigatew ay] | apiga y:usa ans | • N/ A | Yes | No | No | No |
| | apiga y:api | • N/ A | Yes | Yes | No | No |
| | apiga y:cli ertif es | • N/ A | Yes | No | No | No |
| | apiga y:res s | • N/ A | Yes | Yes | No | No |
| | apiga y:dom ames | • AWS: atev omai V2 | Yes | Yes | No | No |
| | apiga y:dom ameac assoc ons | • AWS: atev omai Acce ocia | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | apiga y:vpc s | • N/ A | Yes | No | No | No |
| | apiga y:ALL_ PORTE | • N/ A | No | Yes | No | No |
| Amazon ARC Region switch [arc-regi on-switch ] | arc-regio n-switc plan | • AWS: egic ch:: | Yes | No | No | No |
| Amazon AppFlow [appflow] | appfl onnec | • AWS: low: ectc | Yes | No | No | No |
| | appfl low | • AWS: low: | Yes | No | Yes | Yes |
| Amazon AppIntegr ations [app-inte grations] | app-integ ratio pplic n-assoc tion | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | app-integ ratio ata-integ ratio | • AWS: nteg ns:: nteg n | Yes | No | Yes | Yes |
| | app-integ ratio vent-inte grati | • AWS: nteg ns:: Inte on | Yes | No | Yes | Yes |
| | app-integ ratio ata-integ ratio as socia | • N/ A | Yes | No | No | No |
| | app-integ ratio pplic n | • AWS: nteg ns:: cati | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | app-integ ratio vent-inte grati a ssoci n | • N/ A | Yes | No | No | No |
| Amazon AppStream 2.0 [appstrea m] | appst :imag | • N/ A | Yes | No | No | No |
| | appst :app-bloc k | • AWS: trea pBlc | Yes | No | Yes | Yes |
| | appst :stac | • AWS: trea ack | Yes | No | Yes | Yes |
| | appst :app-bloc k-build | • AWS: trea pBlc lde | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | appst :flee | • AWS: trea eet | Yes | No | Yes | Yes |
| | appst :imag bu ilder | • AWS: trea ageB r | Yes | No | Yes | Yes |
| | appst :appl ion | • AWS: trea plic | Yes | No | Yes | Yes |
| Amazon Athena [athena] | athen tacat | • AWS: na:: ata] | Yes | No | Yes | Yes |
| | athen pacit re serva | • AWS: na:: ityF atic | Yes | No | Yes | Yes |
| | athen rkgro | • AWS: na:: roup | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | athen L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| Amazon Aurora DSQL [dsql] | dsql: ter | • AWS: ::C] | Yes | No | Yes | Yes |
| Amazon Bedrock [bedrock-agentcore ] | bedro a gentc workl ident | • AWS: ockA ore: loac ity | Yes | No | No | No |
| | bedro a gentc code- inte rpret c ustom | • AWS: ockA ore: Inte erCu | Yes | No | No | No |
| | bedro a gentc gatew | • AWS: ockA ore: way | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro a gentc token vau lt | • N/ A | Yes | No | No | No |
| | bedro a gentc memor | • AWS: ockA ore: ry | Yes | No | No | No |
| | bedro a gentc workl ident direc | • N/ A | Yes | No | No | No |
| | bedro a gentc runti | • AWS: ockA ore: ime | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro a gentc brows c ustom | • AWS: ockA ore: serC | Yes | No | No | No |
| | bedro a gentc runti e ndpoi | • AWS: ockA ore: imeE nt | Yes | No | No | No |
| Amazon Bedrock [bedrock] | bedro odel- copy - job | • N/ A | Yes | No | No | No |
| | bedro ustom mod el- deplo ment | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro rompt rou ter | • N/ A | Yes | No | No | No |
| | bedro gent- alia s | • AWS: ock: tAli | Yes | No | Yes | Yes |
| | bedro luepr | • AWS: ock: prir | Yes | No | Yes | Yes |
| | bedro odel- cust omiza - job | • N/ A | Yes | No | No | No |
| | bedro odel- impo rt- job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro ata- autom ation inv ocati | • N/ A | Yes | No | No | No |
| | bedro ata- autom ation inv ocati job | • N/ A | Yes | No | No | No |
| | bedro utoma reaso - polic | • AWS: ock: mate onir cy | Yes | No | No | No |
| | bedro odel- eval uatio job | • N/ A | Yes | No | No | No |
| | bedro essio | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro rompt | • AWS: ock: pt | Yes | No | Yes | Yes |
| | bedro uardr | • AWS: ock: drai | Yes | No | Yes | Yes |
| | bedro sync- invo ke | • N/ A | Yes | No | No | No |
| | bedro low/ alias | • N/ A | Yes | No | No | No |
| | bedro rompt ver sion | • AWS: ock: ptVe | Yes | No | No | No |
| | bedro ata- autom ation pro ject | • AWS: ock: Autc nPrc | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro rovis d- model | • N/ A | Yes | No | No | No |
| | bedro rovis d- model v2 | • N/ A | Yes | No | No | No |
| | bedro pplic n- infer ce- profi e | • AWS: ock: icat fere ofil | Yes | No | Yes | Yes |
| | bedro mport m odel | • N/ A | Yes | No | No | No |
| | bedro low | • AWS: ock: | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro low/ alias | • AWS: ock: Alia | Yes | No | No | No |
| | bedro low- alias | • AWS: ock: Alia | Yes | No | No | No |
| | bedro nowle base | • AWS: ock: ledg | Yes | No | Yes | Yes |
| | bedro gent | • AWS: ock: t | Yes | No | Yes | Yes |
| | bedro odel- invo catio job | • N/ A | Yes | No | No | No |
| | bedro ustom mod el | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | bedro valua - job | • N/ A | Yes | No | No | No |
| Amazon Braket [braket] | brake antum tas k | • N/ A | Yes | No | No | No |
| | brake b | • N/ A | Yes | No | No | No |
| | brake endin li mit | • N/ A | Yes | No | No | No |
| Amazon Chime [chime] | chime ting | • N/ A | Yes | Yes | No | No |
| | chime - media ap plica | • N/ A | Yes | No | No | No |
| | chime | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | chime - insta / bot | • N/ A | Yes | No | No | No |
| | chime ce- profi e- domai | • N/ A | Yes | No | No | No |
| | chime - insta / chann | • N/ A | Yes | Yes | No | No |
| | chime - insta / user | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | chime ia- pipel ne- kines s- video s tream poo l | • N/ A | Yes | No | No | No |
| | chime - insta | • N/ A | Yes | Yes | No | No |
| | chime ia- pipel ne | • N/ A | Yes | Yes | No | No |
| | chime ce- conne tor | • N/ A | Yes | No | No | No |
| | chime | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | chime ia- insig ts- pipel ne- confi urati | • N/ A | Yes | No | No | No |
| | chime _SUPP D | • N/ A | No | Yes | No | No |
| Amazon Cloud Directory [clouddir ectory] | cloud ctory ector | • N/ A | Yes | No | No | No |
| Amazon CloudFron t [cloudfro nt] | cloud t:vpc in | • AWS: dFrc pcOı | Yes | No | No | No |
| | cloud t:con ion- funct ion | • AWS: dFrc onne Func | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | cloud t:dis ution ten ant | • AWS: dFrc istı onTe | Yes | No | No | No |
| | cloud t:dis ution | • AWS: dFrc istı on | Yes | Yes | Yes | Yes |
| | cloud t:any - ip- list | • AWS: dFrc nyca ist | Yes | No | No | No |
| | cloud t:key val ue- store | • AWS: dFrc eyVa ore | Yes | No | No | No |
| | cloud t:key estor | • AWS: dFrc eyVa ore | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | cloud t:str ng- distr butio | • AWS: dFrc trea istr on | Yes | Yes | No | No |
| | cloud t:tru s tore | • N/ A | Yes | No | No | No |
| | cloud t:con ion- group | • AWS: dFrc onne Grou | Yes | No | Yes | Yes |
| | cloud t:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| Amazon CloudSear ch [cloudsea rch] | cloud ch:do | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon CloudWatch Application Insights [applicationinsights] | appli onins s:app tion | • AWS: icat sigh ppli n | Yes | No | Yes | Yes |
| Amazon CloudWatch Application Signals [application-signals] | appli on- signa s:slo | • AWS: icat gnal rvic lObj e | Yes | No | Yes | Yes |
| Amazon CloudWatch Evidently [evidently] | evide :segm | • AWS: entl gmer | Yes | No | No | No |
| | evide :proj launc | • AWS: entl unch | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | evide :proj | • AWS: entl ojec | Yes | No | No | No |
| | evide :proj featu | • AWS: entl atur | Yes | No | No | No |
| | evide :expe nt | • AWS: entl peri | Yes | No | No | No |
| | evide :proj exper t | • AWS: entl peri | Yes | No | No | No |
| Amazon CloudWatch Internet Monitor [internet monitor] | inter onito nitor | • AWS: rnet or:: or | Yes | Yes | Yes | Yes |
| | inter onito L_SUP ED | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon CloudWatch Logs [logs] | logs: group | • AWS: ::Lo p | Yes | Yes | Yes | Yes |
| | logs: very- dest inati | • AWS: ::De yDes ion | Yes | No | Yes | Yes |
| | logs: duled que ry | • N/ A | Yes | No | No | No |
| | logs: inati | • AWS: ::De tior | Yes | Yes | Yes | Yes |
| | logs: very- sour ce | • AWS: ::De ySou | Yes | No | Yes | Yes |
| | logs: aly- detec tor | • AWS: ::Lo alyD or | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | logs:( very | • AWS: ::De y | Yes | No | Yes | Yes |
| Amazon CloudWatch Network Synthetic Monitor [networkmonitor] | netwo nitor itor | • N/ A | Yes | No | No | No |
| | netwo nitor be | • N/ A | Yes | No | No | No |
| Amazon CloudWatch Observability Access Manager [oam] | oam:l | • AWS: :Lir | Yes | Yes | No | No |
| | oam:s | • AWS: :Sir | Yes | Yes | Yes | Yes |
| | oam:A UPPOR | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon CloudWatch Observability Admin Service [observabilityadmin] | obser litya :orga tion- tele metry rul e | • AWS: rvat Admi gani nTel yRul | Yes | No | No | No |
| | obser litya :s3ta ntegr n | • N/ A | Yes | No | No | No |
| | obser litya :tele y- rule | • AWS: rvat Admi leme le | Yes | No | No | No |
| | obser litya :tele y- pipel e | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | obser lityа :orga tion- cent raliz n- rule | • AWS: rvat Admi gani nCer zati e | Yes | No | No | No |
| Amazon CloudWatch Synthetics [syntheti cs] | synth s:gro | • AWS: heti roup | Yes | No | Yes | Yes |
| | synth s:can | • AWS: heti anar | Yes | No | Yes | Yes |
| Amazon CloudWatch [cloudwat ch] | cloud h:met strea | • AWS: dWat etri am | Yes | Yes | Yes | Yes |
| | cloud h:slo | • N/ A | Yes | No | No | No |
| | cloud h:ins - rule | • AWS: dWat nsig e | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | cloudwatch:ala | • AWS: dWat larm | Yes | Yes | Yes | Yes |
| | cloudwatch:ALL_PORTF | • N/A | No | Yes | Yes | Yes |
| Amazon CodeCatalyst [codecatalyst] | codecatalyst:identity-center-applications | • N/A | Yes | No | No | No |
| | codecatalyst:s | • N/A | Yes | No | No | No |
| | codecatalyst:actions | • N/A | Yes | Yes | No | No |
| | codecatalyst:AUPPOR | • N/A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon CodeGuru Profiler [codeguru -profiler ] | codegu profi profi group | • AWS: Guru ler: ilir p | Yes | No | Yes | Yes |
| Amazon CodeGuru Reviewer [codeguru -reviewer ] | codegu revie assoc on | • AWS: Guru wer: sitc ocia | Yes | Yes | Yes | Yes |
| | codegu revie coder w | • N/ A | Yes | No | No | No |
| | codegu revie ALL_SU RTED | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon CodeGuru Security [codeguru -security ] | codeg secur scans | • N/ A | Yes | Yes | No | No |
| | codeg secur ALL_S RTED | • N/ A | No | Yes | No | No |
| Amazon CodeWhisp erer [codewhis perer] | codew erer: ile | • N/ A | Yes | No | No | No |
| | codew erer: omiza | • N/ A | Yes | No | No | No |
| Amazon Cognito Identity [cognito- identity] | cogni i denti denti ol | • AWS: ito: tity | Yes | Yes | Yes | Yes |
| | cogni i denti LL_SU TED | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Cognito Identity [cognito-idp] | cogni i dp:us ol | • AWS: ito: Pool | Yes | Yes | Yes | Yes |
| | cogni i dp:AL PPORT | • N/ A | No | Yes | Yes | Yes |
| Amazon Comprehen d [comprehe nd] | compr d:tar d- senti nt- detec ion- job | • N/ A | Yes | No | No | No |
| | compr d:ent recog r- endpo t | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | compr d:sen nt- detec ion- job | • N/ A | Yes | No | No | No |
| | compr d:fly l | • AWS: rehe lywh | Yes | No | Yes | Yes |
| | compr d:doc t- class ier- endpo int | • N/ A | Yes | No | No | No |
| | compr d:ent recog r | • N/ A | Yes | Yes | No | No |
| | compr d:top detec - job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | compr d:eve detec - job | • N/ A | Yes | No | No | No |
| | compr d:doc t- class ier | • AWS: rehe ocum assi | Yes | Yes | Yes | Yes |
| | compr d:key phr ases- dete ction job | • N/ A | Yes | No | No | No |
| | compr d:doc t- class icati job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | compr d:ent s- detec on- job | • N/ A | Yes | No | No | No |
| | compr d:dom t- langu e- detec on- job | • N/ A | Yes | No | No | No |
| | compr d:fly l/ datas | • N/ A | Yes | No | No | No |
| | compr d:pii ent ities det ectio job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | compr d:ALL_ PORTE | • N/A | No | Yes | Yes | Yes |
| Amazon Connect Cases [cases] | cases ated- item | • N/A | Yes | No | No | No |
| | cases ain/ case/ relat i tem | • N/A | Yes | No | No | No |
| | cases out | • N/A | Yes | No | No | No |
| | cases ld | • N/A | Yes | No | No | No |
| | cases plate | • N/A | Yes | No | No | No |
| | cases ain/ case | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | cases ain | • N/ A | Yes | No | No | No |
| Amazon Connect Customer Profiles [profile] | profi omain ob ject- type s | • AWS: omer les: ctTy | Yes | No | Yes | Yes |
| | profi omain do main- obje ct- types | • N/ A | Yes | No | No | No |
| | profi omain | • AWS: omer les: in | Yes | No | Yes | Yes |
| | profi omain in tegra s | • AWS: omer les: grat | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Connect Outbound Campaigns [connect-campaigns] | conne c ampai campa | • AWS: ectC gns: aigr | Yes | No | Yes | Yes |
| Amazon Connect Voice ID [voiceid] | voice omain | • AWS: eID: in | Yes | No | No | No |
| Amazon Connect [connect] | conne nstan e valua - form | • AWS: ect: uati m | Yes | No | Yes | Yes |
| | conne nstan a gent- stat e | • AWS: ect: tSta | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | conne ildca entst | • N/ A | Yes | No | No | No |
| | conne nstan t ransf d estin n | • AWS: ect: kCor | Yes | Yes | Yes | Yes |
| | conne nstan u se- case | • N/ A | Yes | No | No | No |
| | conne ildca ickco t | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | conne nstan t ask- templ ate | • AWS: ect: Temp | Yes | No | Yes | Yes |
| | conne nstan a gent | • AWS: ect: | Yes | Yes | Yes | Yes |
| | conne raffi di strib n- group | • AWS: ect: ficD buti up | Yes | No | No | No |
| | conne nstan f low- modul e | • AWS: ect: actF dule | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | conne hone- numb er | • AWS: ect: eNum | Yes | No | Yes | Yes |
| | conne nstan a gent- grou p | • AWS: ect: Hier Grou | Yes | No | No | No |
| | conne nstan o perat hours | • AWS: ect: sOfC ion | Yes | No | Yes | Yes |
| | conne nstan s ecuri p rofil | • AWS: ect: rity le | Yes | No | Yes | Yes |
| | conne ildca ntact | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | conne nstan q ueue | • AWS: ect: e | Yes | Yes | Yes | Yes |
| | conne nstan c ontac ev aluat | • N/ A | Yes | No | No | No |
| | conne nstan r ule | • AWS: ect: | Yes | No | Yes | Yes |
| | conne nstan i ntegr n- assoc tion | • AWS: ect: grat soci | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | conne nstan c ontac fl ow | • AWS: ect: actF | Yes | Yes | Yes | Yes |
| | conne nstan v ocabu | • N/ A | Yes | No | No | No |
| | conne nstan | • AWS: ect: ance | Yes | No | Yes | Yes |
| | conne nstan r outin pr ofile | • AWS: ect: ingF e | Yes | Yes | Yes | Yes |
| | conne ildca eue | • N/ A | Yes | No | No | No |
| | conne ontac | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | conne nstan p rompt | • AWS: ect: pt | Yes | No | Yes | Yes |
| | conne LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| Amazon Data Lifecycle Manager [dlm] | dlm:p y | • AWS: :Lif ePol | Yes | Yes | Yes | Yes |
| | dlm:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| Amazon DataZone [datazone ] | dataz domai | • AWS: Zone ain | Yes | No | Yes | Yes |
| Amazon Detective [detectiv e] | detec :grap | • AWS: ctiv aph | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon DocumentD B Elastic Clusters [docdb-el astic] | docdb ela stic: ter | • AWS: BEla :Clu | Yes | No | No | No |
| | docdb ela stic: ter- pg | • AWS: BEla :Clu | Yes | No | No | No |
| | docdb ela stic: ter- snaps hot | • N/ A | Yes | No | No | No |
| Amazon DynamoDB Accelerat or (DAX) [dax] | dax:c | • AWS: :Clu | Yes | No | Yes | Yes |
| Amazon DynamoDB [dynamodb ] | dynam globa le | • AWS: moDE ball | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | dynam table | • AWS: moDE le | Yes | Yes | Yes | Yes |
| | dynam index | • N/ A | Yes | No | No | No |
| | dynam table, str eam | • N/ A | Yes | No | No | No |
| | dynam ALL_SU RTED | • N/ A | No | Yes | Yes | Yes |
| Amazon EC2 Auto Scaling [autoscaling] | autos ng:au aling p | • AWS: Scal Auto ngGr | Yes | No | No | No |
| Amazon EC2 Image Builder [imagebuilder] | image der:i struc - confi ation | • AWS: eBui :Inf uctu figu n | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | imagel der:i - recip | • AWS: eBui :Ima ipe | Yes | No | Yes | Yes |
| | imagel der:c iner- reci pe | • AWS: eBui :Cor rRec | Yes | No | Yes | Yes |
| | imagel der:i | • AWS: eBui :Ima | Yes | No | Yes | Yes |
| | imagel der:w low | • AWS: eBui :Wor | Yes | No | Yes | Yes |
| | imagel der:c nent | • AWS: eBui :Con t | Yes | No | Yes | Yes |
| | imagel der:l ycle- poli cy | • AWS: eBui :Lif ePol | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | imagel der:d ibuti c onfig ion | • AWS: eBui :Dis tior gura | Yes | No | Yes | Yes |
| | imagel der:i - pipel | • AWS: eBui :Ima elir | Yes | No | Yes | Yes |
| Amazon EC2 [ec2] | ec2:i - usage re port | • N/ A | Yes | No | No | No |
| | ec2:i exter resou verif ion- token | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:s ity- group | • AWS: :Sec Grou | Yes | Yes | Yes | Yes |
| | ec2:t ic- mirro - sessi | • AWS: :Tra irro ion | Yes | Yes | Yes | Yes |
| | ec2:i pool | • AWS: :IPA | Yes | Yes | Yes | Yes |
| | ec2:s ity- group - rule | • AWS: :Sec Grou ess<br>• AWS: :Sec Grou ss | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:l - gatew virtu i nterf group | • AWS: :Loc eway alIr ceGr | Yes | No | No | No |
| | ec2:n teway | • AWS: :Nat ay | Yes | Yes | Yes | Yes |
| | ec2:i t- snaps t- task | • N/ A | Yes | Yes | No | No |
| | ec2:i net- gatew ay | • AWS: :Int Gate | Yes | Yes | Yes | Yes |
| | ec2:t it- gatew y | • AWS: :Tra atev | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:d optio | • AWS: :DHC ons | Yes | Yes | Yes | Yes |
| | ec2:i | • N/ A | Yes | Yes | No | No |
| | ec2:n rk- insig ts- acces - scope an alysi | • AWS: :Net nsig cess Anal | Yes | Yes | Yes | Yes |
| | ec2:i ool- ec2 | • N/ A | Yes | Yes | No | No |
| | ec2:t it- gatew y- polic table | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:t it- gatew y- attac ent | • AWS: :Tra atev Atta t<br>• AWS: :Tra atev achm<br>• AWS: :Tra atev ring hmer | Yes | Yes | Yes | Yes |
| | ec2:v e | • AWS: :Vol | Yes | Yes | Yes | Yes |
| | ec2:i t- image t ask | • N/ A | Yes | Yes | No | No |
| | ec2:s t | • AWS: :Sub | Yes | Yes | Yes | Yes |
| | ec2:v | • AWS: :VPC | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:v e ndpoi s ervic pe rmiss | • AWS: :VPC intS ePer ons | Yes | No | Yes | Yes |
| | ec2:c ity- reser vatio | • AWS: :Cap Rese on | Yes | Yes | Yes | Yes |
| | ec2:n rk- acl | • AWS: :Net cl | Yes | Yes | Yes | Yes |
| | ec2:v ied- acces s- trust p rovid | • AWS: :Ver Acce stPr r | Yes | Yes | Yes | Yes |
| | ec2:v g atewa | • AWS: :VPN ay | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:c er-gatew y | • AWS: :Car atev | Yes | Yes | Yes | Yes |
| | ec2:e ic-gpu | • N/ A | Yes | No | No | No |
| | ec2:e icgpu | • N/ A | Yes | No | No | No |
| | ec2:l - gatew route tab le | • AWS: :Loc eway Tabl | Yes | Yes | Yes | Yes |
| | ec2:n rk-insig ts-acces - scope | • AWS: :Net nsig cess | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:t it-gatew y-conne - peer | • AWS: :Tra atev nect | Yes | Yes | Yes | Yes |
| | ec2:v ied-acces s-group | • AWS: :Ver Acce up | Yes | Yes | Yes | Yes |
| | ec2:t ic-mirro - targe | • AWS: :Tra irrc et | Yes | Yes | Yes | Yes |
| | ec2:c pool | • N/ A | Yes | Yes | No | No |
| | ec2:f | • AWS: :EC2 | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:l - gatew route tab le- virtu l- inter ce- group assoc on | • AWS: :Loc eway Tabl uall aceC ssoc n | Yes | Yes | Yes | Yes |
| | ec2:t it- gatew y- multi st- domai | • AWS: :Tra atev tica ain | Yes | Yes | Yes | Yes |
| | ec2:n rk- inter ace | • AWS: :Net nter | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:c ity- manag er- data- e xport | • AWS: :Cap Mana taEx | Yes | No | No | No |
| | ec2:c t- vpn- end point | • AWS: :Cli nEnc | Yes | Yes | Yes | Yes |
| | ec2:s instan - reque | • N/ A | Yes | Yes | No | No |
| | ec2:n rk- insig ts- path | • AWS: :Net nsig th | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:i nce- conne ct- endpo nt | • AWS: :Ins Conr dpoi | Yes | Yes | Yes | Yes |
| | ec2:t ic- mirro - filte r ule | • AWS: :Tra irrc erRu | Yes | No | Yes | Yes |
| | ec2:l - gatew virtu i nterf | • AWS: :Loc eway alIr ce | Yes | No | No | No |
| | ec2:v p eerin co nnect | • AWS: :VPC ngCc ion | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:s hot | • N/ A | Yes | Yes | No | No |
| | ec2:c mer- gatew ay | • AWS: :Cus Gate | Yes | Yes | Yes | Yes |
| | ec2:c ity- block | • N/ A | Yes | No | No | No |
| | ec2:v ied- acces s- endpo t | • AWS: :Ver Acce poir | Yes | Yes | Yes | Yes |
| | ec2:v c onnec | • AWS: :VPN ctic | Yes | Yes | Yes | Yes |
| | ec2:i scope | • AWS: :IPA e | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:h reser on | • N/ A | Yes | Yes | No | No |
| | ec2:r ce- root- v olume tas k | • N/ A | Yes | Yes | No | No |
| | ec2:i nce | • AWS: :Ins | Yes | Yes | Yes | Yes |
| | ec2:f image | • N/ A | Yes | Yes | No | No |
| | ec2:r - serve e ndpoi | • AWS: :Rou verE nt | Yes | No | No | No |
| | ec2:k p air | • AWS: :Key | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:v e ndpoi c onnec | • N/ A | Yes | No | No | No |
| | ec2:d ated- host | • AWS: :Hos | Yes | Yes | Yes | Yes |
| | ec2:l - gatew route tab le- vpc- as socia | • AWS: :Loc eway Tabl ssoc n | Yes | Yes | Yes | Yes |
| | ec2:v e ndpoi s ervic | • AWS: :VPC intS e | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:e s-only- in terne ga teway | • AWS: :Egr lyIr tGat | Yes | Yes | Yes | Yes |
| | ec2:i resou disco | • AWS: :IPA urce very | Yes | Yes | Yes | Yes |
| | ec2:m m odifi on- task | • N/ A | Yes | No | No | No |
| | ec2:n rk- insig ts- analy is | • AWS: :Net nsig alys | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:p ment- grou p | • AWS: :Pla tGrc | Yes | Yes | Yes | Yes |
| | ec2:i nce- event - windo | • N/ A | Yes | Yes | No | No |
| | ec2:i ool- ec2 | • N/ A | Yes | No | No | No |
| | ec2:p x- list | • AWS: :Pre st | Yes | Yes | Yes | Yes |
| | ec2:v e ndpoi | • AWS: :VPC int | Yes | Yes | Yes | Yes |
| | ec2:e ic- ip | • AWS: :EIP | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:e t- insta e- task | • N/ A | Yes | Yes | No | No |
| | ec2:r ved- insta nces | • N/ A | Yes | Yes | No | No |
| | ec2:e t- image t ask | • N/ A | Yes | Yes | No | No |
| | ec2:s t- cidr- re serva | • N/ A | Yes | Yes | No | No |
| | ec2:v f low- log | • AWS: :Flo | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:c ity- reser vatio fl eet | • AWS: :Cap Rese onFl | Yes | Yes | Yes | Yes |
| | ec2:i resou disco - assoc ion | • AWS: :IPA urce very iati | Yes | Yes | Yes | Yes |
| | ec2:t it- gatew y- route t able- anno uncem | • N/ A | Yes | Yes | No | No |
| | ec2:t ic- mirro - filte | • AWS: :Tra irro er | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:o st- lag | • N/ A | Yes | No | No | No |
| | ec2:l - gatew | • N/ A | Yes | No | No | No |
| | ec2:l h- templ e | • AWS: :Lau mpl | Yes | Yes | Yes | Yes |
| | ec2:v b lock- publ ic- acces - exclu n | • AWS: :VPC Publ essB ion | Yes | No | Yes | Yes |
| | ec2:r - table | • AWS: :Rou le | Yes | Yes | Yes | Yes |
| | ec2:i | • AWS: :IPA | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ec2:d rativ po licie re port | • N/ A | Yes | No | No | No |
| | ec2:v ied- acces s- insta e | • AWS: :Ver Acce tanc | Yes | Yes | Yes | Yes |
| | ec2:t it- gatew y- route t able | • AWS: :Tra atev teTa | Yes | Yes | Yes | Yes |
| | ec2:s fleet req uest | • AWS: :Spc t | Yes | Yes | Yes | Yes |
| | ec2:A UPPOR | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon EMR Serverless [emr-serverless] | emr-serverless runs | • N/A | Yes | No | No | No |
| | emr-serverless licat | • AWS: erve ::Ap tior | Yes | Yes | Yes | Yes |
| Amazon EMR on EKS (EMR Containers) [emr-containers] | emr-containers tualc ers/ jobruns | • N/A | Yes | No | No | No |
| | emr-containers tualc ers/ endpoints | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | emr-conta iners urity igura s | • N/ A | Yes | No | No | No |
| | emr-conta iners templ | • N/ A | Yes | No | No | No |
| | emr-conta iners tualc ers | • AWS: onta ::Vi Clus | Yes | No | Yes | Yes |
| Amazon ElastiCac he [elastica che] | elast he:se tygro | • AWS: tiCa Secu roup | Yes | No | Yes | Yes |
| | elast he:pa tergr | • AWS: tiCa Para Grou | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | elast he:us oup | • AWS: tiCa Use | Yes | No | Yes | Yes |
| | elast he:sn ot | • N/ A | Yes | No | No | No |
| | elast he:su group | • AWS: tiCa Subr up | Yes | No | Yes | Yes |
| | elast he:cl r | • AWS: tiCa Cach ter | Yes | Yes | Yes | Yes |
| | elast he:re ed- insta ce | • N/ A | Yes | No | No | No |
| | elast he:se lessc | • AWS: tiCa Serv sCac | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | elast he:re ation p | • AWS: tiCa Repl onGr | Yes | No | Yes | Yes |
| | elast he:se lessc snaps | • N/ A | Yes | No | No | No |
| | elast he:us | • AWS: tiCa User | Yes | No | Yes | Yes |
| | elast he:AL PPORT | • N/ A | No | Yes | Yes | Yes |
| Amazon Elastic Container Registry [ecr-publ ic] | ecr- publi c:rep ory | • AWS: :Pub posi | Yes | No | Yes | Yes |
| Amazon Elastic Container Registry [ecr] | ecr:r itory | • AWS: :Rep ry | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ecr:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| Amazon Elastic Container Service [ecs] | ecs:t | • N/ A | Yes | No | No | No |
| | ecs:c ity- provi der | • AWS: :Cap Prov | Yes | Yes | Yes | Yes |
| | ecs:s ce- revis on | • N/ A | Yes | No | No | No |
| | ecs:s ce | • AWS: :Ser | Yes | Yes | Yes | Yes |
| | ecs:c er | • AWS: :Clu | Yes | Yes | Yes | Yes |
| | ecs:s ce- deplo ment | • N/ A | Yes | No | No | No |
| | ecs:t defin n | • AWS: :Tas niti | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ecs:c iner- inst ance | • N/ A | Yes | No | No | No |
| | ecs:t set | • AWS: :Tas | Yes | Yes | Yes | Yes |
| | ecs:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| Amazon Elastic File System [elasticf ilesystem ] | elast lesys file- syst em | • AWS: :Fil em | Yes | Yes | Yes | Yes |
| | elast lesys acces po int | • AWS: :Acc int | Yes | No | Yes | Yes |
| | elast lesys ALL_S RTED | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Elastic Inference [amazonel asticinfe rence] | amazo stici ence: lerat | • N/ A | Yes | No | No | No |
| Amazon Elastic Kubernete s Service [eks] | eks:c er | • AWS: :Clu | Yes | Yes | Yes | Yes |
| | eks:a s- entry | • AWS: :Acc try | Yes | No | Yes | Yes |
| | eks:a | • AWS: :Adc | Yes | No | Yes | Yes |
| | eks:p entit ociat | • AWS: :Poc ityA atic | Yes | No | Yes | Yes |
| | eks:d oard | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | eks:e a nywhe s ubscr on | • N/ A | Yes | No | No | No |
| | eks:i itypr ercon | • AWS: :Ide Prov onfi | Yes | No | Yes | Yes |
| | eks:n roup | • AWS: :Noc p | Yes | No | Yes | Yes |
| | eks:f tepro | • AWS: :Fa rofi | Yes | No | Yes | Yes |
| | eks:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| Amazon Elastic MapReduce [elasticm apreduce] | elast predu luste | • AWS: :Clu | Yes | Yes | Yes | Yes |
| | elast predu ditor | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | elast: predu otebo e xecut: | • N/ A | Yes | No | No | No |
| | elast: predu tudio | • AWS: :Stu | Yes | No | No | No |
| | elast: predu LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| Amazon Elastic VMware Service [evs] | evs:e onmen | • AWS: :Env ent | Yes | No | No | No |
| Amazon EventBrid ge Pipes [pipes] | pipes e | • AWS: s::F | Yes | Yes | Yes | Yes |
| | pipes _SUPP D | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon EventBridge Scheduler [scheduler] | sched :sche - group | • AWS: dule hedu up | Yes | Yes | Yes | Yes |
| | sched :ALL_ ORTED | • N/ A | No | Yes | Yes | Yes |
| Amazon EventBridge Schemas [schemas] | schem iscov | • AWS: tSch :Dis er | Yes | No | Yes | Yes |
| | schem egist | • AWS: tSch :Reg | Yes | No | Yes | Yes |
| | schem chema | • AWS: tSch :Sch | Yes | No | Yes | Yes |
| Amazon EventBridge [events] | event ent- bus | • AWS: ts:: Bus | Yes | Yes | Yes | Yes |
| | event le | • AWS: ts:: | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | event L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| Amazon FSx [fsx] | fsx:b p | • N/ A | Yes | Yes | No | No |
| | fsx:s ge- virtu l- machi | • AWS: :Sto irtu hine | Yes | No | Yes | Yes |
| | fsx:s hot | • AWS: :Sna | Yes | No | Yes | Yes |
| | fsx:f syste | • AWS: :Fil em | Yes | Yes | Yes | Yes |
| | fsx:a iatio | • AWS: :Dat sito ocia | Yes | No | Yes | Yes |
| | fsx:f cache | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | fsx:v e | • AWS: :Vol | Yes | No | Yes | Yes |
| | fsx:t | • N/ A | Yes | No | No | No |
| | fsx:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| Amazon FinSpace [finspace ] | finsp kxenv ment/ kxda tabas kx datav | • N/ A | Yes | No | No | No |
| | finsp kxenv ment/ kxus er | • N/ A | Yes | No | No | No |
| | finsp envir nt | • AWS: pace iror | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | finsp kxenv ment/ kxda tabas | • N/ A | Yes | No | No | No |
| | finsp kxenv ment/ kxvo lume | • N/ A | Yes | No | No | No |
| | finsp kxenv ment | • N/ A | Yes | No | No | No |
| | finsp kxenv ment/ kxsc aling p | • N/ A | Yes | No | No | No |
| | finsp kxenv ment/ kxcl uster | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Forecast [forecast ] | forec datas i mport job | • N/ A | Yes | No | No | No |
| | forec predi - backt - expor job | • N/ A | Yes | No | No | No |
| | forec forec endpo | • N/ A | Yes | No | No | No |
| | forec datas g roup | • AWS: cast aset | Yes | No | Yes | Yes |
| | forec what- if-f oreca e xport | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | forec monit | • N/A | Yes | No | No | No |
| | forec forec expor job | • N/A | Yes | No | No | No |
| | forec datas | • AWS: cast aset | Yes | No | Yes | Yes |
| | forec what- if-f oreca | • N/A | Yes | No | No | No |
| | forec predi | • N/A | Yes | No | No | No |
| | forec what- if-a nalys | • N/A | Yes | No | No | No |
| | forec expla ility | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Fraud Detector [frauddet ector] | forec expla ility exp ort | • N/ A | Yes | No | No | No |
| | forec forec | • N/ A | Yes | No | No | No |
| | fraud ctor: ctor | • AWS: dDet ::De r | Yes | Yes | Yes | Yes |
| | fraud ctor: ctor- vers ion | • N/ A | Yes | Yes | No | No |
| | fraud ctor: h- predi ion | • N/ A | Yes | No | No | No |
| | fraud ctor: l | • AWS: dDet ::La | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | fraud ctor: t- type | • AWS: dDet ::Ev pe | Yes | No | Yes | Yes |
| | fraud ctor: rnal- mode l | • N/ A | Yes | No | No | No |
| | fraud ctor: h- impor | • N/ A | Yes | No | No | No |
| | fraud ctor: ty- type | • AWS: dDet ::Er ype | Yes | No | Yes | Yes |
| | fraud ctor: ome | • AWS: dDet ::Ou | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | fraud ctor:r l-versi | • N/A | Yes | No | No | No |
| | fraud ctor:: | • AWS: dDet ::Li | Yes | No | Yes | Yes |
| | fraud ctor:: | • N/A | Yes | Yes | No | No |
| | fraud ctor:v able | • AWS: dDet ::Va e | Yes | Yes | Yes | Yes |
| | fraud ctor:r l | • N/A | Yes | Yes | No | No |
| | fraud ctor:A SUPPO | • N/A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon FreeRTOS [freertos] | freer subsc ion | • N/A | Yes | No | No | No |
| | freer confi tion | • N/A | Yes | No | No | No |
| Amazon GameLift Servers [gamelift] | gamel scrip | • AWS: Lift ipt | Yes | No | Yes | Yes |
| | gamel build | • AWS: Lift ld | Yes | No | Yes | Yes |
| | gamel conta group nitio | • AWS: Lift tair upDe ion | Yes | No | No | No |
| | gamel games onque | • AWS: Lift eSes ueue | Yes | No | Yes | Yes |
| | gamel fleet | • AWS: Lift et | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | gamel matchi ngrul | • AWS: Lift chma ules | Yes | No | Yes | Yes |
| | gamel locat | • AWS: Lift atic | Yes | No | Yes | Yes |
| | gamel alias | • AWS: Lift as | Yes | No | Yes | Yes |
| | gamel games rgrou | • AWS: Lift eSer oup | Yes | No | Yes | Yes |
| | gamel conta fleet | • AWS: Lift tair et | Yes | No | No | No |
| | gamel matchi ngcon ratio | • AWS: Lift chma onfi ion | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon GameLift Streams [gamelift streams] | gamel tream plica | • AWS: Lift ms:: cati | Yes | No | No | No |
| | gamel tream reamg | • AWS: Lift ms:: mGrc | Yes | No | No | No |
| Amazon GuardDuty [AWS] | AWS::( dDuty blish estin n | • AWS: dDut blis esti n | Yes | No | No | No |
| Amazon GuardDuty [guarddut y] | guard :malw prote n- plan | • AWS: dDut lwar ecti n | Yes | No | Yes | Yes |
| | guard :dete | • AWS: dDut tect | Yes | Yes | Yes | Yes |
| | guard :dete / ipset | • AWS: dDut Set | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | guard :dete / threa telse | • AWS: dDut reat Set | Yes | Yes | Yes | Yes |
| | guard :dete / filte | • AWS: dDut lter | Yes | Yes | Yes | Yes |
| Amazon Honeycode [honeycod e] | honey :scre a utoma | • N/ A | Yes | No | No | No |
| | honey :work | • N/ A | Yes | No | No | No |
| | honey :tabl | • N/ A | Yes | No | No | No |
| | honey :scre | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Inspector [inspecto r2] | inspe 2:cod n- confi ratio | • AWS: ecto Cis nfig on | Yes | No | No | No |
| | inspe 2:cis con figur n | • AWS: ecto Cis nfig on | Yes | No | No | No |
| | inspe 2:fil | • AWS: ecto Filt | Yes | Yes | Yes | Yes |
| | inspe 2:cod urity int egrat | • N/ A | Yes | No | No | No |
| | inspe 2:cod urity con figur n | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Interacti ve Video Service [ivs] | inspe 2:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| | ivs:p c- key | • AWS: :Pub y | Yes | No | Yes | Yes |
| | ivs:i t- confi ratio | • AWS: :Inc nfig on | Yes | No | Yes | Yes |
| | ivs:r ding- conf igura | • AWS: :Rec gCor atic | Yes | No | Yes | Yes |
| | ivs:t code- conf igura | • N/ A | Yes | No | No | No |
| | ivs:c room | • AWS: hat: | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ivs:p ack-restr ictio po licy | • AWS: :Pla Rest onPc | Yes | No | Yes | Yes |
| | ivs:c el | • AWS: :Cha | Yes | No | Yes | Yes |
| | ivs:p ack-key | • AWS: :Pla KeyF | Yes | No | Yes | Yes |
| | ivs:s m-key | • AWS: :Str y | Yes | No | Yes | Yes |
| | ivs:c sitio | • N/ A | Yes | No | No | No |
| | ivs:s | • AWS: :Sta | Yes | No | Yes | Yes |
| | ivs:s ge-confi urati | • AWS: :Stc onfi ion | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ivs:e er- confi urati | • AWS: :Enc onfi ion | Yes | No | Yes | Yes |
| Amazon Kendra Intellige nt Ranking [kendra-r anking] | kendr ra nking core- exec ution pla n | • AWS: raRa ::E onP | Yes | No | Yes | Yes |
| Amazon Kendra [kendra] | kendr dex | • AWS: ra:: | Yes | No | Yes | Yes |
| | kendr dex/ thesa urus | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | kendr dex/ query - sugge ons- block - list | • N/ A | Yes | No | No | No |
| | kendr dex/ data- sourc | • AWS: ra:: ourc | Yes | No | Yes | Yes |
| | kendr dex/ featu red- resul ts- set | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Keyspaces (for Apache Cassandra ) [cassandr a] | cassa :keys | • AWS: andı yspa | Yes | No | Yes | Yes |
| | cassa :tabl | • AWS: andı ble | Yes | No | No | No |
| Amazon Kinesis Analytics [kinesisa nalytics] | kines alyti pplic n | • AWS: sisA ics: icat | Yes | Yes | Yes | Yes |
| | kines alyti pplic n | • AWS: sisA icsV plic | Yes | Yes | Yes | Yes |
| | kines alyti LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| Amazon Kinesis Data Streams [kinesis] | kines tream | • AWS: sis: am | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | kines tream, con sumer | • AWS: sis: amCc r | Yes | No | Yes | Yes |
| Amazon Kinesis Firehose [firehose ] | fireh deliv tream | • AWS: sisF se:: eryS | Yes | Yes | Yes | Yes |
| | fireh ALL_S RTED | • N/ A | No | Yes | Yes | Yes |
| Amazon Kinesis Video Streams [kinesisv ideo] | kines deo:s m | • AWS: sisV :Str | Yes | No | Yes | Yes |
| | kines deo:c el | • AWS: sisV :Sig gCha | Yes | No | Yes | Yes |
| Amazon Lex [lex] | lex:b c hanne | • N/ A | Yes | No | No | No |
| | lex:t set | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | lex:b a lias | • AWS: :Bot | Yes | No | Yes | Yes |
| | lex:b | • AWS: :Bot | Yes | No | Yes | Yes |
| Amazon Lightsail [lightsai l] | light :keyp | • N/ A | Yes | No | No | No |
| | light :dist tion | • AWS: tsai stri n | Yes | No | Yes | Yes |
| | light :cont rserv | • AWS: tsai ntai | Yes | No | Yes | Yes |
| | light :disk shot | • AWS: tsai skSr t | Yes | No | No | No |
| | light :rela aldat e | • AWS: tsai taba | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | light :cert ate | • AWS: tsai rtif | Yes | No | Yes | Yes |
| | light :buck | • AWS: tsai cket | Yes | No | Yes | Yes |
| | light :inst | • AWS: tsai star | Yes | No | Yes | Yes |
| | light :disk | • AWS: tsai sk | Yes | No | Yes | Yes |
| | light :load ncer | • AWS: tsai adBa r | Yes | No | Yes | Yes |
| | light :doma | • AWS: tsai mair | Yes | No | Yes | Yes |
| | light :inst snaps | • AWS: tsai star psho | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Location [geo] | light :rela aldat esnap | • N/ A | Yes | No | No | No |
| | light :stat | • AWS: tsai atic | Yes | No | Yes | Yes |
| | geo:g nce- colle ction | • AWS: tior fenc ecti | Yes | No | Yes | Yes |
| | geo:t er | • AWS: tior cker | Yes | No | Yes | Yes |
| | geo:a key | • AWS: tior Key | Yes | No | Yes | Yes |
| | geo:p - index | • AWS: tior ceIr | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | geo:r - calcu or | • AWS: tior teCa tor | Yes | No | Yes | Yes |
| | geo:m | • AWS: tior | Yes | No | Yes | Yes |
| Amazon Lookout for Equipment [lookoute quipment] | looko uipme atase | • N/ A | Yes | No | No | No |
| | looko uipme abel- grou p | • N/ A | Yes | No | No | No |
| | looko uipme nfere sched | • AWS: outE ent: renc dule | Yes | No | No | No |
| | looko uipme odel | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Lookout for Metrics [lookoutm etrics] | looko trics ricse | • N/ A | Yes | No | No | No |
| | looko trics malyd tor | • AWS: outM s::A yDet | Yes | No | Yes | Yes |
| | looko trics rt | • AWS: outM s::A | Yes | No | Yes | Yes |
| Amazon Lookout for Vision [lookoutv ision] | looko sion:r l | • N/ A | Yes | No | No | No |
| Amazon MQ [mq] | mq:co uratio | • AWS: onMQ figu n | Yes | Yes | Yes | Yes |
| | mq:br | • AWS: onMQ ker | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | mq:AL PPORT | • N/A | No | Yes | Yes | Yes |
| Amazon Machine Learning [machinel earning] | machi arnin aluat | • N/A | Yes | No | No | No |
| | machi arnin model | • N/A | Yes | No | No | No |
| | machi arnin tchpr tion | • N/A | Yes | No | No | No |
| | machi arnin tasou | • N/A | Yes | No | No | No |
| Amazon Macie [macie2] | macie assif ion-job | • N/A | Yes | No | No | No |
| | macie L_SUP ED | • N/A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Macie [macie] | macie ow-list | • AWS: e::A ist | Yes | No | No | No |
| | macie ber | • N/ A | Yes | No | No | No |
| | macie dings fil ter | • AWS: e::F gsFi | Yes | No | No | No |
| | macie ssifi on-job | • N/ A | Yes | No | No | No |
| | macie tom-data- ident r | • AWS: e::C Data ifie | Yes | No | No | No |
| Amazon Managed Blockchain [managedb lockchain ] | manag ockch propo | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | manag ockch membe | • AWS: gedE hair ber | Yes | No | No | No |
| | manag ockch acces | • AWS: gedE hair essc | Yes | No | Yes | Yes |
| | manag ockch netwo | • N/ A | Yes | No | No | No |
| | manag ockch nodes | • AWS: gedE hair e | Yes | No | No | No |
| | manag ockch invit ns | • N/ A | Yes | No | No | No |
| Amazon Managed Grafana [grafana] | grafa orksp | • AWS: ana: spac | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Managed Service for Prometheus [aps] | aps:s er | • AWS: :Scr | Yes | No | No | No |
| | aps:a lydet r | • AWS: :Anc etec | Yes | No | No | No |
| | aps:w pace | • AWS: :Wor e | Yes | No | Yes | Yes |
| | aps:r roups space | • AWS: :Rul psNa ce | Yes | No | Yes | Yes |
| Amazon Managed Streaming for Apache Kafka [kafka] | kafka - conne on | • AWS: :Vpc ctic | Yes | No | No | No |
| | kafka ster | • AWS: :Clu | Yes | No | No | No |
| | kafka licat | • AWS: :Rep or | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Managed Streaming for Kafka Connect [kafkaconnect] | kafka ect:w r- confi ratio | • AWS: aCor :Wor nfig on | Yes | No | Yes | Yes |
| | kafka ect:c ctor | • AWS: aCor :Cor r | Yes | No | No | No |
| | kafka ect:c m- plugi | • AWS: aCor :Cus ugir | Yes | No | Yes | Yes |
| Amazon Managed Workflows for Apache Airflow [airflow] | airfl nviro t | • AWS: ::Er ment | Yes | No | Yes | Yes |
| Amazon MemoryDB [memorydb] | memor clust | • AWS: ryDB ster | Yes | No | Yes | Yes |
| | memor acl | • AWS: ryDB | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | memor subne up | • AWS: ryDE netC | Yes | No | Yes | Yes |
| | memor reser ode | • N/ A | Yes | No | No | No |
| | memor multi onclu | • AWS: ryDE tiRe lust | Yes | No | No | No |
| | memor user | • AWS: ryDE r | Yes | No | Yes | Yes |
| | memor param group | • AWS: ryDE amet up | Yes | No | Yes | Yes |
| | memor snaps | • N/ A | Yes | No | No | No |
| Amazon Nimble Studio [nimble] | nimbl udio | • AWS: leSt :Stu | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | nimbl unch- prof ile | • N/ A | Yes | No | No | No |
| | nimbl reami s essio | • N/ A | Yes | No | No | No |
| | nimbl reami s essio ba ckup | • N/ A | Yes | No | No | No |
| | nimbl reami i mage | • N/ A | Yes | No | No | No |
| | nimbl udio- comp onent | • N/ A | Yes | No | No | No |
| Amazon One Enterpris e [one] | one:s | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | one:d e- insta e | • N/ A | Yes | No | No | No |
| | one:d e- confi ratio te mplat | • N/ A | Yes | No | No | No |
| Amazon OpenSearc h Ingestion [osis] | osis: line | • AWS: ::Pi e | Yes | No | Yes | Yes |
| Amazon OpenSearc h Serverles s [aoss] | aoss: ectio | • AWS: Sea ver Col n | Yes | Yes | Yes | Yes |
| | aoss: ectio gr oup | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | aoss:A SUPPO | • N/A | No | Yes | Yes | Yes |
| Amazon OpenSearch [es] | es:do | • AWS: tics ::Dc<br>• AWS: Sea vice ain | Yes | Yes | No | No |
| | es:AL PPORT | • N/A | No | Yes | No | No |
| Amazon OpenSearch [opensearch] | opens h:dat rce | • N/A | Yes | No | No | No |
| Amazon Personalize [personalize] | perso ze:da d eleti job | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | perso ze:da t-group | • AWS: onal Data oup | Yes | No | Yes | Yes |
| | perso ze:ba segme job | • N/ A | Yes | No | No | No |
| | perso ze:ca gn | • N/ A | Yes | No | No | No |
| | perso ze:re ender | • N/ A | Yes | No | No | No |
| | perso ze:ba infer - job | • N/ A | Yes | No | No | No |
| | perso ze:ev track | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | perso ze:da t-impor job | • N/ A | Yes | No | No | No |
| | perso ze:da t | • AWS: onal Data | Yes | No | Yes | Yes |
| | perso ze:so on | • AWS: onal Solu | Yes | No | Yes | Yes |
| | perso ze:fi | • N/ A | Yes | No | No | No |
| | perso ze:da t-expor job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Pinpoint SMS and Voice Service [sms-voic e] | sms-voice :send id | • AWS: OICE der1 | Yes | Yes | No | No |
| | sms-voice :prot confi tion | • AWS: OICE tect gura | Yes | No | No | No |
| | sms-voice :opt-out-list | • AWS: OICE Outl | Yes | Yes | No | No |
| | sms-voice :phon nu mber | • AWS: OICE neNu | Yes | Yes | No | No |
| | sms-voice :pool | • AWS: OICE l | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sms-voice :conf ation set | • AWS: OICE figu nSet | Yes | Yes | No | No |
| | sms-voice :ALL_ ORTED | • N/ A | No | Yes | No | No |
| Amazon Pinpoint [mobileta rgeting] | mobil getin mplat | • AWS: oint Temp<br>• AWS: oint hTem<br>• AWS: oint ppTe e<br>• AWS: oint ilTe e | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | mobil getin ps | • AWS: oint | Yes | No | Yes | Yes |
| Amazon Q Business Q Apps [qapps] | qapps licat qapp/ sess ion | • N/ A | Yes | No | No | No |
| | qapps licat qapp | • N/ A | Yes | No | No | No |
| Amazon Q Business [qbusiness] | qbusi :appl ion/ plugi n | • AWS: ines ugir | Yes | No | No | No |
| | qbusi :appl ion/ retri ever | • AWS: ines trie | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | qbusi :appl ion/ index / data- sou rce | • AWS: ines taSc | Yes | No | No | No |
| | qbusi :appl ion | • AWS: ines plic | Yes | No | No | No |
| | qbusi :appl ion/ web- e xperi | • AWS: ines bExp ce | Yes | No | No | No |
| | qbusi :appl ion/ index | • AWS: ines dex | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Q in Connect [wisdom] | wisdo ntent ass ociat | • N/ A | Yes | No | No | No |
| | wisdo ntent | • N/ A | Yes | Yes | No | No |
| | wisdo sista | • AWS: om:: tant | Yes | Yes | Yes | Yes |
| | wisdo ick- respo nse | • AWS: om:: Resp | Yes | No | No | No |
| | wisdo - agent | • AWS: om:: nt | Yes | No | Yes | Yes |
| | wisdo ssage tem plate | • AWS: om:: geTe e | Yes | No | No | No |
| | wisdo owled b ase | • AWS: om:: edge | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | wisdo ssion | • N/ A | Yes | Yes | No | No |
| | wisdo - promp | • AWS: om:: mpt | Yes | No | No | No |
| | wisdo - guard l | • AWS: om:: rdra | Yes | No | No | No |
| | wisdo socia | • AWS: om:: tant iati | Yes | Yes | Yes | Yes |
| | wisdo L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| Amazon QLDB [qldb] | qldb: er | • AWS: ::Le | Yes | No | No | No |
| | qldb: am | • AWS: ::St | Yes | No | No | No |
| | qldb: er/ table | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon QuickSigh t [quicksig ht] | quick: t:vpc ectio | • AWS: kSig PCCo ion | Yes | No | No | No |
| | quick: t:ana s | • AWS: kSig naly | Yes | No | No | No |
| | quick: t:fol | • AWS: kSig olde | Yes | No | No | No |
| | quick: t:cus ermis s | • AWS: kSig ustc issi | Yes | No | No | No |
| | quick: t:bra | • N/ A | Yes | No | No | No |
| | quick: t:use | • N/ A | Yes | No | No | No |
| | quick: t:dat rce | • AWS: kSig ataS | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | quick t:tem e | • AWS: kSic empl | Yes | No | No | No |
| | quick t:top | • AWS: kSic opic | Yes | No | No | No |
| | quick t:ema c ustom ion- templ ate | • N/ A | Yes | No | No | No |
| | quick t:the | • AWS: kSic heme | Yes | No | No | No |
| | quick t:cus zatio | • N/ A | Yes | No | No | No |
| | quick t:flo | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | quick t:act conne | • N/ A | Yes | No | No | No |
| | quick t:nam ce | • N/ A | Yes | No | No | No |
| | quick t:dat | • AWS kSig ataS | Yes | No | No | No |
| | quick t:das rd | • AWS kSig ashB | Yes | No | No | No |
| Amazon RDS [neptune-graph] | neptu g raph: rt- task | • N/ A | Yes | No | No | No |
| | neptu g raph: h | • AWS uneG :Gra | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | neptu g raph: h- snaps t | • N/ A | Yes | No | No | No |
| Amazon RDS [rds] | rds:c er- snaps ot | • N/ A | Yes | No | No | No |
| | rds:d | • AWS: B::D ance<br>• AWS: :DBI ce | Yes | No | Yes | Yes |
| | rds:g lclus | • AWS: :Glc uste | Yes | No | No | No |
| | rds:g l- clust | • AWS: :Glc uste | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | rds:s p | • AWS: :DBS Grou | Yes | Yes | Yes | Yes |
| | rds:c er- auto- b ackup | • N/ A | Yes | No | No | No |
| | rds:d yment | • N/ A | Yes | No | No | No |
| | rds:p | • AWS: une: rame oup | Yes | Yes | Yes | Yes |
| | rds:c er- pg | • AWS: une: uste mete p | Yes | Yes | Yes | Yes |
| | rds:s hot- tenan t- datab e | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | rds:e | • AWS: B::E ubsc on | Yes | Yes | Yes | Yes |
| | rds:p | • AWS: :DBF terC | Yes | Yes | Yes | Yes |
| | rds:t t- group | • AWS: :DBF arge p | Yes | Yes | Yes | Yes |
| | rds:c er | • AWS: B::D ter | Yes | No | Yes | Yes |
| | rds:s hot | • N/ A | Yes | No | No | No |
| | rds:d pr oxy | • AWS: :DBF | Yes | Yes | Yes | Yes |
| | rds:e | • AWS: :Eve scri | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | rds:c er- endpo nt | • N/ A | Yes | Yes | No | No |
| | rds:i ratio | • AWS: :Int ion | Yes | No | No | No |
| | rds:r | • N/ A | Yes | Yes | No | No |
| | rds:a backu | • N/ A | Yes | No | No | No |
| | rds:s p | • AWS: :DBS tyGr | Yes | Yes | Yes | Yes |
| | rds:c | • AWS: :Cus Engi sior | Yes | No | Yes | Yes |
| | rds:d pr oxy- endpo int | • AWS: :DBF ndpc | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | rds:c er-pg | • AWS: :DBC rPar rGrc | Yes | Yes | Yes | Yes |
| | rds:o p | • AWS: :Opt oup | Yes | No | No | No |
| | rds:o | • AWS: :Opt oup | Yes | Yes | Yes | Yes |
| | rds:d | • AWS: une: star | Yes | No | Yes | Yes |
| | rds:s p | • AWS: B::D etGr | Yes | Yes | Yes | Yes |
| | rds:t t-datab e | • N/ A | Yes | No | No | No |
| | rds:s p | • AWS: une: bnet | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | rds:c er-pg | • AWS: B::D terP terC | Yes | Yes | Yes | Yes |
| | rds:A UPPOR | • N/A | No | Yes | Yes | Yes |
| Amazon Redshift Serverles s [redshift -serverle ss] | redsh serve s:rec ypoin | • N/A | Yes | No | No | No |
| | redsh serve s:wor up | • AWS: hift rles rkgr | Yes | Yes | Yes | Yes |
| | redsh serve s:nam ce | • AWS: hift rles mesp | Yes | Yes | Yes | Yes |
| | redsh serve s:sna t | • AWS: hift rles apsh | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | redsh serve s:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| Amazon Redshift [redshift ] | redsh event cript | • AWS: hift ntSu ptic | Yes | Yes | Yes | Yes |
| | redsh hsmco urati | • N/ A | Yes | Yes | No | No |
| | redsh subne up | • AWS: hift ster tGrc | Yes | Yes | Yes | Yes |
| | redsh snaps opygr | • N/ A | Yes | Yes | No | No |
| | redsh qev2i plica | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | redsh secur roupi ss | • AWS: hift ster ityC ngre | Yes | No | No | No |
| | redsh names | • N/ A | Yes | No | No | No |
| | redsh snaps chedu | • N/ A | Yes | Yes | No | No |
| | redsh secur roup | • AWS: hift ster ityC | Yes | No | No | No |
| | redsh hsmcl certi te | • N/ A | Yes | Yes | No | No |
| | redsh redsh dcapp tion | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | redsh clust | • AWS: hift ster | Yes | Yes | Yes | Yes |
| | redsh snaps | • N/ A | Yes | Yes | No | No |
| | redsh usage t | • N/ A | Yes | No | No | No |
| | redsh integ on | • AWS: hift egra | Yes | No | Yes | Yes |
| | redsh param group | • AWS: hift ster eter | Yes | Yes | Yes | Yes |
| | redsh ALL_S RTED | • N/ A | No | Yes | Yes | Yes |
| Amazon Rekogniti on [rekognit ion] | rekog on:pr t/ versi | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | rekog on:pr t | • AWS: gnit Proj | Yes | No | No | No |
| | rekog on:co tion | • AWS: gnit Coll n | Yes | No | Yes | Yes |
| | rekog on:st proce | • AWS: gnit Stre cess | Yes | No | No | No |
| Amazon Route 53 Profiles [route53p rofiles] | route ofile ofile ass ociat | • AWS: e53F es:: leAs tior | Yes | No | Yes | Yes |
| | route ofile ofile | • AWS: e53F es:: le | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Route 53 Recovery Controls [route53-recovery-control] | route r ecove c ontro ntrol l/ safet ule | • AWS: e53F ryCc ::Sa ule | Yes | No | Yes | Yes |
| | route r ecove c ontro uster | • AWS: e53F ryCc ::Cl | Yes | No | Yes | Yes |
| | route r ecove c ontro ntrol l | • AWS: e53F ryCc ::Cc Pane | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Route 53 Recovery Readiness [route53-recovery-readiness] | route r ecove r eadin recov group | • AWS: e53F ryRe ss:: eryC | Yes | No | Yes | Yes |
| | route r ecove r eadin readi - check | • AWS: e53F ryRe ss:: ness | Yes | No | Yes | Yes |
| | route r ecove r eadin cell | • AWS: e53F ryRe ss:: | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | route r ecove r eadin resou set | • AWS: e53F ryRe ss:: rceS | Yes | No | Yes | Yes |
| Amazon Route 53 Resolver [route53r esolver] | route solve solve ru le | • AWS: e53F er:: verF | Yes | Yes | Yes | Yes |
| | route solve rewal do main- list | • AWS: e53F er:: allD List | Yes | No | Yes | Yes |
| | route solve solve en dpoin | • AWS: e53F er:: verE nt | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | route solve solve qu ery- log- c onfig | • AWS: e53F er:: ver( oggi fig | Yes | No | Yes | Yes |
| | route solve rewal ru le- group | • AWS: e53F er:: allF oup | Yes | No | Yes | Yes |
| | route solve rewal ru le- group assoc on | • AWS: e53F er:: allF oupA atic | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | route solve tpost res olver | • AWS: e53F er:: stRe r | Yes | No | No | No |
| | route solve L_SUP ED | • N/ A | No | Yes | Yes | Yes |
| Amazon Route 53 [route53] | route ealth k | • AWS: e53: thCh | Yes | No | Yes | Yes |
| | route omain | • N/ A | Yes | No | No | No |
| | route osted | • AWS: e53: edZo | Yes | Yes | Yes | Yes |
| | route LL_SU TED | • N/ A | No | Yes | Yes | Yes |
| Amazon S3 Express [s3expres s] | s3exp :acce int | • AWS: pres cess | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | s3exp :buck | • AWS: pres rect cket | Yes | No | Yes | Yes |
| Amazon S3 Glacier [glacier] | glaci aults | • N/ A | Yes | No | No | No |
| Amazon S3 Tables [s3tables ] | s3tab Table et | • AWS: bles leBu | Yes | No | No | No |
| | s3tab table | • AWS: bles le | Yes | No | No | No |
| Amazon S3 Vectors [s3vector s] | s3vec :inde | • AWS: ctor dex | Yes | No | No | No |
| | s3vec :vect cket | • AWS: ctor ctor t | Yes | No | No | No |
| Amazon S3 [s3] | s3:ac grant tance | • AWS: Acce nts] ce | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | s3:bu | • AWS: Buck | Yes | Yes | Yes | Yes |
| | s3:jo | • N/ A | Yes | No | No | No |
| | s3:ac - grant | • AWS: Acce nt | Yes | No | No | No |
| | s3:st e- lens | • AWS: Stor ns | Yes | Yes | Yes | Yes |
| | s3:ac - grant l ocati | • AWS: Acce ntsL on | Yes | No | No | No |
| | s3:ac grant ation | • AWS: Acce ntsL on | Yes | No | No | No |
| | s3:st e- lens- gr oup | • AWS: Stor nsGr | Yes | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | s3:ac point | • AWS: Acce nt | Yes | No | Yes | Yes |
| | s3:AL PPORT | • N/ A | No | Yes | Yes | Yes |
| Amazon SES [ses] | ses:i ity | • AWS: :Ema ntit<br>• AWS: oint ::Ic y | Yes | No | Yes | Yes |
| | ses:d ated- ip-p ool | • AWS: :Dec dIpF<br>• AWS: oint ::De edIp | Yes | No | Yes | Yes |
| | ses:c ct- list | • AWS: :Cor ist | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ses:m anage in gress poi nt | • AWS: :Mai gerI sPoi | Yes | No | Yes | Yes |
| | ses:c gurat set | • AWS: :Cor atic<br>• AWS: oint ::Cc rati | Yes | No | Yes | Yes |
| | ses:m anage ad dress lis t | • AWS: :Mai gerA sLis | Yes | No | No | No |
| | ses:m - regio e ndpoi | • AWS: :Mul ionE nt | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | ses:m anage ar chive | • AWS: :Mai gerA e | Yes | No | Yes | Yes |
| | ses:m anage tr affic pol icy | • AWS: :Mai gerT cPol | Yes | No | Yes | Yes |
| | ses:m anage ru le- set | • AWS: :Mai gerR t | Yes | No | Yes | Yes |
| Amazon SNS [sns] | sns:t | • AWS: :Top | Yes | Yes | Yes | Yes |
| | sns:A UPPOR | • N/ A | No | Yes | Yes | Yes |
| Amazon SQS [sqs] | sqs:q | • AWS: :Que | Yes | Yes | Yes | Yes |
| | sqs:A UPPOR | • N/ A | No | Yes | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon SageMaker [sagemake r] | sagem :imag | • AWS: Make age | Yes | No | Yes | Yes |
| | sagem :mode qu ality job - defin on | • AWS: Make delC yJob itic | Yes | No | Yes | Yes |
| | sagem :moni ng- sched le | • AWS: Make nitc chec | Yes | No | Yes | Yes |
| | sagem :tran m- job | • N/ A | Yes | No | No | No |
| | sagem :code rep osito | • AWS: Make deRe ory | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :imag sion | • AWS: Make age\ n | Yes | No | No | No |
| | sagem :expe nt | • N/ A | Yes | Yes | No | No |
| | sagem :acti | • N/ A | Yes | Yes | No | No |
| | sagem :hype pa ramet t uning job | • N/ A | Yes | No | No | No |
| | sagem :mode bi as- job- de finit | • AWS: Make delB bDef on | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :app- imag e- confi | • AWS: Make pIma fig | Yes | Yes | Yes | Yes |
| | sagem :mode | • AWS: Make del | Yes | No | Yes | Yes |
| | sagem :trai - plan | • N/ A | Yes | No | No | No |
| | sagem :work e | • N/ A | Yes | No | No | No |
| | sagem :mode ex plain ity- job- d efini | • AWS: Make delE nabi obDe ion | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :mode ca rd | • AWS: Make delC | Yes | No | Yes | Yes |
| | sagem :mode ca rd- expor - job | • N/ A | Yes | No | No | No |
| | sagem :notel - insta - lifec e- confi | • AWS: Make tebc tanc cycl ig | Yes | No | Yes | Yes |
| | sagem :notel - insta | • AWS: Make tebc tanc | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :comp ion- job | • N/ A | Yes | No | No | No |
| | sagem :mode pa ckage | • AWS: Make delP e | Yes | Yes | Yes | Yes |
| | sagem :data qua lity- job- defin n | • AWS: Make taQu JobD tior | Yes | No | Yes | Yes |
| | sagem :user pro file | • AWS: Make erPr | Yes | No | Yes | Yes |
| | sagem :doma | • AWS: Make mair | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :mlfl t racki s erver | • AWS: Make flow ingS | Yes | No | Yes | Yes |
| | sagem :edge pac kagin job | • N/ A | Yes | No | No | No |
| | sagem :clus | • AWS: Make uste | Yes | No | Yes | Yes |
| | sagem :devi | • AWS: Make vice | Yes | No | No | No |
| | sagem :feat group | • AWS: Make atur p | Yes | No | Yes | Yes |
| | sagem :arti | • N/ A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :stud l ifecy confi | • AWS: Make udic ycle g | Yes | No | Yes | Yes |
| | sagem :clus sched - confi | • N/ A | Yes | No | No | No |
| | sagem :auto job | • N/ A | Yes | No | No | No |
| | sagem :app | • AWS: Make p | Yes | No | Yes | Yes |
| | sagem :spac | • AWS: Make ace | Yes | No | Yes | Yes |
| | sagem :infe e- compo nt | • AWS: Make fere mpor | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :endp | • AWS: Make dpoi | Yes | No | Yes | Yes |
| | sagem :work | • AWS: Make rkte | Yes | No | Yes | Yes |
| | sagem :infe e- exper ent | • AWS: Make fere peri | Yes | No | Yes | Yes |
| | sagem :opti tion- job | • N/ A | Yes | No | No | No |
| | sagem :algo m | • N/ A | Yes | No | No | No |
| | sagem :pipe / execu n | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :pipe - execu n | • N/ A | Yes | No | No | No |
| | sagem :proj | • AWS: Make ojec | Yes | Yes | Yes | Yes |
| | sagem :mode pa ckage gro up | • AWS: Make delP eGrc | Yes | Yes | Yes | Yes |
| | sagem :labe - job | • N/ A | Yes | No | No | No |
| | sagem :edge dep loyme | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :trai - job | • N/ A | Yes | Yes | No | No |
| | sagem :comp quota | • N/ A | Yes | No | No | No |
| | sagem :rese - capac | • N/ A | Yes | No | No | No |
| | sagem :cont | • N/ A | Yes | Yes | No | No |
| | sagem :part app | • AWS: Make rtne | Yes | No | No | No |
| | sagem :expe nt- trial | • N/ A | Yes | No | No | No |
| | sagem :hub | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :flow def initi | • N/ A | Yes | Yes | No | No |
| | sagem :pipe | • AWS: Make peli | Yes | Yes | Yes | Yes |
| | sagem :line group | • N/ A | Yes | No | No | No |
| | sagem :infe e- recom ndati job | • N/ A | Yes | No | No | No |
| | sagem :devi f leet | • AWS: Make vice | Yes | No | No | No |
| | sagem :hub- cont ent | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | sagem :expe nt-trial compo | • N/A | Yes | No | No | No |
| | sagem :endp - confi | • AWS: Make dpoi fig | Yes | No | Yes | Yes |
| | sagem :proc ng-job | • AWS: Make oces ob | Yes | Yes | Yes | Yes |
| | sagem :huma ta sk-ui | • N/A | Yes | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon SageMaker geospatial capabilities [sagemaker-geospatial] | sagem - geosp al:ra - data- col lecti | • N/A | Yes | No | No | No |
| | sagem - geosp al:ea obser on- job | • N/A | Yes | No | No | No |
| | sagem - geosp al:ve - enric nt- job | • N/A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Security Lake [securitylake] | secur ake:d lake | • AWS: rity :Dat | Yes | Yes | No | No |
| | secur ake:s riber | • AWS: rity :Sub er | Yes | Yes | No | No |
| | secur ake:A UPPOR | • N/ A | No | Yes | No | No |
| Amazon Simple Workflow Service [swf] | swf:d n | • N/ A | Yes | No | No | No |
| Amazon Textract [textract] | textr adapt | • N/ A | Yes | Yes | No | No |
| | textr ALL_S RTED | • N/ A | No | Yes | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon Timestrea m InfluxDB [timestre am-influx db] | times m- influ b:db- inst ance | • N/ A | Yes | No | No | No |
| Amazon Timestrea m [timestre am] | times m:dat e | • AWS: stre atab | Yes | No | Yes | Yes |
| | times m:dat e/ table | • AWS: stre able | Yes | No | Yes | Yes |
| | times m:sch ed- query | • AWS: stre chec uery | Yes | No | Yes | Yes |
| Amazon Transcrib e [transcri be] | trans e:voc ary- filte r | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | trans e:voc ary | • N/ A | Yes | No | No | No |
| | trans e:tra iptio job | • N/ A | Yes | No | No | No |
| | trans e:med - trans ption job | • N/ A | Yes | No | No | No |
| | trans e:med - vocab ry | • N/ A | Yes | No | No | No |
| | trans e:med - scrib job | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | trans e:lan e-model | • N/A | Yes | No | No | No |
| Amazon Translate [translat e] | trans :para - data | • N/A | Yes | No | No | No |
| | trans :term ogy | • N/A | Yes | No | No | No |
| Amazon VPC Lattice [vpc-latt ice] | vpc- latti ce:se e/ liste r/ rule | • AWS: atti ule | Yes | No | Yes | Yes |
| | vpc- latti ce:se enetw ervic ociat | • AWS: atti ervi work ceAs tior | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | vpc-latti ce:se e/ liste r | • AWS: atti iste | Yes | No | Yes | Yes |
| | vpc-latti ce:ac logsu iptio | • AWS: atti cces ubsc on | Yes | No | Yes | Yes |
| | vpc-latti ce:se enetw esour socia | • AWS: atti ervi work rceA atic | Yes | No | No | No |
| | vpc-latti ce:do verif ion | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | vpc-latti ce:re ceend tasso ion | • N/ A | Yes | No | No | No |
| | vpc-latti ce:se enetw pcass tion | • AWS: atti ervi work soci | Yes | No | Yes | Yes |
| | vpc-latti ce:se e | • AWS: atti ervi | Yes | No | Yes | Yes |
| | vpc-latti ce:se enetw | • AWS: atti ervi work | Yes | No | Yes | Yes |
| | vpc-latti ce:re cecon ratio | • AWS: atti esou nfig on | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | vpc-latti ce:ta group | • AWS: atti arge p | Yes | No | Yes | Yes |
| | vpc-latti ce:re cegat | • AWS: atti esou tewa | Yes | No | No | No |
| Amazon Verified Permissio ns [verified permissio ns] | verif ermis s:pol store | • AWS: fiec ssic olic e | Yes | No | Yes | Yes |
| Amazon WorkLink [worklink ] | workl fleet | • N/ A | Yes | Yes | No | No |
| Amazon WorkMail [workmail ] | workm organ ion | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Amazon WorkSpaces Secure Browser [workspaces-web] | works s-web:p tal | • AWS: Spac ::Pc | Yes | No | Yes | Yes |
| | works s-web:i ccess ings | • AWS: Spac ::Ip sSet | Yes | No | Yes | Yes |
| | works s-web:u racce gging ings | • AWS: Spac ::Us essL gSet | Yes | No | Yes | Yes |
| | works s-web:d aprot onset s | • AWS: Spac ::Da tect ttir | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | works s- web:s sionl r | • AWS: Spac ::Se Logg | Yes | No | No | No |
| | works s- web:u rsett | • AWS: Spac ::Us ting | Yes | No | Yes | Yes |
| | works s- web:b wsers ngs | • AWS: Spac ::Br Sett | Yes | No | Yes | Yes |
| | works s- web:i ntity ider | • AWS: Spac ::Id yPro | Yes | No | No | No |
| | works s- web:n works ngs | • AWS: Spac ::Ne Sett | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | works s- web:t ststo | • AWS: Spac ::Tı ore | Yes | No | Yes | Yes |
| Amazon WorkSpace s Secure Browser [workspac esweb] | works sweb: tityp der | • AWS: Spac ::Ic yPrc | Yes | No | No | No |
| Amazon WorkSpace s Thin Client [thinclie nt] | thinc t:env ment | • AWS: Spac nCli Envi nt | Yes | No | No | No |
| | thinc t:env ments | • AWS: Spac nCli Envi nt | Yes | No | No | No |
| | thinc t:dev | • N/ A | Yes | No | No | No |
| | thinc t:dev | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | thinc t:sof eset | • N/ A | Yes | No | No | No |
| Amazon WorkSpace s [workspac es] | works s:dir ry | • N/ A | Yes | Yes | No | No |
| | works s:wor ce | • AWS: Spac orks | Yes | Yes | No | No |
| | works s:wor cebun | • N/ A | Yes | Yes | No | No |
| | works s:wor ceima | • N/ A | Yes | Yes | No | No |
| | works s:con ional | • AWS: Spac onne Alia | Yes | Yes | Yes | Yes |
| | works s:wor cespo | • AWS: Spac orks Pool | Yes | No | Yes | Yes |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON synta** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| | works s:wor ceipg | • N/ A | Yes | Yes | No | No |
| | works s:ALL_ PORTE | • N/ A | No | Yes | Yes | Yes |
| Deprecate d - AWS IoT 1-Click [iot1clic k] | iot1c :devi | • N/ A | Yes | No | No | No |
| | iot1c :proj | • N/ A | Yes | No | No | No |
| Deprecate d AWS IoT RoboRunne r [iotrobor unner] | iotro nner: | • N/ A | Yes | No | No | No |
| | iotro nner: / worke f leet | • N/ A | Yes | No | No | No |

| | | | Basic Compliance Rules | | Required Tag Keys | |
|---|---|---|---|---|---|---|
| **Service** | **Tag Polic JSON syntax** | **Cloud ation Alias** | **Reporting Mode** | **Enforceme nt Mode** | **Reporting Mode** | **Enforce for IaC** |
| Multi-party approval [mpa] | mpa:a val-team | • AWS: :App Team | Yes | No | No | No |
| | mpa:i ity-sourc e | • AWS: :Ide Sou | Yes | No | No | No |
| Service Quotas [servicequotas] | servi otas: a | • N/A | Yes | No | No | No |
| route53globalresolver [route53globalresolver] | route obalr ver:f all-domain-list | • N/A | Yes | No | No | No |

- Consultez la documentation Terraform pour la prise en charge des types de ressources dans AWS Terraform Provider.
- Consultez la documentation de Pulumi pour la prise en charge des types de ressources dans Pulumi Cloud.

## Régions prises en charge

Les fonctions de politique de balises sont disponibles dans les régions suivantes :

| Nom de la région | Paramètre de région |
|---|---|
| Région Est des États-Unis (Nord Virginie)[1] | **us-east-1** |
| Région USA Est (Ohio) | us-east-2 |
| Région US West (N. California) | us-west-1 |
| Région USA Ouest (Oregon) | us-west-2 |
| Région Afrique (Le Cap) | af-south-1 |
| Région Asie-Pacifique (Hong Kong) | ap-east-1 |
| Asie-Pacifique (Taipei) [2] | ap-east-2 |
| Région Asie-Pacifique (Mumbai) | ap-south-1 |
| Asie-Pacifique (Hyderabad) [2] | ap-south-2 |
| Région Asia Pacific (Tokyo) | ap-northeast-1 |
| Région Asia Pacific (Seoul) | ap-northeast-2 |
| Région Asie-Pacifique (Osaka) | ap-northeast-3 |
| Région Asia Pacific (Singapore) | ap-southeast-1 |
| Région Asia Pacific (Sydney) | ap-southeast-2 |
| Région Asie-Pacifique (Jakarta) [2] | ap-southeast-3 |
| Asie-Pacifique (Melbourne) [2] | ap-southeast-4 |
| Région Asie-Pacifique (Malaisie) | ap-southeast-5 |
| Asie-Pacifique (Nouvelle Zélande) [2] | ap-southeast-6 |

| Nom de la région | Paramètre de région |
| --- | --- |
| Asie-Pacifique (Thaïlande) | `ap-southeast-7` |
| Région Canada (Centre) | `ca-central-1` |
| Canada Ouest (Calgary) [2] | `ca-west-1` |
| Région Chine (Beijing) | `cn-north-1` |
| Région Chine (Ningxia) | `cn-northwest-1` |
| Région Europe (Francfort) | `eu-central-1` |
| Région Europe (Zurich) [2] | `eu-central-2` |
| Région Europe (Milan) | `eu-south-1` |
| Europe (Espagne) [2] | `eu-south-2` |
| Région Europe (Irlande) | `eu-west-1` |
| Région Europe (Londres) | `eu-west-2` |
| Région Europe (Paris) | `eu-west-3` |
| Région Europe (Stockholm) | `eu-north-1` |
| Région Mexique (Centre) | `mx-central-1` |
| Région du Moyen-Orient (Émirats arabes unis) [2] | `me-central-1` |
| Région Moyen-Orient (Bahreïn) | `me-south-1` |
| Région Amérique du Sud (Sao Paulo) | `sa-east-1` |
| Israël (Tel Aviv) [2] | `il-central-1` |
| AWS GovCloud (USA Est) | `us-gov-east-1` |
| AWS GovCloud (US-Ouest) | `us-gov-west-1` |

[1]Vous devez spécifier la **`us-east-1`** Région lorsque vous appelez les opérations suivantes des Organisations :

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Toute autre opération sur la racine d'une organisation, telle que ListRoots.

Vous devez également spécifier la région **`us-east-1`** lorsque vous appelez les opérations d'API de balisage des groupes de ressources suivantes qui font partie de la fonction des stratégies de balises :

- DescribeReportCreation
- GetComplianceSummary
- StartReportCreation

> **Note**
>
> Pour évaluer la conformité aux politiques de balises à l'échelle de l'organisation, vous devez également avoir accès à un compartiment Amazon S3 dans la région USA Est (Virginie du Nord) pour le stockage des rapports. Pour plus d'informations, consultez la politique relative aux compartiments Amazon S3 pour le stockage des rapports dans le Guide de l'utilisateur AWS des ressources de balisage.

[2]Ces régions doivent être activées manuellement. Pour en savoir plus sur l'activation et la désactivation Régions AWS, voir Spécifier les comptes que Régions AWS votre compte peut utiliser dans le Guide de référence sur la gestion des AWS comptes. La console Resource Groups n'est pas disponible dans ces régions.

## Politiques relatives aux applications de chat

Les politiques relatives aux applications de chat vous AWS Organizations permettent de contrôler l'accès aux comptes de votre organisation à partir d'applications de chat telles que Slack et Microsoft Teams.

Amazon Q Developer in chat applications est un AWS service qui permet DevOps aux équipes de développement de logiciels d'utiliser les forums de discussion des programmes de messagerie pour

surveiller les événements opérationnels et y répondre AWS Cloud. Dans les applications de chat, Amazon Q Developer traite Service AWS les notifications provenant d'Amazon Simple Notification Service (Amazon SNS) et les transmet aux forums de discussion afin que les équipes puissent les analyser et y donner suite immédiatement, où qu'elles se trouvent.

## Comment fonctionnent les politiques relatives aux applications de chat

À l'aide des politiques des applications de chat, le compte de gestion ou l'administrateur délégué d'une organisation peut effectuer les opérations suivantes au sein de l'organisation :

- Vérifiez quelles applications de chat compatibles (Amazon Chime, Microsoft Teams et Slack) peuvent être utilisées.
- Limitez l'accès des clients de chat à des espaces de travail (Slack) et à des équipes (Microsoft Teams) spécifiques.
- Limitez la visibilité des chaînes Slack aux chaînes publiques ou privées.
- Définissez et appliquez des paramètres de rôle spécifiques.

Les politiques des applications de chat limitent les paramètres au niveau du compte, tels que les paramètres des rôles et les politiques de protection des chaînes, et ont priorité sur eux. Vous pouvez accéder aux politiques des applications de chat et les modifier depuis le développeur Amazon Q dans les applications de chat ou dans la console Organizations.

Une fois les politiques associées aux comptes et aux unités organisationnelles (UO), tout développeur Amazon Q actuel et futur utilisant les configurations d'applications de chat pour les comptes concernés se conformera automatiquement aux paramètres de gouvernance et d'autorisation. Pour plus d'informations, voir Comprendre l'héritage des politiques de gestion.

Si vous essayez d'effectuer une action limitée par une politique d'applications de chat, un message d'erreur vous informera que l'action n'est pas autorisée en raison de la politique des applications de chat et vous recommandera de contacter le compte de gestion ou l'administrateur délégué de votre organisation.

> **Note**
>
> Les politiques des applications de chat sont validées lors de l'exécution. Cela signifie que la conformité des ressources existantes est contrôlée en permanence. Il n'y a aucun chevauchement avec les autorisations IAM existantes, car les autorisations IAM basées sur

l'exécution pour envoyer des notifications ou interagir avec Amazon Q Developer dans les applications de chat ne sont actuellement pas prises en charge.

## Commencer à utiliser les politiques relatives aux applications de chat

Suivez ces étapes pour commencer à utiliser les politiques des applications de chat.

1. Découvrez les autorisations dont vous devez disposer pour effectuer les tâches de politique des applications de chat.
2. Activez les politiques relatives aux applications de chat pour votre organisation.
3. Créez une politique pour les applications de chat.
4. Associez la politique des applications de chat à la racine, à l'unité d'organisation ou au compte de votre organisation.
5. Consultez la politique combinée des applications de chat efficaces qui s'applique à un compte.

Pour effectuer toutes ces étapes, vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

Autres informations

- Apprenez la syntaxe des politiques des applications de chat et consultez des exemples de politiques

## Syntaxe de politique des applications de chat et exemples

Cette rubrique décrit la syntaxe des politiques des applications de chat et fournit des exemples.

Syntaxe des politiques relatives aux applications de chat

Une politique d'application de chat est un fichier en texte brut structuré selon les règles du JSON. La syntaxe des politiques des applications de chat suit celle des types de politiques de gestion. Pour une présentation complète de cette syntaxe, consultez Fonctionnement de l'héritage des politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques du type de politique des applications de chat.

L'exemple suivant montre la syntaxe de base d'une politique d'applications de chat :

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled" // enabled | disabled
             },
             "workspaces": { // limit 255
                   "@@assign":[
                      "Slack-Workspace-Id"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private" // public | private
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role" // user_role | channel_role
                   ]
                }
             },
             "overrides":{ // limit 255
                "Slack-Workspace-Id":{
                   "supported_channel_types":{
                      "@@assign":[
                         "public" // public | private
                      ]
                   },
                   "supported_role_settings":{
                      "@@assign":[
                         "user_role" // user_role | channel_role
                      ]
                   }
                }
             }
          },
          "microsoft_teams":{
             "client":{
                "@@assign":"enabled"
             },
```

```
            "tenants":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "@@assign":[
                     "Microsoft-Teams-Team-Id"
                  ]
               }
            },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role" // user_role | channel_role
                  ]
               }
            },
            "overrides":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "Microsoft-Teams-Team-Id":{
                     "supported_role_settings":{
                        "@@assign":[
                           "user_role" // user_role | channel_role
                        ]
                     }
                  }
               }
            }
         },
         "chime":{
           "client":{
              "@@assign":"disabled" // enabled | disabled
           }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled" // enabled | disabled
         }
      }
   }
}
```

Cette politique relative aux applications de chat inclut les éléments suivants :

- Le nom de clé du champ `chatbot`. Les politiques des applications de chat commencent toujours par ce nom de clé fixe. Il s'agit de la première ligne de cet exemple de politique.
- En dessous `chatbot` se trouve un `platforms` bloc qui contient la configuration des différentes applications de chat prises en charge : Slack, Microsoft Teams et Amazon Chime.
  - Pour Slack, les champs suivants sont disponibles :
    - `"client"`:
      - `"enabled"`: le client Slack est activé. Les intégrations Slack sont autorisées.
      - `"disabled"`: Le client Slack est désactivé. Les intégrations Slack ne sont pas autorisées.
    - `"workspaces"`: liste séparée par des virgules des espaces de travail Slack autorisés. Dans cet exemple, les espaces de travail Slack autorisés sont *`Slack-Workspace-Id1`* et. *`Slack-Workspace-Id2`*
    - `"default"`: paramètres par défaut pour les espaces de travail Slack.
      - `"supported_channel_types"`:
        - `"public"`: les espaces de travail Slack concernés autorisent les chaînes publiques Slack par défaut.
        - `"private"`: les espaces de travail Slack concernés autorisent les chaînes privées Slack par défaut.
      - `supported_role_settings`:
        - `"user_role"`: les espaces de travail Slack concernés autorisent les rôles IAM au niveau utilisateur par défaut.
        - `"channel_role"`: les espaces de travail Slack concernés autorisent les rôles IAM au niveau du canal par défaut.
    - `"overrides"`: les paramètres de remplacement pour les espaces de travail Slack.
      - *`Slack-Workspace-Id2`*: liste séparée par des virgules des espaces de travail Slack auxquels le paramètre de dérogation s'applique. Dans cet exemple, l'espace de travail Slack est*`Slack-Workspace-Id2`*.
        - `"supported_channel_types"`:
          - `"public"`: remplacez le paramètre indiquant si les espaces de travail Slack concernés autorisent les chaînes Slack publiques.
          - `"private"`: remplacez le paramètre indiquant si les espaces de travail Slack concernés autorisent les chaînes Slack privées.
        - `supported_role_settings`:

        - `"user_role"`: remplacez le paramètre indiquant si les espaces de travail Slack concernés autorisent les rôles IAM au niveau utilisateur.
        - `"channel_role"`: remplacez le paramètre indiquant si les espaces de travail Slack concernés autorisent les rôles IAM au niveau de la chaîne.
- Pour Microsoft Teams, les champs suivants sont disponibles :
    - `"client"`:
        - `"enabled"`: Le client Microsoft Teams est activé. Les intégrations avec Microsoft Teams sont autorisées.
        - `"disabled"`: Le client Microsoft Teams est désactivé. Les intégrations Microsoft Teams ne sont pas autorisées.
    - `"tenants"`: liste séparée par des virgules des locataires Microsoft Teams autorisés. Dans cet exemple, le locataire autorisé est*`Microsoft-Teams-Tenant-Id`*.
        - *`Microsoft-Teams-Tenant-Id`*: liste séparée par des virgules des équipes autorisées au sein du locataire. Dans cet exemple, l'équipe autorisée est*`Microsoft-Teams-Team-Id`*.
    - `"default"`: paramètres par défaut pour les équipes au sein du locataire.
        - `supported_role_settings`:
            - `"user_role"`: les équipes concernées autorisent les rôles IAM au niveau utilisateur par défaut.
            - `"channel_role"`: Les équipes concernées autorisent les rôles IAM au niveau du canal par défaut.
    - `"overrides"`: les paramètres de remplacement pour les clients Microsoft Teams.
        - *`Microsoft-Teams-Tenant-Id`*: liste séparée par des virgules des locataires auxquels le paramètre de dérogation s'applique. Dans cet exemple, le locataire est*`Microsoft-Teams-Tenant-Id`*.
            - *`Microsoft-Teams-Team-Id`*: liste séparée par des virgules des équipes au sein du locataire. Dans cet exemple, l'équipe autorisée est*`Microsoft-Teams-Team-Id`*.
                - `supported_role_settings`:
                    - `"user_role"`: remplacez le paramètre indiquant si les équipes concernées autorisent les rôles IAM au niveau utilisateur.
                    - `"channel_role"`: remplacez le paramètre indiquant si les équipes concernées autorisent les rôles IAM au niveau du canal.
- Pour Amazon Chime, les champs suivants sont disponibles :

  - `"client"`:
    - `"enabled"`: Le client Amazon Chime est activé. Les intégrations Amazon Chime sont autorisées.
    - `"disabled"`: Le client Amazon Chime est désactivé. Les intégrations Amazon Chime ne sont pas autorisées.
- En dessous`chatbot`, il existe un `default` bloc qui désactive Amazon Q Developer dans les applications de chat de l'organisation, à moins qu'il ne soit remplacé à un niveau inférieur. Cette valeur par défaut désactive également toute nouvelle application de chat prise en charge par Amazon Q Developer dans les applications de chat. Par exemple, si Amazon Q Developer prend en charge une nouvelle application de chat dans les applications de chat, cette nouvelle application de chat par défaut est également désactivée.

> **Note**
>
> Pour plus d'informations sur les rôles IAM au niveau du canal et les rôles IAM au niveau utilisateur, consultez Comprendre les autorisations d'Amazon Q Developer dans les applications de chat dans le Guide de l'administrateur d'Amazon Q Developer dans les applications de chat.

Exemples de politiques relatives aux applications de chat

Les exemples de politiques qui suivent sont fournis à titre informatif uniquement.

Exemple 1 : autoriser uniquement les chaînes Slack privées dans un espace de travail spécifique, désactiver Microsoft Teams, tous les modes d'authentification sont pris en charge

La politique suivante est axée sur le contrôle des configurations autorisées pour les intégrations de chatbot Slack et Microsoft Teams.

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
```

```
            "@@assign": [
               "Slack-Workspace-Id"
            ]
         },
         "default": {
            "supported_channel_types": {
               "@@assign": [
                  "private"
               ]
            },
            "supported_role_settings": {
               "@@assign": [
                  "channel_role",
                  "user_role"
               ]
            }
         }
      },
      "microsoft_teams": {
         "client": {
            "@@assign": "disabled"
         }
      },
      "chime":{
         "client":{
            "@@assign":"disabled"
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
   }
}
```

Pour Slack

- Le client Slack est activé.
- Seul l'espace de travail Slack spécifique *Slack-Workspace-Id* est autorisé.

- Les paramètres par défaut autorisent uniquement les chaînes privées Slack, les rôles IAM au niveau des canaux et les rôles IAM au niveau des utilisateurs.

Pour Microsoft Team

- Le client Microsoft Teams est désactivé.

Pour Amazon Chime

- Le client Amazon Chime est désactivé.

Détails supplémentaires

- Le `default` bloc situé en bas définit la désactivation du client, ce qui désactive Amazon Q Developer dans les applications de chat de l'organisation, sauf si cela est annulé à un niveau inférieur. Cette valeur par défaut désactive également toute nouvelle application de chat prise en charge par Amazon Q Developer dans les applications de chat. Par exemple, si Amazon Q Developer prend en charge une nouvelle application de chat dans les applications de chat, cette nouvelle application de chat par défaut est également désactivée.

Exemple 2 : autoriser uniquement les intégrations Slack avec des rôles IAM de niveau utilisateur

La politique suivante adopte une approche plus permissive à l'égard de Slack, en autorisant tous les espaces de travail Slack mais en limitant le mode d'authentification aux seuls rôles IAM au niveau utilisateur.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client":{
               "@@assign":"enabled"
            },
            "workspaces":
               {
                  "@@assign":[
                     "*"
                  ]
               },
```

```
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
   }
}
```

Pour Slack

- Le client Slack est activé.
- Aucun espace de travail Slack spécifique n'est défini à l'aide du caractère générique"*". Tous les espaces de travail sont donc autorisés.
- Les paramètres par défaut autorisent uniquement les rôles IAM au niveau utilisateur.

Pour Microsoft Team

- Le client Microsoft Teams est désactivé.

Pour Amazon Chime

- Le client Amazon Chime est désactivé.

Détails supplémentaires

- Le `default` bloc situé en bas définit la désactivation du client, ce qui désactive Amazon Q Developer dans les applications de chat de l'organisation, sauf si cela est annulé à un niveau inférieur. Cette valeur par défaut désactive également toute nouvelle application de chat prise en charge par Amazon Q Developer dans les applications de chat. Par exemple, si Amazon Q Developer prend en charge une nouvelle application de chat dans les applications de chat, cette nouvelle application de chat par défaut est également désactivée.

Exemple 3 : autoriser uniquement les intégrations Microsoft Teams dans un locataire spécifique

L'exemple de politique suivant verrouille l'organisation pour autoriser uniquement les intégrations de chatbot Microsoft Teams au sein du locataire spécifié, tout en bloquant complètement les intégrations Slack.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client": {
               "@@assign": "disabled"
            },
         },
         "microsoft_teams":{
            "client": {
               "@@assign": "enabled"
            },
            "tenants":{
               "Microsoft-Teams-Tenant-Id":{
                  "@@assign":[
                     "*"
                  ]
               }
            }
         },
         "chime": {
            "client":{
               "@@assign": "disabled"
            }
         }
      }
   }
```

```
}
```

Pour Slack

- Le client Slack est désactivé.

Pour Microsoft Team

- Seul un locataire spécifique *`Microsoft-Teams-Tenant-Id`* est autorisé, en utilisant le joker `"*"` pour autoriser toutes les équipes au sein de ce locataire.

Pour Amazon Chime

- Le client Amazon Chime est désactivé.

Détails supplémentaires

- Le `default` bloc situé en bas définit la désactivation du client, ce qui désactive Amazon Q Developer dans les applications de chat de l'organisation, sauf si cela est annulé à un niveau inférieur. Cette valeur par défaut désactive également toute nouvelle application de chat prise en charge par Amazon Q Developer dans les applications de chat. Par exemple, si Amazon Q Developer prend en charge une nouvelle application de chat dans les applications de chat, cette nouvelle application de chat par défaut est également désactivée.

Exemple 4 : autorise un développeur Amazon Q restreint dans les applications de chat à accéder aux espaces de travail Slack et à un client Microsoft Teams

La politique suivante autorise un accès restreint aux développeurs Amazon Q dans les applications de chat pour certains espaces de travail Slack et pour un client Microsoft Teams.

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled"
             },
             "workspaces": {
                   "@@assign":[
```

```
                "Slack-Workspace-Id1",
                "Slack-Workspace-Id2"
            ]
        },
        "default":{
            "supported_channel_types":{
                "@@assign":[
                    "private"
                ]
            },
            "supported_role_settings":{
                "@@assign":[
                    "user_role"
                ]
            }
        },
        "overrides":{
            "Slack-Workspace-Id2":{
                "supported_channel_types":{
                    "@@assign":[
                        "public",
                        "private"
                    ]
                },
                "supported_role_settings":{
                    "@@assign":[
                        "channel_role",
                        "user_role"
                    ]
                }
            }
        }
    },
    "microsoft_teams":{
        "client":{
            "@@assign":"enabled"
        },
        "tenants":{
            "Microsoft-Teams-Tenant-Id":{
                "@@assign":[
                    "Microsoft-Teams-Team-Id"
                ]
            }
        },
```

```
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            },
            "overrides":{
               "Microsoft-Teams-Tenant-Id":{
                  "Microsoft-Teams-Team-Id":{
                     "supported_role_settings":{
                        "@@assign":[
                           "channel_role",
                           "user_role"
                        ]
                     }
                  }
               }
            }
         },
         "default":{
            "client":{
               "@@assign":"disabled"
            }
         }
      }
   }
```

Pour Slack

- Le client Slack est activé.
- Les espaces de travail Slack autorisés sont *Slack-Workspace-Id1* et. *Slack-Workspace-Id2*
- Les paramètres par défaut de Slack sont d'autoriser uniquement les chaînes privées et les rôles IAM au niveau utilisateur.
- Il existe une dérogation à l'espace de travail *Slack-Workspace-Id2* qui autorise à la fois les chaînes publiques et privées ainsi que les rôles IAM au niveau du canal et les rôles IAM au niveau de l'utilisateur.

Pour Microsoft Team

- Microsoft Teams est activé.
- Les locataires Teams autorisés font *`Microsoft-Teams-Tenant-Id`* partie de l'équipe*`Microsoft-Teams-Team-Id`*.
- Les paramètres par défaut autorisent uniquement les rôles IAM au niveau utilisateur.
- Il existe une dérogation pour le locataire *`Microsoft-Teams-Tenant-Id`* qui autorise à la fois les rôles IAM au niveau du canal et les rôles IAM au niveau de l'utilisateur pour l'équipe. *`Microsoft-Teams-Team-Id`*

Détails supplémentaires

- Le `default` bloc situé en bas définit la désactivation du client, ce qui désactive Amazon Q Developer dans les applications de chat de l'organisation, sauf si cela est annulé à un niveau inférieur. Cela signifie qu'Amazon Chime est désactivé dans cet exemple. Cette valeur par défaut désactive également toute nouvelle application de chat prise en charge par Amazon Q Developer dans les applications de chat. Par exemple, si Amazon Q Developer prend en charge une nouvelle application de chat dans les applications de chat, cette nouvelle application de chat par défaut est également désactivée.

## Politiques de désactivation des services IA

AWS Les services d'intelligence artificielle peuvent utiliser et stocker du contenu client pour améliorer le service, par exemple pour résoudre des problèmes opérationnels, évaluer les performances du service, déboguer ou former des modèles. À cette fin, nous pouvons stocker ce contenu à l' Région AWS extérieur de l' Région AWS endroit où vous utilisez le service. Vous pouvez refuser l'utilisation de votre contenu pour améliorer le service en utilisant la politique de AWS Organizations désinscription.

Vous pouvez créer des politiques de désinscription pour un service d'IA individuel ou pour tous les services pris en charge par des politiques de désinscription des services d'IA. Vous pouvez également consulter la politique effective applicable à chaque compte pour connaître les effets de vos choix de paramètres.

Pour des informations plus détaillées, consultez la section Services de AWS Machine Learning et d'intelligence artificielle dans les AWS Conditions d'utilisation. Pour obtenir la liste des services pris en charge par les politiques de désinscription des services d'IA, consultez la section Liste des services d'IA pris en charge.

Rubriques



## Considérations relatives à l'utilisation des politiques de désabonnement des services d'IA

La désinscription supprime tout le contenu historique associé

Lorsque vous refusez l'utilisation du contenu par un service d' AWS intelligence artificielle, ce service supprime tout le contenu historique associé qui a été partagé AWS avant que vous ne définissiez l'option. Cette suppression est limitée au contenu stocké qui n'est pas nécessaire pour fournir les fonctions du service.

Par exemple, lorsque vous utilisez un service alors que vous êtes inscrit, ce service peut stocker des copies de votre contenu afin d'améliorer le service. Lorsque vous vous désinscrivez, toutes les copies stockées par le service à cette fin sont supprimées, mais le contenu utilisé pour vous fournir le service n'est pas supprimé.

## Mise en route avec les politiques de désactivation des services IA

Suivez ces étapes pour commencer à utiliser les politiques de désactivation des services d'intelligence artificielle (IA).

1. Découvrez les autorisations dont vous devez disposer pour effectuer des tâches de politique de sauvegarde
2. Activez les politiques de désactivation des services IA pour votre organisation.
3. Créez une politique de désactivation des services IA.
4. Attachez la politique de désactivation des services IA à la racine, une UO ou un compte de votre organisation.
5. Affichez la politique combinée de désactivation des services IA qui s'applique à un compte.

Pour toutes ces étapes, vous devez vous connecter en tant qu'utilisateur Gestion des identités et des accès AWS (IAM), assumer un rôle IAM ou vous connecter en tant qu'utilisateur root (ce n'est pas recommandé) dans le compte de gestion de l'organisation.

Autres informations

- Découvrir la syntaxe de politique pour les politiques de désactivation des services IA et consulter des exemples de politiques

## Se désinscrire de tous les services d' AWS IA pris en charge

Dans cette rubrique :

- Vous pouvez vous désinscrire en sélectionnant un seul bouton dans la AWS Organizations console.
- Vous pouvez vous désinscrire en joignant l'exemple de politique fourni à l'aide du AWS CLI & AWS SDKs.
- Vous pouvez consulter la liste des services Services AWS pris en charge par la politique de désinscription des services d'IA.

### Se désinscrire de tous les services d'IA pris en charge

Vous pouvez empêcher votre organisation que son contenu soit utilisé à des fins d'amélioration des services en créant et en joignant une politique de désinscription des services d'intelligence artificielle. Cette politique s'applique à tous les services d' AWS IA pris en charge actuels et futurs. Les comptes des membres ne peuvent pas mettre à jour la politique.

AWS Management Console

Pour vous désinscrire de tous les services d'IA

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques de désinscription des services d'intelligence artificielle, choisissez Se désinscrire de tous les services.
3. Sur la page de confirmation de désinscription de tous les services, choisissez Se désinscrire de tous les services.

AWS CLI & AWS SDKs

Pour vous désinscrire de tous les services d'IA

1. Copiez « Exemple 1 : désactivation de tous les services d'IA pour tous les comptes de l'organisation » dans les exemples de désactivation des services d'IA.
2. Suivez les instructions de la section Déconnexion et désactivation des services d'intelligence artificielle.

> **Note**
>
> Des étapes supplémentaires sont nécessaires pour vous désinscrire d'Amazon Monitron. Pour plus d'informations, consultez Conditions de service AWS.

Liste des services pris en charge par la politique de désinscription des services d'IA

Voici une liste des services Services AWS pris en charge par la politique de désinscription des services d'intelligence artificielle :

- Opération d'IA Amazon
- Analyse vocale du SDK Amazon Chime
- Amazon CloudWatch
- Amazon CodeGuru Profiler
- Amazon CodeWhisperer (fait désormais partie d'Amazon Q Developer)
- Amazon Comprehend
- Amazon Connect
- Optimisation d'Amazon Connect
- Lentilles de contact Amazon Connect
- AWS Service de Migration de Base de Données
- Amazon DataZone (et Amazon SageMaker Data Agent)
- Agent AWS DevOps
- Résolution des entités AWS
- Amazon Fraud Detector

- AWS Glue
- Amazon GuardDuty
- Amazon Lex
- Amazon Polly
- Amazon Q
- Amazon Quick
- Amazon Rekognition
- Amazon Security Lake
- AWS Supply Chain
- Amazon Textract
- Amazon Transcribe
- AWS Transform
- Amazon Translate
- Amazon WorkSpaces
- AWS Security Hub

## Syntaxe des politiques de désactivation des services IA et exemples

Cette rubrique décrit la syntaxe des politiques de désactivation des services d'intelligence artificielle (IA) et fournit des exemples.

### Syntaxe des politiques de désactivation des services IA

Une politique de désactivation des services IA est un fichier texte brut qui est structuré conformément aux règles de JSON. La syntaxe des politiques de désactivation des services IA suit celle des types de politique de gestion. Pour une présentation complète de cette syntaxe, consultez Fonctionnement de l'héritage des politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques du type de politique de désactivation des services IA.

> **Important**
>
> L'usage des majuscules dans les valeurs décrites dans cette section est importante. Entrez les valeurs avec des lettres majuscules et minuscules, comme indiqué dans cette rubrique. Les politiques ne fonctionnent pas si vous faites un usage inattendu des majuscules.

La politique suivante illustre la syntaxe élémentaire des politiques de désactivation des services IA. Si cet exemple était attaché directement à un compte, un service serait désactivé pour ce compte et un autre serait activé. D'autres services peuvent être activés ou désactivés par des politiques héritées de niveaux supérieurs (politiques d'UO ou de racine).

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Imaginez l'exemple de politique suivant attaché à la racine de l'organisation. Il définit que, par défaut tous les services IA sont désactivés pour l'organisation. Cela inclut automatiquement tous les services IA qui ne sont pas autrement explicitement exemptés, y compris tous les services IA que AWS pourrait déployer à l'avenir. Vous pouvez associer des politiques relatives aux enfants aux comptes OUs ou directement à ceux-ci afin de remplacer ce paramètre pour n'importe quel service d'intelligence artificielle, à l'exception d'Amazon Comprehend. La deuxième entrée de l'exemple suivant utilise `@@operators_allowed_for_child_policies` défini à `none` pour empêcher ce remplacement. La troisième entrée de l'exemple fait une exemption à l'échelle de l'organisation pour Amazon Rekognition. Il active ce service pour l'ensemble de l'organisation, mais la politique permet aux politiques enfants de supplanter ce réglage le cas échéant.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La syntaxe d'une politique de désactivation des services IA inclut les éléments suivants :

- L'élément `services`. Une politique de désactivation des services IA est identifiée par ce nom fixe comme l'élément contenant JSON le plus à l'extérieur.

  Une politique de désactivation des services IA peut comporter une ou plusieurs déclarations sous l'élément `services`. Chaque instruction contient les éléments suivants :

  - Clé de nom de service qui identifie un service d' AWS IA. Les noms de clé suivants sont valides pour ce champ :
    - **`default`** : représente tous les services IA actuellement disponibles et inclut implicitement et automatiquement tous les services IA qui pourraient être ajoutés à l'avenir.
    - `aiops`
    - `aidevops`
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`
    - `connect`
    - `connectamd`
    - `connectoptimization`
    - `contactlens`
    - `datazone`

- `dms`
- `entityresolution`
- `frauddetector`
- `glue`
- `guardduty`
- `lex`
- `polly`
- `q`
- `quicksightq`
- `rekognition`
- `securitylake`
- `textract`
- `transcribe`
- `transform`
- `translate`
- `workspaces`
- `securityhub`

Chaque instruction de politique identifiée par une clé de nom de service peut contenir les éléments suivants :

- La clé `opt_out_policy`. Cette clé doit être présente. C'est la seule clé que vous pouvez placer sous une clé de nom de service.

  La clé `opt_out_policy` peut contenir uniquement l'opérateur `@@assign` avec une des valeurs suivantes :

  - `optOut` : vous choisissez de désactiver l'utilisation du contenu pour le service IA spécifié.
  - `optIn` : vous choisissez d'activer l'utilisation du contenu pour le service IA spécifié.

  > **Remarques**
  >
  > - Vous ne pouvez pas utiliser les opérateurs d'héritage `@@append` et `@@remove` dans les politiques de désactivation des services IA.

- Vous ne pouvez pas utiliser l'opérateur `@@enforced_for` dans les politiques de désactivation des services IA.

- À n'importe quel niveau, vous pouvez spécifier l'opérateur `@@operators_allowed_for_child_policies` pour contrôler ce que les politiques enfants peuvent faire pour remplacer les paramètres imposés par les politiques parentes. Vous pouvez spécifier l'une des valeurs suivantes :
  - `@@assign` : les politiques enfants de cette politique peuvent utiliser l'opérateur `@@assign` pour remplacer la valeur héritée par une valeur différente.
  - `@@none` : les politiques enfants de cette politique ne peuvent pas modifier la valeur.

  Le comportement de `@@operators_allowed_for_child_policies` dépend de l'endroit où vous le placez. Vous pouvez utiliser les emplacements suivants :
  - Sous la clé `services` : détermine si une politique enfant peut compléter ou modifier la liste des services de la politique effective.
  - Sous la clé d'un service IA spécifique ou la clé `default` : détermine si une politique enfant peut compléter ou modifier la liste des clés sous cette entrée spécifique.
  - Sous la clé `opt_out_policies` pour un service spécifique : détermine si une politique enfant peut modifier uniquement le paramètre de ce service spécifique.

Exemples de politique de désactivation des services IA

Les exemples de politiques qui suivent sont fournis à titre informatif uniquement.

Exemple 1 : Désactiver tous les services IA pour tous les comptes de l'organisation

L'exemple suivant illustre une politique que vous pourriez attacher à la racine de votre organisation pour désactiver les services IA pour les comptes de votre organisation.

> **Tip**
>
> Si vous copiez l'exemple suivant à l'aide du bouton Copier dans le coin supérieur droit de l'exemple, la copie n'inclut pas les numéros de ligne. Elle est prête à être collée.

```
| {
|     "services": {
```

```
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] : Le `"@@operators_allowed_for_child_policies": ["@@none"]` qui est sous `services` empêche toute politique enfant d'ajouter de nouvelles sections pour des services individuels autres que la section `default` qui est déjà là. `Default` est l'espace réservé qui représente « tous les services IA ».
- [2] : Le `"@@operators_allowed_for_child_policies": ["@@none"]` qui est sous `default` empêche toute politique enfant d'ajouter de nouvelles sections autres que la section `opt_out_policy` qui est déjà là.
- [3] : Le `"@@operators_allowed_for_child_policies": ["@@none"]` qui est sous `opt_out_policy` empêche les politiques enfants de changer la valeur du paramètre `optOut` ou d'ajouter des paramètres supplémentaires.

Exemple 2 : Définir un paramètre par défaut de l'organisation pour tous les services, mais autoriser les politiques enfants à remplacer le paramètre pour des services individuels

L'exemple de politique suivant définit une valeur par défaut à l'échelle de l'organisation pour tous les services IA. La valeur pour `default` empêche une politique enfant de modifier la valeur `optOut` pour le service `default`, l'espace réservé pour tous les services IA. Si cette politique est appliquée en tant que politique parente en l'attachant à la racine ou à une unité d'organisation, les politiques enfants peuvent toujours modifier le paramètre de désactivation pour chaque service, comme indiqué dans la deuxième politique.

- Puisqu'il n'y a pas d'opérateur `"@@operators_allowed_for_child_policies": ["@@none"]` sous la clé `services`, les politiques enfants peuvent ajouter de nouvelles sections pour des services individuels.
- Le `"@@operators_allowed_for_child_policies": ["@@none"]` qui est sous `default` empêche toute politique enfant d'ajouter de nouvelles sections autres que la section `opt_out_policy` qui est déjà là.

- Le `"@@operators_allowed_for_child_policies": ["@@none"]` qui est sous `opt_out_policy` empêche les politiques enfants de changer la valeur du paramètre `optOut` ou d'ajouter des paramètres supplémentaires.

Politique parente de désactivation des services d'IA de l'utilisateur root de l'organisation

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

L'exemple de politique suivant suppose que l'exemple de politique précédent est attaché à la racine de l'organisation ou à une unité d'organisation parente et que vous attachez cet exemple à un compte affecté par la politique parent. Il remplace le paramètre de désactivation par défaut et active explicitement uniquement le service Amazon Lex.

Politique enfant de désactivation des services IA

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La politique effective qui en résulte Compte AWS est que le compte opte uniquement pour Amazon Lex et se désactive de tous les autres services d' AWS IA en raison du paramètre de `default` désinscription hérité de la politique parent.

Exemple 3 : Définir une politique de désactivation des services IA à l'échelle de l'organisation pour un seul service

L'exemple suivant illustre une politique de désactivation des services IA qui définit un paramètre `optOut` pour un seul service IA. Si cette politique est attachée à la racine de l'organisation, elle empêche toute politique enfant de remplacer le paramètre `optOut` pour ce service précis. Les autres services ne sont pas concernés par cette politique, mais peuvent être affectés par les politiques relatives aux enfants dans d'autres comptes OUs ou comptes.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

## Politiques du Security Hub

AWS Security Hub les politiques fournissent aux équipes de sécurité une approche centralisée pour gérer les configurations de sécurité au sein de leurs équipes AWS Organizations. En tirant parti de ces politiques, vous pouvez établir et maintenir des contrôles de sécurité cohérents grâce à un mécanisme de configuration central. Cette intégration vous permet de combler les lacunes en matière de couverture de sécurité en créant des politiques conformes aux exigences de sécurité de votre entreprise et en les appliquant de manière centralisée à tous les comptes et unités organisationnelles (OUs).

Les politiques du Security Hub sont entièrement intégrées AWS Organizations, ce qui permet aux comptes de gestion ou aux administrateurs délégués de définir et d'appliquer les configurations de sécurité. Lorsque des comptes rejoignent votre organisation, ils héritent automatiquement des politiques applicables en fonction de leur emplacement dans la hiérarchie organisationnelle. Cela garantit que vos normes de sécurité sont appliquées de manière cohérente au fur et à mesure que votre organisation se développe. Les politiques respectent les structures organisationnelles existantes et offrent de la flexibilité dans la manière dont les configurations de sécurité sont distribuées, tout en maintenant le contrôle centralisé des paramètres de sécurité critiques.

## Caractéristiques et avantages clés

Les politiques du Security Hub fournissent un ensemble complet de fonctionnalités qui vous aident à gérer et à appliquer les configurations de sécurité au sein de votre AWS entreprise. Ces fonctionnalités rationalisent la gestion de la sécurité tout en garantissant un contrôle constant de votre environnement multi-comptes.

- Activez Security Hub de manière centralisée sur tous les comptes et régions de votre organisation
- Créez des politiques de sécurité qui définissent votre configuration de sécurité pour tous les comptes et OUs
- Appliquez automatiquement des configurations de sécurité aux nouveaux comptes lorsqu'ils rejoignent votre organisation
- Garantissez des paramètres de sécurité cohérents au sein de votre entreprise
- Empêcher les comptes membres de modifier les configurations de sécurité au niveau de l'organisation

## Quelles sont les politiques de Security Hub ?

Les politiques du Security Hub sont des AWS Organizations politiques qui fournissent un contrôle centralisé des configurations de sécurité des comptes de votre entreprise. Ces politiques fonctionnent parfaitement pour vous aider AWS Organizations à établir et à maintenir des normes de sécurité cohérentes dans l'ensemble de votre environnement multi-comptes.

Lorsque vous implémentez les politiques du Security Hub, vous pouvez définir des configurations de sécurité spécifiques qui se propagent automatiquement au sein de votre organisation. Cela garantit que tous les comptes, y compris les comptes nouvellement créés, sont conformes aux exigences de sécurité et aux meilleures pratiques de votre organisation.

Ces politiques vous aident également à maintenir la conformité en appliquant des contrôles de sécurité cohérents et en empêchant les comptes individuels de modifier les paramètres de sécurité au niveau de l'organisation. Cette approche centralisée réduit considérablement les frais administratifs liés à la gestion des configurations de sécurité dans des AWS environnements complexes et de grande envergure.

## Comment fonctionnent les politiques du Security Hub

Lorsque vous associez une politique Security Hub à votre organisation ou unité organisationnelle, elle est AWS Organizations automatiquement évaluée et appliquée en fonction du périmètre que vous

définissez. Le processus d'application des politiques suit des règles spécifiques de résolution des conflits :

Lorsque des régions apparaissent à la fois dans les listes d'activation et de désactivation, la configuration de désactivation est prioritaire. Par exemple, si une région est répertoriée dans les configurations d'activation et de désactivation, Security Hub sera désactivé dans cette région.

Lorsque l'activation `ALL_SUPPORTED` est spécifiée, Security Hub est activé dans toutes les régions actuelles et futures, sauf s'il est explicitement désactivé. Cela vous permet de maintenir une couverture de sécurité complète à mesure que vous vous AWS étendez dans de nouvelles régions.

Les politiques relatives aux enfants peuvent modifier les paramètres des politiques parentales à l'aide d'opérateurs d'héritage, ce qui permet un contrôle granulaire à différents niveaux organisationnels. Cette approche hiérarchique garantit que les unités organisationnelles spécifiques peuvent personnaliser leurs paramètres de sécurité tout en maintenant les contrôles de base.

## Terminologie

Cette rubrique utilise les termes suivants pour aborder les politiques du Security Hub.

Terminologie des politiques du Security Hub

| Durée | Définition |
|---|---|
| Stratégie effective | Politique finale qui s'applique à un compte après avoir combiné toutes les politiques héritées. |
| Héritage de politique | Processus par lequel les comptes héritent des politiques des unités organisationnelles parentes. |
| Administrateur délégué | Un compte désigné pour gérer les politiques du Security Hub au nom de l'organisation. |
| Rôle lié à un service | Rôle IAM qui permet à Security Hub d'interagir avec d'autres AWS servi ces. |

## Cas d'utilisation des politiques du Security Hub

Les politiques du Security Hub répondent aux défis courants de gestion de la sécurité dans les environnements multi-comptes. Les cas d'utilisation suivants montrent comment les entreprises mettent généralement en œuvre ces politiques pour améliorer leur posture de sécurité.

Exemple de cas d'utilisation : exigences de conformité régionales

Une multinationale a besoin de différentes configurations de Security Hub pour différentes régions géographiques. Ils créent une politique parent qui active Security Hub dans toutes les régions en utilisant`ALL_SUPPORTED`, puis utilisent des politiques relatives aux enfants pour désactiver des régions spécifiques où différents contrôles de sécurité sont requis. Cela leur permet de respecter les réglementations régionales tout en garantissant une couverture de sécurité complète.

Exemple de cas d'utilisation : normes de sécurité pour les équipes de développement

Une organisation de développement de logiciels met en œuvre les politiques du Security Hub qui permettent de surveiller les régions de production tout en préservant la gestion des régions de développement. Ils utilisent des listes de régions explicites dans leurs politiques plutôt que `ALL_SUPPORTED` pour maintenir un contrôle précis sur la couverture de surveillance de la sécurité. Cette approche leur permet d'appliquer des contrôles de sécurité plus stricts dans les environnements de production tout en préservant la flexibilité dans les domaines de développement.

## Héritage et application des politiques

Comprendre comment les politiques sont héritées et appliquées est essentiel pour une gestion efficace de la sécurité au sein de votre entreprise. Le modèle d'héritage suit la AWS Organizations hiérarchie, garantissant ainsi une application prévisible et cohérente des politiques.

- Les politiques associées au niveau racine s'appliquent à tous les comptes
- Les comptes héritent des politiques de leurs unités organisationnelles mères
- Plusieurs politiques peuvent s'appliquer à un seul compte
- Les politiques plus spécifiques (plus proches du compte dans la hiérarchie) ont priorité

## Validation de politique

Lors de la création des politiques Security Hub, les validations suivantes ont lieu :

- Les noms de région doivent être des identifiants de AWS région valides

- Les régions doivent être prises en charge par Security Hub
- La structure des politiques doit suivre les règles AWS Organizations de syntaxe des politiques
- Les deux `enable_in_regions` et `disable_in_regions` les listes doivent être présentes, bien qu'elles puissent être vides

## Considérations régionales et régions prises en charge

Les politiques du Security Hub s'appliquent à plusieurs régions, ce qui nécessite un examen attentif de vos exigences de sécurité globales. Comprendre le comportement régional vous aide à mettre en œuvre des contrôles de sécurité efficaces sur l'ensemble du territoire mondial de votre entreprise.

- L'application des politiques se fait indépendamment dans chaque région
- Vous pouvez spécifier les régions à inclure ou à exclure dans vos politiques
- Les nouvelles régions sont automatiquement incluses lorsque vous utilisez l'`ALL_SUPPORTED`option
- Les politiques s'appliquent uniquement aux régions où Security Hub est disponible

## Étapes suivantes

Pour commencer à utiliser les politiques du Security Hub, procédez comme suit :

1. Consultez les conditions préalables dans les politiques de Getting Started with Security Hub
2. Planifiez votre stratégie politique à l'aide de notre guide des meilleures pratiques
3. En savoir plus sur la syntaxe des politiques et consulter des exemples de politiques

## Commencer à utiliser les politiques du Security Hub

Avant de configurer les politiques de Security Hub, assurez-vous de bien comprendre les prérequis et les exigences de mise en œuvre. Cette rubrique vous guide tout au long du processus de configuration et de gestion de ces politiques dans votre organisation.

Avant de commencer

Passez en revue les exigences suivantes avant de mettre en œuvre les politiques du Security Hub :

- Votre compte doit faire partie d'une AWS Organizations organisation
- Vous devez être connecté en tant que :

  - Le compte de gestion de l'organisation
  - Un compte d'administrateur délégué autorisé à gérer les politiques du Security Hub
- Vous devez activer l'accès sécurisé pour Security Hub dans votre organisation
- Vous devez activer le type de politique Security Hub à la racine de votre organisation

Vérifiez également que :

- Security Hub est pris en charge dans les régions où vous souhaitez appliquer des politiques
- Le rôle `AWSServiceRoleForSecurityHubV2` lié au service est configuré dans votre compte de gestion. Pour vérifier que ce rôle existe, exécutez`aws iam get-role --role-name AWSServiceRoleForSecurityHubV2`. Si vous devez créer ce rôle, vous pouvez exécuter ce rôle `aws securityhub enable-security-hub-v2` dans n'importe quelle région à partir de votre compte de gestion ou le créer directement en exécutant`aws iam create-service-linked-role --aws-service-name securityhubv2.amazonaws.com`.

Étapes d'implémentation

Pour mettre en œuvre efficacement les politiques du Security Hub, suivez ces étapes dans l'ordre. Chaque étape garantit une configuration correcte et permet d'éviter les problèmes courants lors de l'installation. Le compte de gestion ou l'administrateur délégué peut effectuer ces étapes via la AWS Organizations console, l'interface de ligne de AWS commande (AWS CLI) ou AWS SDKs.

1. Activez un accès sécurisé pour Security Hub.
2. Activez les politiques du Security Hub pour votre organisation.
3. Créez une politique Security Hub.
4. Associez la politique Security Hub à la racine, à l'unité d'organisation ou au compte de votre organisation.
5. Consultez la politique Security Hub combinée et efficace qui s'applique à un compte.

Pour toutes ces étapes, vous devez vous connecter en tant qu'utilisateur Gestion des identités et des accès AWS (IAM), assumer un rôle IAM ou vous connecter en tant qu'utilisateur root (ce n'est pas recommandé) dans le compte de gestion de l'organisation.

Autres informations

- Apprenez la syntaxe des politiques du Security Hub et consultez des exemples de politiques

## Bonnes pratiques relatives à l'utilisation des politiques du Security Hub

Lorsque vous mettez en œuvre les politiques du Security Hub au sein de votre organisation, le respect des meilleures pratiques établies permet de garantir le déploiement et la maintenance réussis de vos configurations de sécurité. Ces directives abordent spécifiquement les aspects uniques de la gestion et de l'application des politiques du Security Hub au sein de ce dernier AWS Organizations.

### Principes de conception des politiques

Avant de créer des politiques Security Hub, définissez des principes clairs pour votre structure de politique. Simplifiez les politiques et évitez les règles complexes à attributs croisés ou imbriquées qui compliquent la détermination du résultat final. Commencez par des politiques générales au niveau de la racine de l'organisation et affinez-les au besoin par le biais de politiques relatives aux enfants.

Envisagez d'utiliser des listes de régions vides de manière stratégique. Vous pouvez laisser ce `enable_in_regions` champ vide lorsque vous devez uniquement désactiver Security Hub dans des régions spécifiques, ou le laisser `disable_in_regions` vide pour éviter que les régions ne soient gérées par des règles. Cette flexibilité vous permet de garder un contrôle précis sur votre couverture de surveillance de sécurité.

### Stratégies de gestion des régions

Lorsque vous gérez des régions par le biais des politiques du Security Hub, tenez compte de ces approches éprouvées. À utiliser `ALL_SUPPORTED` lorsque vous souhaitez inclure automatiquement les futures régions dans votre couverture de sécurité. Pour un contrôle plus précis, listez explicitement les régions plutôt que de vous fier à celles-ci`ALL_SUPPORTED`, en particulier lorsque différentes régions nécessitent des configurations de sécurité différentes.

Documentez les exigences spécifiques à votre région, en particulier pour :

- Régions soumises à des obligations de conformité qui nécessitent des configurations spécifiques
- Différences entre environnement de développement et environnement de production
- Régions optionnelles soumises à des considérations spéciales
- Régions dans lesquelles Security Hub doit rester désactivé

### Politique de planification successorale

Planifiez soigneusement la structure d'héritage de vos polices afin de maintenir un contrôle de sécurité efficace tout en garantissant la flexibilité nécessaire. Documentez quelles unités

organisationnelles peuvent modifier les politiques héritées et quelles modifications sont autorisées. Envisagez de restreindre les opérateurs d'héritage (@ @assign, @ @append, @ @remove) au niveau des parents lorsque vous devez appliquer des contrôles de sécurité stricts.

Surveillance et validation

Mettez en œuvre des pratiques de surveillance régulières pour garantir l'efficacité de vos politiques. Passez régulièrement en revue les pièces jointes aux politiques, en particulier après des changements organisationnels. Vérifiez que les configurations régionales correspondent à la couverture de sécurité prévue, en particulier lors de l'utilisation `ALL_SUPPORTED` ou de la gestion de plusieurs listes de régions.

Stratégies de dépannage

Lors de la résolution des problèmes liés aux politiques du Security Hub, concentrez-vous d'abord sur la priorité et l'héritage des politiques. N'oubliez pas que les configurations de désactivation ont priorité sur les configurations d'activation lorsque les régions apparaissent dans les deux listes. Consultez les chaînes d'héritage des politiques pour comprendre comment les politiques relatives aux parents et aux enfants se combinent pour créer une politique efficace pour chaque compte.

## Syntaxe et exemples de politiques du Security Hub

Les politiques de Security Hub suivent une syntaxe JSON standardisée qui définit la manière dont Security Hub est activé et configuré au sein de votre organisation. La compréhension de la structure des politiques vous aide à créer des politiques efficaces répondant à vos exigences de sécurité.

Considérations

Avant de créer des politiques Security Hub, comprenez les points essentiels suivants concernant la syntaxe des politiques :

- Les deux `enable_in_regions` `disable_in_regions` listes sont obligatoires dans la politique, bien qu'elles puissent être vides
- Lors du traitement de politiques efficacesdisable_in_regions, a priorité sur `enable_in_regions`
- Les politiques relatives aux enfants peuvent modifier les politiques parentales à l'aide d'opérateurs d'héritage, sauf si elles sont explicitement limitées
- La `ALL_SUPPORTED` désignation inclut à la fois les régions actuelles et futures
- Les noms de région doivent être valides et disponibles dans Security Hub

### Structure politique de base

Une politique Security Hub utilise cette structure de base :

```
{
  "securityhub": {
    "enable_in_regions": {
      "@@append": ["ALL_SUPPORTED"],
      "@@operators_allowed_for_child_policies": ["@@all"]
    },
    "disable_in_regions": {
      "@@append": [],
      "@@operators_allowed_for_child_policies": ["@@all"]
    }
  }
}
```

### Composants de politique

Les politiques du Security Hub contiennent les éléments clés suivants :

`securityhub`

Le conteneur de premier niveau pour les paramètres de politique

Obligatoire pour toutes les politiques du Security Hub

`enable_in_regions`

Liste des régions dans lesquelles Security Hub doit être activé

Peut contenir des noms de régions spécifiques ou `ALL_SUPPORTED`

Champ obligatoire mais peut être vide

Lors de l'utilisation`ALL_SUPPORTED`, inclut les futures régions

`disable_in_regions`

Liste des régions dans lesquelles Security Hub doit être désactivé

Peut contenir des noms de régions spécifiques ou `ALL_SUPPORTED`

Champ obligatoire mais peut être vide

A priorité sur le `enable_in_regions` cas où les régions apparaissent dans les deux listes

Opérateurs d'héritage

@ @assign - Remplace les valeurs héritées

@ @append - Ajoute de nouvelles valeurs aux valeurs existantes

@ @remove - Supprime des valeurs spécifiques des paramètres hérités

Exemples de politiques relatives au Security Hub

Les exemples suivants illustrent les configurations de politique courantes du Security Hub.

L'exemple ci-dessous active Security Hub dans toutes les régions actuelles et futures. En l'utilisant `ALL_SUPPORTED` dans la `enable_in_regions` liste et en la laissant `disable_in_regions` vide, cette politique garantit une couverture de sécurité complète à mesure que de nouvelles régions deviennent disponibles.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

Cet exemple désactive Security Hub dans toutes les régions, y compris dans les régions futures, car `disable_in_regions` la liste a priorité sur. `enable_in_regions`

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2"
         ]
```

```
      },
      "disable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      }
   }
}
```

L'exemple suivant montre comment les politiques relatives aux enfants peuvent modifier les paramètres des politiques parentes à l'aide d'opérateurs d'héritage. Cette approche permet un contrôle granulaire tout en préservant la structure globale des politiques. La politique relative aux enfants ajoute une nouvelle région `enable_in_regions` et en supprime une`disable_in_regions`.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@append":[
            "eu-central-1"
         ]
      },
      "disable_in_regions":{
         "@@remove":[
            "us-west-2"
         ]
      }
   }
}
```

Cet exemple montre comment activer Security Hub dans plusieurs régions spécifiques sans l'utiliser`ALL_SUPPORTED`. Cela permet de contrôler avec précision les régions dans lesquelles Security Hub est activé, tout en laissant les régions non spécifiées non gérées par la politique.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2",
            "eu-west-1",
            "ap-southeast-1"
```

```
         ]
      },
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

L'exemple suivant montre comment gérer les exigences de conformité régionales en activant Security Hub dans la plupart des régions tout en le désactivant explicitement dans des emplacements spécifiques. La `disable_in_regions` liste est prioritaire, ce qui garantit que Security Hub reste désactivé dans ces régions, quels que soient les autres paramètres de politique.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ap-east-1",
            "me-south-1"
         ]
      }
   }
}
```

## Politiques d'Amazon Bedrock

Les politiques d'Amazon Bedrock vous permettent d'appliquer automatiquement les mesures de protection configurées dans Amazon Bedrock Guardrails à tous les éléments de la structure de votre organisation pour tous les appels d'inférence de modèles adressés à Amazon Bedrock. Il n'est donc plus nécessaire de configurer un garde-corps individuel pour chaque compte. Amazon Bedrock Guardrails fournit des garanties configurables pour aider à créer en toute sécurité des applications d'IA générative à grande échelle, avec une approche standard pour un large éventail de modèles de base, notamment : les modèles pris en charge par Amazon Bedrock, les modèles affinés et les modèles hébergés en dehors d'Amazon Bedrock.

Les politiques d'Amazon Bedrock dans AWS Organizations vous permettent de référencer un garde-corps créé dans votre compte de gestion au format JSON. Vous pouvez associer n'importe quelle politique à l'élément requis de la structure de votre organisation, tel que la racine, les unités organisationnelles (OUs) et les comptes individuels. AWS Organizations applique des règles d'héritage pour combiner les politiques, ce qui se traduit par une politique efficace pour chaque compte qui dicte la manière dont les garanties sont appliquées à votre application d'IA générative.

## Comment ça marche

Les politiques d'Amazon Bedrock vous permettent de contrôler l'application automatique des garanties au sein de barrières de sécurité sur plusieurs comptes, ce qui vous permet d'appliquer des barrières de sécurité sur tous les modèles ou sur un sous-ensemble de modèles pour les appels d'inférence vers Amazon Bedrock. Vous devez faire référence à une version spécifique du garde-fou approprié dans votre politique, conformément aux exigences responsables de votre organisation en matière d'IA. Cela est spécifique à la AWS région où se trouve votre garde-corps, et vous devez disposer de garde-corps différents pour chaque AWS région où vous souhaitez appliquer des contrôles de sécurité. Vous pouvez ensuite associer cette politique à n'importe quel nœud de l'organisation, et les comptes situés sous ce nœud hériteront automatiquement de ces garanties et les appliqueront à chaque modèle d'invocation à Amazon Bedrock.

Les politiques d'Amazon Bedrock vous aident à garantir des contrôles de sécurité cohérents dans l'ensemble de votre organisation et fournissent une approche centralisée pour créer en toute sécurité des applications d'IA générative à grande échelle.

## Commencer à utiliser les politiques d'Amazon Bedrock

Avant de configurer les politiques d'Amazon Bedrock, assurez-vous de bien comprendre les prérequis et les exigences de mise en œuvre. Cette rubrique vous guide tout au long du processus de configuration et de gestion de ces politiques au sein de votre organisation.

Avant de commencer

Passez en revue les exigences suivantes avant de mettre en œuvre les politiques d'Amazon Bedrock :

- Votre compte doit faire partie d'une AWS organisation
- Vous devez être connecté sous l'une des formes suivantes :
  - Le compte de gestion de l'organisation
  - Un compte d'administrateur délégué autorisé à gérer les politiques d'Amazon Bedrock

- Vous devez activer le type de politique Amazon Bedrock à la racine de votre organisation

### Étapes d'implémentation

Pour mettre en œuvre efficacement les politiques d'Amazon Bedrock, suivez ces étapes dans l'ordre. Chaque étape garantit une configuration correcte et permet d'éviter les problèmes courants lors de l'installation. Le compte de gestion ou l'administrateur délégué peut effectuer ces étapes via la AWS Organizations console, l'interface de ligne de AWS commande (AWS CLI) ou AWS SDKs.

1. Activez les politiques Amazon Bedrock pour votre organisation.
2. Créez une politique Amazon Bedrock.
3. Associez la politique Amazon Bedrock à la racine, à l'unité d'organisation ou au compte de votre organisation.
4. Consultez la politique combinée en vigueur d'Amazon Bedrock qui s'applique à un compte.

## Bonnes pratiques relatives à l'utilisation des politiques d'Amazon Bedrock

### Utiliser un identifiant de garde-corps valide

Un identifiant incorrect ou mal formé entraînera l'échec de tous les appels d'API Amazon Bedrock au sein de l'organisation cible. Surveillez CloudTrail les alertes de politique efficaces non valides afin de détecter rapidement les erreurs de configuration.

### Exclure les politiques de raisonnement automatique

Les garde-fous qui incluent une politique de raisonnement automatique ne sont pas pris en charge pour l'application au niveau de l'organisation. Vérifiez que le garde-corps Amazon Bedrock que vous avez sélectionné n'en contient pas.

### Accordez les autorisations IAM nécessaires

Utilisez les politiques basées sur les ressources d'Amazon Bedrock Guardrails pour autoriser l'organisation et ses comptes membres à évaluer le garde-fou appliqué lors de l'exécution.

### Consultez les limites de service d'Amazon Bedrock pour les rambardes

Les appels relatifs au compte d'un membre utilisant la politique Amazon Bedrock seront pris en compte dans le calcul des Quotas de Service pour le membre. Consultez la console Service Quotas et assurez-vous que les limites d'exécution de Guardrails sont suffisantes pour votre volume d'appels.

Commencez petit, puis agrandissez

Attachez votre politique à quelques comptes pour commencer, en vous assurant qu'elle est appliquée comme vous le souhaitez. Assurez-vous de vérifier que les autorisations Guardrail sont configurées pour autoriser l'accès entre comptes.

Validez les modifications apportées à vos politiques Amazon Bedrock à l'aide de DescribeEffectivePolicy

Après avoir modifié une politique Amazon Bedrock, vérifiez les politiques en vigueur pour les comptes représentatifs situés en dessous du niveau auquel vous avez apporté la modification. Vous pouvez consulter la politique effective à l'aide de la console AWS de gestion, de l'opération `DescribeEffectivePolicy` API ou de l'une de ses variantes de AWS CLI ou de AWS SDK. Assurez-vous que la modification que vous avez apportée a eu l'impact escompté sur la politique effective.

Communiquez et entraînez-vous

Assurez-vous que vos organisations comprennent l'objectif et l'impact de vos politiques Amazon Bedrock. Fournissez des conseils clairs sur le comportement d'Amazon Bedrock Guardrails et sur ce à quoi vous pouvez vous attendre.

## Syntaxe et exemples de politiques Amazon Bedrock

Une politique Amazon Bedrock est un fichier en texte brut structuré selon les règles du JSON. La syntaxe des politiques Amazon Bedrock suit celle de tous les types de politiques de gestion. Pour plus d'informations, voir Syntaxe des politiques et héritage pour les types de politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques du type de politique Amazon Bedrock.

L'exemple de politique Amazon Bedrock suivant montre la syntaxe de base de la politique Amazon Bedrock :

```
{
    "bedrock": {
        "guardrail_inference": {
            "us-east-1": {
                "config_1": {
                    "identifier": {
                        "@@assign": "arn:aws:bedrock:us-east-1:123456789012:guardrail/
hu1dlsv9wy1d:1"
```

```
                    },
                    "selective_content_guarding": {
                        "system": {
                            "@@assign": "selective"
                        },
                        "messages": {
                            "@@assign": "comprehensive"
                        }
                    },
                    "model_enforcement": {
                        "included_models": {
                            "@@assign": ["ALL"]
                        },
                        "excluded_models": {
                            "@@assign": ["amazon.titan-embed-text-v2:0", "cohere.embed-
english-v3"]
                        }
                    }
                }
            }
        }
    }
}
```

La syntaxe de la politique Amazon Bedrock inclut les éléments suivants :

`"bedrock"`

La clé de niveau supérieur pour les documents de politique d'Amazon Bedrock.

`"guardrail_inference"`

Définit la configuration de renforcement des garde-corps.

`<region>`

Région dans laquelle la politique sera appliquée. Par exemple, `"us-east-1"`.

`"config_1"`

Identifiant de configuration pour les paramètres du garde-corps.

`"identifier"` (Obligatoire)

Guardrail ARN, suivi `:version` de la version Guardrail.

- Le garde-corps doit appartenir au compte de gestion. Vous ne pouvez pas créer de politique à l'aide d'un garde-corps provenant d'un autre compte.
- Le garde-corps doit avoir une version, et cette version ne peut pas être DRAFT. Pour créer une version de votre garde-corps, consultez la section Créer une version d'un garde-corps dans le guide de l'utilisateur d'Amazon Bedrock.
- Le Guardrail doit avoir une politique basée sur les ressources qui permet aux membres de l'organisation d'appeler. `ApplyGuardrail`
- Le garde-corps doit être créé et utilisé dans la région spécifiée.

`"selective_content_guarding"` (facultatif)

Amazon Bedrock APIs permet de marquer du contenu spécifique dans la saisie que l'appelant souhaite que les garde-corps traitent. Ces paramètres permettent aux responsables de l'application de contrôler s'ils doivent ou non respecter les décisions de balisage du contenu prises par l'appelant. Lorsque cela est spécifié, l'un `"system"` des `"messages"` deux est requis.

`"system"` (facultatif)

Choisissez la manière dont les instructions du système seront traitées par les glissières de sécurité. La valeur par défaut est `comprehensive` lorsqu'elle n'est pas spécifiée.

- `"comprehensive"`: évaluez l'ensemble du contenu indépendamment des balises de contenu de protection.
- `"selective"`: évaluez uniquement le contenu inclus dans les balises de contenu Guard. N'évalue aucun contenu lorsqu'aucune balise n'est spécifiée.

`"messages"` (facultatif)

Choisissez la manière dont le contenu des messages contenant les conversations entre l'utilisateur et l'assistant sera traité par des garde-fous. La valeur par défaut est `comprehensive` lorsqu'elle n'est pas spécifiée.

- `"comprehensive"`: évaluez l'ensemble du contenu indépendamment des balises de contenu de protection.
- `"selective"`: évaluez uniquement le contenu inclus dans les balises de contenu Guard. Évalue tout le contenu des messages lorsqu'aucune balise n'est spécifiée.

`"model_enforcement"` (facultatif)

Informations spécifiques au modèle pour la configuration du garde-corps imposé. Si elle n'est pas présente, la configuration est appliquée à tous les modèles.

`"included_models"` (Obligatoire)

Liste des modèles sur lesquels renforcer le garde-corps. Lorsqu'il est vide, applique l'application à tous les modèles. Accepte également le mot clé « ALL » pour inclure explicitement tous les modèles.

`"excluded_models"` (Obligatoire)

Modèles à exclure de l'application du garde-corps. Lorsqu'il est vide, aucun modèle n'est exclu de l'application. Si un modèle est présent à la fois dans les listes des modèles inclus et exclus, il est exclu.

## Politiques d'Amazon Inspector

Les politiques Amazon Inspector vous permettent d'activer et de gérer Amazon Inspector de manière centralisée pour tous les comptes de votre AWS organisation. Avec une politique Amazon Inspector, vous spécifiez les entités organisationnelles (root ou comptes) sur lesquelles Amazon Inspector est automatiquement activé et lié au compte d'administrateur délégué Amazon Inspector. OUs Vous pouvez utiliser les politiques d'Amazon Inspector pour simplifier l'intégration à l'échelle du service et garantir une activation cohérente d'Amazon Inspector dans tous les comptes existants et nouvellement créés.

### Caractéristiques et avantages clés

Les politiques d'Amazon Inspector vous permettent de définir les types de scan qui doivent être activés pour votre organisation ou des sous-ensembles de celle-ci, afin de garantir une couverture cohérente et de réduire les efforts manuels. Une fois mis en œuvre, ils vous aident à intégrer automatiquement de nouveaux comptes et à maintenir votre base de référence en matière de numérisation à mesure que votre entreprise évolue.

### Comment ça marche

Lorsque vous associez une politique Amazon Inspector à une entité organisationnelle, cette politique active automatiquement Amazon Inspector pour tous les comptes membres compris dans cette zone. De plus, si vous avez finalisé la configuration d'Amazon Inspector en enregistrant un administrateur délégué pour Amazon Inspector, ce compte bénéficiera d'une visibilité centralisée des vulnérabilités sur les comptes de l'organisation sur lesquels Amazon Inspector est activé.

Les politiques d'Amazon Inspector peuvent être appliquées à l'ensemble de l'organisation, à des unités organisationnelles spécifiques (OUs) ou à des comptes individuels. Les comptes qui

rejoignent l'organisation, ou qui migrent vers une unité d'organisation associée à une politique Amazon Inspector, héritent automatiquement de la politique, et Amazon Inspector est activé et lié à l'administrateur délégué d'Amazon Inspector. Les politiques d'Amazon Inspector vous permettent d'activer le EC2 scan Amazon, le scan Amazon ECR ou Lambda Standard et le scan de code, ainsi que la sécurité du code. Les paramètres de configuration et les règles de suppression spécifiques peuvent être gérés via le compte d'administrateur délégué de l'organisation.

Lorsque vous associez une politique Amazon Inspector à votre organisation ou unité organisationnelle, AWS Organizations évalue automatiquement la politique et l'applique en fonction du champ d'application que vous définissez. Le processus d'application des politiques suit des règles spécifiques de résolution des conflits :

- Lorsque des régions apparaissent à la fois dans les listes d'activation et de désactivation, la configuration de désactivation est prioritaire. Par exemple, si une région est répertoriée à la fois dans les configurations d'activation et de désactivation, Amazon Inspector sera désactivé dans cette région.
- Lorsque l'activation `ALL_SUPPORTED` est spécifiée, Amazon Inspector est activé dans toutes les régions actuelles et futures, sauf s'il est explicitement désactivé. Cela vous permet de maintenir une couverture complète à mesure que vous vous AWS étendez dans de nouvelles régions.
- Les politiques relatives aux enfants peuvent modifier les paramètres des politiques parentales à l'aide d'opérateurs d'héritage, ce qui permet un contrôle granulaire à différents niveaux organisationnels. Cette approche hiérarchique garantit que les unités organisationnelles spécifiques peuvent personnaliser leurs paramètres de sécurité tout en maintenant les contrôles de base.

### Terminologie

Cette rubrique utilise les termes suivants pour aborder les politiques d'Amazon Inspector.

| Durée | Définition |
| --- | --- |
| Stratégie effective | Politique finale qui s'applique à un compte après avoir combiné toutes les politiques héritées. |
| Héritage de politique | Processus par lequel les comptes héritent des politiques des unités organisationnelles parentes. |

| Durée | Définition |
| --- | --- |
| Administrateur délégué | Un compte désigné pour gérer les politiques d'Amazon Inspector au nom de l'organisation. |
| Rôle lié à un service | Rôle IAM qui permet à Amazon Inspector d'interagir avec d'autres AWS services. |

### Cas d'utilisation des politiques d'Amazon Inspector

Organisations qui lancent des charges de travail à grande échelle sur plusieurs comptes peuvent utiliser cette politique pour garantir que tous les comptes activent immédiatement les types de scan appropriés et éviter les lacunes. Les environnements axés sur la réglementation ou la conformité peuvent utiliser des politiques secondaires pour annuler ou limiter les types de numérisation par unité d'organisation. Les environnements à croissance rapide peuvent automatiser l'activation des comptes nouvellement créés afin qu'ils soient toujours conformes aux normes de base.

### Héritage et application des politiques

Comprendre comment les politiques sont héritées et appliquées est essentiel pour une gestion efficace de la sécurité au sein de votre entreprise. Le modèle d'héritage suit la hiérarchie AWS des Organisations, garantissant ainsi une application prévisible et cohérente des politiques.

- Les politiques associées au niveau racine s'appliquent à tous les comptes
- Les comptes héritent des politiques de leurs unités organisationnelles mères
- Plusieurs politiques peuvent s'appliquer à un seul compte
- Les politiques plus spécifiques (plus proches du compte dans la hiérarchie) ont priorité

### Validation de politique

Lors de la création des politiques Amazon Inspector, les validations suivantes ont lieu :

- Les noms de région doivent être des identifiants de AWS région valides
- Les régions doivent être prises en charge par Amazon Inspector
- La structure des politiques doit suivre les règles de syntaxe AWS des politiques des Organisations
- Les deux `enable_in_regions` et `disable_in_regions` les listes doivent être présentes, bien qu'elles puissent être vides

### Considérations régionales et régions prises en charge

Les politiques d'Amazon Inspector s'appliquent uniquement dans les régions où un accès sécurisé est disponible pour Amazon Inspector et AWS Organizations. Comprendre le comportement régional vous aide à mettre en œuvre des contrôles de sécurité efficaces sur l'ensemble du territoire mondial de votre entreprise.

- L'application des politiques se fait indépendamment dans chaque région
- Vous pouvez spécifier les régions à inclure ou à exclure dans vos politiques
- Les nouvelles régions sont automatiquement incluses lorsque vous utilisez l'`ALL_SUPPORTED`option
- Les politiques s'appliquent uniquement aux régions dans lesquelles Amazon Inspector est disponible

### Comportement du détachement

Si vous supprimez une politique Amazon Inspector, Amazon Inspector reste activé sur les comptes précédemment couverts. Toutefois, les modifications futures de la structure organisationnelle (telles que l'ajout de nouveaux comptes ou le transfert de comptes existants dans l'unité d'organisation) n'activeront plus automatiquement Amazon Inspector. Toute activation supplémentaire doit être effectuée manuellement ou en rattachant une politique.

## Détails supplémentaires

### Administrateur délégué

Un seul administrateur délégué peut être enregistré pour Amazon Inspector dans une organisation. Vous devez le configurer dans la console Amazon Inspector ou via APIs avant de joindre les politiques Amazon Inspector.

### Conditions préalables

Vous devez activer l'accès sécurisé pour les AWS Organizations, avoir un administrateur délégué enregistré pour Amazon Inspector et disposer de rôles liés à un service dans tous les comptes.

### Régions prises en charge

Toutes les régions dans lesquelles Amazon Inspector est disponible.

## Commencer à utiliser les politiques d'Amazon Inspector

Avant de configurer les politiques Amazon Inspector, assurez-vous de bien comprendre les prérequis et les exigences de mise en œuvre. Cette rubrique vous guide tout au long du processus de configuration et de gestion de ces politiques dans votre organisation.

### En savoir plus sur les autorisations requises

Pour activer ou joindre les politiques Amazon Inspector, vous devez disposer des autorisations suivantes dans le compte de gestion :

- `organizations:EnableAWSServiceAccess` pour `inspector2.amazonaws.com`
- `organizations:RegisterDelegatedAdministrator` pour `inspector2.amazonaws.com`
- `organizations:AttachPolicy`, `organizations:CreatePolicy`, `organizations:DescribeEffectivePolicy`
- `inspector2:Enable`(pour le compte de gestion et l'administrateur délégué)

### Avant de commencer

Passez en revue les exigences suivantes avant de mettre en œuvre les politiques d'Amazon Inspector :

- Votre compte doit faire partie d'une AWS organisation
- Vous devez être connecté en tant que :
  - Le compte de gestion de l'organisation
  - Administrateur délégué d'une AWS organisation autorisé à gérer les politiques d'Amazon Inspector
- Vous devez activer l'accès sécurisé pour Amazon Inspector dans votre organisation
- Vous devez activer le type de politique Amazon Inspector à la racine de votre organisation

Vérifiez également que :

- Amazon Inspector est pris en charge dans les régions où vous souhaitez appliquer des politiques
- Le rôle `AWSServiceRoleForInspectorV2` lié au service est configuré dans votre compte de gestion. Pour vérifier que ce rôle existe, exécutez`aws iam get-role --role-name AWSServiceRoleForInspectorV2`. Si vous devez créer ce rôle, vous pouvez exécuter ce rôle

`aws inspector2 enable` dans n'importe quelle région à partir de votre compte de gestion ou le créer directement en exécutant`aws iam create-service-linked-role --aws-service-name inspector2.amazonaws.com`.

### Étapes d'implémentation

Pour mettre en œuvre efficacement les politiques d'Amazon Inspector, suivez ces étapes dans l'ordre. Chaque étape garantit une configuration correcte et permet d'éviter les problèmes courants lors de l'installation. Le compte de gestion ou l'administrateur délégué peut effectuer ces étapes via la AWS Organizations console, l'interface de ligne de AWS commande (AWS CLI) ou AWS SDKs.

1. Activez un accès sécurisé pour Amazon Inspector.
2. Activez les politiques Amazon Inspector pour votre organisation.
3. Créez une politique Amazon Inspector.
4. Associez la politique Amazon Inspector à la racine, à l'unité d'organisation ou au compte de votre organisation.
5. Consultez la politique Amazon Inspector en vigueur combinée qui s'applique à un compte.

### Création d'une politique Amazon Inspector

#### Autorisations minimales

Pour créer une politique Amazon Inspector, vous devez disposer des autorisations suivantes :

- `organizations:CreatePolicy`

#### AWS Console de gestion

Pour créer une politique Amazon Inspector

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Définissez un administrateur délégué pour le service utilisé dans la console Amazon Inspector.
3. Une fois que l'administrateur délégué a été configuré pour Amazon Inspector, rendez-vous sur la console de AWS l'organisation pour configurer les politiques. Sur la console de AWS l'organisation, rendez-vous sur la page Amazon Inspector Policies, puis choisissez Create policy.

4. Sur la page Créer une nouvelle politique Amazon Inspector, entrez le nom de la politique et une description de la politique facultative.
5. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, veuillez consulter Ressources de balisage AWS Organizations.
6. Entrez ou collez le texte de la politique dans la zone de code JSON. Pour plus d'informations sur la syntaxe des politiques Amazon Inspector et pour des exemples de politiques que vous pouvez utiliser comme point de départ, consultezSyntaxe et exemples de politiques Amazon Inspector.
7. Lorsque vous avez terminé la modification de votre politique, choisissez Créer la politique dans l'angle inférieur droit de la page.

## Bonnes pratiques relatives à l'utilisation des politiques d'Amazon Inspector

Lorsque vous mettez en œuvre les politiques Amazon Inspector au sein de votre organisation, le respect des meilleures pratiques établies permet de garantir un déploiement et une maintenance réussis.

### Commencez simplement en réalisant de petites modifications

Commencez par activer les politiques Amazon Inspector dans une unité organisationnelle limitée (par exemple, « Security Pilot ») afin de valider le comportement attendu avant de les déployer sur tous les comptes. Cette approche progressive vous permet d'identifier et de résoudre les problèmes potentiels dans un environnement contrôlé avant un déploiement à grande échelle.

### Mettre en place des processus de révision

Surveillez régulièrement les nouveaux comptes qui rejoignent votre organisation et vérifiez qu'ils héritent automatiquement de l'activation d'Amazon Inspector. Passez en revue les champs d'application des politiques tous les trimestres pour vous assurer que votre couverture de sécurité reste conforme à votre structure organisationnelle et à vos exigences en matière de sécurité.

### Validez les modifications en utilisant DescribeEffectivePolicy

Après avoir joint ou modifié une politique, lancez-vous vers `DescribeEffectivePolicy` des comptes représentatifs afin de vous assurer que l'activation d'Amazon Inspector est correctement prise en compte. Cette étape de validation vous permet de confirmer que vos modifications de politique ont l'effet escompté dans l'ensemble de votre organisation.

Communiquez et entraînez-vous

Indiquez aux propriétaires de comptes qu'Amazon Inspector sera activé automatiquement et que les résultats pourront apparaître dans leur tableau de bord Security Hub ou Amazon Inspector une fois qu'ils seront liés à l'administrateur délégué d'Amazon Inspector. Une communication claire permet de s'assurer que les titulaires de comptes comprennent la surveillance de sécurité en place et peuvent réagir de manière appropriée aux constatations.

Planifiez votre stratégie d'administrateur délégué

Désignez un compte de sécurité ou de conformité en tant qu'administrateur délégué d'Amazon Inspector. Définissez l'administrateur délégué depuis la console Amazon Inspector ou via AWS Organizations APIs. Cette approche permet une surveillance et une gestion cohérentes de la sécurité au sein de votre organisation.

Gérer les considérations régionales

Activez Amazon Inspector dans les régions où s'exécutent vos charges de travail. Tenez compte de vos exigences de conformité et de vos besoins opérationnels lorsque vous déterminez les régions qui nécessitent une couverture Amazon Inspector. Documentez les exigences spécifiques à votre région afin de maintenir une surveillance cohérente de la sécurité dans l'ensemble de votre infrastructure.

## Syntaxe et exemples de politiques Amazon Inspector

Les politiques d'Amazon Inspector suivent une syntaxe JSON standardisée qui définit la manière dont Amazon Inspector est activé et configuré au sein de votre organisation. Une politique Amazon Inspector est un document JSON structuré selon la syntaxe de la politique de gestion des AWS Organizations. Il définit les entités organisationnelles pour lesquelles Amazon Inspector sera automatiquement activé.

Structure politique de base

Une politique Amazon Inspector utilise cette structure de base :

```
{
    "inspector": {
        "enablement": {
            "ec2_scanning": {
                "enable_in_regions": {
                    "@@assign": ["us-east-1", "us-west-2"]
                },
                "disable_in_regions": {
```

```
                    "@@assign": ["eu-west-1"]
                }
            }
        }
    }
}
```

Composants de politique

Les politiques d'Amazon Inspector contiennent les éléments clés suivants :

`inspector`

La clé de niveau supérieur pour les documents de politique Amazon Inspector, qui est requise pour toutes les politiques Amazon Inspector.

`enablement`

Définit la manière dont Amazon Inspector est activé au sein de l'organisation et contient les configurations des types de scan.

`Regions (Array of Strings)`

Spécifie les régions dans lesquelles Amazon Inspector doit être activé automatiquement.

Exemples de politiques Amazon Inspector

Les exemples suivants illustrent les configurations de politique courantes d'Amazon Inspector.

Exemple 1 — Activer Amazon Inspector à l'échelle de l'organisation

L'exemple suivant active Amazon Inspector dans `us-east-1` et `us-west-2` pour tous les comptes de la racine de l'organisation.

Créez un fichier `inspector-policy-enable.json` :

```
{
  "inspector": {
    "enablement": {
      "lambda_standard_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "us-east-1",
            "us-west-2"
```

```
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        },
        "lambda_code_scanning": {
          "enable_in_regions": {
            "@@assign": [
              "us-east-1",
              "us-west-2"
            ]
          },
          "disable_in_regions": {
            "@@assign": [
              "eu-west-1"
            ]
          }
        }
      },
      "ec2_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "us-east-1",
            "us-west-2"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        }
      },
      "ecr_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "us-east-1",
            "us-west-2"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-1"
```

```
          ]
        }
      },
      "code_repository_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "us-east-1",
            "us-west-2"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        }
      }
    }
  }
}
```

Lorsqu'ils sont connectés à la racine, tous les comptes de l'organisation activent automatiquement Amazon Inspector, et les résultats de leur analyse sont mis à la disposition de l'administrateur délégué d'Amazon Inspector.

Créez et attachez la politique :

```
POLICY_ID=$(aws organizations create-policy \
  --content file://inspector-policy-enable.json \
  --name InspectorOrgPolicy \
  --type INSPECTOR_POLICY \
  --description "Inspector organization policy to enable all resources in IAD and PDX."
 \
  --query 'Policy.PolicySummary.Id' \
  --output text)
aws organizations attach-policy --policy-id $POLICY_ID --target-id <root-id>
```

Tout nouveau compte rejoignant l'organisation hérite automatiquement de l'activation.

S'ils sont détachés, les comptes existants restent activés, mais les comptes futurs ne le sont pas automatiquement :

```
aws organizations detach-policy --policy-id $POLICY_ID --target-id <root-id>
```

Exemple 2 — Activer Amazon Inspector pour une unité d'organisation spécifique

Créez un fichier `inspector-policy-eu-west-1.json` :

```
{
  "inspector": {
    "enablement": {
      "lambda_standard_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-2"
          ]
        },
        "lambda_code_scanning": {
          "enable_in_regions": {
            "@@assign": [
              "eu-west-1"
            ]
          },
          "disable_in_regions": {
            "@@assign": [
              "eu-west-2"
            ]
          }
        }
      },
      "ec2_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-2"
          ]
        }
      },
      "ecr_scanning": {
```

```
        "enable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-2"
          ]
        }
      },
      "code_repository_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-2"
          ]
        }
      }
    }
  }
}
```

Joignez-le à une unité d'organisation pour vous assurer qu'Amazon Inspector `eu-west-1` sera activé sur tous les comptes de production inclus et qu'ils seront liés à l'administrateur délégué d'Amazon Inspector :

```
aws organizations update-policy --policy-id $POLICY_ID --content file://inspector-
policy-eu-west-1.json --description "Inspector organization policy - Enable all (eu-
west-1)"
aws organizations attach-policy --policy-id $POLICY_ID --target-id ou-aaaa-12345678
```

Les comptes extérieurs à l'UO ne sont pas affectés.

## Mettre à niveau les politiques de déploiement

AWS Organizations les politiques de déploiement des mises à niveau vous permettent de gérer de manière centralisée et d'échelonner les mises à niveau automatiques sur plusieurs AWS ressources

et comptes de votre organisation. Grâce à ces politiques, vous pouvez définir l'ordre dans lequel les ressources reçoivent les mises à niveau, en veillant à ce que les modifications soient validées dans des environnements moins critiques avant d'entrer en production.

Dans les environnements cloud complexes d'aujourd'hui, la gestion des mises à niveau sur de nombreux comptes et ressources peut s'avérer difficile. Les politiques de déploiement des mises à niveau répondent à ce défi en proposant une approche systématique de mise en œuvre des mises à niveau. En utilisant ces politiques, vous pouvez aligner votre processus de mise à niveau sur les pratiques de gestion du changement de votre organisation, en réduisant les risques et en améliorant l'efficacité opérationnelle.

Les politiques de déploiement des mises à niveau tirent parti de la structure hiérarchique de AWS Organizations pour appliquer des politiques à l'ensemble de votre organisation ou à des unités organisationnelles spécifiques (OUs). Cette intégration vous permet de gérer les mises à niveau à grande échelle, éliminant ainsi le besoin de coordination manuelle ou de scripts d'automatisation personnalisés.

## Caractéristiques et avantages clés

Les politiques de déploiement des mises à niveau fournissent des fonctionnalités complètes de gestion des mises à niveau tout en offrant des avantages significatifs aux entreprises qui gèrent des ressources sur plusieurs comptes et environnements. Le tableau suivant décrit les principales fonctionnalités et les avantages associés :

Caractéristiques et avantages des politiques de déploiement des mises à niveau

| Fonctionnalité | Description | Principaux avantages |
|---|---|---|
| Système de commande de mise à niveau | Système à trois niveaux (premier, deuxième, dernier) avec chronométrage configurable | • Tester les mises à niveau dans des environnements de pré-production |
| | | • Minimiser les risques liés aux charges de travail de production |
| Gestion basée sur des politiques | Contrôle centralisé via AWS Organizations | • Gérez plusieurs comptes à partir d'un seul point |
| | | • Réduisez les frais administratifs |

| Fonctionnalité | Description | Principaux avantages |
| --- | --- | --- |
| Ciblage des ressources | Options de ciblage basées sur les balises et les unités d'organisation | • Cibler des groupes de ressources spécifiques |
| | | • Appliquer les politiques à grande échelle |
| Planification automatisée | Fonctionne avec les fenêtres de maintenance existantes | • Éliminez la coordination manuelle |
| | | • Maintenir des modèles de mise à niveau cohérents |
| Intégration de service | Fonctionne avec les mécanismes AWS de mise à niveau des services | • Surveillez les événements avec Amazon EventBridge |
| Contrôles de conformité | Héritage et application des politiques | • Appliquer les normes organisationnelles |
| | | • Respecter les exigences de conformité |

Pour plus d'informations sur l'héritage des politiques, consultezFonctionnement de l'héritage des politiques de gestion.

## Quelles sont les politiques de déploiement des mises à niveau ?

Les politiques de déploiement des mises à niveau sont un ensemble de règles qui déterminent comment et quand les mises à niveau automatiques sont appliquées à vos AWS ressources. Ces politiques vous permettent de définir différents ordres de mise à niveau pour vos ressources, généralement en fonction de vos environnements de développement, de test et de production. Vous pouvez ainsi vous assurer que les mises à niveau sont d'abord appliquées aux systèmes moins critiques, ce qui vous permet d'identifier et de résoudre les problèmes avant qu'ils n'affectent vos charges de travail de production.

Les politiques prennent en charge trois ordres de mise à niveau : le premier, le deuxième et le dernier. Ces commandes créent une approche progressive des mises à niveau, les ressources étant désignées comme « premières » recevant les améliorations dans un premier temps, suivies de

« secondes » après une période d'attente, et enfin « dernières » après une autre période d'attente. Cette approche échelonnée vous donne le temps de valider les mises à niveau à chaque étape avant qu'elles ne passent à des systèmes plus critiques.

Les politiques de déploiement des mises à niveau sont particulièrement utiles pour les organisations dotées de structures multicomptes complexes ou soumises à des exigences strictes en matière de gestion du changement. Ils fournissent un équilibre entre la maintenance up-to-date des systèmes et la minimisation du risque d'interruptions des services critiques liées aux mises à niveau.

## Comment fonctionnent les politiques de déploiement des mises à niveau

Les politiques de déploiement des mises à niveau s'intègrent parfaitement à votre AWS infrastructure et à vos processus existants. Lorsque vous créez et attachez une politique de déploiement de mise à niveau à une unité organisationnelle, elle s'applique à tous les comptes de cette unité d'organisation. Vous pouvez ensuite utiliser des balises de ressources ou des ordres de patch pour spécifier quelles ressources doivent être mises à niveau dans quel ordre.

Lorsqu'un AWS service pris en charge publie une mise à niveau, il consulte les politiques de déploiement de la mise à niveau afin de déterminer l'ordre dans lequel les ressources doivent recevoir la mise à niveau. Le service applique d'abord la mise à niveau aux ressources marquées comme « Premières » pendant leurs fenêtres de maintenance configurées. Après une période d'attente spécifique au service, généralement d'une semaine environ, les ressources marquées comme « Deuxième » deviennent éligibles à la mise à niveau. Enfin, après une nouvelle période d'attente, les ressources marquées comme « Dernières » reçoivent la mise à niveau.

Ce processus garantit que les mises à niveau sont appliquées de manière contrôlée et prévisible dans l'ensemble de votre organisation. Il vous permet de surveiller l'impact des mises à niveau à chaque étape et de prendre des mesures correctives si nécessaire avant que les modifications n'atteignent vos environnements les plus critiques. La nature automatisée de ce processus réduit les frais opérationnels liés à la gestion des mises à niveau, tout en vous fournissant le contrôle et la visibilité dont vous avez besoin pour maintenir la stabilité et la sécurité de vos AWS ressources.

## Terminologie

Voici les principaux termes que vous devez comprendre lorsque vous travaillez avec des politiques de déploiement des mises à niveau :

Conditions de la politique de déploiement des mises à niveau

| Durée | Définition |
| --- | --- |
| Date d'activité | Date à laquelle l'AmVu devient visible dans l'API Describe Pending Maintenance Actions et disponible pour l'application. |
| AmVu (mise à niveau automatique des versions mineures) | Processus de mise à niveau automatique pour les versions mineures des moteurs de base de données. |
| Stratégie effective | Ensemble final de règles qui s'appliquent à un compte ou à une ressource après avoir pris en compte toutes les politiques héritées et directement associées. |
| Fenêtre de maintenance | Période récurrente pendant laquelle des mises à niveau automatiques peuvent être appliquées à une ressource. Les politiques de déploiement des mises à niveau fonctionnent dans ces fenêtres de maintenance configurées. |
| Unité d'organisation (UO) | Un conteneur pour les AWS comptes de votre organisation. Des politiques de déploiement des mises à niveau peuvent être associées au niveau de l'unité d'organisation pour affecter tous les comptes qu'elle contient. |
| Ordre des patchs | Ordre dans lequel les ressources reçoivent les mises à niveau (première, deuxième, dernière). |
| Objectif de la politique | L'étendue à laquelle s'applique une politique de déploiement de mise à niveau, qui peut concerner une organisation entière OUs, des comptes spécifiques ou des comptes individuels. |
| Balises de ressources | Paires clé-valeur qui peuvent être utilisées pour identifier les ressources devant suivre des ordres de mise à niveau spécifiques dans le cadre d'une politique. |
| Fenêtre de planification | Période pendant laquelle les ressources d'un ordre de correctif spécifique reçoivent des mises à niveau. |

| Durée | Définition |
| --- | --- |
| Période d'attente spécifique au service | Intervalle de temps désigné entre les ressources de mise à niveau des différents ordres de mise à niveau. Cette période varie en fonction du AWS service et du type de mise à niveau. |
| Ordre de mise à niveau | Désignation qui détermine à quel moment une ressource reçoit des améliorations par rapport aux autres ressources. Peut être réglé sur Premier, Deuxième ou Dernier. |
| Politique de déploiement des mises à niveau | Type de AWS Organizations politique utilisé pour gérer les calendriers de mise à niveau entre les ressources. |

## Cas d'utilisation des politiques de déploiement des mises à niveau

Organisations de tailles et de secteurs d'activité différents peuvent tirer parti des politiques de déploiement des mises à niveau. Les scénarios fictifs suivants illustrent les problèmes courants liés à la gestion des mises à niveau et montrent comment les politiques de déploiement des mises à niveau fournissent des solutions efficaces. Ces exemples sont basés sur des expériences clients typiques, mais ont été simplifiés pour mettre en évidence les principaux avantages et les modèles de mise en œuvre.

De nombreuses entreprises sont confrontées à des défis similaires : elles doivent conserver leurs ressources up-to-date avec les dernières versions tout en minimisant les risques pour leurs environnements de production. Sans approche centralisée basée sur des règles, les équipes ont souvent recours à des processus manuels ou à des scripts d'automatisation complexes. Les exemples suivants montrent comment deux organisations différentes peuvent résoudre des problèmes similaires à l'aide de politiques de déploiement des mises à niveau :

Exemple de cas d'utilisation : société mondiale de services financiers

Une société de services financiers gère des centaines de bases de données Aurora PostgreSQL sur plusieurs comptes. AWS Avant les politiques de déploiement des mises à niveau, leur DevOps équipe passait plusieurs jours par mois à coordonner manuellement les mises à niveau des bases de données, en veillant à ce que les modifications soient testées dans les environnements de développement avant d'atteindre les systèmes de production. En mettant en œuvre des politiques de déploiement des mises à niveau, ils :

- Bases de données de développement étiquetées avec ordre de mise à niveau « First »
- Bases de données QA assignées à l'ordre de mise à niveau « Second »
- Bases de données de production désignées comme « dernier » ordre de mise à niveau
- Réduction de la coordination des mises à niveau de plusieurs jours à quelques minutes
- Validation automatique des modifications d'abord dans les environnements inférieurs
- Maintien de la conformité à leurs exigences en matière de gestion du changement

Exemple de cas d'utilisation : fournisseur de plateforme d'appareils IoT

Une entreprise d'IoT traite des millions d'événements liés à des appareils par jour à l'aide de plusieurs bases de données Amazon RDS. Ils devaient s'assurer que les mises à niveau automatiques des versions mineures ne perturberaient pas leurs services de production. À l'aide de politiques de déploiement des mises à niveau, ils :

- A créé une politique qui s'applique à l'ensemble de leur structure organisationnelle
- Environnements Canary configurés pour recevoir les mises à niveau en premier
- Configuration de la surveillance dans les environnements de mise à niveau précoce
- Temps gagné pour détecter et résoudre les problèmes éventuels avant les mises à niveau de production
- Remplacement de l'automatisation complexe des mises à niveau personnalisées par une politique simple
- Maintien d'une haute disponibilité pour leurs charges de travail de production tout en restant à jour avec les versions des bases de données

## AWS Services pris en charge

Les politiques de déploiement des mises à niveau s'intègrent aux AWS services suivants tout en prenant en charge les mises à niveau automatiques des versions mineures :

Services pris en charge pour les politiques de déploiement des mises à niveau

| Nom du service | Objectif |
| --- | --- |
| Amazon Aurora PostgreSQL-Compatible Edition | Mises à niveau automatiques des versions mineures |

| Nom du service | Objectif |
| --- | --- |
| Amazon Aurora MySQL-Compatible Edition | Mises à niveau automatiques des versions mineures |
| Amazon Relational Database Service pour PostgreSQL | Mises à niveau automatiques des versions mineures |
| Amazon Relational Database Service pour SQL Server | Mises à niveau automatiques des versions mineures |
| Amazon Relational Database Service pour Oracle | Mises à niveau automatiques des versions mineures |
| Amazon Relational Database Service pour MariaDB | Mises à niveau automatiques des versions mineures |
| Amazon Relational Database Service pour MySQL | Mises à niveau automatiques des versions mineures |
| Amazon Relational Database Service pour DB2 | Mises à niveau automatiques des versions mineures |

## Conditions préalables

Les conditions requises et les autorisations requises sont les suivantes pour gérer les politiques de déploiement des mises à niveau dans : AWS Organizations

- AWS Organizations compte de gestion ou accès administrateur délégué
- Ressources des services pris en charge (actuellement les moteurs de base de données Amazon Aurora et Amazon Relational Database Service)
- Autorisations IAM appropriées pour gérer les politiques de déploiement des mises à niveau

## Étapes suivantes

Pour commencer à utiliser les politiques de déploiement des mises à niveau :

1. Consultez le Commencer à utiliser les politiques de déploiement des mises à niveau pour savoir comment créer et gérer des politiques
2. Découvrez comment mettre Bonnes pratiques relatives à l'utilisation des politiques de déploiement des mises à niveau en œuvre des politiques de déploiement des mises à niveau
3. Comprendre Syntaxe et exemples de politique de déploiement des mises à niveau

## Commencer à utiliser les politiques de déploiement des mises à niveau

Suivez ces étapes pour mettre en œuvre des politiques de déploiement des mises à niveau dans votre organisation. Chaque étape renvoie à des informations détaillées qui vous aideront à mener à bien la mise en œuvre.

Avant de commencer

Vérifiez que vous disposez des éléments suivants :

- Accès administratif à AWS Organizations
- Ressources des AWS services pris en charge (tels qu'Aurora ou Amazon Relational Database Service)
- Autorisations IAM nécessaires configurées

Étapes d'implémentation

1. Activez les politiques de déploiement des mises à niveau pour votre organisation.
2. Découvrez comment fonctionnent les politiques de déploiement des mises à niveau.
   - Identifier les environnements de développement, de test et de production
   - Déterminez quelles ressources doivent être mises à niveau en premier, en deuxième et en dernier
   - Documentez votre stratégie de balisage pour l'identification des ressources
3. Création d'une politique de déploiement des mises à niveau:
   - Définissez l'ordre de déploiement par défaut (unité organisationnelle ou niveau du compte)
   - Spécifier le ciblage des ressources en utilisant des balises
   - Configurer toutes les exclusions de politique
4. Associez une politique de déploiement des mises à niveau à un compte de membre unique que vous pouvez utiliser pour les tests. :

- Commencez par une unité organisationnelle de test
- Vérifier l'héritage des politiques
- Confirmer le statut des pièces jointes aux politiques

5. Étiquetez vos ressources en fonction de votre stratégie d'ordre de mise à niveau :
   - Appliquer des balises aux ressources de développement pour les premières mises à niveau
   - Ressources de test d'étiquettes pour les mises à niveau de second ordre
   - Désignez les ressources de production pour les mises à niveau de dernière commande
6. Surveillez et validez la politique :
   - Vérifiez les attributions des ordres de surclassement
   - Vérifier les effets des politiques sur les ressources de test
7. Testez le processus de mise à niveau :
   - Attendez qu'une mise à niveau de service soit disponible
   - Surveillez la progression de la mise à niveau dans vos environnements
   - Vérifiez que les mises à niveau suivent la commande que vous avez spécifiée
8. Activez les politiques de déploiement des mises à niveau pour les unités organisationnelles supplémentaires selon les besoins

Autres informations

- Apprenez la syntaxe des politiques de déploiement des mises à niveau et consultez des exemples de politiques

## Bonnes pratiques relatives à l'utilisation des politiques de déploiement des mises à niveau

AWS recommande les meilleures pratiques suivantes pour l'utilisation des politiques de déploiement des mises à niveau.

Rubriques

- Commencez petit et agrandissez progressivement
- Mettre en place des processus de révision
- Validez efficacement les modifications de politique
- Surveiller et communiquer les modifications

- Maintien de la conformité et de la sécurité
- Optimisez l'efficacité opérationnelle

### Commencez petit et agrandissez progressivement

Commencez votre mise en œuvre par une politique de test associée à un compte unique dans un environnement non critique. Cette approche vous permet de valider le comportement et l'impact des politiques de déploiement des mises à niveau sans risquer de perturber les charges de travail critiques. Une fois que vous avez confirmé que la politique fonctionne comme prévu, déplacez-la progressivement vers le haut de votre structure organisationnelle pour inclure davantage de comptes et d'unités organisationnelles.

Cette mise à l'échelle progressive vous aide à identifier et à résoudre les problèmes dès le début du processus de mise en œuvre. Envisagez de créer un groupe pilote de ressources représentant la diversité de votre environnement tout en minimisant les risques opérationnels. Documentez les résultats de chaque phase d'expansion pour éclairer les futurs déploiements et ajustements des politiques.

### Mettre en place des processus de révision

Mettez en œuvre des processus de révision réguliers pour surveiller les nouveaux attributs de la politique de déploiement des mises à niveau et évaluer les exceptions aux politiques. Ces examens doivent être conformes aux exigences opérationnelles et de sécurité de votre organisation. Créez un calendrier pour examiner l'efficacité des politiques et conservez la documentation de tout ajustement effectué.

Votre processus de révision doit inclure des évaluations régulières des ressources régies par des politiques, la vérification que les commandes de mise à niveau sont conformes à la stratégie que vous avez prévue et une évaluation de toute exception aux politiques. Envisagez d'établir des critères pour déterminer quand les politiques doivent être mises à jour et de tenir un journal des modifications pour suivre l'évolution des politiques au fil du temps.

### Validez efficacement les modifications de politique

Après avoir modifié une politique de déploiement des mises à niveau, vérifiez les politiques efficaces pour les comptes représentatifs à chaque niveau de votre organisation. Utilisez la console AWS de gestion ou `DescribeEffectivePolicy` l'opération API pour vérifier que vos modifications ont l'impact escompté. Cette validation doit inclure la vérification des ressources des différentes unités organisationnelles et la confirmation que l'héritage fonctionne comme prévu.

Portez une attention particulière aux ressources auxquelles des ordres de mise à niveau explicites sont attribués par rapport à celles qui utilisent des valeurs par défaut. Établissez une liste de contrôle de validation qui inclut la vérification du ciblage basé sur les balises, la confirmation des alignements des fenêtres de maintenance et le test de l'héritage des politiques.

Surveiller et communiquer les modifications

Établissez une surveillance complète de vos politiques de déploiement des mises à niveau et créez des canaux de communication clairs pour partager les informations relatives aux mises à niveau. Documentez des procédures claires pour gérer les échecs de mise à niveau et créez des plans de réponse pour différents scénarios.

Maintenez une communication régulière avec les équipes qui gèrent les ressources affectées par les politiques de mise à niveau. Envisagez de créer des tableaux de bord offrant une visibilité sur les mises à niveau à venir et leur progression prévue dans vos environnements.

Maintien de la conformité et de la sécurité

Auditez régulièrement vos politiques de déploiement des mises à niveau pour vous assurer qu'elles sont conformes à vos exigences de conformité. Documentez toutes les décisions politiques et conservez des enregistrements clairs des modèles de mise à niveau et des exceptions. Mettez en œuvre des contrôles de sécurité relatifs aux modifications des politiques et maintenez une piste d'audit des modifications de politique à l'aide de AWS CloudTrail.

Passez régulièrement en revue les autorisations d'accès aux fonctions de gestion des politiques et implémentez l'accès du moindre privilège pour l'administration des politiques. Créez des procédures pour les modifications d'urgence des politiques et maintenez la documentation des exigences de mise à niveau liées à la sécurité.

Optimisez l'efficacité opérationnelle

Concevez vos politiques de manière à minimiser les frais d'exploitation tout en maintenant les contrôles nécessaires. Pour éviter tout comportement involontaire, ne réutilisez pas les balises dans différents cas d'utilisation. Automatisez le contrôle de conformité aux politiques dans la mesure du possible et créez des procédures opérationnelles standard pour les tâches courantes de gestion des politiques.

Envisagez de créer des modèles pour différents types de scénarios de mise à niveau et conservez la documentation des modèles de politiques efficaces. L'examen régulier des indicateurs opérationnels peut aider à identifier les opportunités d'optimisation des politiques et d'amélioration des processus.

# Syntaxe et exemples de politique de déploiement des mises à niveau

Une politique de déploiement des mises à niveau définit la manière dont les AWS services appliquent les mises à niveau automatiques à l'ensemble de vos ressources. La compréhension de la syntaxe des politiques vous permet de créer des politiques efficaces qui répondent aux exigences de mise à niveau de votre organisation.

Rubriques



## Considérations

Lors de la mise en œuvre des politiques de déploiement des mises à niveau, tenez compte des facteurs importants suivants :

- Les noms des politiques doivent être uniques au sein de votre organisation et doivent être clairs et descriptifs. Choisissez des noms qui reflètent l'objectif et la portée de la politique. Pour de plus amples informations, veuillez consulter Optimisez l'efficacité opérationnelle.
- Les tests sont essentiels avant un déploiement à grande échelle. Validez d'abord les nouvelles politiques dans les environnements non liés à la production, puis étendez-les progressivement pour garantir le comportement souhaité. Pour de plus amples informations, veuillez consulter Commencez petit et agrandissez progressivement.
- Les modifications de politique peuvent prendre plusieurs heures pour se propager au sein de votre organisation. Planifiez vos mises en œuvre en conséquence et assurez-vous qu'une surveillance appropriée est en place. Pour de plus amples informations, veuillez consulter Surveiller et communiquer les modifications.
- Le formatage JSON doit être valide et respecter la taille maximale de la politique de 5 120 octets. Simplifiez au maximum les structures des politiques tout en répondant à vos exigences.
- Des révisions régulières des politiques contribuent à maintenir l'efficacité. Planifiez des évaluations périodiques de vos politiques pour vous assurer qu'elles continuent de répondre aux besoins de votre organisation. Pour de plus amples informations, veuillez consulter Mettre en place des processus de révision.

- Les ressources sans ordre de mise à niveau attribué sont par défaut du « deuxième » ordre. Envisagez de définir explicitement des ordres de mise à niveau pour les ressources critiques plutôt que de vous fier aux valeurs par défaut. Pour de plus amples informations, veuillez consulter Validez efficacement les modifications de politique.
- Les mises à niveau manuelles ont la priorité sur les ordres de mise à niveau définis par des règles. Assurez-vous que vos processus de gestion des modifications tiennent compte des scénarios de mise à niveau automatiques et manuels. Pour de plus amples informations, veuillez consulter Mettre en place des processus de révision.

> **Note**
>
> Lorsque vous mettez en œuvre des politiques de déploiement de mise à niveau basées sur des balises à partir de votre compte de gestion, sachez que le compte de gestion ne peut pas afficher ou accéder directement aux balises au niveau des ressources dans les comptes membres. Nous recommandons d'établir un processus dans le cadre duquel les comptes membres appliquent des balises de ressources cohérentes, puis de créer des politiques au niveau de l'organisation qui font référence à ces balises. Cela garantit une bonne coordination entre le balisage au niveau des ressources et l'application des politiques organisationnelles. Vous pouvez également l'utiliser Politiques de balises pour maintenir la cohérence des balises lorsque les ressources sont balisées au sein de votre organisation.

### Structure politique de base

Les politiques de déploiement des mises à niveau utilisent une structure JSON qui inclut les principaux éléments suivants :

- Métadonnées relatives aux politiques (telles que les informations de version)
- Règles de ciblage des ressources
- Spécifications des commandes de mise à niveau
- Messages d'exception facultatifs
- Attributs spécifiques au service

L'exemple suivant montre une structure de politique de déploiement de mise à niveau de base :

```
{
```

```
   "upgrade_rollout":{
      "default":{
         "patch_order":{
            "@@assign":"last"
         }
      },
      "tags":{
         "devtag":{
            "tag_values":{
               "tag1":{
                  "patch_order":{
                     "@@assign":"first"
                  }
               },
               "tag2":{
                  "patch_order":{
                     "@@assign":"second"
                  }
               },
               "tag3":{
                  "patch_order":{
                     "@@assign":"last"
                  }
               }
            }
         }
      }
   }
}
```

Composants de politique

Une politique de déploiement des mises à niveau se compose de deux composants clés qui fonctionnent ensemble pour contrôler la manière dont les mises à niveau sont appliquées à l'ensemble de vos ressources. Ces composants incluent des options de configuration pour les comportements par défaut et les remplacements basés sur des balises. Comprendre comment ces composants interagissent vous aide à créer des politiques efficaces qui répondent aux besoins de votre organisation.

Configuration de l'ordre des correctifs par défaut

Lorsque vous créez une politique de déploiement de mise à niveau sans spécifier de dérogations spécifiques aux ressources, toutes les ressources utilisent par défaut un ordre de mise à niveau de

base. Vous pouvez définir cette valeur par défaut à l'aide du champ « par défaut » de votre politique. Les ressources sans attribution explicite d'ordre de mise à niveau via des balises suivront cet ordre par défaut.

> **Note**
>
> L'expérience console actuelle nécessite la spécification d'un ordre par défaut.

L'exemple suivant montre comment configurer toutes les ressources pour qu'elles reçoivent les mises à niveau en dernier par défaut, sauf si elles sont remplacées par des balises. Cette approche est utile lorsque vous souhaitez vous assurer que la plupart des ressources sont mises à jour ultérieurement dans le cycle de mise à niveau :

```
"upgrade_rollout": {
    "default": {
        "patch_order": "last"
    }
}
```

Modification du niveau de ressource via des balises

Vous pouvez annuler l'ordre de mise à niveau par défaut pour des ressources spécifiques à l'aide de balises. Cela vous permet de créer un contrôle granulaire sur les ressources qui reçoivent des mises à niveau et dans quel ordre. Par exemple, vous pouvez attribuer différents ordres de mise à niveau en fonction de vos types d'environnement, des étapes de développement ou de la criticité de votre charge de travail.

L'exemple suivant montre comment configurer les ressources de développement pour recevoir les mises à niveau en premier et les ressources de production pour les recevoir en dernier. Cette configuration garantit que vos environnements de développement peuvent valider les mises à niveau avant qu'elles ne soient mises en production :

```
"upgrade_rollout": {
    "tags": {
        "environment": {
            "tag_values": {
                "development": {
                    "patch_order": "first"
                },
```

```
                "production": {
                    "patch_order": "last"
                }
            }
        }
    }
}
```

Exemples de politiques de déploiement des mises à niveau

Voici les scénarios courants relatifs aux politiques de déploiement des mises à niveau :

Exemple 1 : environnement de développement d'abord

Cet exemple montre comment configurer les ressources de votre environnement de développement pour qu'elles reçoivent d'abord les mises à niveau. En ciblant les ressources à l'aide de la balise d'environnement « développement », vous vous assurez que vos environnements de développement sont les premiers à recevoir et à valider les nouvelles mises à niveau. Ce modèle permet d'identifier les problèmes potentiels avant que les mises à niveau n'atteignent des environnements plus critiques :

```
{
    "tags": {
        "environment": {
            "tag_values": {
                "development": {
                    "upgrade_order": "first"
                }
            }
        }
    }
}
```

Exemple 2 : dernier environnement de production

Cet exemple montre comment garantir que vos environnements de production reçoivent les mises à niveau en dernier. En affectant explicitement les ressources étiquetées en production à la dernière commande de mise à niveau, vous maintenez la stabilité de votre environnement de production tout en permettant des tests adéquats dans les environnements de pré-production. Cette approche est particulièrement utile pour les organisations ayant des exigences strictes en matière de gestion du changement :

```
{
    "tags": {
        "environment": {
            "tag_values": {
                "production": {
                    "upgrade_order": "last"
                }
            }
        }
    }
}
```

Exemple 3 : plusieurs ordres de mise à niveau utilisant des balises

L'exemple suivant montre comment utiliser une clé de balise unique avec des valeurs différentes pour spécifier les trois ordres de mise à niveau. Cette approche est utile lorsque vous souhaitez gérer les commandes de mise à niveau via un schéma de balisage unique :

```
{
   "upgrade_rollout":{
      "default":{
         "patch_order":{
            "@@assign":"last"
         }
      },
      "tags":{
         "devtag":{
            "tag_values":{
               "tag1":{
                  "patch_order":{
                     "@@assign":"first"
                  }
               },
               "tag2":{
                  "patch_order":{
                     "@@assign":"second"
                  }
               },
               "tag3":{
                  "patch_order":{
                     "@@assign":"last"
                  }
               }
```

```
            }
         }
      }
   }
}
```

# Politiques Amazon S3

Les politiques Amazon S3 vous permettent de gérer de manière centralisée les configurations des ressources Amazon S3 à grande échelle sur l'ensemble des comptes d'une organisation. Les politiques Amazon S3 prennent actuellement en charge les paramètres de blocage de l'accès public.

Vous pouvez utiliser une politique Amazon S3 pour spécifier s'il faut activer ou désactiver les quatre paramètres de blocage de l'accès public, et cette spécification s'appliquera à toutes les ressources Amazon S3 au sein des comptes sélectionnés. Vous pouvez utiliser les paramètres de blocage de l'accès public dans une politique Amazon S3 pour appliquer une posture de sécurité cohérente au sein de votre organisation et éliminer les frais opérationnels liés à la gestion des configurations de comptes individuels.

## Comment ça marche

Lorsque vous associez une politique Amazon S3 à une entité organisationnelle, elle définit les paramètres qui s'appliquent à toutes les ressources Amazon S3 au sein des comptes relevant de cette étendue. Ces configurations remplacent les paramètres au niveau du compte, ce qui vous permet de gérer de manière centralisée les paramètres Amazon S3.

Les politiques Amazon S3 peuvent être appliquées à l'ensemble d'une organisation, à des unités organisationnelles (OUs) ou à des comptes individuels. Les comptes rejoignant une organisation hériteront automatiquement de toutes les politiques Amazon S3 en fonction de leur emplacement dans la hiérarchie de l'organisation.

Comportement de détachement : si une politique Amazon S3 est dissociée, les comptes reprennent automatiquement leur configuration précédente au niveau du compte. Amazon S3 préserve les paramètres d'origine au niveau du compte afin de permettre une restauration fluide.

## Fonctions principales

- Contrôle unifié : les quatre paramètres d'accès public par blocs (BlockPublicAcls, BlockPublicPolicy, IgnorePublicAcls, RestrictPublicBuckets) sont contrôlés ensemble en tant que configuration unique

- Héritage automatique : les nouveaux comptes héritent automatiquement des politiques en fonction de leur placement organisationnel
- Protection de remplacement : empêche les modifications au niveau du compte lorsque les politiques de l'organisation sont actives
- Restauration fluide : les paramètres du compte d'origine sont préservés et restaurés lorsque les politiques sont détachées

## Conditions préalables

Avant d'utiliser les politiques Amazon S3, assurez-vous d'avoir :

- Une AWS organisation en mode toutes les fonctionnalités
- Autorisations pour gérer AWS les politiques des organisations (organisations : CreatePolicyAttachPolicy, organisations :, etc.)
- Le type de politique Amazon S3 activé pour votre organisation

## Bonnes pratiques relatives à l'utilisation des politiques Amazon S3

Lors de la mise en œuvre des politiques Amazon S3 au sein de votre organisation, le respect des meilleures pratiques établies permet de garantir un déploiement et une maintenance réussis.

Commencez simplement en réalisant de petites modifications

Pour simplifier le débogage, commencez par des politiques simples et apportez des modifications à un élément à la fois. Validez le comportement et l'impact de chaque modification avant d'effectuer la suivante. Vous réduisez ainsi le nombre de variables dont vous devez tenir compte lorsqu'une erreur ou un résultat inattendu se produit.

Mettre en place des processus de révision

Mettez en œuvre des processus pour surveiller les nouveaux attributs des politiques, évaluer les exceptions aux politiques et apporter des ajustements afin de maintenir l'alignement sur les exigences opérationnelles et de sécurité de votre organisation.

Validez les modifications apportées à vos politiques Amazon S3 à l'aide de DescribeEffectivePolicy

Après avoir modifié une politique Amazon S3, vérifiez les politiques en vigueur pour les comptes représentatifs situés en dessous du niveau auquel vous avez apporté la modification. Vous

pouvez consulter la politique effective à l'aide de la console AWS de gestion, de l'opération DescribeEffectivePolicy API ou de l'une de ses variantes de AWS CLI ou de AWS SDK. Assurez-vous que la modification que vous avez apportée a eu l'impact escompté sur la politique effective.

Communiquez et entraînez-vous

Assurez-vous que votre organisation comprend l'objectif et l'impact de vos politiques. Fournissez des conseils clairs sur les comportements attendus et sur la manière de gérer les défaillances dues à l'application des politiques.

Planifier pour répondre aux besoins légitimes d'accès du public

Avant de mettre en œuvre des politiques au niveau de l'organisation, identifiez les comptes qui nécessitent des compartiments Amazon S3 publics à des fins commerciales légitimes (telles que l'hébergement de sites Web statiques). Envisagez d'utiliser l'attachement à une politique au niveau de l'unité d'organisation ou au niveau du compte pour exclure ces comptes, ou pour regrouper les besoins en compartiments publics dans des comptes dédiés.

Surveiller l'application des politiques

AWS CloudTrail À utiliser pour surveiller l'attachement aux politiques et les mesures d'application. Définissez EventBridge des règles pour automatiser les réponses aux violations ou aux modifications des politiques.

## Syntaxe et exemples de politiques Amazon S3

Une politique Amazon S3 est un fichier en texte brut structuré selon les règles du JSON. La syntaxe des politiques Amazon S3 suit celle de tous les types de politiques de gestion. Pour de plus amples informations, veuillez consulter Fonctionnement de l'héritage des politiques de gestion. Cette rubrique se concentre sur l'application de cette syntaxe générale aux exigences spécifiques des politiques Amazon S3 et aux paramètres de blocage de l'accès public qu'elles permettent de gérer.

L'exemple de politique Amazon S3 suivant montre la syntaxe de base de la politique :

```
{
    "s3_attributes": {
        "public_access_block_configuration": {
            "@@assign": "all"
        }
    }
```

```
}
```

La syntaxe de la politique Amazon S3 inclut les éléments suivants

`s3_attributes`

La clé de niveau supérieur pour la configuration des politiques Amazon S3.

`public_access_block_configuration`

Définit le comportement de blocage de l'accès public pour l'organisation.

`@@assign`

L'opérateur d'affectation qui accepte l'une des deux valeurs suivantes :

- `"all"`- Active les quatre paramètres d'accès public par bloc d'Amazon S3 au niveau de l'organisation
- `"none"`- Désactive le contrôle au niveau de l'organisation, permettant aux comptes individuels de gérer leurs propres paramètres de blocage de l'accès public

Amazon S3 Block Public Access possède quatre paramètres qui contrôlent l'accès public :

1. BlockPublicAcls- Amazon S3 bloquera les autorisations d'accès public appliquées aux buckets ou objets récemment ajoutés, et empêchera la création de nouvelles listes de contrôle d'accès public (ACLs) pour les buckets et objets existants. Ce paramètre ne modifie aucune autorisation existante qui autorise l'accès public aux ressources Amazon S3 à l'aide de ACLs.
2. BlockPublicPolicy- Amazon S3 bloquera les nouvelles politiques relatives aux compartiments et aux points d'accès qui accordent un accès public aux compartiments et aux objets. Ce paramètre ne modifie aucune politique existante qui autorise l'accès public aux ressources Amazon S3.
3. IgnorePublicAcls- Amazon S3 ignorera tout ACLs ce qui accorde un accès public aux compartiments et aux objets.
4. RestrictPublicBuckets- Amazon S3 ignorera l'accès public et entre comptes pour les compartiments ou les points d'accès avec des politiques qui accordent un accès public aux compartiments et aux objets.

Lorsque vous définissez `@@assign` cette option`"all"`, les quatre paramètres sont consolidés et activés au niveau de l'organisation, offrant ainsi une protection complète contre l'accès public à tous les comptes de votre organisation.

# AWS Shield Politiques du directeur de la sécurité réseau

AWS Shield Network Security Director permet de sécuriser votre AWS environnement en découvrant vos ressources informatiques, réseau et de sécurité réseau. Le directeur de la sécurité réseau évalue la configuration de sécurité de chaque ressource en analysant la topologie du réseau et les configurations de sécurité par rapport aux AWS meilleures pratiques et aux informations sur les menaces.

AWS Shield Les politiques de Network Security Director vous permettent d'activer et de gérer de manière centralisée Network Security Director sur tous les comptes de votre AWS organisation. Avec une politique Network Security Director, vous spécifiez les entités organisationnelles (root ou comptes) sur lesquelles Network Security Director est activé. OUs Lorsque des comptes rejoignent votre organisation, ils héritent automatiquement des politiques applicables en fonction de leur emplacement dans la hiérarchie organisationnelle. Cela garantit que vos ressources sont analysées pour détecter les lacunes de configuration de la sécurité réseau à mesure que votre entreprise se développe. Les politiques respectent les structures organisationnelles existantes et offrent une certaine flexibilité pour déterminer quels comptes sont analysés.

AWS Shield Network Security Director est actuellement disponible en version préliminaire.

## Comment ça marche

Lorsque vous associez une politique AWS Shield Network Security Director à une entité organisationnelle, la politique active automatiquement Network Security Director pour tous les comptes membres compris dans cette zone. En outre, si vous avez finalisé la configuration de AWS Shield Network Security Director en enregistrant un administrateur délégué, ce compte bénéficiera d'une visibilité centralisée sur le niveau de sécurité réseau des comptes de l'organisation sur lesquels AWS Shield Network Security Director est activé.

AWS Shield Les politiques du Network Security Director peuvent être appliquées à l'ensemble de l'organisation, à des unités organisationnelles spécifiques (OUs) ou à des comptes individuels. Les comptes qui rejoignent l'organisation, ou qui migrent vers une unité d'organisation associée à une politique, héritent automatiquement de la politique et ont le AWS Shield Network Security Director activé et lié à l'administrateur délégué du Network Security Director. Les politiques du Network Security Director vous permettent d'effectuer une analyse du réseau, de consulter la topologie du réseau et les résultats de sécurité du réseau pour vos ressources, et de recevoir des recommandations pour remédier aux lacunes de configuration. Les paramètres de configuration spécifiques et la suppression des résultats individuels peuvent être gérés via le compte d'administrateur délégué du Network Security Director de l'organisation.

Lorsque vous associez une politique AWS Shield Network Security Director à votre organisation ou unité organisationnelle, AWS Organizations évalue automatiquement la politique et l'applique en fonction du périmètre que vous définissez. La logique d'application des politiques suit des règles spécifiques de résolution des conflits :

- Lorsque des régions apparaissent à la fois dans les listes d'activation et de désactivation, la configuration de désactivation est prioritaire. Par exemple, si une région est répertoriée dans les configurations d'activation et de désactivation, AWS Shield Network Security Director sera désactivé dans cette région.
- Lorsque l'activation `ALL_SUPPORTED` est spécifiée, AWS Shield Network Security Director est activé dans toutes les régions actuelles et futures, sauf s'il est explicitement désactivé. Cela vous permet de maintenir une couverture complète à mesure que vous vous AWS étendez dans de nouvelles régions.

## Commencer à utiliser les politiques de AWS Shield Network Security Director

Avant de configurer les politiques de Network Security Director, assurez-vous de bien comprendre les prérequis et les exigences de mise en œuvre. Cette rubrique vous guide tout au long du processus de configuration et de gestion de ces politiques au sein de votre organisation.

Avant de commencer

Passez en revue les exigences suivantes avant de mettre en œuvre les politiques du AWS Shield Network Security Director :

- Votre compte doit faire partie d'une AWS organisation
- Vous devez être connecté sous l'une des formes suivantes :
  - Le compte de gestion de l'organisation
  - Administrateur délégué d'une AWS organisation autorisé à gérer les politiques AWS Shield du Network Security Director
- Vous devez activer l'accès sécurisé pour Network Security Director dans votre organisation
- Vous devez activer le type de politique Network Security Director à la racine de votre organisation

Vérifiez également que :

- AWS Shield Network Security Director est pris en charge dans les régions où vous souhaitez appliquer des politiques

- Le rôle lié au service AWS Shield Network Security Director est configuré dans votre compte de gestion. Si vous devez créer ce rôle, vous pouvez le créer directement en exécutant`aws iam create-service-linked-role --aws-service-name network-director.amazonaws.com`.

### Étapes d'implémentation

Pour mettre en œuvre efficacement les politiques du Network Security Director, suivez ces étapes dans l'ordre. Chaque étape garantit une configuration correcte et permet d'éviter les problèmes courants lors de l'installation. Ces étapes peuvent être effectuées via la AWS Organizations console, l'interface de ligne de AWS commande (AWS CLI) ou AWS SDKs.

1. Activez un accès sécurisé pour AWS Shield Network Security Director.
2. Activez les politiques du AWS Shield Network Security Director pour votre organisation.
3. Créez une politique de directeur de sécurité AWS Shield réseau.
4. Associez la politique à la racine, à l'unité d'organisation ou au compte de votre organisation.
5. Consultez la politique combinée efficace du directeur de la sécurité réseau qui s'applique à un compte.

## AWS Shield Syntaxe et exemples de politique du Network Security Director

Les politiques de Network Security Director suivent une syntaxe JSON standardisée qui définit la manière dont Network Security Director est activé et configuré au sein de votre organisation. Une politique AWS Shield Network Security Director est un document JSON structuré selon la syntaxe de la politique de gestion des AWS Organizations. Il définit les entités organisationnelles pour lesquelles AWS Shield Network Security Director sera automatiquement activé.

### Structure politique de base

Une politique de AWS Shield Network Security Director utilise cette structure de base :

```
{
    "network_security_director": {
        "enablement": {
            "network_security_scan": {
                "enable_in_regions": {
                    "@@assign": ["us-east-1", "eu-west-1"]
                },
```

```
                "disable_in_regions": {
                    "@@assign": []
                    }
                }
            },
        }
    }
}
```

Composants de politique

AWS Shield Les politiques du Network Security Director contiennent les éléments clés suivants :

`network_security_director`

La clé de niveau supérieur pour les documents de politique de Network Security Director, qui est requise pour toutes les politiques de Network Security Director.

`enablement`

Définit le mode d'activation du Network Security Director au sein de l'organisation et contient les configurations de scan.

`network_security_scan`

Définit la configuration d'application pour l'analyse de sécurité du réseau.

`enable_in_regions`

Identifiant de configuration pour les paramètres régionaux. Définit l'endroit où le scan de sécurité réseau doit être activé.

`disable_in_regions`

Identifiant de configuration pour les paramètres régionaux. Définit l'endroit où le scan de sécurité réseau doit être désactivé.

# Administrateur délégué pour AWS Organizations

Nous vous recommandons d'utiliser le compte AWS Organizations de gestion, ses utilisateurs et ses rôles uniquement pour les tâches qui doivent être effectuées par ce compte. Nous vous recommandons également de stocker vos ressources AWS dans d'autres comptes membres de l'organisation et de les garder en dehors du compte de gestion. Cela est dû au fait que les

fonctionnalités de sécurité telles que les politiques de contrôle des services des Organisations (SCPs) ne limitent pas les utilisateurs ou les rôles dans le compte de gestion.

À partir du compte de gestion de l'organisation, vous pouvez déléguer la gestion des politiques pour les organisations à des comptes membres spécifiques afin d'effectuer des actions de politique qui ne sont par défaut disponibles que pour le compte de gestion.

Par exemple, les politiques de délégation basées sur les ressources, voir. Exemples de politiques basées sur les ressources pour AWS Organizations

Rubriques

- Créez une politique de délégation basée sur les ressources avec AWS Organizations
- Mettez à jour une politique de délégation basée sur les ressources avec AWS Organizations
- Consultez une politique de délégation basée sur les ressources avec AWS Organizations
- Supprimer une politique de délégation basée sur les ressources avec AWS Organizations

## Créez une politique de délégation basée sur les ressources avec AWS Organizations

À partir du compte de gestion, créez une politique de délégation basée sur les ressources pour votre organisation et ajoutez une déclaration indiquant quels comptes membres peuvent effectuer des actions sur les politiques. Vous pouvez ajouter plusieurs déclarations dans la politique pour indiquer un ensemble d'autorisations différent pour les comptes membres.

Autorisations minimales

Pour créer la politique de délégation basée sur les ressources, vous devez disposer des autorisations nécessaires pour exécuter les actions suivantes :

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

En outre, vous devez accorder aux rôles et aux utilisateurs du compte administrateur délégué les autorisations IAM correspondant aux actions requises. Sans autorisations IAM, on suppose que le principal appelant ne dispose pas des autorisations requises pour gérer les AWS Organizations politiques.

AWS Management Console

Ajoutez des instructions à la politique de délégation basée sur les ressources dans la AWS Management Console à l'aide de l'une des méthodes suivantes :

- Politique JSON : collez et personnalisez un exemple de politique de délégation basée sur les ressources à utiliser dans votre compte, ou saisissez votre propre document de politique JSON dans l'éditeur JSON.
- Éditeur visuel : créez une nouvelle politique de délégation dans l'éditeur visuel, qui vous guide dans la création d'une politique de délégation sans avoir à écrire de syntaxe JSON.

Utiliser l'éditeur de stratégie JSON pour créer une politique de délégation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Cliquez sur Paramètres.
3. Dans la section Administrateur délégué pour AWS Organizations, choisissez Delegate (Déléguer) pour créer la politique de délégation Organizations.
4. Entrez un document de stratégie JSON. Pour de plus amples informations sur le langage de la stratégie IAM, consultez la référence de politique JSON IAM.
5. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés durant la validation de la politique, puis sélectionnez Create policy (Créer une politique).

Utiliser l'éditeur visuel pour créer une politique de délégation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Cliquez sur Paramètres.
3. Dans la section Administrateur délégué pour AWS Organizations, choisissez Delegate (Déléguer) pour créer la politique de délégation Organizations.
4. Sur la page Create Delegation policy (Créer une politique de délégation), choisissez Add new statement (Ajouter une nouvelle déclaration).
5. Réglez l'effet sur `Allow`.

6. Ajoutez `Principal` pour définir les comptes membres auxquels vous souhaitez déléguer.
7. Dans la liste des actions, choisissez les actions que vous souhaitez déléguer. Vous pouvez utiliser les actions de filtrage pour affiner les choix.
8. Pour spécifier si le compte de membre délégué peut associer des politiques à la racine de l'organisation ou aux unités organisationnelles (OUs), définissez`Resources`. Vous devez également sélectionner `policy` comme type de ressource. Vous pouvez spécifier des ressources de la manière suivante :

   - Choisissez Add a resource (Ajouter une ressource) et créez l'ARN (Amazon Resource Name) en suivant les instructions de la boîte de dialogue.
   - Répertoriez les ressources ARNs manuellement dans l'éditeur. Pour plus d'informations sur la syntaxe de l'ARN, consultez Amazon Resource Name (ARN) dans le Guide de référence AWS général. Pour plus d'informations sur ARNs l'utilisation de l'élément ressource d'une stratégie, voir Éléments de stratégie IAM JSON : Ressource.
9. Choisissez Add a condition (Ajouter une condition) pour spécifier d'autres conditions, notamment le type de politique que vous souhaitez déléguer. Choisissez la clé de condition, la clé de balise, le qualificateur et l'opérateur de la condition, puis saisissez une **`Value`**. Lorsque vous avez terminé, choisissez Add condition (Ajouter une condition). Pour plus d'informations sur l'élément Condition, consultez Éléments de politique JSON IAM : Condition dans la référence de politique JSON IAM.
10. Pour ajouter d'autres blocs d'autorisation, choisissez Add new statement (Ajouter une nouvelle déclaration). Pour chaque bloc, répétez les étapes 5 à 9.
11. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés durant la validation de la politique, puis sélectionnez Create policy (Créer une politique) pour enregistrer votre travail.

AWS CLI & AWS SDKs

Création d'une politique de délégation

Vous pouvez utiliser la commande suivante pour créer une politique de délégation :

- AWS CLI: put-resource-policy

  L'exemple suivant crée une politique de délégation.

```
$ aws organizations put-resource-policy --content
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK : PutResourcePolicy

Actions de politique de délégation prises en charge

Les actions suivantes sont prises en charge pour la politique de délégation :

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource

- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Clés de condition prises en charge

Seules les clés de condition prises en charge par AWS Organizations peuvent être utilisées pour la politique de délégation. Pour plus d'informations, consultez la section Clés de condition pour AWS Organizations la référence d'autorisation de service.

## Mettez à jour une politique de délégation basée sur les ressources avec AWS Organizations

À partir du compte de gestion, mettez à jour une politique de délégation basée sur les ressources pour votre organisation et ajoutez une déclaration indiquant quels comptes membres peuvent effectuer des actions sur les politiques. Vous pouvez ajouter plusieurs déclarations dans la politique pour indiquer un ensemble d'autorisations différent pour les comptes membres.

Autorisations minimales

Pour mettre à jour la politique de délégation basée sur les ressources, vous devez disposer des autorisations nécessaires pour exécuter les actions suivantes :

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

En outre, vous devez accorder aux rôles et aux utilisateurs du compte administrateur délégué les autorisations IAM correspondant aux actions requises. Sans autorisations IAM, on suppose que le principal appelant ne dispose pas des autorisations requises pour gérer les AWS Organizations politiques.

AWS Management Console

Ajoutez des instructions à la politique de délégation basée sur les ressources dans la AWS Management Console à l'aide de l'une des méthodes suivantes :

- Politique JSON : collez et personnalisez un exemple de politique de délégation basée sur les ressources à utiliser dans votre compte, ou saisissez votre propre document de politique JSON dans l'éditeur JSON.
- Éditeur visuel : créez une nouvelle politique de délégation dans l'éditeur visuel, qui vous guide dans la création d'une politique de délégation sans avoir à écrire de syntaxe JSON.

Utiliser l'éditeur de stratégie JSON pour mettre à jour une politique de délégation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Cliquez sur Paramètres.
3. Dans la AWS Organizations section Administrateur délégué pour, choisissez Modifier pour mettre à jour la politique de délégation des Organisations.
4. Entrez un document de stratégie JSON. Pour de plus amples informations sur le langage de la stratégie IAM, consultez la référence de politique JSON IAM.
5. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés lors de la validation des politiques, puis choisissez Créer une politique.

Utiliser l'éditeur visuel pour mettre à jour une politique de délégation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Cliquez sur Paramètres.
3. Dans la AWS Organizations section Administrateur délégué pour, choisissez Modifier pour mettre à jour la politique de délégation des Organisations.
4. Sur la page Create Delegation policy (Créer une politique de délégation), choisissez Add new statement (Ajouter une nouvelle déclaration).
5. Réglez l'effet sur `Allow`.
6. Ajoutez `Principal` pour définir les comptes membres auxquels vous souhaitez déléguer.
7. Dans la liste des actions, choisissez les actions que vous souhaitez déléguer. Vous pouvez utiliser les actions de filtrage pour affiner les choix.

8. Pour spécifier si le compte de membre délégué peut associer des politiques à la racine de l'organisation ou aux unités organisationnelles (OUs), définissez`Resources`. Vous devez également sélectionner `policy` comme type de ressource. Vous pouvez spécifier des ressources de la manière suivante :

   - Choisissez Add a resource (Ajouter une ressource) et créez l'ARN (Amazon Resource Name) en suivant les instructions de la boîte de dialogue.
   - Répertoriez les ressources ARNs manuellement dans l'éditeur. Pour plus d'informations sur la syntaxe de l'ARN, consultez Amazon Resource Name (ARN) dans le Guide de référence AWS général. Pour plus d'informations sur ARNs l'utilisation de l'élément ressource d'une stratégie, voir Éléments de stratégie IAM JSON : Ressource.

9. Choisissez Add a condition (Ajouter une condition) pour spécifier d'autres conditions, notamment le type de politique que vous souhaitez déléguer. Choisissez la clé de condition, la clé de balise, le qualificateur et l'opérateur de la condition, puis saisissez une **`Value`**. Lorsque vous avez terminé, choisissez Add condition (Ajouter une condition). Pour plus d'informations sur l'élément Condition, consultez Éléments de politique JSON IAM : Condition dans la référence de politique JSON IAM.
10. Pour ajouter d'autres blocs d'autorisation, choisissez Add new statement (Ajouter une nouvelle déclaration). Pour chaque bloc, répétez les étapes 5 à 9.
11. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés lors de la validation de la politique, puis choisissez Enregistrer la politique.

AWS CLI & AWS SDKs

Création ou mise à jour d'une politique de délégation

Vous pouvez utiliser les commandes suivantes pour mettre à jour une politique de délégation :

- AWS CLI: put-resource-policy

  L'exemple suivant crée ou met à jour la politique de délégation.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK : PutResourcePolicy

Actions de politique de délégation prises en charge

Les actions suivantes sont prises en charge pour la politique de délégation :

- `AttachPolicy`
- `CreatePolicy`
- `DeletePolicy`

- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource

- `UpdatePolicy`

Clés de condition prises en charge

Seules les clés de condition prises en charge par AWS Organizations peuvent être utilisées pour la politique de délégation. Pour plus d'informations, consultez la section Clés de condition pour AWS Organizations la référence d'autorisation de service.

## Consultez une politique de délégation basée sur les ressources avec AWS Organizations

À partir du compte de gestion, consultez la politique de délégation basée sur les ressources de votre organisation pour comprendre quels administrateurs délégués ont accès à la gestion de quels types de politiques.

> **Autorisations minimales**
>
> Pour créer ou mettre à jour la politique de délégation basée sur les ressources, vous devez disposer de l'autorisation d'exécuter les actions suivantes : `organizations:DescribeResourcePolicy`.

AWS Management Console

Pour afficher une politique de délégation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Cliquez sur Paramètres.
3. Dans la section Administrateur délégué pour AWS Organizations, faites défiler la page pour afficher la politique de délégation complète.

AWS CLI & AWS SDKs

Afficher une politique de délégation

Vous pouvez utiliser la commande suivante pour supprimer une politique de délégation :

- AWS CLI: describe-resource-policy

  L'exemple suivant extrait la politique.

  ```
  $ aws organizations describe-resource-policy
  ```

- AWS SDK : DescribeResourcePolicy

## Supprimer une politique de délégation basée sur les ressources avec AWS Organizations

Lorsque vous n'avez plus besoin de déléguer la gestion des politiques dans votre organisation, vous pouvez supprimer la stratégie de délégation basée sur les ressources du compte de gestion de l'organisation.

> **Important**
>
> Si vous supprimez votre politique de délégation basée sur les ressources, vous ne pouvez pas la récupérer.

> **Autorisations minimales**
>
> Pour supprimer la politique de délégation basée sur les ressources, vous devez disposer de l'autorisation d'exécuter les actions suivantes : `organizations:DeleteResourcePolicy`.

AWS Management Console

Pour supprimer une politique de délégation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Cliquez sur Paramètres.
3. Dans la section Administrateur délégué pour AWS Organizations, choisissez Supprimer.

4. Dans la boîte de dialogue de confirmation Delete Policy (Supprimer la politique), tapez **`delete`**. Choisissez Delete policy (Supprimer la politique).

AWS CLI & AWS SDKs

Supprimer une politique de délégation

Vous pouvez utiliser la commande suivante pour supprimer une politique de délégation :

- AWS CLI: delete-resource-policy

  L'exemple suivant supprime la politique.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK : DeleteResourcePolicy

## Désactivation d'un type de politique

Avant de pouvoir créer et attacher une politique à votre organisation, vous devez activer l'utilisation de ce type de politique. L'activation d'un type de politique se fait une fois pour toutes à la racine de l'organisation. Vous pouvez activer un type de politique uniquement à partir du compte de gestion de l'organisation ou d'un compte de membre désigné comme administrateur délégué.

Autorisations minimales

Pour activer un type de politique, vous devez avoir l'autorisation d'exécuter les actions suivantes :

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:ListRoots` — requis uniquement si vous utilisez la console Organizations

### AWS Management Console

Pour activer un type de politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques, choisissez le nom du type de politique que vous souhaitez activer.
3. Sur la page du type de politique, choisissez Activer ***policy type***.

   La page est remplacée par une liste des politiques disponibles du type spécifié.

### AWS CLI & AWS SDKs

Pour activer un type de politique

Vous pouvez utiliser l'une des commandes suivantes pour activer un type de politique :

- AWS CLI: enable-policy-type

L'exemple suivant montre comment activer les politiques de sauvegarde pour votre organisation. Notez que vous devez spécifier l'ID de la racine de votre organisation.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

La liste des `PolicyTypes` dans la sortie inclut désormais le type de politique spécifié avec le `Status` « `ENABLED` ».

- AWS SDKs: EnablePolicyType

# Désactivation d'un type de politique

Si vous ne souhaitez plus utiliser un certain type de politique dans votre organisation, vous pouvez désactiver ce type pour empêcher son utilisation accidentelle. Vous pouvez désactiver un type de politique uniquement pour le compte de gestion de l'organisation ou pour un compte de membre désigné comme administrateur délégué.

## Considérations

Les politiques désactivées sont détachées de toutes les entités mais ne sont pas supprimées

Lorsque vous désactivez un type de politique, toutes les politiques du type spécifié sont automatiquement détachées de toutes les entités de la racine de l'organisation. Les politiques ne sont pas supprimées.

(Type de politique de contrôle des services uniquement) Toutes les entités de la racine sont initialement attachées uniquement au **`FullAWSAccess`** SCP par défaut

(Type de politique SCP uniquement) Si vous réactivez le type de politique SCP ultérieurement, toutes les entités de la racine de l'organisation sont initialement attachées uniquement à la SCP `FullAWSAccess` par défaut. Les pièces jointes SCPs aux entités sont perdues lorsqu'elles SCPs sont désactivées dans l'organisation. Si vous souhaitez les réactiver ultérieurement SCPs, vous devez les rattacher à la racine de l'organisation et aux comptes OUs, le cas échéant.

## Désactiver un type de politique

Autorisations minimales

Pour désactiver SCPs, vous devez être autorisé à exécuter les actions suivantes :

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations

- `organizations:ListRoots` — requis uniquement si vous utilisez la console Organizations

### AWS Management Console

Pour désactiver un type de politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques, choisissez le nom du type de politique que vous souhaitez désactiver.
3. Sur la page du type de politique, choisissez Désactiver ***policy type***.
4. Dans la boîte de dialogue de confirmation, saisissez le mot **`disable`**, puis choisissez Désactiver.

   La liste des politiques disponibles du type spécifié disparaît.

### AWS CLI & AWS SDKs

Pour désactiver un type de politique

Vous pouvez utiliser l'une des commandes suivantes pour désactiver un type de politique :

- AWS CLI: disable-policy-type

  L'exemple suivant montre comment désactiver les politiques de sauvegarde pour votre organisation. Notez que vous devez spécifier l'ID de la racine de votre organisation.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
```

```
    }
}
```

La liste des `PolicyTypes` dans la sortie n'inclut plus le type de politique spécifié.

- AWS SDKs: DisablePolicyType

# Création de politiques d'organisation avec AWS Organizations

Après avoir activé les politiques pour votre organisation, vous pouvez créer une politique.

Cette rubrique décrit comment créer des politiques avec AWS Organizations. Une politique définit les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS.

Rubriques

- Création d'une politique de contrôle des services (SCP)
- Création d'une politique de contrôle des ressources (RCP)
- Création d'une politique déclarative
- Création d'une politique de sauvegarde
- Création d'une politique en matière de balises
- Création d'une politique pour les applications de chat
- Créer une politique de désinscription des services d'IA
- Création d'une politique de déploiement des mises à niveau
- Création d'une politique Security Hub

## Création d'une politique de contrôle des services (SCP)

Autorisations minimales

Pour créer SCPs, vous devez être autorisé à exécuter l'action suivante :

- `organizations:CreatePolicy`

AWS Management Console

Pour créer une politique de contrôle des services

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de contrôle des services, choisissez Créer une politique.
3. Dans la page Créer une politique de contrôle des services, saisissez un Nom de politique et éventuellement une Description de la politique.
4. (Facultatif) Ajoutez une ou plusieurs balises en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, consultez Ressources de balisage AWS Organizations.

   > **Note**
   >
   > Dans la plupart des étapes qui suivent, nous discutons de l'utilisation des contrôles sur le côté droit de l'éditeur JSON pour construire la politique, élément par élément. Alternativement, vous pouvez, à tout moment, simplement saisir du texte dans l'éditeur JSON sur le côté gauche de la fenêtre. Vous pouvez taper directement ou procéder par copier-coller.

5. Pour créer la politique, les étapes ultérieures varient selon que vous souhaitez ajouter une instruction qui refuse ou autorise l'accès. Pour de plus amples informations, veuillez consulter Évaluation du SCP. Si vous utilisez `Deny` des instructions, vous disposez d'un contrôle supplémentaire car vous pouvez restreindre l'accès à des ressources spécifiques, définir SCPs les conditions d'entrée en vigueur et utiliser l'NotActionélément. Pour de plus amples informations sur la syntaxe, consultez Syntaxe d'une stratégie de contrôle de service.

   Pour ajouter une instruction qui refuse l'accès :

   a. Dans le volet droit Modifier le relevé de l'éditeur, sous Ajouter des actions, sélectionnez un AWS service.

      À mesure que vous choisissez des options sur la droite, l'éditeur JSON est mis à jour pour afficher la politique JSON correspondante à gauche.

b. Lorsque vous sélectionnez un service, une liste s'ouvre qui contient les actions disponibles pour ce service. Vous pouvez choisir Toutes les actions ou choisir une ou plusieurs actions individuelles que vous souhaitez refuser.

   L'éditeur JSON situé à gauche se met à jour pour inclure les actions que vous avez sélectionnées.

   > **Note**
   >
   > Si vous sélectionnez une action individuelle, puis revenez en arrière et sélectionnez également Toutes les actions, l'entrée attendue pour `servicename:*` est ajoutée au JSON, mais les actions individuelles que vous avez précédemment sélectionnées sont laissées dans le JSON et ne sont pas supprimées.

c. Si vous souhaitez ajouter des actions à partir de services supplémentaires, vous pouvez choisir Tous les services en haut de la zone Instruction, puis répéter les deux étapes précédentes selon vos besoins.

d. Spécifiez les ressources à inclure dans l'instruction.

   - À côté de Ajouter une ressource, choisissez Ajouter.
   - Dans la boîte de dialogue Ajouter une ressource, choisissez dans la liste le service dont les ressources doivent être contrôlées. Vous ne pouvez choisir que parmi les services que vous avez sélectionnés à l'étape précédente.
   - Sous Type de ressource, choisissez le type de ressource que vous souhaitez contrôler.
   - Enfin, complétez l'Amazon Resource Name (ARN) dans ARN de la ressource pour identifier la ressource spécifique dont vous souhaitez contrôler l'accès. Vous devez remplacer tous les espaces réservés qui sont entourés d'accolades `{}`. Vous pouvez spécifier des caractères génériques (`*`) là où la syntaxe ARN de ce type de ressource le permet. Reportez-vous à la documentation d'un type de ressource spécifique pour plus d'informations sur l'emplacement où vous pouvez utiliser des caractères génériques.
   - Enregistrez votre ajout à la politique en choisissant Ajouter la ressource. L'élément `Resource` dans le JSON reflète vos ajouts ou modifications. L'élément Ressource est obligatoire.

> **Tip**
>
> Pour spécifier toutes les ressources pour le service sélectionné, choisissez Toutes les ressources dans la liste ou modifiez directement l'instruction `Resource` dans le JSON pour lire `"Resource":"*"`.

e. (Facultatif) Pour spécifier des conditions qui limitent le moment où une instruction de politique est en vigueur, à côté de Ajouter une condition, choisissez Ajouter.

- Clé de condition : dans la liste, vous pouvez choisir n'importe quelle clé de condition disponible pour tous les AWS services (par exemple,`aws:SourceIp`) ou une clé spécifique au service pour un seul des services que vous avez sélectionnés pour cette instruction.
- Qualificateur — (Facultatif) Lorsque la demande comporte plusieurs valeurs pour une clé de contexte à valeurs multiples, vous pouvez spécifier un qualificatif pour tester les demandes par rapport aux valeurs. Pour plus d'informations, reportez-vous à la section Clés contextuelles à valeur unique ou à valeurs multiples dans le guide de l'utilisateur IAM. Pour vérifier si une demande peut avoir plusieurs valeurs, consultez les actions, les ressources et les clés de condition Services AWS dans la référence d'autorisation de service.
  - Par défaut – Teste une valeur unique de la demande par rapport à la valeur de la clé de condition de la politique. La condition renvoie la valeur Vrai si la valeur dans la demande correspond à la valeur de la politique. Si la politique spécifie plusieurs valeurs, elles sont traitées comme un test « ou » et la condition renvoie Vrai si les valeurs de la demande correspondent à l'une des valeurs de la politique.
  - Pour n'importe quelle valeur dans une demande – Lorsque la demande peut avoir plusieurs valeurs, cette option teste si au moins une des valeurs de demande correspond à au moins l'une des valeurs de clé de condition de la politique. La condition renvoie la valeur Vrai si l'une des valeurs de clé de la demande correspond à l'une des valeurs de condition de la politique. Si aucune clé ne correspond ou si l'ensemble de données est inexistant (null), la condition renvoie la valeur Faux.
  - Pour toutes les valeurs d'une demande – Lorsque la demande peut avoir plusieurs valeurs, cette option teste si chaque valeur de la demande correspond à une valeur de clé de condition dans la politique. La condition renvoie la valeur Vrai si chaque

valeur de clé de la demande correspond à au moins une valeur de la politique. Elle renvoie également la valeur Vrai si la demande ne comprend pas de clés ou si les valeurs de clé aboutissent à un ensemble de données nul, tel qu'une chaîne vide.

- Opérateur – L'opérateurspécifie le type de comparaison à effectuer. Les options présentées dépendent du type de données de la clé de condition. Par exemple, la clé de condition globale `aws:CurrentTime` vous permet de choisir parmi l'un des opérateurs de comparaison de dates ou `Null`, que vous pouvez utiliser pour tester si la valeur est présente dans la demande.

  Pour n'importe quel opérateur de condition, à l'exception du `Null` test, vous pouvez choisir l'IfExistsoption.

- Valeur – (Facultatif) Spécifiez une ou plusieurs valeurs pour lesquelles vous souhaitez tester la demande.

Choisissez Ajouter une condition.

Pour de plus amples informations sur les clés de condition, consultez Éléments de politique JSON IAM : Condition dans le Guide de l'utilisateur IAM.

6. Pour ajouter une instruction qui autorise l'accès :

   a. Dans l'éditeur JSON à gauche, changez la ligne `"Effect": "Deny"` en `"Effect": "Allow"`.

   À mesure que vous choisissez des options sur la droite, l'éditeur JSON est mis à jour pour afficher la politique JSON correspondante à gauche.

   b. Lorsque vous sélectionnez un service, une liste s'ouvre qui contient les actions disponibles pour ce service. Vous pouvez choisir Toutes les actions ou choisir une ou plusieurs actions individuelles que vous souhaitez autoriser.

   L'éditeur JSON situé à gauche se met à jour pour inclure les actions que vous avez sélectionnées.

   > **Note**
   >
   > Si vous sélectionnez une action individuelle, puis revenez en arrière et sélectionnez également Toutes les actions, l'entrée attendue pour *`servicename`*`:*` est ajoutée au JSON, mais les actions individuelles que vous

avez précédemment sélectionnées sont laissées dans le JSON et ne sont pas supprimées.

c. Si vous souhaitez ajouter des actions à partir de services supplémentaires, vous pouvez choisir Tous les services en haut de la zone Instruction, puis répéter les deux étapes précédentes selon vos besoins.

7. (Facultatif) Pour ajouter une instruction supplémentaire à la politique, choisissez Ajouter une instruction) et utilisez l'éditeur visuel pour créer la prochaine instruction.
8. Lorsque vous avez fini d'ajouter des instructions, choisissez Créer la politique) pour enregistrer la politique de contrôle des services (SCP) achevée.

Votre nouvelle politique SCP s'affiche dans la liste des politiques de l'organisation. Vous pouvez désormais associer votre SCP à la racine ou aux comptes. OUs

AWS CLI & AWS SDKs

Pour créer une politique de contrôle des services

Vous pouvez utiliser l'une des commandes suivantes pour créer une politique SCP :

- AWS CLI : create-policy

  L'exemple suivant suppose que vous disposez d'un fichier nommé `Deny-IAM.json` contenant le texte de politique JSON. Il utilise ce fichier pour créer une nouvelle politique de contrôle des services.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
```

```
        },
         "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> SCPs n'ont aucun effet sur le compte de gestion et dans quelques autres situations. Pour de plus amples informations, veuillez consulter Tâches et entités non limitées par SCPs.

## Création d'une politique de contrôle des ressources (RCP)

> **Autorisations minimales**
>
> Pour créer RCPs, vous devez être autorisé à exécuter l'action suivante :
>
> - `organizations:CreatePolicy`

AWS Management Console

Pour créer une politique de contrôle des ressources

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Stratégie de contrôle des ressources, choisissez Créer une politique.
3. Sur la page Créer une nouvelle stratégie de contrôle des ressources, entrez le nom de la stratégie et une description de la stratégie facultative.
4. (Facultatif) Ajoutez une ou plusieurs balises en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, consultez Ressources de balisage AWS Organizations.

> **Note**
>
> Dans la plupart des étapes qui suivent, nous discutons de l'utilisation des contrôles sur le côté droit de l'éditeur JSON pour construire la politique, élément par élément. Alternativement, vous pouvez, à tout moment, simplement saisir du texte dans l'éditeur JSON sur le côté gauche de la fenêtre. Vous pouvez taper directement ou procéder par copier-coller.

5. Pour ajouter une déclaration, procédez comme suit :

   a. Dans le volet droit Modifier le relevé de l'éditeur, sous Ajouter des actions, sélectionnez un AWS service.

      À mesure que vous choisissez des options sur la droite, l'éditeur JSON est mis à jour pour afficher la politique JSON correspondante à gauche.

   b. Lorsque vous sélectionnez un service, une liste s'ouvre qui contient les actions disponibles pour ce service. Vous pouvez choisir Toutes les actions ou choisir une ou plusieurs actions individuelles que vous souhaitez refuser.

      L'éditeur JSON situé à gauche se met à jour pour inclure les actions que vous avez sélectionnées.

      > **Note**
      >
      > Si vous sélectionnez une action individuelle, puis revenez en arrière et sélectionnez également Toutes les actions, l'entrée attendue pour `servicename:*` est ajoutée au JSON, mais les actions individuelles que vous avez précédemment sélectionnées sont laissées dans le JSON et ne sont pas supprimées.

   c. Si vous souhaitez ajouter des actions à partir de services supplémentaires, vous pouvez choisir Tous les services en haut de la zone Instruction, puis répéter les deux étapes précédentes selon vos besoins.

   d. Spécifiez les ressources à inclure dans l'instruction.

      - À côté de Ajouter une ressource, choisissez Ajouter.

- Dans la boîte de dialogue Ajouter une ressource, choisissez dans la liste le service dont les ressources doivent être contrôlées. Vous ne pouvez choisir que parmi les services que vous avez sélectionnés à l'étape précédente.
- Sous Type de ressource, choisissez le type de ressource que vous souhaitez contrôler.
- Renseignez le nom de la ressource Amazon (ARN) dans Resource ARN pour identifier la ressource spécifique à laquelle vous souhaitez contrôler l'accès. Vous devez remplacer tous les espaces réservés qui sont entourés d'accolades `{}`. Vous pouvez spécifier des caractères génériques (`*`) là où la syntaxe ARN de ce type de ressource le permet. Consultez la documentation d'un type de ressource spécifique pour savoir où vous pouvez utiliser des caractères génériques.
- Enregistrez votre ajout à la politique en choisissant Ajouter la ressource. L'élément `Resource` dans le JSON reflète vos ajouts ou modifications. L'élément Ressource est obligatoire.

> **Tip**
>
> Pour spécifier toutes les ressources pour le service sélectionné, choisissez Toutes les ressources dans la liste ou modifiez directement l'instruction `Resource` dans le JSON pour lire `"Resource":"*"`.

e. (Facultatif) Pour spécifier des conditions qui limitent le moment où une instruction de politique est en vigueur, à côté de Ajouter une condition, choisissez Ajouter.

- Clé de condition : dans la liste, vous pouvez choisir n'importe quelle clé de condition disponible pour tous les AWS services (par exemple,`aws:SourceIp`) ou une clé spécifique au service pour un seul des services que vous avez sélectionnés pour cette instruction.
- Qualificateur — (Facultatif) Lorsque la demande comporte plusieurs valeurs pour une clé de contexte à valeurs multiples, vous pouvez spécifier un qualificatif pour tester les demandes par rapport aux valeurs. Pour plus d'informations, reportez-vous à la section Clés contextuelles à valeur unique ou à valeurs multiples dans le guide de l'utilisateur IAM. Pour vérifier si une demande peut avoir plusieurs valeurs, consultez les actions, les ressources et les clés de condition Services AWS dans la référence d'autorisation de service.

- Par défaut – Teste une valeur unique de la demande par rapport à la valeur de la clé de condition de la politique. La condition renvoie la valeur Vrai si la valeur dans la demande correspond à la valeur de la politique. Si la politique spécifie plusieurs valeurs, elles sont traitées comme un test « ou » et la condition renvoie Vrai si les valeurs de la demande correspondent à l'une des valeurs de la politique.
- Pour n'importe quelle valeur dans une demande – Lorsque la demande peut avoir plusieurs valeurs, cette option teste si au moins une des valeurs de demande correspond à au moins l'une des valeurs de clé de condition de la politique. La condition renvoie la valeur Vrai si l'une des valeurs de clé de la demande correspond à l'une des valeurs de condition de la politique. Si aucune clé ne correspond ou si l'ensemble de données est inexistant (null), la condition renvoie la valeur Faux.
- Pour toutes les valeurs d'une demande – Lorsque la demande peut avoir plusieurs valeurs, cette option teste si chaque valeur de la demande correspond à une valeur de clé de condition dans la politique. La condition renvoie la valeur Vrai si chaque valeur de clé de la demande correspond à au moins une valeur de la politique. Elle renvoie également la valeur Vrai si la demande ne comprend pas de clés ou si les valeurs de clé aboutissent à un ensemble de données nul, tel qu'une chaîne vide.

- Opérateur – L'opérateurspécifie le type de comparaison à effectuer. Les options présentées dépendent du type de données de la clé de condition. Par exemple, la clé de condition globale `aws:CurrentTime` vous permet de choisir parmi l'un des opérateurs de comparaison de dates ou `Null`, que vous pouvez utiliser pour tester si la valeur est présente dans la demande.

  Pour n'importe quel opérateur de condition, à l'exception du `Null` test, vous pouvez choisir l'IfExistsoption.
- Valeur – (Facultatif) Spécifiez une ou plusieurs valeurs pour lesquelles vous souhaitez tester la demande.

Choisissez Ajouter une condition.

Pour de plus amples informations sur les clés de condition, consultez Éléments de politique JSON IAM : Condition dans le Guide de l'utilisateur IAM.

f. (Facultatif) Pour utiliser l'élément `NotAction` afin de refuser l'accès à toutes les actions à l'exception de celles que vous avez spécifiées, remplacez `Action` dans le panneau de gauche par `NotAction`, juste après l'élément `"Effect": "Deny",`. Pour plus

d'informations, consultez la section Éléments de politique JSON IAM : NotAction dans le guide de l'utilisateur IAM.

6. (Facultatif) Pour ajouter une instruction supplémentaire à la politique, choisissez Ajouter une instruction) et utilisez l'éditeur visuel pour créer la prochaine instruction.
7. Lorsque vous avez terminé d'ajouter des instructions, choisissez Create policy pour enregistrer le RCP terminé.

Votre nouveau RCP apparaît dans la liste des politiques de l'organisation. Vous pouvez désormais associer votre RCP à la racine ou aux comptes. OUs

AWS CLI & AWS SDKs

Pour créer une politique de contrôle des ressources

Vous pouvez utiliser l'une des commandes suivantes pour créer un RCP :

- AWS CLI : create-policy

L'exemple suivant suppose que vous disposez d'un fichier nommé `Deny-IAM.json` contenant le texte de politique JSON. Il utilise ce fichier pour créer une nouvelle politique de contrôle des ressources.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMRCP \
    --type RESOURCE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMRCP",
            "Description": "Deny all IAM actions",
            "Type": "RESOURCE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
```

```
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> RCPs n'ont aucun effet sur le compte de gestion et dans quelques autres situations. Pour de plus amples informations, veuillez consulter Ressources et entités non limitées par RCPs.

## Création d'une politique déclarative

> **Autorisations minimales**
>
> Pour créer une politique déclarative, vous devez être autorisé à exécuter l'action suivante :
>
> - `organizations:CreatePolicy`

AWS Management Console

Pour créer une politique déclarative

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques déclaratives, choisissez Créer une politique.
3. Sur la page Créer une nouvelle politique déclarative pour EC2, entrez le nom de la politique et une description de la politique facultative.
4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, veuillez consulter Ressources de balisage AWS Organizations.
5. Vous pouvez créer la politique à l'aide de l'Éditeur visuel, de la manière décrite dans cette procédure. Vous pouvez également taper ou coller du texte de politique dans l'onglet JSON.

Pour plus d'informations sur la syntaxe des politiques déclaratives, consultezSyntaxe de politique déclarative et exemples.

Si vous choisissez d'utiliser l'éditeur visuel, sélectionnez l'attribut de service que vous souhaitez inclure dans votre politique déclarative. Pour de plus amples informations, veuillez consulter Supporté Services AWS et attributs.

6. Choisissez Ajouter un attribut de service, puis configurez l'attribut selon vos spécifications. Pour des informations plus détaillées sur chaque effet, voirSyntaxe de politique déclarative et exemples.
7. Lorsque vous avez terminé la modification de votre politique, choisissez Créer la politique dans l'angle inférieur droit de la page.

AWS CLI & AWS SDKs

Pour créer une politique déclarative

Vous pouvez utiliser l'une des méthodes suivantes pour créer une politique déclarative :

- AWS CLI : create-policy

1. Créez une politique déclarative comme la suivante et stockez-la dans un fichier texte.

```
{
    "ec2_attributes": {
        "image_block_public_access": {
            "state": {
                "@@assign": "block_new_sharing"
            }
        }
    }
}
```

Cette politique déclarative précise que tous les comptes concernés par la politique doivent être configurés de telle sorte que les nouvelles Amazon Machine Images (AMIs) ne soient pas partageables publiquement. Pour plus d'informations sur la syntaxe des politiques déclaratives, consultezSyntaxe de politique déclarative et exemples.

2. Importez le fichier de politique JSON pour créer une nouvelle politique dans l'organisation. Dans cet exemple, le fichier JSON précédent était nommé `policy.json`.

```
$ aws organizations create-policy \
    --type DECLARATIVE_POLICY_EC2 \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "DECLARATIVE_POLICY_EC2"
        }
    }
}
```

- AWS SDKs: CreatePolicy

Suite des opérations

Après avoir créé une politique déclarative, évaluez l'état de préparation à l'aide du rapport sur l'état du compte. Vous pouvez ensuite appliquer vos configurations de base. Pour ce faire, vous pouvez associer la politique à la racine de l'organisation, aux unités organisationnelles (OUs), Comptes AWS au sein de votre organisation, ou à une combinaison de ces éléments.

## Création d'une politique de sauvegarde

**Autorisations minimales**

Pour créer une politique de sauvegarde, vous devez posséder l'autorisation d'exécuter l'action suivante :

- `organizations:CreatePolicy`

### AWS Management Console

Vous pouvez créer une politique de sauvegarde AWS Management Console dans le de l'une des deux manières suivantes :

- Un éditeur visuel qui vous permet de choisir des options et de générer le texte de politique JSON pour vous.
- Un éditeur de texte qui vous permet de créer directement le texte de politique JSON.

L'éditeur visuel facilite le processus, mais limite votre flexibilité. C'est un excellent moyen de créer vos premières politiques et de les utiliser facilement. Une fois que vous avez compris leur fonctionnement et que vous avez commencé à éprouver les limites de l'éditeur visuel, vous pouvez ajouter des fonctionnalités avancées à vos politiques en modifiant vous-même le texte de la politique JSON. L'éditeur visuel utilise uniquement l'opérateur de réglage de valeur @@assign et ne fournit aucun accès aux opérateurs de contrôle enfants. Vous pouvez ajouter les opérateurs de contrôle enfants uniquement si vous modifiez manuellement le texte de la politique JSON.

Pour créer une politique de sauvegarde

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de sauvegarde, choisissez Créer une politique.
3. Dans la page Créer une politique, saisissez un Nom de politique et une description facultative pour la politique.
4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.
5. Vous pouvez créer la politique à l'aide de l'Éditeur visuel, de la manière décrite dans cette procédure. Vous pouvez également taper ou coller du texte de politique dans l'onglet JSON. Pour de plus amples informations sur la syntaxe des politiques de sauvegarde, consultez Syntaxe et exemples d'une politique de sauvegarde.

   Si vous choisissez d'utiliser l'Éditeur visuel, sélectionnez les options de sauvegarde appropriées à votre scénario. Un plan de sauvegarde se compose de trois parties. Pour de

plus amples informations sur ces éléments d'un plan de sauvegarde, consultez Création d'un plan de sauvegarde et Affectation de ressources dans le Guide du développeur AWS Backup .

a. Détails généraux d'un plan de sauvegarde

   - Le Nom du plan de sauvegarde peut uniquement contenir des caractères alphanumériques, des traits d'union et de soulignement.
   - Vous devez sélectionner au moins une Région du plan de sauvegarde dans la liste. Le plan peut sauvegarder des ressources uniquement dans les Régions AWS sélectionnées.

b. Une ou plusieurs règles de sauvegarde qui spécifient comment et quand AWS Backup doit fonctionner. Chaque règle de sauvegarde définit les éléments suivants :

   - Une planification qui inclut la fréquence de la sauvegarde et la fenêtre horaire pendant laquelle la sauvegarde peut se produire.
   - Le nom du coffre-fort de sauvegarde à utiliser. Le Nom du coffre-fort de sauvegarde peut uniquement contenir des caractères alphanumériques, des traits d'union et de soulignement. Le coffre-fort de sauvegarde doit exister avant que le plan puisse s'exécuter correctement. Créez le coffre à l'aide de la AWS Backup console ou AWS CLI des commandes.
   - (Facultatif) Une ou plusieurs règles Copier vers une région pour copier également la sauvegarde dans des coffres-forts d'autres régions Régions AWS.
   - Une ou plusieurs paires de clés et de valeurs de balises à attacher aux points de restauration de sauvegarde créés à chaque exécution de ce plan de sauvegarde.
   - Des options de cycle de vie qui spécifient le moment des transitions de la sauvegarde vers le stockage à froid et sa date d'expiration.

   Choisissez Ajouter une règle pour ajouter au plan chaque règle dont vous avez besoin.

   Pour plus d'informations sur les règles de sauvegarde, consultez Règles de sauvegarde dans le Guide du développeur AWS Backup .

c. Une affectation de ressources qui spécifie celles que AWS Backup doit sauvegarder avec ce plan. L'attribution est effectuée en spécifiant les paires de balises qui permettent AWS Backup de rechercher et de faire correspondre les ressources.

   - Le Nom de l'affectation de ressources peut uniquement contenir des caractères alphanumériques, des traits d'union et de soulignement.

- Spécifiez le rôle IAM que AWS Backup doit utiliser pour effectuer la sauvegarde par son nom.

  Dans la console, vous ne spécifiez pas l'ARN (Amazon Resource Name) entier. Vous devez inclure à la fois le nom du rôle et son préfixe qui spécifie le type de rôle. Les préfixes sont généralement `role` ou `service-role`, et ils sont séparés du nom du rôle par une barre oblique ('/'). Par exemple, vous pouvez saisir `role/MyRoleName` ou `service-role/MyManagedRoleName`. Il est converti en un ARN complet pour vous lorsqu'il est stocké dans le JSON sous-jacent.

  > **Important**
  >
  > Le rôle IAM spécifié doit déjà exister dans le compte auquel la politique est appliquée. Si ce n'est pas le cas, le plan de sauvegarde peut démarrer avec succès les tâches de sauvegarde, mais celles-ci échoueront.

- Spécifiez une ou plusieurs paires constituées d'une Clé de balise de ressource et de Valeurs de balises pour identifier les ressources que vous voulez sauvegarder. S'il y a plus d'une valeur de balise, ces valeurs doivent être séparées par des virgules.

Choisissez Ajouter une affectation pour ajouter chaque affectation de ressources configurée au plan de sauvegarde.

Pour de plus amples informations, consultez Affecter des ressources à un plan de sauvegarde dans le Guide du développeur AWS Backup .

6. Lorsque vous avez terminé la création de votre politique, choisissez Créer la politique. La politique apparaît dans votre liste des politiques de sauvegarde disponibles.

AWS CLI & AWS SDKs

Pour créer une politique de sauvegarde

Vous pouvez utiliser l'une des méthodes suivantes pour créer une politique de sauvegarde :

- AWS CLI : create-policy

  Créez un plan de sauvegarde sous la forme d'un texte JSON similaire à ce qui suit et stockez-le dans un fichier texte. Pour obtenir des règles complètes pour la syntaxe, consultez Syntaxe et exemples d'une politique de sauvegarde.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII" ] }
                        }
                    }
                }
            }
    }
}
```

Ce plan de sauvegarde indique que AWS Backup doit sauvegarder toutes les ressources concernées Comptes AWS qui se trouvent dans le champ spécifié Régions AWS et dont la balise `dataType` a une valeur de`PII`.

Ensuite importez le fichier de politique JSON contenant le plan de sauvegarde pour créer une nouvelle politique dans l'organisation. Notez l'ID de politique à la fin de l'ARN de politique dans la sortie.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDKs: CreatePolicy

## Création d'une politique en matière de balises

> **Autorisations minimales**
>
> Pour créer des politiques de balises, vous avez besoin d'une autorisation pour effectuer l'action suivante :
>
> - `organizations:CreatePolicy`

Vous pouvez créer une politique en matière de AWS Management Console balises de deux manières :

- Un éditeur visuel qui vous permet de choisir des options et de générer le texte de politique JSON pour vous.
- Un éditeur de texte qui vous permet de créer directement le texte de politique JSON.

L'éditeur visuel facilite le processus, mais limite votre flexibilité. C'est un excellent moyen de créer vos premières politiques et de les utiliser facilement. Une fois que vous avez compris leur fonctionnement et que vous avez commencé à éprouver les limites de l'éditeur visuel, vous pouvez ajouter des fonctionnalités avancées à vos politiques en modifiant vous-même le texte de la politique JSON. L'éditeur visuel utilise uniquement l'opérateur de réglage de valeur @@assign et ne fournit aucun accès aux opérateurs de contrôle enfants. Vous pouvez ajouter les opérateurs de contrôle enfants uniquement si vous modifiez manuellement le texte de la politique JSON.

AWS Management Console

Vous pouvez créer une politique en matière de AWS Management Console balises de deux manières :

- Un éditeur visuel qui vous permet de choisir des options et de générer le texte de politique JSON pour vous.
- Un éditeur de texte qui vous permet de créer directement le texte de politique JSON.

L'éditeur visuel facilite le processus, mais limite votre flexibilité. C'est un excellent moyen de créer vos premières politiques et de les utiliser facilement. Une fois que vous avez compris leur fonctionnement et que vous avez commencé à éprouver les limites de l'éditeur visuel, vous pouvez ajouter des fonctionnalités avancées à vos politiques en modifiant vous-même le texte de la politique JSON. L'éditeur visuel utilise uniquement l'opérateur de réglage de valeur @@assign et ne fournit aucun accès aux opérateurs de contrôle enfants. Vous pouvez ajouter les opérateurs de contrôle enfants uniquement si vous modifiez manuellement le texte de la politique JSON.

Pour créer une politique de balises

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de balises, choisissez Créer une politique.
3. Dans la page Créer une politique, saisissez un Nom de politique et une description facultative pour la politique.

4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à l'objet de politique lui-même. Ces balises ne font pas partie de la politique. Pour cela, choisissez Ajouter une balise, puis saisissez une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, consultez Ressources de balisage AWS Organizations.
5. Vous pouvez créer la politique de balises à l'aide de l'éditeur visuel, comme décrit dans cette procédure. Vous pouvez également saisir ou coller une politique de balises dans l'onglet JSON. Pour de plus amples informations sur la syntaxe des politiques de balises, consultez Syntaxe des politiques de balises.

   Si vous choisissez d'utiliser l'éditeur visuel, spécifiez les éléments suivants :
6. Pour Nouvelle clé de balise 1, spécifiez le nom d'une clé de balise à ajouter.
7. Pour les options de conformité, vous pouvez sélectionner les options suivantes :

   a. Utilisez la capitalisation que vous avez spécifiée ci-dessus pour la clé de balise. Laissez cette option désactivée (valeur par défaut) pour spécifier que la politique de balise parent héritée, le cas échéant, doit définir le traitement au cas par cas pour la clé de balise.

      Cochez cette option si vous souhaitez exiger une capitalisation spécifique pour la clé de balise à l'aide de cette politique. Si vous cochez cette case, la capitalisation que vous avez spécifiée pour la clé de balise remplace le traitement de la casse spécifié dans une politique parente héritée.

      Si aucune politique parente n'existe et que vous ne sélectionnez pas cette option, seules les clés de balise ne comportant que des caractères minuscules sont considérées comme conformes. Pour de plus amples informations sur l'héritage des politiques parentes, consultez Fonctionnement de l'héritage des politiques de gestion.

      > **Tip**
      >
      > Envisagez d'utiliser l'exemple de politique de balises fourni sous la rubrique Exemple 1 : Définition d'une casse de clé de balise à l'échelle de l'organisation pour vous aider à créer une politique de balises qui définit des clés de balise et leur traitement de la casse. Attachez-la à la racine de l'organisation. Plus tard, vous pourrez créer et associer des politiques de balisage supplémentaires

à des comptes OUs ou à des comptes afin de créer des règles de balisage supplémentaires.

b. Spécifiez les valeurs autorisées pour cette clé de balise : activez cette option si vous souhaitez ajouter des valeurs autorisées pour cette clé de balise à toutes les valeurs héritées d'une politique parent.

   Par défaut, cette case est désactivée, ce qui signifie que seules les valeurs héritées d'une politique parente sont considérées comme conformes. Si aucune politique parente n'existe ou ne spécifie de valeurs de balise, toutes les valeurs (y compris aucune valeur) sont considérées comme conformes.

   Pour mettre à jour la liste des valeurs de balise admises, sélectionnez Spécifier des valeurs admises pour cette clé de balise, puis Spécifier des valeurs. Lorsque vous y êtes invité, entrez les nouvelles valeurs (une par case) et choisissez Enregistrer les modifications.

8. Pour les types de ressources à appliquer, vous pouvez sélectionner Empêcher les opérations non conformes pour cette balise.

   Nous vous recommandons de laisser cette option désactivée (par défaut), sauf si vous êtes habitué à utiliser les politiques relatives aux balises. Veillez à consulter les recommandations de la rubrique Renforcez la cohérence du balisage et procédez à des tests minutieux. Sinon, vous risquez d'empêcher des utilisateurs de comptes de votre organisation de baliser les ressources dont ils ont besoin.

   Si vous souhaitez appliquer la conformité à cette clé de balise, cochez la case, puis sélectionnez Spécifier les valeurs admises. Lorsque vous y êtes invité, sélectionnez les types de ressources à inclure dans la politique. Ensuite, choisissez Enregistrer les modifications.

   > ⚠ Important
   >
   > Lorsque vous sélectionnez cette option, toutes les opérations qui manipulent des balises pour des ressources dont le type est spécifié ne réussissent que si l'opération aboutit à des balises conformes à la politique.

9. (Facultatif) Pour ajouter une autre clé de balise à cette politique de balises, choisissez Ajouter une clé de balise. Ensuite, effectuez les étapes 6 à 9 pour définir la clé de balise.

10. Lorsque vous avez terminé de créer votre politique de balises, choisissez Enregistrer les modifications.

AWS CLI & AWS SDKs

Pour créer une politique de balises

Vous pouvez utiliser l'une des méthodes suivantes pour créer une politique de balises :

- AWS CLI : create-policy

  Vous pouvez utiliser un éditeur de texte quelconque pour créer une politique de balises. Utilisez la syntaxe JSON et enregistrez la politique de balises dans un fichier portant un nom et une extension quelconque à l'emplacement de votre choix. Les politiques de balises peuvent comporter un maximum de 2 500 caractères, espaces inclus. Pour de plus amples informations sur la syntaxe des politiques de balises, consultez Syntaxe des politiques de balises.

  Pour créer une politique de balises

  1. Créez dans un fichier texte une politique de balises semblable à la suivante :

     Contenu de `testpolicy.json` :

     ```
     {
         "tags": {
             "CostCenter": {
                 "tag_key": {
                     "@@assign": "CostCenter"
                 }
             }
         }
     }
     ```

     Cette politique de balises définit la clé de balise `CostCenter`. La balise peut accepter n'importe quelle valeur ou aucune valeur. Une telle politique signifie qu'une ressource à laquelle le CostCenter tag est attaché avec ou sans valeur est conforme.

  2. Créez une politique avec le contenu de politique figurant dans le fichier. Un espace blanc supplémentaire dans la sortie a été tronqué pour plus de lisibilité.

     ```
     $ aws organizations create-policy \
     ```

```
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n\n"
    }
}
```

- AWS SDKs: CreatePolicy

## Création d'une politique pour les applications de chat

> **Autorisations minimales**
>
> Pour créer une politique d'applications de chat, vous devez être autorisé à exécuter l'action suivante :
>
> - `organizations:CreatePolicy`

### AWS Management Console

Vous pouvez créer une politique pour les applications AWS Management Console de chat de deux manières :

- Un éditeur visuel qui vous permet de choisir des options et de générer le texte de politique JSON pour vous.
- Un éditeur de texte qui vous permet de créer directement le texte de politique JSON.

L'éditeur visuel facilite le processus, mais limite votre flexibilité. C'est un excellent moyen de créer vos premières politiques et de les utiliser facilement. Une fois que vous avez compris leur fonctionnement et que vous avez commencé à éprouver les limites de l'éditeur visuel, vous pouvez ajouter des fonctionnalités avancées à vos politiques en modifiant vous-même le texte de la politique JSON. L'éditeur visuel utilise uniquement l'opérateur de réglage de valeur @@assign et ne fournit aucun accès aux opérateurs de contrôle enfants. Vous pouvez ajouter les opérateurs de contrôle enfants uniquement si vous modifiez manuellement le texte de la politique JSON.

Pour créer une politique en matière d'applications de chat

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Chatbot, choisissez Créer une politique.
3. Sur la page de stratégie de création de nouvelles applications de chat, entrez le nom de la politique et une description de la politique facultative.
4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, veuillez consulter Ressources de balisage AWS Organizations.
5. Vous pouvez créer la politique à l'aide de l'Éditeur visuel, de la manière décrite dans cette procédure. Vous pouvez également taper ou coller du texte de politique dans l'onglet JSON. Pour plus d'informations sur la syntaxe des politiques des applications de chat, consultezSyntaxe de politique des applications de chat et exemples.

   Si vous choisissez d'utiliser l'éditeur visuel, configurez la politique de vos applications de chat en spécifiant les contrôles d'accès pour les clients de chat.

   a. Choisissez l'une des options suivantes pour configurer l'accès au client de chat Amazon Chime

      - Refusez l'accès au carillon.
      - Autoriser l'accès à Chime.

   b. Choisissez l'une des options suivantes pour définir l'accès au client de chat Microsoft Teams

      - Refuser l'accès à toutes les équipes

- Autoriser l'accès à toutes les équipes
- Restreindre l'accès aux équipes nommées

c. Choisissez l'une des options suivantes pour configurer l'accès au client de chat Slack

- Refuser l'accès à tous les espaces de travail Slack
- Autoriser l'accès à tous les espaces de travail Slack
- Restreindre l'accès aux espaces de travail Slack nommés

> **Note**
>
> En outre, vous pouvez sélectionner Limiter l'utilisation d'Amazon Q Developer dans les applications de chat aux seules chaînes privées de Slack.

d. Sélectionnez les options suivantes pour définir les types d'autorisations IAM

- Activer le rôle IAM au niveau de la chaîne : tous les membres de la chaîne partagent les autorisations du rôle IAM pour exécuter des tâches dans une chaîne. Un rôle de chaîne est approprié si les membres de la chaîne ont besoin des mêmes autorisations.
- Activer le rôle IAM au niveau de l'utilisateur : les membres de la chaîne doivent choisir un rôle d'utilisateur IAM pour effectuer des actions (nécessite un accès à la console pour choisir les rôles). Les rôles d'utilisateur sont appropriés si les membres de la chaîne ont besoin d'autorisations différentes et peuvent choisir leurs rôles d'utilisateur.

6. Lorsque vous avez terminé la création de votre politique, choisissez Créer la politique. La politique apparaît dans votre liste de politiques de sauvegarde du chatbot.

AWS CLI & AWS SDKs

Pour créer une politique en matière d'applications de chat

Vous pouvez utiliser l'une des méthodes suivantes pour créer une politique d'applications de chat :

- AWS CLI : create-policy

Vous pouvez utiliser n'importe quel éditeur de texte pour créer une politique d'applications de chat. Utilisez la syntaxe JSON et enregistrez la politique des applications de chat sous forme de fichier avec le nom et l'extension de votre choix à l'emplacement de votre choix. Les politiques relatives aux applications de chat peuvent comporter un maximum de ? caractères, y

compris les espaces. Pour de plus amples informations sur la syntaxe des politiques de balises, consultez Syntaxe de politique des applications de chat et exemples.

Pour créer une politique en matière d'applications de chat

1. Créez une politique d'applications de chat dans un fichier texte similaire à ce qui suit :

   Contenu de `testpolicy.json` :

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

   Cette politique relative aux applications de chat autorise uniquement les chaînes privées Slack dans un espace de travail spécifique, désactive Microsoft Teams et prend en charge tous les paramètres de rôle.

2. Créez une politique avec le contenu de politique figurant dans le fichier. Un espace blanc supplémentaire dans la sortie a été tronqué pour plus de lisibilité.

```
$ aws organizations create-policy \
    --name "MyTestChatbotPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type CHATBOT_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-a1b2c3d4e5",
            "Name": "MyTestChatApplicationsPolicy",
            "Description": "My Test policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-
Id"]},"supported_channel_types":{"@@assign":["private"]}},"microsoft_teams":
{"client":{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: CreatePolicy

## Créer une politique de désinscription des services d'IA

> **Autorisations minimales**
>
> Pour créer une politique de désactivation des services IA, vous devez disposer de l'autorisation d'exécuter l'action suivante :
>
> - `organizations:CreatePolicy`

### AWS Management Console

Pour créer une politique de désactivation des services IA

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de désactivation des services IA choisissez Créer une politique.
3. Dans la page Créer une politique de désactivation des services IA, saisissez un Nom de politique et éventuellement une description de la politique.
4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, consultez Ressources de balisage AWS Organizations.
5. Saisissez ou collez le texte de la politique dans l'onglet JSON. Pour plus d'informations sur la syntaxe des politiques de désactivation des services IA, consultez Syntaxe des politiques de désactivation des services IA et exemples. Pour obtenir des exemples de politiques que vous pouvez utiliser comme point de départ, consultez Exemples de politique de désactivation des services IA.
6. Lorsque vous avez terminé la modification de votre politique, choisissez Créer la politique dans l'angle inférieur droit de la page.

### AWS CLI & AWS SDKs

Pour créer une politique de désactivation des services IA

Vous pouvez utiliser l'une des commandes suivantes pour créer une politique de balises :

- AWS CLI : create-policy

  1. Créez une politique de désactivation des services IA comme ci-dessous et stockez-la dans un fichier texte. Notez que « `optOut` » et « `optIn` » sont sensibles à la casse.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
```

```
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Cette politique de désactivation des services IA spécifie que tous les comptes concernés par la politique sont exclus de tous les services IA, à l'exception d'Amazon Rekognition.

2. Importez le fichier de politique JSON pour créer une nouvelle politique dans l'organisation. Dans cet exemple, le fichier JSON précédent était nommé `policy.json`.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS SDKs: CreatePolicy

# Création d'une politique de déploiement des mises à niveau

**Autorisations minimales**

Pour créer une politique de déploiement des mises à niveau, vous devez être autorisé à exécuter l'action suivante :

- `organizations:CreatePolicy`

AWS Management Console

Pour créer une politique de déploiement des mises à niveau

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de déploiement de la mise à niveau, choisissez Créer une politique.
3. Sur la page Créer une nouvelle politique de déploiement de mise à niveau, entrez le nom de la politique et une description de la politique facultative.
4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50 balises à une politique. Pour de plus amples informations, veuillez consulter Ressources de balisage AWS Organizations.
5. Vous pouvez créer la politique à l'aide de l'Éditeur visuel, de la manière décrite dans cette procédure. Vous pouvez également taper ou coller du texte de politique dans l'onglet JSON. Pour de plus amples informations, veuillez consulter Syntaxe et exemples de politique de déploiement des mises à niveau.

   Si vous choisissez d'utiliser l'éditeur visuel, sélectionnez l'ordre de mise à niveau que vous souhaitez utiliser pour votre politique de déploiement des mises à niveau. Pour plus d'informations sur les commandes de surclassement, consultezQuelles sont les politiques de déploiement des mises à niveau ?.
6. Sous Ordre des politiques et ressources, sélectionnez Premier, Deuxième ou Dernier dans le menu.

7. (Facultatif) Pour cibler des ressources individuelles avec cette politique, sélectionnez Remplacer des ressources spécifiques, puis procédez comme suit :

   a. Dans Clé, entrez le nom de la ressource que vous souhaitez remplacer.

   b. Dans Valeur, entrez l'ARN de la ressource.

   c. Dans Ordre de mise à niveau, choisissez l'ordre préféré qui doit être appliqué à cette ressource.

   d. Si des ressources supplémentaires doivent être spécifiées, choisissez Ajouter une balise, puis répétez les étapes précédentes pour définir la clé de balise.

8. Lorsque vous avez terminé la modification de votre politique, choisissez Créer la politique dans l'angle inférieur droit de la page.

Votre nouvelle politique apparaît dans la liste des politiques de déploiement des mises à niveau. Vous pouvez désormais associer votre politique à la racine ou aux comptes. OUs

AWS CLI & AWS SDKs

Pour créer une politique de déploiement des mises à niveau

Vous pouvez utiliser l'une des méthodes suivantes pour créer une politique de déploiement des mises à niveau :

- AWS CLI : create-policy

1. Créez une politique de déploiement de mise à niveau comme celle ci-dessous, et stockez-la dans un fichier texte.

```
{
    "upgrade_rollout": {
        "default": {
            "patch_order": {
                "@@assign": "last"
            }
        },
        "tags": {
            "my_patch_order_tag": {
                "tag_values": {
                    "tag1": {
                        "patch_order": {
                            "@@assign": "first"
```

```
                        }
                    },
                    "tag2": {
                        "patch_order": {
                            "@@assign": "second"
                        }
                    },
                    "tag3": {
                        "patch_order": {
                            "@@assign": "last"
                        }
                    }
                }
            }
        }
    }
}
```

Cette politique de déploiement des mises à niveau définit l'ordre dans lequel les AWS services appliquent les mises à niveau automatiques à l'ensemble de vos ressources. Pour plus d'informations sur la syntaxe de la politique de déploiement des mises à niveau, consultezSyntaxe et exemples de politique de déploiement des mises à niveau.

2. Importez le fichier de politique JSON pour créer une nouvelle politique dans l'organisation. Dans cet exemple, le fichier JSON précédent était nommé `policy.json`.

```
$ aws organizations create-policy \
    --type UPGRADE_ROLLOUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
"Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
upgrade_rollout_policy/p-i9j8k7l6m5",
            "Name": "MyTestPolicy",
            "Description": "My test policy",
            "Type": "UPGRADE_ROLLOUT_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\n    \"upgrade_rollout\": {\n        \"default\": {\n
          \"patch_order\": {\n                \"@@assign\": \"last\"\n
      }\n        },\n        \"tags\": {\n            \"my_patch_order_tag\":
 {\n                \"tag_values\": {\n                    \"tag1\": {\n
                  \"patch_order\": {\n                            \"@@assign
\": \"first\"\n                        }\n                    },\n
          \"tag2\": {\n                        \"patch_order\": {\n
                  \"@@assign\": \"second\"\n                        }\n
               },\n                    \"tag3\": {\n
 \"patch_order\": {\n                            \"@@assign\": \"last\"\n
                    }\n                }\n                }\n
  }\n        }\n    }\n}\n"
    }
}
```

- AWS SDKs: CreatePolicy

## Création d'une politique Security Hub

> **Autorisations minimales**
>
> Pour créer une politique Security Hub, vous devez être autorisé à exécuter l'action suivante :
>
> - `organizations:CreatePolicy`

AWS Management Console

Pour créer une politique Security Hub

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Security Hub, choisissez Create policy.
3. Sur la page Create new Security Hub policy, entrez le nom de la politique et une description de la politique facultative.
4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à la politique en choisissant Ajouter une balise, puis en saisissant une clé et éventuellement une valeur. Laisser la valeur vide la définit à une chaîne vide ; elle ne prend pas la valeur `null`. Vous pouvez attacher jusqu'à 50

balises à une politique. Pour de plus amples informations, veuillez consulter Ressources de balisage AWS Organizations.

5. Entrez ou collez le texte de la politique dans la zone de code JSON. Pour plus d'informations sur la syntaxe de la politique Security Hub, consultezSyntaxe et exemples de politiques du Security Hub. Pour obtenir des exemples de politiques que vous pouvez utiliser comme point de départ, consultez Exemples de politiques relatives au Security Hub.
6. Lorsque vous avez terminé la modification de votre politique, choisissez Créer la politique dans l'angle inférieur droit de la page.

AWS CLI & AWS SDKs

Pour créer une politique Security Hub

Vous pouvez utiliser l'une des méthodes suivantes pour créer une politique Security Hub :

- AWS CLI : create-policy

  Exemple : créer une politique qui active Security Hub dans toutes les régions prises en charge

  L'exemple suivant suppose que vous disposez d'un fichier nommé `testPolicy_enableAllSupportedRegions.json` contenant le texte de politique JSON. Il utilise ce fichier pour créer une nouvelle politique Security Hub.

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions.json \
    --name "testPolicy_enableAllSupportedRegions" \
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "testPolicy_enableAllSupportedRegions",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

Exemple : créer une politique qui active Security Hub dans toutes les régions prises en charge, mais qui le désactive dans la région us-east-1

L'exemple suivant suppose que vous disposez d'un fichier nommé `testPolicy_enableAllSupportedRegions_Disable_us-east-1.json` contenant le texte de politique JSON. Il utilise ce fichier pour créer une nouvelle politique Security Hub.

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions_Disable_us-east-1.json
 \
    --name "testPolicy_enableAllSupportedRegions_Disable_us-east-1" \
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions but
 disable in us-east-1 Region" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66217dwpos",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66217dwpos",
            "Name": "testPolicy_enableAllSupportedRegions_Disable_us-east-1",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions but disable in us-east-1 Region",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[\n        \"us-east-1\"\n      ]\n
    }\n  }\n}\n"
    }
}
```

- AWS SDKs: CreatePolicy

# Mettre à jour les politiques de l'organisation avec AWS Organizations

Lorsque les exigences de votre politique changent, vous pouvez mettre à jour une politique existante.

Cette rubrique décrit comment mettre à jour les politiques avec AWS Organizations. Une politique définit les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS.

Rubriques



## Mettre à jour une politique de contrôle des services (SCP)

Une fois connecté au compte de gestion de votre organisation, vous pouvez renommer ou modifier le contenu d'une politique. La modification du contenu d'une politique SCP affecte immédiatement tous les utilisateurs, groupes et rôles de tous les comptes attachés.

**Autorisations minimales**

Pour mettre à jour une SCP, vous devez être autorisé à effectuer les actions suivantes :

- `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).
- `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

### AWS Management Console

Pour mettre à jour une politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de contrôle des services, choisissez le nom de la politique que vous souhaitez mettre à jour.
3. Sur la page des détails de la politique, choisissez Modifier la politique.
4. Effectuez une ou plusieurs des modifications suivantes :
   - Vous pouvez renommer la politique en saisissant un nouveau nom dans Nom de la politique.
   - Vous pouvez en changer la description en saisissant un nouveau texte dans Description de la politique.
   - Vous pouvez modifier le texte de la politique en modifiant la politique au format JSON dans le panneau de gauche. Par ailleurs, vous pouvez choisir une instruction dans l'éditeur situé à droite et en modifier les éléments à l'aide des commandes. Pour de plus amples informations sur chaque contrôle, consultez Création d'une procédure SCP plus haut dans cette rubrique.
5. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

### AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des commandes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

  L'exemple suivant renomme une politique.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
```

```
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

L'exemple suivant ajoute ou modifie la description d'une politique de contrôle des services.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

L'exemple suivant modifie le document de politique de la SCP en spécifiant un fichier contenant le nouveau texte de politique JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

## Mettre à jour une politique de contrôle des ressources (RCP)

Une fois connecté au compte de gestion de votre organisation, vous pouvez renommer ou modifier le contenu d'une politique. La modification du contenu d'un RCP affecte immédiatement toutes les ressources de tous les comptes attachés.

> **Autorisations minimales**
>
> Pour mettre à jour un RCP, vous devez être autorisé à exécuter les actions suivantes :
>
> - `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).
> - `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

AWS Management Console

Pour mettre à jour une politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

2. Sur la page Stratégie de contrôle des ressources, choisissez le nom de la stratégie que vous souhaitez mettre à jour.
3. Sur la page des détails de la politique, choisissez Modifier la politique.
4. Effectuez une ou plusieurs des modifications suivantes :

   - Vous pouvez renommer la politique en saisissant un nouveau nom dans Nom de la politique.
   - Vous pouvez en changer la description en saisissant un nouveau texte dans Description de la politique.
   - Vous pouvez modifier le texte de la politique en modifiant la politique au format JSON dans le panneau de gauche. Par ailleurs, vous pouvez choisir une instruction dans l'éditeur situé à droite et en modifier les éléments à l'aide des commandes. Pour plus de détails sur chaque contrôle, consultez la section Création d'une procédure RCP plus haut dans cette rubrique.
5. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des commandes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

  L'exemple suivant renomme une politique.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
```

```
        },
        "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

L'exemple suivant ajoute ou modifie la description d'une politique de contrôle des ressources.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

L'exemple suivant modifie le document de politique du RCP en spécifiant un fichier contenant le nouveau texte de politique JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
```

```
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

## Mettre à jour une politique déclarative

> **Autorisations minimales**
>
> Pour mettre à jour une politique déclarative, vous devez être autorisé à exécuter les actions suivantes :
>
> - `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).
> - `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut l'"Amazon Resource Name (ARN) de la politique spécifiée (ou « * »).

### AWS Management Console

Pour mettre à jour une politique déclarative

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques déclaratives, choisissez le nom de la politique que vous souhaitez mettre à jour.
3. Sur la page de détails de la politique, choisissez Modifier la politique.
4. Vous pouvez saisir un nouveau Nom de la politique, une Description de la politique ou modifier le texte de politique JSON. Pour plus d'informations sur la syntaxe des politiques déclaratives, consultezSyntaxe de politique déclarative et exemples.

5. Lorsque vous avez terminé de mettre à jour la politique, choisissez Enregistrer les modifications.

### AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

L'exemple suivant renomme une politique déclarative.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2-configuration":{"ec2_attributes":
{"image_block_public_access":{"state":{"@@assign":"block_new_sharing"}}}}".
    }
}
```

L'exemple suivant ajoute ou modifie la description d'une politique déclarative.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
```

```
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
    }
}
```

- AWS SDKs: UpdatePolicy

## Mettre à jour une politique de sauvegarde

Lorsque que vous êtes connecté au compte de gestion de votre organisation, vous pouvez modifier une politique qui demande des modifications dans votre organisation.

> **Autorisations minimales**
>
> Pour mettre à jour une politique de sauvegarde, vous devez avoir l'autorisation d'effectuer les actions suivantes :
>
> - `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique à mettre à jour (ou « * »).
> - `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique à mettre à jour (ou « * »).

AWS Management Console

Pour mettre à jour une politique de sauvegarde

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de sauvegarde, choisissez le nom de la politique que vous souhaitez mettre à jour.
3. Choisissez Modifier la politique.

4. Vous pouvez saisir un nouveau Nom de la politique et une Description de la politique. Vous pouvez modifier le contenu de la politique à l'aide de l'Éditeur visuel ou en modifiant directement le JSON.
5. Lorsque vous avez terminé de mettre à jour la politique, choisissez Enregistrer les modifications.

### AWS CLI & AWS SDKs

Pour mettre à jour une politique de sauvegarde

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une politique de sauvegarde :

- AWS CLI : update-policy

  L'exemple suivant renomme une politique de sauvegarde.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

  L'exemple suivant ajoute ou remplace la description d'une politique de sauvegarde.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

L'exemple suivant modifie le document de politique JSON attaché à une politique de sauvegarde. Dans cet exemple, le contenu est extrait d'un fichier appelé `policy.json` et contenant le texte suivant :

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" },
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" },
```

```
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS SDKs: UpdatePolicy

# Mettre à jour une politique en matière de balises

**Autorisations minimales**

Pour mettre à jour une politique de balises, vous devez avoir l'autorisation d'effectuer les actions suivantes :

- `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).
- `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

## AWS Management Console

Pour mette à jour une politique de balises

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de balises, choisissez le nom de la politique que vous souhaitez mettre à jour.
3. Choisissez Modifier la politique.
4. Vous pouvez saisir un nouveau Nom de la politique et une Description de la politique. Vous pouvez modifier le contenu de la politique à l'aide de l'Éditeur visuel ou en modifiant le JSON.
5. Lorsque vous avez terminé de mettre à jour la politique de balises, choisissez Enregistrer les modifications.

## AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

L'exemple suivant renomme une politique de balises.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

L'exemple suivant ajoute ou remplace la description d'une politique de balises.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

L'exemple suivant modifie le document de politique JSON attaché à une politique de désactivation des services IA. Dans cet exemple, le contenu est extrait d'un fichier appelé `policy.json` et contenant le texte suivant :

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDKs: UpdatePolicy

# Mettre à jour une politique relative aux applications de chat

**Autorisations minimales**

Pour mettre à jour la politique d'une application de chat, vous devez être autorisé à exécuter les actions suivantes :

- `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).
- `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

## AWS Management Console

Pour mettre à jour une politique relative aux applications de chat

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du chatbot, choisissez la politique des applications de chat que vous souhaitez mettre à jour.
3. Choisissez Modifier la politique.
4. Vous pouvez saisir un nouveau Nom de la politique et une Description de la politique. Vous pouvez modifier le contenu de la politique à l'aide de l'Éditeur visuel ou en modifiant le JSON.
5. Lorsque vous avez terminé de mettre à jour la politique de balises, choisissez Enregistrer les modifications.

## AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

L'exemple suivant renomme une politique d'applications de chat.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed chat applications policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
            "Name": "Renamed chat applications policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-Id"]},"default":
{"supported_channel_types":{"@@assign":["private"]}}},"microsoft_teams":{"client":
{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: UpdatePolicy

## Mettre à jour une politique de désinscription des services d'IA

> **Autorisations minimales**
>
> Pour mettre à jour une politique de désactivation des services IA, vous devez avoir l'autorisation d'effectuer les actions suivantes :
>
> - `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).
> - `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut l'"Amazon Resource Name (ARN) de la politique spécifiée (ou « * »).

### AWS Management Console

Pour mettre à jour une politique de désactivation des services IA

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de désactivation des services IA, choisissez le nom de la politique que vous souhaitez mettre à jour.
3. Sur la page de détails de la politique, choisissez Modifier la politique.
4. Vous pouvez saisir un nouveau Nom de la politique, une Description de la politique ou modifier le texte de politique JSON. Pour plus d'informations sur la syntaxe des politiques de désactivation des services IA, consultez Syntaxe des politiques de désactivation des services IA et exemples. Pour obtenir des exemples de politiques que vous pouvez utiliser comme point de départ, consultez Exemples de politique de désactivation des services IA.
5. Lorsque vous avez terminé de mettre à jour la politique, choisissez Enregistrer les modifications.

### AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

  L'exemple suivant renomme une politique de désactivation des services IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
```

```
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

L'exemple suivant montre comment ajouter ou modifier la description d'une politique de désactivation des services IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

L'exemple suivant modifie le document de politique JSON attaché à une politique de désactivation des services IA. Dans cet exemple, le contenu est extrait d'un fichier appelé `policy.json` et contenant le texte suivant :

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS SDKs: UpdatePolicy

## Mettre à jour une politique de Security Hub

> **Autorisations minimales**
>
> Pour mettre à jour une politique Security Hub, vous devez être autorisé à exécuter les actions suivantes :
>
> - `organizations:UpdatePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

- `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut l'"Amazon Resource Name (ARN) de la politique spécifiée (ou « * »).

AWS Management Console

Pour mettre à jour une politique Security Hub

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Security Hub, choisissez le nom de la politique que vous souhaitez mettre à jour.
3. Sur la page de détails de la politique, choisissez Modifier la politique.
4. Vous pouvez saisir un nouveau Nom de la politique, une Description de la politique ou modifier le texte de politique JSON. Pour plus d'informations sur la syntaxe des politiques du Security Hub, consultezSyntaxe et exemples de politiques du Security Hub. Pour obtenir des exemples de politiques que vous pouvez utiliser comme point de départ, consultez Exemples de politiques relatives au Security Hub.
5. Lorsque vous avez terminé de mettre à jour la politique, choisissez Enregistrer les modifications.

AWS CLI & AWS SDKs

Pour mettre à jour une politique

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une politique :

- AWS CLI : update-policy

  L'exemple suivant renomme une politique Security Hub.

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "Renamed policy"
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "Renamed policy",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

L'exemple suivant ajoute ou modifie la description d'une politique Security Hub.

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "My new description",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

- AWS SDKs: UpdatePolicy

# Modification des balises associées aux politiques de l'organisation avec AWS Organizations

Cette rubrique explique comment modifier les balises associées aux politiques AWS Organizations. Une politique définit les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS.

Rubriques



## Modifier les balises associées à une politique de contrôle des services (SCP)

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les balises attachées à une politique SCP. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.

Autorisations minimales

Pour modifier les balises attachées à une politique SCP dans votre organisation , vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:DescribePolicy` — requis uniquement si vous utilisez la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

### AWS Management Console

Pour modifier les balises attachées à une politique de contrôle des services (SCP)

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de contrôle des services, choisissez le nom de la politique à laquelle sont attachées les balises que vous souhaitez modifier.
3. Sur la page des détails de politique, cochez la caseBalises, puis choisissezGérer les balises.
4. Effectuez une ou plusieurs des modifications suivantes :
   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier directement la clé de la balise. Pour modifier une clé, vous devez supprimer la balise avec l'ancienne clé, puis ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer).
   - Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.
5. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

### AWS CLI & AWS SDKs

Pour modifier les balises attachées à une politique de contrôle des services (SCP)

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises attachées à une SCP :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

# Modifier les balises associées à une politique de contrôle des ressources (RCP)

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les balises associées à un RCP. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.

Autorisations minimales

Pour modifier les balises associées à un RCP dans votre AWS organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:DescribePolicy` — requis uniquement si vous utilisez la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Pour modifier les balises associées à un RCP

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Stratégie de contrôle des ressources, choisissez le nom de la politique avec les balises que vous souhaitez modifier.
3. Sur la page des détails de la politique, choisissez l'onglet Balises, puis sélectionnez Gérer les balises.
4. Effectuez une ou plusieurs des modifications suivantes :

   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier directement la clé de la balise. Pour modifier une clé, vous devez supprimer la balise avec l'ancienne clé, puis ajouter une balise avec la nouvelle clé.

- Vous pouvez supprimer une balise existante en choisissant Supprimer).
- Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.

5. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

AWS CLI & AWS SDKs

Pour modifier les balises associées à un RCP

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises associées à un RCP :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

## Modifier les balises associées à une politique déclarative

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les balises associées à une politique déclarative. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.

Autorisations minimales

Pour modifier les balises associées à une politique déclarative dans votre AWS organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:DescribePolicy` — requis uniquement si vous utilisez la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

### AWS Management Console

Pour modifier les balises associées à une politique déclarative

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques déclaratives, choisissez le nom de la politique avec les balises que vous souhaitez modifier.
3. Sur la page de détails de la politique choisie, choisissez l'onglet Balises, puis Gérer les balises.
4. Vous pouvez effectuer l'une des actions suivantes sur cette page :
   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer.
   - Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.
5. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

### AWS CLI & AWS SDKs

Pour modifier les balises associées à une politique déclarative

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises associées à une politique déclarative :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

# Modifier les balises associées à une politique de sauvegarde

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les balises attachées à une politique de sauvegarde. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.

Autorisations minimales

Pour modifier les balises attachées à une politique de sauvegarde dans votre organisation , vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` (console uniquement — pour accéder à la politique)
- `organizations:DescribePolicy` (console uniquement — pour accéder à la politique)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Pour modifier les balises attachées à une politique de sauvegarde

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Page Politiques de sauvegarde
3. Choisissez le nom de la politique possédant les balises que vous souhaitez modifier.

   La page détaillée de la politique s'affiche.
4. Dans l'onglet Balises, choisissez Gérer les balises.
5. Vous pouvez effectuer l'une des actions suivantes sur cette page :

   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer.

- Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.

6. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

AWS CLI & AWS SDKs

Pour modifier les balises attachées à une politique de sauvegarde

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises attachées à une politique de sauvegarde :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

## Modifier les balises associées à une politique en matière de balises

Lorsque vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer des balises attachées à une politique de balises. Pour ce faire, exécutez les étapes suivantes.

Autorisations minimales

Pour modifier les balises attachées à une politique de balises dans votre organisation , vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` (console uniquement — pour accéder à la politique)
- `organizations:DescribePolicy` (console uniquement — pour accéder à la politique)
- `organizations:TagResource`
- `organizations:UntagResource`

### AWS Management Console

Pour modifier les balises attachées à une politique de balises

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de balises, choisissez le nom de la politique à laquelle sont attachées les balises que vous souhaitez modifier.
3. Sur la page de détails de la politique choisie, choisissez l'onglet Balises, puis Gérer les balises.
4. Vous pouvez effectuer l'une des actions suivantes sur cette page :
   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer.
   - Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.
5. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

### AWS CLI & AWS SDKs

Pour modifier les balises attachées à une politique de balises

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises attachées à une politique de balises :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

# Modifier les balises associées à une politique d'applications de chat

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les balises associées à une politique d'applications de chat. Pour ce faire, exécutez les étapes suivantes.

Autorisations minimales

Pour modifier les balises associées à une politique d'applications de chat dans votre organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` (console uniquement — pour accéder à la politique)
- `organizations:DescribePolicy` (console uniquement — pour accéder à la politique)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Pour modifier les balises associées à la politique d'une application de chat

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Chatbot, choisissez le nom de la politique avec les balises que vous souhaitez modifier.
3. Sur la page de détails de la politique choisie, choisissez l'onglet Balises, puis Gérer les balises.
4. Vous pouvez effectuer l'une des actions suivantes sur cette page :

   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer.
   - Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous

laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.

5. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

AWS CLI & AWS SDKs

Pour modifier les balises associées à la politique d'une application de chat

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises associées à une politique d'applications de chat :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

## Modifier les balises associées à une politique de désinscription des services d'IA

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter ou supprimer les balises attachées à une politique de désinscription des services IA. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.

Autorisations minimales

Pour modifier les balises attachées à une politique de désactivation des services IA dans votre organisation , vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:DescribePolicy` — requis uniquement si vous utilisez la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

### AWS Management Console

Pour modifier les balises attachées à une politique de désactivation des services IA

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de désactivation des services IA, choisissez le nom de la politique à laquelle sont attachées les balises que vous souhaitez modifier.
3. Sur la page de détails de la politique choisie, choisissez l'onglet Balises, puis Gérer les balises.
4. Vous pouvez effectuer l'une des actions suivantes sur cette page :
   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer.
   - Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.
5. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

### AWS CLI & AWS SDKs

Pour modifier les balises attachées à une politique de désactivation des services IA

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises attachées à une politique de désactivation des services IA :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

# Modifier les balises associées à une politique Security Hub

Lorsque vous vous connectez au compte de gestion de votre entreprise, vous pouvez ajouter ou supprimer les balises associées à une politique du Security Hub. Pour plus d'informations sur le balisage, consultez Ressources de balisage AWS Organizations.

Autorisations minimales

Pour modifier les balises associées à une politique Security Hub dans votre organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
- `organizations:DescribePolicy` — requis uniquement si vous utilisez la console Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Pour modifier les balises associées à une politique du Security Hub

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Security Hub, choisissez le nom de la politique avec les balises que vous souhaitez modifier.
3. Sur la page de détails de la politique choisie, choisissez l'onglet Balises, puis Gérer les balises.
4. Vous pouvez effectuer l'une des actions suivantes sur cette page :
   - Modifiez la valeur d'une balise en entrant une nouvelle valeur en remplacement de l'ancienne. Vous ne pouvez pas modifier la clé. Pour changer une clé, vous devez supprimer la balise avec l'ancienne clé et ajouter une balise avec la nouvelle clé.
   - Vous pouvez supprimer une balise existante en choisissant Supprimer.

- Ajoutez une nouvelle paire clé/valeur de balise. Choisissez Ajouter une balise, puis entrez le nouveau nom de la clé et éventuellement une valeur dans les champs prévus. Si vous laissez vide le champ Valeur, la valeur est une chaîne vide ; elle ne prend pas la valeur `null`.

5. Choisissez Enregistrer les modifications une fois que vous avez effectué tous les ajouts, suppressions et modifications que vous souhaitez.

AWS CLI & AWS SDKs

Pour modifier les balises associées à une politique du Security Hub

Vous pouvez utiliser l'une des commandes suivantes pour modifier les balises associées à une politique Security Hub :

- AWS CLI : tag-resource et untag-resource
- AWS SDKs : TagResource et UntagResource

# Joindre les politiques de l'organisation à AWS Organizations

Cette rubrique décrit comment associer des politiques à AWS Organizations. Une politique définit les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS.

Rubriques

- Joignez des politiques à AWS Organizations

## Joignez des politiques à AWS Organizations

Autorisations minimales

Pour associer des politiques, vous devez être autorisé à exécuter l'action suivante :

- `organizations:AttachPolicy`

Autorisations minimales

Pour associer une politique d'autorisation (SCP ou RCP) à une racine, à une unité d'organisation ou à un compte, vous devez être autorisé à exécuter l'action suivante :

- `organizations:AttachPolicy` avec un élément `Resource` dans la même instruction de politique qui inclut « * » ou l'Amazon Resource Name (ARN) de la politique spécifiée et l'ARN de la racine, de l'unité d'organisation ou du compte auquel vous voulez attacher la politique

AWS Management Console

Service control policies (SCPs)

Vous pouvez attacher une politique SCP en accédant à la politique, à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez attacher la politique.

Pour attacher une SCP en accédant à la racine, à l'unité d'organisation ou au compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la case à cocher en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une SCP, puis activez-la. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans Politiques de contrôle des services, choisissez Attacher.
4. Recherchez la politique que vous souhaitez et choisissez Attacher la politique.

   La liste des pièces jointes dans l' SCPs onglet Politiques est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement, affectant les autorisations des utilisateurs et rôles IAM du compte attaché ou de tous les comptes sous la racine ou l'unité d'organisation attachée.

Pour attacher une SCP en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de contrôle des services, choisissez le nom de la politique que vous souhaitez attacher.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attach policy (Attacher la politique).

   La liste des pièces jointes dans l' SCPs onglet Cibles est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement, affectant les autorisations des utilisateurs et rôles IAM du compte attaché ou de tous les comptes sous la racine ou l'unité d'organisation attachée.

Resource control policies (RCPs)

Vous pouvez associer un RCP soit en accédant à la stratégie, soit en accédant à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez associer la politique.

Pour associer un RCP en accédant à la racine, à l'unité d'organisation ou au compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la Comptes AWSpage, naviguez jusqu'à la racine, l'unité d'organisation ou le compte auquel vous souhaitez associer un RCP, puis cochez la case correspondante. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans l'entrée relative aux politiques de contrôle des ressources, choisissez Attacher.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

La liste des pièces jointes dans l' RCPs onglet Politiques est mise à jour pour inclure le nouvel ajout. Le changement de politique prend effet immédiatement, affectant les autorisations des ressources du compte rattaché ou de tous les comptes sous la racine ou l'unité d'organisation attachée.

Pour attacher un RCP en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Stratégie de contrôle des ressources, choisissez le nom de la stratégie que vous souhaitez associer.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attach policy (Attacher la politique).

   La liste des pièces jointes dans l' RCPs onglet Cibles est mise à jour pour inclure le nouvel ajout. Le changement de politique prend effet immédiatement, affectant les autorisations des ressources du compte rattaché ou de tous les comptes sous la racine ou l'unité d'organisation attachée.

## Declarative policies

Vous pouvez associer une politique déclarative soit en accédant à la stratégie, soit en accédant à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez associer la politique.

Pour associer une politique déclarative en accédant à la racine, à l'unité d'organisation ou au compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.

2. Dans la page Comptes AWS, accédez au nom de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une politique et choisissez ce nom. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans l'entrée relative aux politiques déclaratives, choisissez Joindre.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

   La liste des politiques déclaratives jointes dans l'onglet Politiques est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Pour joindre une politique déclarative en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques déclaratives, choisissez le nom de la politique que vous souhaitez associer.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attach policy (Attacher la politique).

   La liste des politiques déclaratives jointes dans l'onglet Cibles est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

## Backup policies

Vous pouvez attacher une politique de sauvegarde en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez attacher la politique.

Pour attacher une politique de sauvegarde en accédant à la racine, à l'unité d'organisation ou au compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez au nom de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une politique et choisissez ce nom. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans Politiques de sauvegarde, choisissez Attacher.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

   La liste des politiques de sauvegarde attachées sur l'onglet Politiques est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Pour attacher une politique de sauvegarde en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de sauvegarde, choisissez le nom de la politique que vous souhaitez attacher.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attacher la politique.

   La liste des politiques de sauvegarde attachées sur l'onglet Cibles est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Tag policies

Vous pouvez attacher une politique de balises en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez attacher la politique.

Pour attacher une politique de balises en accédant à la racine, à une unité d'organisation ou à un compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez au nom de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une politique et choisissez ce nom. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans Politiques de balises, choisissez Attacher.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

   La liste des politiques de balises attachées sur l'onglet Politiques est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Pour attacher une politique de balises en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de balises, choisissez le nom de la politique que vous souhaitez attacher.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attacher la politique.

La liste des politiques de balises attachées sur l'onglet Cibles est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

## Chat applications policies

Vous pouvez joindre une politique d'applications de chat soit en accédant à la politique, soit en accédant à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez associer la politique.

Pour associer une politique d'applications de chat en accédant à la racine, à l'unité d'organisation ou au compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez au nom de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une politique et choisissez ce nom. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans l'entrée relative aux politiques des applications de chat, choisissez Joindre.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

   La liste des politiques des applications de chat jointes dans l'onglet Politiques est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Pour joindre une politique d'applications de chat en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Chatbot, choisissez le nom de la politique que vous souhaitez associer.
3. Dans l'onglet Cibles, choisissez Attacher.

4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ▶ pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attach policy (Attacher la politique).

   La liste des politiques relatives aux applications de chat jointes dans l'onglet Cibles est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

## AI services opt-out policies

Vous pouvez attacher une politique de désactivation des services IA en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez attacher la politique.

Pour attacher une politique de désactivation des services IA en accédant à la racine, à une unité d'organisation ou à un compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez au nom de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une politique et choisissez ce nom. Vous devrez peut-être développer OUs (choisir le ▶ pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Politiques, dans Politiques de désactivation des services IA, choisissez Attacher.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

   La liste des politiques de désactivation des services IA attachées sur l'onglet Politiques est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Pour attacher une politique de désactivation des services IA en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de désactivation des services IA, choisissez le nom de la politique que vous souhaitez attacher.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attacher la politique.

   La liste des politiques de désactivation des services IA attachées sur l'onglet Cibles est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

## Security Hub policies

Vous pouvez associer une politique Security Hub soit en accédant à la politique, soit en accédant à la racine, à l'unité d'organisation ou au compte auquel vous souhaitez associer la politique.

Pour associer une politique Security Hub en accédant à la racine, à l'unité d'organisation ou au compte

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez au nom de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher une politique et choisissez ce nom. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
3. Dans l'onglet Policies, dans l'entrée relative aux politiques du Security Hub, choisissez Attach.
4. Recherchez la politique souhaitée et choisissez Attacher la politique.

La liste des politiques Security Hub jointes dans l'onglet Policies est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

Pour associer une politique Security Hub en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Security Hub, choisissez le nom de la politique que vous souhaitez associer.
3. Dans l'onglet Cibles, choisissez Attacher.
4. Choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte auquel vous souhaitez attacher la politique. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix.
5. Choisissez Attach policy (Attacher la politique).

   La liste des politiques Security Hub jointes dans l'onglet Targets est mise à jour pour inclure le nouvel ajout. La modification de la politique prend effet immédiatement.

AWS CLI & AWS SDKs

Pour joindre une politique

Les exemples de code suivants illustrent comment utiliser `AttachPolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
```

```
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to attach an AWS Organizations policy to an organization,
    /// an organizational unit, or an account.
    /// </summary>
    public class AttachPolicy
    {
        /// <summary>
        /// Initializes the Organizations client object and then calls the
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous AttachPolicyà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour attacher une stratégie à une racine, une unité d'organisation ou un compte

Exemple 1

L'exemple suivant montre comment attacher une politique de contrôle des services (SCP) à une unité d'organisation :

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Exemple 2

L'exemple suivant montre comment attacher une politique de contrôle des services directement à un compte :

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Pour plus de détails sur l'API, reportez-vous AttachPolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Pour plus de détails sur l'API, consultez AttachPolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

## SAP ABAP

### Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        lo_org->attachpolicy(
          iv_policyid = iv_policy_id
          iv_targetid = iv_target_id ).
        MESSAGE 'Policy attached to target.' TYPE 'I'.
      CATCH /aws1/cx_orgaccessdeniedex.
```

```
        MESSAGE 'You do not have permission to attach the policy.' TYPE 'E'.
      CATCH /aws1/cx_orgpolicynotfoundex.
        MESSAGE 'The specified policy does not exist.' TYPE 'E'.
      CATCH /aws1/cx_orgtargetnotfoundex.
        MESSAGE 'The specified target does not exist.' TYPE 'E'.
      CATCH /aws1/cx_orgduplicateplyatta00.
        MESSAGE 'The policy is already attached to the target.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous AttachPolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

La modification de la politique prend effet immédiatement, affectant les autorisations des utilisateurs et rôles IAM du compte attaché ou de tous les comptes sous la racine ou l'unité d'organisation attachée.

# Dissocier les politiques de l'organisation avec AWS Organizations

Cette rubrique décrit comment détacher les politiques avec AWS Organizations. Une politique définit les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS.

Rubriques

- Détachez les politiques avec AWS Organizations

## Détachez les politiques avec AWS Organizations

Autorisations minimales

Pour dissocier une politique de la racine, de l'unité d'organisation ou du compte de l'organisation, vous devez être autorisé à exécuter l'action suivante :

- `organizations:DetachPolicy`

> **Note**
>
> Vous ne pouvez pas dissocier la dernière politique d'autorisation (SCP ou RCP) d'une racine, d'une unité d'organisation ou d'un compte. Au moins un SCP et un RCP doivent être connectés à chaque racine, unité d'organisation et compte à tout moment.

AWS Management Console

Service control policies (SCPs)

Vous pouvez détacher une politique SCP en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher la politique.

Pour détacher une SCP en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Politiques, choisissez la case d'option en regard de la SCP à détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des pièces jointes SCPs est mise à jour. Le changement de politique provoqué par le détachement de la SCP prend effet immédiatement. Par exemple, détacher une SCP affecte immédiatement les autorisations des utilisateurs et rôles IAM dans le ou les comptes anciennement attachés sous la racine d'organisation ou l'unité d'organisation anciennement attachée.

Pour détacher une SCP en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de contrôle des services, choisissez le nom de la politique que vous souhaitez détacher d'une racine, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

   La liste des pièces jointes SCPs est mise à jour. Le changement de politique provoqué par le détachement de la SCP prend effet immédiatement. Par exemple, détacher une SCP affecte immédiatement les autorisations des utilisateurs et rôles IAM dans le ou les comptes anciennement attachés sous la racine d'organisation ou l'unité d'organisation anciennement attachée.

Resource control policies (RCPs)

Vous pouvez détacher un RCP soit en accédant à la politique, soit à la racine, à l'unité d'organisation ou au compte duquel vous souhaitez détacher la politique. Une fois que vous avez détaché un RCP d'une entité, ce RCP ne s'applique plus aux ressources affectées par l'entité désormais détachée.

> **Note**
>
> Vous ne pouvez pas détacher la politique **`RCPFullAWSAccess`**
> La `RCPFullAWSAccess` politique est automatiquement attachée à la racine, à chaque unité d'organisation et à chaque compte de votre organisation. Vous ne pouvez pas dissocier cette politique.

Pour détacher un RCP en accédant à la racine, à l'unité d'organisation ou au compte auquel il est attaché

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Politiques, cliquez sur le bouton radio à côté du RCP que vous souhaitez détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des pièces jointes RCPs est mise à jour. Le changement de politique provoqué par le détachement du RCP prend effet immédiatement. Par exemple, le détachement d'un RCP affecte immédiatement les autorisations des utilisateurs et des rôles IAM dans le compte ou les comptes relevant de l'organisation racine ou de l'unité d'organisation précédemment attachée.

Pour détacher un RCP en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Stratégie de contrôle des ressources, choisissez le nom de la politique que vous souhaitez dissocier d'une racine, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

La liste des pièces jointes RCPs est mise à jour. Le changement de politique provoqué par le détachement du RCP prend effet immédiatement. Par exemple, le détachement d'un RCP affecte immédiatement les autorisations des utilisateurs et des rôles IAM dans le compte ou les comptes relevant de l'organisation racine ou de l'unité d'organisation précédemment attachée.

### Declarative policies

Vous pouvez détacher une politique déclarative en accédant à la stratégie ou à la racine, à l'unité d'organisation ou au compte dont vous souhaitez la détacher.

Pour détacher une politique déclarative en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Politiques, cliquez sur le bouton radio à côté de la politique déclarative que vous souhaitez détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des politiques déclaratives jointes est mise à jour. La modification de la politique prend effet immédiatement.

Pour détacher une politique déclarative en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques déclaratives, choisissez le nom de la politique que vous souhaitez dissocier d'une racine, d'une unité d'organisation ou d'un compte.

3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

   La liste des politiques déclaratives jointes est mise à jour. La modification de la politique prend effet immédiatement.

## Backup policies

Vous pouvez détacher une politique de sauvegarde en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher la politique.

Pour détacher une politique de sauvegarde en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Politiques, choisissez la case d'option en regard de la politique de sauvegarde à détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des politiques de sauvegarde attachées est mise à jour. La modification de la politique prend effet immédiatement.

Pour détacher une politique de sauvegarde en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de sauvegarde, choisissez le nom de la politique que vous souhaitez détacher d'une racine, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

   La liste des politiques de sauvegarde attachées est mise à jour. La modification de la politique prend effet immédiatement.

Tag policies

Vous pouvez détacher une politique de balises en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher la politique.

Pour détacher une politique de balises en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Politiques, choisissez la case d'option en regard de la politique de balises à détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

La liste des politiques de balises attachées est mise à jour. La modification de la politique prend effet immédiatement.

Pour détacher une politique de balises en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de balises, choisissez le nom de la politique que vous souhaitez détacher d'une racine, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

   La liste des politiques de balises attachées est mise à jour. La modification de la politique prend effet immédiatement.

Chat applications policies

Vous pouvez détacher une politique d'applications de chat soit en accédant à la politique, soit en accédant à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher la politique.

Pour détacher la politique d'une application de chat en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le )

pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.

3. Dans l'onglet Politiques, cliquez sur le bouton radio à côté de la politique des applications de chat que vous souhaitez détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des politiques relatives aux applications de chat jointes est mise à jour. La modification de la politique prend effet immédiatement.

Pour détacher une politique d'applications de chat en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Chatbot, choisissez le nom de la politique que vous souhaitez dissocier d'un root, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

   La liste des politiques relatives aux applications de chat jointes est mise à jour. La modification de la politique prend effet immédiatement.

## AI services opt-out policies

Vous pouvez détacher une politique de désactivation des services IA en accédant à la politique ou à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher la politique.

Pour détacher une politique de désactivation des services IA en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Politiques, choisissez la case d'option en regard de la politique de désactivation des services IA à détacher, puis choisissez Détacher.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des politiques de désactivation des services IA attachées est mise à jour. La modification de la politique prend effet immédiatement.

Pour détacher une politique de désactivation des services IA en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de désactivation des services IA, choisissez le nom de la politique que vous souhaitez détacher d'une racine, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

   La liste des politiques de désactivation des services IA joints est mise à jour. La modification de la politique prend effet immédiatement.

### Security Hub policies

Vous pouvez détacher une politique Security Hub soit en accédant à la politique, soit à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher la politique.

Pour détacher une politique Security Hub en accédant à la racine, à l'unité d'organisation ou au compte auquel elle est attachée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, accédez à la racine, à l'unité d'organisation ou au compte dont vous souhaitez détacher une politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix. Choisissez le nom de la racine, de l'unité d'organisation ou du compte.
3. Dans l'onglet Policies, cliquez sur le bouton radio à côté de la politique Security Hub que vous souhaitez détacher, puis choisissez Detach.
4. Dans la boîte de dialogue de confirmation, choisissez Détacher la politique.

   La liste des politiques Security Hub jointes est mise à jour. La modification de la politique prend effet immédiatement.

Pour détacher une politique Security Hub en accédant à la politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Security Hub, choisissez le nom de la politique que vous souhaitez dissocier d'une racine, d'une unité d'organisation ou d'un compte.
3. Dans la page Cibles, choisissez la case d'option en regard de la racine, de l'unité d'organisation ou du compte dont vous souhaitez détacher la politique. Vous devrez peut-être développer OUs (choisir le ) pour trouver l'unité d'organisation ou le compte de votre choix.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

La liste des politiques Security Hub jointes est mise à jour. La modification de la politique prend effet immédiatement.

AWS CLI & AWS SDKs

Pour joindre une politique

Les exemples de code suivants illustrent comment utiliser `DetachPolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";
        var targetId = "r-0000";
```

```
            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous DetachPolicyà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour détacher une stratégie d'une racine, d'une unité d'organisation ou d'un compte

L'exemple suivant indique comment détacher une politique d'une unité d'organisation :

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Pour plus de détails sur l'API, reportez-vous DetachPolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Pour plus de détails sur l'API, consultez DetachPolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
TRY.
    lo_org->detachpolicy(
      iv_policyid = iv_policy_id
      iv_targetid = iv_target_id ).
    MESSAGE 'Policy detached from target.' TYPE 'I'.
  CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to detach the policy.' TYPE 'E'.
  CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
  CATCH /aws1/cx_orgtargetnotfoundex.
    MESSAGE 'The specified target does not exist.' TYPE 'E'.
  CATCH /aws1/cx_orgpolicynotattex.
    MESSAGE 'The policy is not attached to the target.' TYPE 'E'.
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous DetachPolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

Le changement de politique prend effet immédiatement, affectant les autorisations des utilisateurs IAM, les rôles et les ressources, le cas échéant, dans le compte attaché ou sur tous les comptes relevant de la racine ou de l'unité d'organisation attachée.

## Obtenir des informations sur les politiques de votre organisation

Cette rubrique décrit les différentes méthodes permettant d'obtenir des informations détaillées sur les politiques de votre organisation. Ces procédures s'appliquent à tous les types de politiques. Vous devez activer un type de politique sur la racine de l'organisation avant de pouvoir attacher des politiques de ce type à des entités de cette racine d'organisation.

Rubriques



## Liste de toutes les politiques

> **Autorisations minimales**
>
> Pour répertorier les politiques au sein de votre organisation, vous devez disposer de l'autorisation suivante :
>
> - `organizations:ListPolicies`

Vous pouvez consulter les politiques de votre organisation dans AWS Management Console ou à l'aide d'une commande AWS Command Line Interface (AWS CLI) ou d'une opération du AWS SDK.

AWS Management Console

Pour répertorier toutes les politiques votre organisation

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques, choisissez le type de politique que vous souhaitez répertorier.

   Si le type de politique spécifié est activé, la console affiche la liste de toutes les politiques de ce type actuellement disponibles dans l'organisation.
3. Retournez à la page Politiques et répétez la procédure pour chaque type de politique.

AWS CLI & AWS SDKs

Les exemples de code suivants illustrent comment utiliser `ListPolicies`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
            MaxResults = 5,
        };
```

```
            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous ListPoliciesà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour extraire une liste de toutes les politiques d'une organisation d'un certain type

L'exemple suivant montre comment obtenir une liste de SCPs, comme indiqué par le paramètre de filtre :

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

La sortie inclut une liste des politiques avec des informations récapitulatives :

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- Pour plus de détails sur l'API, reportez-vous ListPoliciesà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Pour plus de détails sur l'API, consultez ListPolicieslе AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       oo_result = lo_org->listpolicies(       " oo_result is returned for
testing purposes. "
         iv_filter = iv_filter ).
       DATA(lt_policies) = oo_result->get_policies( ).
       MESSAGE 'Retrieved list of policies.' TYPE 'I'.
     CATCH /aws1/cx_orgaccessdeniedex.
       MESSAGE 'You do not have permission to list policies.' TYPE 'E'.
     CATCH /aws1/cx_orgawsorgsnotinuseex.
       MESSAGE 'Your account is not a member of an organization.' TYPE 'E'.
   ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous ListPoliciesà la section de référence du AWS SDK pour l'API SAP ABAP.

## Liste des politiques attachées à une racine, une unité d'organisation ou un compte

> **Autorisations minimales**
>
> Pour répertorier les politiques qui sont attachées à une racine, une unité d'organisation ou un compte au sein de votre entreprise, vous devez disposer de l'autorisation suivante :
>
> - `organizations:ListPoliciesForTarget` avec un élément `Resource` dans la même instruction de politique que celle qui inclut l'Amazon Resource Name (ARN) de la cible spécifiée (ou « * »).

AWS Management Console

Pour répertorier toutes les politiques qui sont attachées directement à une racine, une unité d'organisation ou un compte spécifié

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Comptes AWS, choisissez le nom de la racine, de l'UO ou du compte dont vous souhaitez afficher les politiques. Il se peut que vous deviez développer OUs (choisir le ▶ ) pour trouver l'unité d'organisation souhaitée.
3. Sur la page de la racine, de l'UO ou du compte, choisissez l'onglet Politiques.

   L'onglet Politiques affiche toutes les politiques attachées à cette racine, cette UO ou ce compte, regroupées par type de politique.

AWS CLI & AWS SDKs

Pour répertorier toutes les politiques qui sont attachées directement à une racine, une UO ou un compte spécifié

Vous pouvez utiliser l'une des commandes suivantes pour répertorier les politiques qui sont attachées à une entité :

- AWS CLI: list-policies-for-target

  L'exemple suivant répertorie toutes les politiques de contrôle des services attachées à l'unité d'organisation spécifiée. Vous devez spécifier à la fois l'ID de la racine, de l'unité d'organisation ou du compte et le type de politique que vous souhaitez répertorier.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
```

```
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPoliciesForTarget

## Liste de toutes les OUs racines et de tous les comptes auxquels une politique est attachée

> **Autorisations minimales**
>
> Pour répertorier les entités auxquelles une politique est attachée, vous devez disposer de l'autorisation suivante :
>
> - `organizations:ListTargetsForPolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

### AWS Management Console

Pour répertorier toutes les OUs racines et tous les comptes associés à une politique spécifiée

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques, choisissez le type de politique, puis choisissez le nom de la politique dont vous souhaitez examiner les attachements.
3. Choisissez l'onglet Cibles pour afficher une table de chaque racine, unité d'organisation et compte auxquels la politique choisie est attachée.

### AWS CLI & AWS SDKs

Pour répertorier toutes les OUs racines et tous les comptes associés à une politique spécifiée

Vous pouvez utiliser l'une des commandes suivantes pour répertorier les entités dotées d'une politique :

- AWS CLI: list-targets-for-policy

  L'exemple suivant montre toutes les pièces jointes à root et tient compte de la politique spécifiée. OUs

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWS SDKs: ListTargetsForPolicy

# Obtention de détails sur une politique

**Autorisations minimales**

Pour afficher les détails d'une politique, vous devez disposer de l'autorisation suivante :

- `organizations:DescribePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique spécifiée (ou « * »).

AWS Management Console

Pour obtenir des détails sur une politique

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques, choisissez le type de politique de la politique à examiner, puis choisissez le nom de la politique.

   La page de politique affiche les informations disponibles sur la politique, notamment son ARN, sa description et ses attachements.

   - L'onglet Contenu affiche le contenu actuel de la politique au format JSON.
   - L'onglet Cibles affiche la liste des racines et des comptes auxquels la politique est attachée. OUs
   - L'onglet Balises affiche les balises attachées à la politique. Remarque : l'onglet Balises n'est pas disponible pour les politiques gérées AWS .

   Pour modifier la politique, choisissez Modifier la politique. Étant donné que chaque type de politique a des exigences de mise à jour différentes, reportez-vous aux instructions de création et de mise à jour des politiques du type de politique spécifié.

AWS CLI & AWS SDKs

Les exemples de code suivants illustrent comment utiliser `DescribePolicy`.

CLI

AWS CLI

Pour obtenir les informations sur une politique

L'exemple suivant montre comment demander des informations sur une politique :

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

La sortie inclut un objet de politique contenant des informations sur la politique :

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Pour plus de détails sur l'API, reportez-vous DescribePolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Pour plus de détails sur l'API, consultez DescribePolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

## SAP ABAP

### Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        oo_result = lo_org->describepolicy(     " oo_result is returned for
testing purposes. "
          iv_policyid = iv_policy_id ).
        DATA(lo_policy) = oo_result->get_policy( ).
        MESSAGE 'Retrieved policy details.' TYPE 'I'.
      CATCH /aws1/cx_orgaccessdeniedex.
```

```
        MESSAGE 'You do not have permission to describe the policy.' TYPE 'E'.
      CATCH /aws1/cx_orgpolicynotfoundex.
        MESSAGE 'The specified policy does not exist.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous DescribePolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

# Supprimer les politiques de l'organisation avec AWS Organizations

Lorsque vous n'avez plus besoin d'une politique et que vous l'avez détachée de toutes les unités organisationnelles (OUs) et de tous les comptes, vous pouvez la supprimer.

Cette rubrique décrit comment supprimer des politiques avec AWS Organizations. Une politique définit les contrôles que vous souhaitez appliquer à un groupe de Comptes AWS.

Rubriques

- Supprimer les politiques avec AWS Organizations

## Supprimer les politiques avec AWS Organizations

Quand vous êtes connecté au compte de gestion de votre organisation, vous pouvez supprimer une politique dont vous n'avez plus besoin dans votre organisation.

Avant de supprimer une politique, vous devez d'abord la détacher de toutes les entités attachées.

> **Note**
>
> - Vous ne pouvez supprimer aucun SCP AWS géré tel que le SCP nommé. `FullAWSAccess`
> - Vous ne pouvez supprimer aucun RCP AWS géré tel que le RCP nommé. `RCPFullAWSAccess`

> **Autorisations minimales**
>
> Pour supprimer une politique, vous devez être autorisé à exécuter l'action suivante :

- `organizations:DeletePolicy`

AWS Management Console

Service control policies (SCPs)

Pour supprimer une SCP

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Politiques de contrôle des services, choisissez le nom de la SCP que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.
4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

Resource control policies (RCPs)

Pour supprimer un RCP

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de contrôle des ressources, choisissez le nom du RCP que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles,

puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.

4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

### Declarative policies

Pour supprimer une politique déclarative

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques déclaratives, choisissez le nom de la politique que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.
4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

### Backup policies

Pour supprimer une politique de sauvegarde

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de sauvegarde, choisissez le nom de la politique de sauvegarde que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique de sauvegarde que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case

d'option en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.

4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

Tag policies

Pour supprimer une politique de balises

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques relatives aux balises, choisissez la politique que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.
4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

Chat applications policies

Pour supprimer une politique d'applications de chat

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Chatbot, choisissez le nom de la politique que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option

en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.

4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

### AI services opt-out policies

Pour supprimer une politique de désactivation des services IA

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Politiques de désactivation des services IA, choisissez le nom de la politique que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.
4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

### Security Hub policies

Pour supprimer une politique Security Hub

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page des politiques du Security Hub, choisissez le nom de la politique que vous souhaitez supprimer.
3. Vous devez d'abord détacher la politique que vous souhaitez supprimer de toutes les racines et de tous OUs les comptes. Choisissez l'onglet Cibles, cochez la case d'option

en regard de chaque racine, unité d'organisation ou compte affiché dans la liste Cibles, puis choisissez Détacher. Dans la boîte de dialogue de confirmation, choisissez Détacher. Répétez l'opération jusqu'à ce que toutes les cibles soient supprimées.

4. En haut de la page, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

AWS CLI & AWS SDKs

Pour supprimer une politique

Les exemples de code suivants illustrent comment utiliser `DeletePolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
```

```
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";

            var request = new DeletePolicyRequest
            {
                PolicyId = policyId,
            };

            var response = await client.DeletePolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous DeletePolicyà la section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour supprimer une politique

L'exemple suivant montre comment supprimer une stratégie d'une organisation. L'exemple suppose que vous avez préalablement détaché la stratégie de toutes les entités :

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Pour plus de détails sur l'API, reportez-vous DeletePolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Pour plus de détails sur l'API, consultez DeletePolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        lo_org->deletepolicy(
          iv_policyid = iv_policy_id ).
        MESSAGE 'Policy deleted.' TYPE 'I'.
      CATCH /aws1/cx_orgaccessdeniedex.
        MESSAGE 'You do not have permission to delete the policy.' TYPE 'E'.
      CATCH /aws1/cx_orgpolicynotfoundex.
        MESSAGE 'The specified policy does not exist.' TYPE 'E'.
      CATCH /aws1/cx_orgpolicyinuseex.
        MESSAGE 'The policy is still attached to one or more targets.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous DeletePolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

# Ressources de balisage AWS Organizations

Une balise est une étiquette d'attribut personnalisée que vous ajoutez à une AWS ressource pour faciliter l'identification, l'organisation et la recherche de ressources. Chaque balise se compose de deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Une clé de balise est sensible à la casse et peut contenir 128 caractères au plus.
- Une valeur de balise (par exemple, `111122223333` ou `Production`). Les valeurs de balise peuvent comporter jusqu'à 256 caractères et, comme les clés de balise, sont sensibles à la casse. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si la valeur de balise est omise, cela équivaut à utiliser une chaîne vide.

Pour plus d'informations sur les caractères autorisés dans une clé ou une valeur de balise, consultez Paramètre Tags de l'API Tag dans la Référence d'API de balisage de Resource Groups.

Vous pouvez utiliser des balises pour classer les ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour plus d'informations, consultez la section Meilleures pratiques en matière de balisage AWS des ressources.

> **Tip**
>
> Vous pouvez utiliser des politiques de balises pour vous aider à standardiser les balises entre les ressources des comptes de votre organisation.

Rubriques



## Considérations

AWS Organizations prend en charge les opérations de balisage suivantes lorsque vous êtes connecté au compte de gestion :

Vous pouvez ajouter des balises aux ressources d'organisation suivantes

- Comptes AWS
- Unités organisationnelles
- Racine de l'organisation
- Stratégies

Vous pouvez ajouter des tags aux moments suivants

- Lorsque vous créez la ressource : spécifiez les balises dans la console Organizations ou utilisez le paramètre `Tags` avec l'un des opérations d'API `Create`. Cela ne s'applique pas à la racine de l'organisation.
- Après avoir créé la ressource : utilisez la console Organizations ou appelez l'opération `TagResource`.

Autres considérations

Vous pouvez afficher les balises de toutes les ressources pouvant être AWS Organizations étiquetées en utilisant la console ou en appelant l'`ListTagsForResource`opération.

Vous pouvez supprimer des balises d'une ressource en spécifiant les clés à supprimer à l'aide de la console ou en appelant l'opération `UntagResource`.

# Utilisation de balises

Les balises vous permettent d'organiser les ressources de votre organisation en les regroupant en catégories pertinentes. Par exemple, vous pouvez affecter une balise « Department » qui suit le département propriétaire. Vous pouvez affecter une balise « Environment » pour suivre si une ressource donnée fait partie de vos environnements alpha, bêta, gamma ou de production.

Vous pouvez également utiliser des balises pour :

- Appliquez des normes de balisage à vos ressources.
- Contrôler l'accès à vos ressources.

# Ajout, mise à jour et suppression de balises

Lorsque vous vous connectez au compte de gestion de votre organisation, vous pouvez ajouter des balises aux ressources de votre organisation.

## Ajout de balises lors de la création d'une ressource

Autorisations minimales

Pour ajouter des balises à une ressource lorsque vous la créez, vous avez besoin des autorisations suivantes :

- Autorisation de créer une ressource du type spécifié
- `organizations:TagResource`
- `organizations:ListTagsForResource` — requis uniquement si vous utilisez la console Organizations

Vous pouvez inclure des clés et des valeurs de balise qui sont attachées aux ressources suivantes lors de leur création.

- Compte AWS
  - Compte créé
  - Compte invité
- Unité d'organisation (UO)
- Politique
  - Politique de contrôle des services
  - Politique de contrôle des ressources
  - Politique déclarative
  - Politique de sauvegarde
  - Politique de balises
  - Politique relative aux applications de chat
  - Politique de désactivation des services IA

La racine de l'organisation est créée lors de la création initiale de l'organisation, de sorte que vous ne pouvez y ajouter des balises qu'en tant que ressource existante.

## Ajout ou mise à jour de balises pour une ressource existante

Vous pouvez également ajouter de nouvelles balises ou mettre à jour les valeurs des balises attachées à des ressources existantes.

> **Autorisations minimales**
>
> Pour ajouter des balises aux ressources de votre organisation ou les mettre à jour, vous avez besoin des autorisations suivantes :
>
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` — requis uniquement si vous utilisez la console Organizations
>
> Pour supprimer des balises de ressources de votre organisation, vous avez besoin des autorisations suivantes :
>
> - `organizations:UntagResource`

AWS Management Console

Pour ajouter, mettre à jour ou supprimer des balises pour une ressource existante

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Accédez au compte, à la racine, à l'unité d'organisation ou à la politique, choisissez son nom puis cliquez dessus pour ouvrir sa page de détails.
3. Dans l'onglet Balises, choisissez Gérer les balises.
4. Vous pouvez ajouter de nouvelles balises, modifier les valeurs de balises existantes ou supprimer des balises.

   Pour ajouter une balise, choisissez Ajouter une balise, puis saisissez une Clé et éventuellement une Valeur pour la balise.

Pour supprimer une identification, choisissez Supprimer.

Les clés et les valeurs des balises distinguent les majuscules et minuscules. Utilisez la capitalisation que vous souhaitez standardiser. Vous devez également vous conformer aux exigences de toutes les politiques de balises qui s'appliquent.

5. Répétez l'étape précédente autant de fois que vous le souhaitez.
6. Choisissez Enregistrer les modifications.

AWS CLI & AWS SDKs

Pour ajouter des balises à une ressource existante ou les mettre à jour

Vous pouvez utiliser l'une des commandes suivantes pour ajouter des balises aux ressources balisables de votre organisation :

- AWS CLI : tag-resource
- AWS SDKs: TagResource

Pour supprimer des balises d'une ressource de votre organisation

Vous pouvez utiliser l'une des commandes suivantes pour supprimer des balises :

- AWS CLI : untag-resource
- AWS SDKs: UntagResource

# Approbation multipartite pour AWS Organizations

L'approbation multipartite est une fonctionnalité AWS Organizationsqui vous permet de protéger une liste prédéfinie d'opérations par le biais d'un processus d'approbation distribué. Utilisez l'approbation multipartite pour établir des flux de travail d'approbation et transformer les processus de sécurité en décisions basées sur le travail d'équipe.

Quand utiliser l'approbation multipartite :

- Vous devez vous aligner sur le principe Zero Trust selon lequel « ne faites jamais confiance, vérifiez toujours »
- Vous devez vous assurer que les bons humains ont accès aux bonnes choses de la bonne manière
- Vous avez besoin d'une prise de décision distribuée pour les opérations sensibles ou critiques
- Vous devez vous protéger contre les opérations imprévues sur des ressources sensibles ou critiques
- Vous avez besoin d'examens et d'approbations formels pour des raisons d'audit ou de conformité

Pour plus d'informations, voir Qu'est-ce que l'approbation multipartite dans le Guide de l'utilisateur de l'approbation multipartite.

# Utilisation AWS Organizations avec d'autres Services AWS

Vous pouvez utiliser l'accès sécurisé pour permettre à un AWS service pris en charge que vous spécifiez, appelé service sécurisé, d'effectuer des tâches au sein de votre organisation et de ses comptes en votre nom. Cela implique l'octroi d'autorisations au service approuvé mais n'affecte pas par ailleurs les autorisations pour les utilisateurs et les rôles . Lorsque vous activez l'accès, le service approuvé peut créer un rôle IAM appelé rôle lié à un service dans chaque compte de votre organisation, chaque fois qu'il en a besoin. Ce rôle dispose d'une politique d'autorisations qui autorise le service approuvé à effectuer les tâches qui sont décrites dans la documentation de ce service. Cela vous permet de spécifier des paramètres et des détails de configuration que vous voulez que le service approuvé gère en votre nom dans les comptes de votre organisation. Le service approuvé crée des rôles liés au service uniquement lorsqu'il doit effectuer des actions de gestion au niveau des comptes, et pas nécessairement dans tous les comptes de l'organisation.

**Important**

Lorsque l'option est disponible, nous vous recommandons vivement d'activer et de désactiver l'accès sécurisé en utilisant uniquement la console du service sécurisé, ou ses équivalents de fonctionnement AWS CLI ou d'API. Cela permet au service approuvé d'effectuer toute initialisation requise lors de l'activation de l'accès approuvé, par exemple la création des ressources requises et le nettoyage qui s'impose des ressources lors de la désactivation de l'accès approuvé.

Pour plus d'informations sur la façon d'activer ou de désactiver l'accès aux services approuvés à votre organisation à l'aide du service approuvé, consultez En savoir plussous la colonne Prise en charge de l'accès approuvé à l'adresse Services AWS que vous pouvez utiliser avec AWS Organizations.

Si vous désactivez l'accès à l'aide de la console Organizations, de commandes CLI ou d'opérations API, il se passe ce qui suit :

- Le service ne peut plus créer un rôle lié à un service dans les comptes de votre organisation. Cela signifie que le service ne peut pas effectuer d'opérations en votre nom sur les nouveaux comptes de votre organisation. Le service peut toujours effectuer des opérations dans des comptes plus anciens jusqu'à ce que le service ait terminé son nettoyage à partir d' AWS Organizations.
- Le service ne peut plus effectuer de tâches dans les comptes de membres de l'organisation, sauf si ces opérations sont explicitement autorisées par les politiques IAM

associées à vos rôles. Cela inclut toute agrégation de données des comptes membres vers le compte de gestion ou vers un compte d'administrateur délégué, le cas échéant.

- Certains services détectent cela et nettoient toutes les données ou ressources restantes liées à l'intégration, tandis que d'autres services cessent d'accéder à l'organisation, mais laissent les données historiques et la configuration en place pour prendre en charge une éventuelle réactivation de l'intégration.

Au lieu de cela, en utilisant la console ou des commandes de l'autre service pour désactiver l'intégration, vous permettez à l'autre service de nettoyer toutes les ressources nécessaires uniquement pour l'intégration. La façon dont le service nettoie ses ressources dans les comptes de l'organisation dépend de ce service. Pour plus d'informations, consultez la documentation de l'autre service AWS .

## Autorisations requises pour activer l'accès approuvé

L'accès sécurisé nécessite des autorisations pour deux services : AWS Organizations et le service sécurisé. Pour activer l'accès approuvé, choisissez l'un des scénarios suivants :

- Si vous disposez d'informations d'identification avec des autorisations à la fois dans le service sécurisé AWS Organizations et dans le service sécurisé, activez l'accès à l'aide des outils (console ou AWS CLI) fournis par le service sécurisé. Cela permet au service d'activer un accès sécurisé AWS Organizations en votre nom et de créer toutes les ressources nécessaires au fonctionnement du service dans votre organisation.

  Les autorisations minimales pour ces informations d'identification sont les suivantes :

  - `organizations:EnableAWSServiceAccess`. Vous pouvez également utiliser la clé de condition `organizations:ServicePrincipal` avec cette opération pour limiter les demandes que ces opérations effectuent à une liste de noms de principaux de service approuvé. Pour de plus amples informations, veuillez consulter Clés de condition.
  - `organizations:ListAWSServiceAccessForOrganization`— Obligatoire si vous utilisez la AWS Organizations console.
  - Les autorisations minimales qui sont requises par le service approuvé dépendent du service. Pour plus d'informations, consultez la documentation du service approuvé.

- Si une personne possède des informations d'identification avec des autorisations AWS Organizations mais qu'une autre possède des informations d'identification avec des autorisations dans le service sécurisé, effectuez ces étapes dans l'ordre suivant :

  1. La personne qui possède des informations d'identification et des autorisations AWS Organizations doit utiliser la AWS Organizations console AWS CLI, le ou un AWS SDK pour permettre un accès sécurisé au service sécurisé. Cette opération accorde à l'autre service l'autorisation d'effectuer sa configuration requise dans l'organisation lorsque l'étape suivante (étape 2) est exécutée.

     Les AWS Organizations autorisations minimales sont les suivantes :

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`— Obligatoire uniquement si vous utilisez la AWS Organizations console

     Pour connaître les étapes permettant d'activer l'accès sécurisé dans AWS Organizations, voirProcédure pour activer ou désactiver l'accès approuvé.

  2. La personne qui dispose des informations d'identification avec des autorisations dans le service approuvé permet à ce service de fonctionner avec AWS Organizations. Cela indique au service d'effectuer toute initialisation nécessaire, telle que la création de toutes les ressources requises par le service approuvé pour fonctionner dans l'organisation. Pour plus d'informations, consultez les instructions propres au service concerné dans Services AWS que vous pouvez utiliser avec AWS Organizations.

## Autorisations requises pour désactiver l'accès approuvé

Lorsque vous ne voulez plus autoriser le service approuvé à fonctionner dans votre organisation ni ses comptes, choisissez l'un des scénarios suivants.

> **Important**
>
> La désactivation de l'accès au service approuvé n'empêche pas les utilisateurs et les rôles dotés des autorisations appropriées d'utiliser ce service. Pour empêcher complètement les utilisateurs et les rôles d'accéder à un AWS service, vous pouvez supprimer les autorisations IAM qui accordent cet accès, ou vous pouvez utiliser les politiques de contrôle des services (SCPs) dans AWS Organizations.

Vous ne pouvez faire une demande que SCPs pour les comptes des membres. SCPs ne s'appliquent pas au compte de gestion. Nous vous recommandons de ne pas exécuter de services dans le compte de gestion. Exécutez-les plutôt dans des comptes membres où vous pouvez contrôler la sécurité en utilisant SCPs.

- Si vous disposez d'informations d'identification avec des autorisations à la fois pour le service sécurisé AWS Organizations et pour le service sécurisé, désactivez l'accès à l'aide des outils (console ou AWS CLI) disponibles pour le service sécurisé. Le service est ensuite nettoyé via la suppression des ressources qui ne sont plus nécessaires et la désactivation de l'accès approuvé pour le service dans AWS Organizations en votre nom.

  Les autorisations minimales pour ces informations d'identification sont les suivantes :

  - `organizations:DisableAWSServiceAccess`. Vous pouvez également utiliser la clé de condition `organizations:ServicePrincipal` avec cette opération pour limiter les demandes que ces opérations effectuent à une liste de noms de principaux de service approuvé. Pour de plus amples informations, veuillez consulter Clés de condition.
  - `organizations:ListAWSServiceAccessForOrganization`— Obligatoire si vous utilisez la AWS Organizations console.
  - Les autorisations minimales requises par le service approuvé dépendent du service. Pour plus d'informations, consultez la documentation du service approuvé.
- Si les informations d'identification contenant des autorisations AWS Organizations ne sont pas celles du service sécurisé, effectuez ces étapes dans l'ordre suivant :
  1. La personne avec des autorisations dans le service approuvé commence par désactiver l'accès à l'aide de ce service. Cela ordonne au service approuvé de nettoyer en supprimant les ressources requises pour l'accès approuvé. Pour plus d'informations, consultez les instructions propres au service concerné dans Services AWS que vous pouvez utiliser avec AWS Organizations.
  2. La personne autorisée AWS Organizations peut ensuite utiliser la AWS Organizations console ou un AWS SDK pour désactiver l'accès au service sécurisé. AWS CLI Cela élimine de l'organisation et de ses comptes les autorisations pour le service approuvé.

     Les AWS Organizations autorisations minimales sont les suivantes :

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`— Obligatoire uniquement si vous utilisez la AWS Organizations console

Pour connaître les étapes à suivre pour désactiver l'accès sécurisé dans AWS Organizations, consultezProcédure pour activer ou désactiver l'accès approuvé.

# Procédure pour activer ou désactiver l'accès approuvé

Si vous disposez d'autorisations uniquement pour AWS Organizations et que vous souhaitez activer ou désactiver l'accès sécurisé à votre organisation au nom de l'administrateur de l'autre AWS service, suivez la procédure suivante.

**Important**

Lorsque l'option est disponible, nous vous recommandons vivement d'activer et de désactiver l'accès sécurisé en utilisant uniquement la console du service sécurisé, ou ses équivalents de fonctionnement AWS CLI ou d'API. Cela permet au service approuvé d'effectuer toute initialisation requise lors de l'activation de l'accès approuvé, par exemple la création des ressources requises et le nettoyage qui s'impose des ressources lors de la désactivation de l'accès approuvé.
Pour plus d'informations sur la façon d'activer ou de désactiver l'accès aux services approuvés à votre organisation à l'aide du service approuvé, consultez En savoir plussous la colonne Prise en charge de l'accès approuvé à l'adresse Services AWS que vous pouvez utiliser avec AWS Organizations.
Si vous désactivez l'accès à l'aide de la console Organizations, de commandes CLI ou d'opérations API, il se passe ce qui suit :

- Le service ne peut plus créer un rôle lié à un service dans les comptes de votre organisation. Cela signifie que le service ne peut pas effectuer d'opérations en votre nom sur les nouveaux comptes de votre organisation. Le service peut toujours effectuer des opérations dans des comptes plus anciens jusqu'à ce que le service ait terminé son nettoyage à partir d' AWS Organizations.
- Le service ne peut plus effectuer de tâches dans les comptes de membres de l'organisation, sauf si ces opérations sont explicitement autorisées par les politiques IAM associées à vos rôles. Cela inclut toute agrégation de données des comptes membres vers le compte de gestion ou vers un compte d'administrateur délégué, le cas échéant.
- Certains services détectent cela et nettoient toutes les données ou ressources restantes liées à l'intégration, tandis que d'autres services cessent d'accéder à l'organisation, mais

laissent les données historiques et la configuration en place pour prendre en charge une éventuelle réactivation de l'intégration.

Au lieu de cela, en utilisant la console ou des commandes de l'autre service pour désactiver l'intégration, vous permettez à l'autre service de nettoyer toutes les ressources nécessaires uniquement pour l'intégration. La façon dont le service nettoie ses ressources dans les comptes de l'organisation dépend de ce service. Pour plus d'informations, consultez la documentation de l'autre AWS service.

AWS Management Console

Pour activer l'accès au service approuvé

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Services, recherchez la ligne du service que vous souhaitez activer et choisissez son nom.
3. Choisissez Activer l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, cochez la case Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
5. Si vous activez l'accès, dites à l'administrateur de l'autre AWS service qu'il peut désormais activer l'autre service pour qu'il fonctionne avec celui-ci AWS Organizations.

Pour désactiver l'accès au service approuvé

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans la page Services, recherchez la ligne du service que vous souhaitez désactiver et choisissez son nom.
3. Attendez que l'administrateur de l'autre service vous indique que le service est désactivé et que les ressources ont été nettoyées.

4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.

AWS CLI, AWS API

Pour activer ou désactiver l'accès à un service approuvé

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour activer ou désactiver l'accès aux services sécurisés :

- AWS CLI: AWS organisations enable-aws-service-access
- AWS CLI: AWS organisations disable-aws-service-access
- AWS API : Activer AWSService l'accès
- AWS API : Désactiver AWSService l'accès

# AWS Organizations et rôles liés aux services

AWS Organizations utilise des rôles liés aux services IAM pour permettre aux services fiables d'effectuer des tâches en votre nom sur les comptes membres de votre organisation. Lorsque vous configurez un service approuvé et l'autorisez à s'intégrer à votre organisation, ce service peut demander à ce qu' AWS Organizations crée un rôle lié à un service dans son compte membre. Le service approuvé fait cela de façon asynchrone selon les besoins et pas nécessairement dans tous les comptes de l'organisation au même moment. Le rôle lié à un service possède des autorisations IAM prédéfinies qui permettent au service approuvé d'effectuer uniquement des tâches spécifiques au sein de ce compte. D'une manière générale, AWS gère tous les rôles liés à un service. En d'autres termes, vous ne pouvez pas modifier les rôles ou les politiques attachées.

Pour rendre cela possible, lorsque vous créez un compte dans une organisation ou lorsque vous acceptez une invitation à joindre votre compte existant à une organisation, AWS Organizations alloue au compte membre un rôle lié à un service nommé `AWSServiceRoleForOrganizations`. Seul le AWS Organizations service lui-même peut assumer ce rôle. Le rôle dispose d'autorisations qui permettent de créer des rôles liés AWS Organizations à un service pour d'autres personnes. Services AWS Ce rôle lié à un service est présent dans toutes les organisations.

Bien que cela ne soit pas conseillé, si seules des fonctions de facturation consolidée sont activées pour votre organisation, le rôle lié à un service nommé `AWSServiceRoleForOrganizations` n'est jamais utilisé et vous pouvez le supprimer. Si par la suite vous souhaitez activer toutes les fonctions

dans votre organisation, le rôle sera requis et vous devrez le restaurer. Les vérifications suivantes sont effectuées lorsque vous initiez le processus d'activation de toutes les fonctions :

- Pour chaque compte membre qui a été invité à rejoindre l'organisation : l'administrateur du compte reçoit un message lui demandant son accord d'activer toutes les fonctions. Pour accepter la demande, l'administrateur doit avoir les autorisations `organizations:AcceptHandshake` et `iam:CreateServiceLinkedRole` si le rôle lié à un service (`AWSServiceRoleForOrganizations`) n'existe pas déjà. Si le rôle `AWSServiceRoleForOrganizations` existe déjà, l'administrateur a uniquement besoin de l'autorisation `organizations:AcceptHandshake` pour accepter la demande. Lorsque l'administrateur accepte la demande, AWS Organizations crée le rôle lié au service s'il n'existe pas déjà.
- Pour chaque compte membre qui a été créé dans l'organisation : l'administrateur du compte reçoit une demande de recréer le rôle lié à un service. (L'administrateur du compte membre ne reçoit aucune demande visant à activer toutes les fonctions dans la mesure où l'administrateur du compte de gestion (anciennement appelé « compte principal ») est considéré comme le propriétaire des comptes membres créés.) AWS Organizations crée le rôle lié à un service lorsque l'administrateur du compte membre accepte la demande. L'administrateur doit disposer des autorisations `organizations:AcceptHandshake` et `iam:CreateServiceLinkedRole` pour accepter la proposition avec succès.

Après avoir activé toutes les fonctions dans votre organisation, vous n'aurez plus la possibilité de supprimer le rôle lié au service `AWSServiceRoleForOrganizations` dans aucun des comptes.

> **Important**
>
> AWS Organizations SCPs n'affectez jamais les rôles liés aux services. Ces rôles sont dispensés de toute restriction SCP.

## Utilisation du rôle lié au service AWSService RoleForDeclarativePolicies EC2 Report

Le rôle `AWSServiceRoleForDeclarativePoliciesEC2Report` lié à un service est utilisé par les Organisations pour décrire les états des attributs des comptes membres afin de créer des rapports

sur les politiques déclaratives. Les autorisations du rôle sont définies dans leAWS politique gérée : DeclarativePoliciesEC2Report.

# Services AWS que vous pouvez utiliser avec AWS Organizations

AWS Organizations Vous pouvez ainsi effectuer des activités de gestion de comptes à grande échelle en consolidant plusieurs comptes au Comptes AWS sein d'une seule organisation. La consolidation des comptes simplifie l'utilisation des autres comptes Services AWS. Vous pouvez tirer parti des services de gestion multicomptes disponibles dans AWS Organizations Select Services AWS pour effectuer des tâches sur tous les comptes membres de votre organisation.

Le tableau suivant répertorie les services Services AWS que vous pouvez utiliser et AWS Organizations les avantages de l'utilisation de chaque service à l'échelle de l'organisation.

Accès fiable : vous pouvez activer un AWS service compatible pour effectuer des opérations Comptes AWS dans l'ensemble de votre organisation. Pour de plus amples informations, veuillez consulter Utilisation AWS Organizations avec d'autres Services AWS.

Administrateur délégué pour Services AWS : un AWS service compatible peut enregistrer un compte de AWS membre dans l'organisation en tant qu'administrateur des comptes de l'organisation dans ce service. Pour de plus amples informations, veuillez consulter Administrateur délégué pour Services AWS ce travail avec les Organizations.

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Gestion de compte AWS<br><br>Gérez les détails et les métadonnées de l'ensemble Comptes AWS | Gérez les détails du compte, les contacts alternatifs et les régions pour | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| de votre organisation. | tous les Comptes A\ membres de votre organisation. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Application Migration Service<br><br>AWS Application Migration Service permet aux entreprises AWS d' lift-and-shiftaccéder à un grand nombre de serveurs physiques, virtuels ou cloud sans problèmes de compatibilité, sans interruption des performances ou sans longues périodes de transition. | Vous pouvez gérer des migrations à grande échelle sur plusieurs comptes. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Artifact<br><br>Téléchargez les rapports AWS de conformité en matière de sécurité tels que les rapports ISO et PCI. | Vous pouvez accepter des accords pour tous les comptes de votre organisation. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Audit Manager<br><br>Automatisez la collecte continue de preuves pour vous aider à auditer votre utilisation des services cloud. | Auditez en permanence votre AWS utilisation sur plusieurs comptes de votre organisation afin de simplifier la façon dont vous évaluez les risques et la conformité. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Backup<br><br>Gérez et surveillez les sauvegardes sur tous les comptes de votre organisation. | Vous pouvez configurer et gérer des plans de sauvegarde pour l'ensemble de votre organisation ou pour des groupes de comptes au sein de vos unités organisationnelles (OUs). Vous pouvez surveiller de manière centralisée les sauvegard | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | es de tous vos comptes. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Billing and Cost Management<br><br>Fournit une vue d'ensemble de vos données de gestion financière AWS dans le cloud et vous aide à prendre des décisions plus rapides et plus éclairées. | Permet aux données de répartition des coûts fractionnés de récupérer AWS Organizations des informations, le cas échéant, et de collecter des données de télémétrie pour les services de données de répartition des coûts partagés auxquels | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | vous avez souscrit.<br><br>Pour plus d'informations, voir Qu'est-ce que c'est AWS Billing and Cost Management ? dans le guide de l'utilisateur de Billing and Cost Management. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS CloudFormation StackSets<br><br>Créez, mettez à jour ou supprimez des piles dans plusieurs comptes et régions en une seule opération. | Un utilisateur dans le compte de gestion ou un compte administrateur délégué peut créer un jeu de piles avec des autorisations gérées par service qui déploie des instances de piles sur des comptes de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS CloudTrail<br><br>Assurez la gouvernance, la conformité, ainsi que l'audit opérationnel et des risques de votre compte. | Un utilisateur disposant d'un compte de gestion ou d'administrateur délégué peut créer un suivi d'organisation ou un magasin de données d'événements qui journalise tous les événements de tous les comptes d'une organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon CloudWatch<br><br>Surveillez vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez les utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos ressources et vos applications. | L'intégration avec les Organisations présente deux avantages CloudWatch. Tout d'abord, en intégrant Organizations, vous pouvez l'utiliser CloudWatch pour découvrir et comprendre l'état de la configuration télémétrique de vos AWS ressource | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | s à partir d'une vue centrale dans la CloudWatch console.<br><br>Ensuite, lorsque vous pouvez utiliser Network Flow Monitor CloudWatch pour obtenir de la visibilité sur les indicateurs de performance du réseau, en l'intégrant à Organizations, vous pouvez | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | consulter les informations de performance du réseau pour les ressources de plusieurs comptes au lieu d'un seul compte. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Optimiseur de calcul AWS<br><br>Obtenez des recommandations d'optimisation du AWS calcul. | Vous pouvez analyser toutes les ressources qui se trouvent dans les comptes de votre organisation pour obtenir des recommandations d'optimisation.<br><br>Pour de plus amples informations, consultez Comptes pris en charge par Compute Optimizer | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | dans le Guide de l'utilisateur Optimiseur de calcul AWS . | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Config<br><br>Évaluez et auditez les configurations de vos ressources AWS . | Vous pouvez obtenir une vue à l'échelle de l'organisation de votre état de conformité. Vous pouvez également utiliser les opérations AWS Config d'API pour gérer les AWS Config règles et les packs de conformité Comptes A\ dans | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus :<br><br>Règles de configuration<br><br>Packs de conformité<br><br>Regroupement de données multi-comptes et multi-régions | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | l'ensemble de votre organisation.<br><br>Vous pouvez utiliser un compte d'administrateur délégué pour agréger les données de configuration des ressources et de conformité de tous les comptes membres d'une organisation dans AWS Organizations. Pour | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | de plus amples informations, consultez Enregistrer un administrateur délégué dans le Guide du développeur AWS Config . | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Control Tower<br><br>Configurez et gérez un environnement AWS multi-compte conforme et sécurisé. | Vous pouvez configurer une zone d'atterrissage, un environnement multi-comptes pour toutes vos AWS ressources. Cet environnement inclut une organisation et des entités d'organisation. Vous pouvez utiliser cet environnement pour appliquer les réglement | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | ations de conformité à l'ensemble de vos activités Comptes A\<br><br>Pour plus d'informations, consultez Comment AWS Control Tower fonctionne et Gestion des comptes via AWS Organizations dans le Guide de l'utilisateur AWS Control Tower . | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Hub d'optimisation des coûts AWS<br><br>Recueillez des recommandations de coûts pour tous les produits AWS d'optimisation. | Vous pouvez facilement identifier, filtrer et agréger les recommandations d'optimisation des AWS coûts sur l'ensemble de vos comptes AWS Organizations membres et de vos AWS régions.<br><br>Pour plus d'informations, voir Cost Optimization Hub dans le guide de | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | l'utilisateur du Cost Optimization Hub. | | | |
| Amazon Detective<br><br>Générez des visualisations à partir de vos données de journal afin d'analyser, d'examiner et d'identifier rapidement la cause racine des résultats de sécurité ou des activités suspectes. | Vous pouvez intégrer Amazon Detective AWS Organizations pour vous assurer que votre graphe de comportement de Detective fournit une visibilité sur l'activité de tous les comptes de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon DevOps Guru<br><br>Analysez les données opérationnelles, ainsi que les métriques et les événements de l'application afin d'identifier les comportements qui s'écartent des modèles de fonctionnement normaux. Les utilisateurs sont avertis lorsque DevOps Guru détecte un problème ou un risque opérationnel. | Vous pouvez l'intégrer AWS Organizations pour gérer les informations provenant de tous les comptes de l'ensemble de votre organisation. Vous pouvez déléguer un administrateur pour afficher, trier et filtrer les informations de tous les comptes afin | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | d'obtenir l'état de toutes les applications contrôlées à l'échelle de l'organisation. | | | |
| AWS Directory Service<br><br>Configurez et exécutez des annuaires dans le AWS cloud ou connectez vos AWS ressources à un répertoire Microsoft Active Directory existant sur site. | Vous pouvez l'intégrer AWS Organizations pour Directory Service un partage d'annuaire fluide entre plusieurs comptes et n'importe quel VPC d'une région. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon EventBridge<br><br>Surveillez vos AWS ressources et les applications que vous exécutez AWS en temps réel. | Vous pouvez activer le partage de tous les EventBridge événements Amazon, anciennement Amazon CloudWatch Events, sur tous les comptes de votre organisation.<br><br>Pour plus d'informations, consultez la section Envoyer et recevoir | ⊗Non | ⊗Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | des EventBridge événements Amazon entre les deux Comptes A\ dans le guide de EventBridge l'utilisateur Amazon. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon Elastic Compute Cloud<br><br>Amazon VPC IP Address Manager (IPAM) fournit une capacité de calcul évolutive à la demande dans le cloud. AWS | Permettez à l'administrateur des organisations de créer un rapport indiquant la configuration existante pour les comptes de son organisation lors de l'utilisation de la fonctionnalité de politiques déclaratives. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Gestionnaire de capacité EC2<br><br>EC2 Capacity Manager s'est regroupé pour afficher, analyser et gérer votre utilisation des capacités dans le cadre des réservations EC2 On-Demand, Spot et Capacity. | L'utilisation d'EC2 Capacity Manager avec AWS l'intégration de l'organisation vous permet de visualiser, d'analyser et de gérer l'utilisation des capacités dans l'ensemble de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon Elastic Kubernetes Service<br><br>Le tableau de bord Amazon EKS fournit une visibilité et une gestion agrégées des clusters Kubernetes dans le cloud. AWS | Permettez à l'administrateur des organisations de consulter les données du tableau de bord consolidé concernant les ressources du cluster, notamment la distribution des versions, l'état de santé et les exigences de mise à niveau au sein | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | de leur organisation. | | | |
| AWS Firewall Manager<br><br>Configurez et gérez de façon centrale les règles de pare-feu pour les applications web sur l'ensemble de vos comptes et applications. | Vous pouvez configurer et gérer les AWS WAF règles de manière centralisée pour tous les comptes de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon GuardDuty<br><br>GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les informations provenant de diverses sources de données. Il utilise des flux d'intelligence de menaces et le machine learning pour identifier toute activité inattendue et potentiellement non autorisée et malveillante au sein de votre environnement AWS . | Vous pouvez désigner un compte membre GuardDuty pour consulter et gérer tous les comptes de votre organisation. L'ajout de comptes membres active GuardDuty automatiquement ces comptes dans les comptes sélectionnés Région AWS. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | Vous pouvez également automatiser GuardDuty l'activation des nouveaux comptes ajoutés à votre organisation.<br><br>Pour plus d'informations, consultez GuardDuty la section Organizations du guide de GuardDuty l'utilisateur Amazon. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Health<br><br>Bénéficiez d'une visibilité sur les événements susceptibles d'affecter les performances de vos ressources ou les problèmes de disponibilité pour Services AWS. | Vous pouvez agréger AWS Health les événements entre les comptes de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Gestion des identités et des accès AWS<br><br>Contrôlez en toute sécurité l'accès aux AWS ressources. | Vous pouvez utiliser les données sur les services consultés en dernier dans IAM pour vous aider à mieux comprendre les activités AWS au sein de votre organisation. Vous pouvez utiliser ces données pour créer et mettre à jour des politiques de contrôle | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | des services (SCPs) qui limitent l'accès aux seuls AWS services utilisés par les comptes de votre organisation.<br><br>Pour obtenir un exemple, consultez Utilisation des données pour affiner les autorisations d'une unité d'organisation dans le | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | Guide de l'utilisateur IAM.<br><br>La gestion de l'accès root IAM vous permet de gérer de manière centralisée les informations d'identification des utilisateurs root et d'effectuer des tâches privilégiées sur les comptes des membres. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| IAM Access Analyzer<br><br>Analysez les politiques basées sur les ressources de votre AWS environnement pour identifier les politiques qui accordent l'accès à un principal en dehors de votre zone de confiance. | Vous pouvez désigner un compte membre comme administrateur pour IAM Access Analyzer.<br><br>Pour de plus amples informations, consultez Activation d'Access Analyzer dans le Guide de l'utilisateur IAM. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon Inspector<br><br>Analysez automatiquement vos AWS charges de travail pour détecter les vulnérabilités afin de découvrir les instances Amazon EC2 et les images de conteneur résidant dans Amazon ECR afin de détecter les vulnérabilités logicielles et l'exposition involontaire au réseau. | Déléguez un administrateur pour activer ou désactiver les analyses des comptes membres, afficher les données de résultats agrégées de l'ensemble de l'organisation, créer et gérer les règles de suppression.<br><br>Pour plus d'informations, | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | consultez Gestion de plusieurs comptes avec AWS Organizations dans le Guide de l'utilisateur Amazon Inspector. | | | |
| AWS License Manager<br><br>Simplifiez le processus d'apport de licences de logiciels dans le cloud. | Vous pouvez autoriser la découverte entre compte de ressources de calcul dans l'ensemble de votre organisation. | Oui<br><br>En savoir plus | Oui<br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon Macie<br><br>Découvre et classe votre contenu métier stratégique à l'aide du Machine Learning pour vous aider à répondre aux exigences en matière de sécurité des données et de confidentialité. Il évalue en permanence votre contenu stocké dans Amazon S3 et vous informe des problèmes potentiels. | Vous pouvez configurer Amazon Macie pour tous les comptes de votre organisation afin d'obtenir une vue consolidée de toutes vos données dans Amazon S3, sur tous les comptes d'un compte administrateur Macie désigné. Vous pouvez | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | configurer Macie de manière à protéger automatiquement les ressources des nouveaux comptes au fur et à mesure que votre organisation se développe. Vous êtes averti du besoin de corriger les erreurs de configuration de politique dans les compartiments S3 pour | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | l'ensemble de votre organisation. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Managed Services (AMS) Rapports en libre-service (SSR)<br><br>Collecte des données provenant de divers AWS services natifs et donne accès à des rapports sur les principales offres AMS. Le SSR fournit les informations que vous pouvez utiliser pour soutenir les opérations, la gestion des configurations, la gestion des actifs, la gestion de la sécurité et la conformité. | Vous pouvez activer le SSR agrégé, une fonctionnalité qui permet aux clients de consulter des rapports en libre-service consolidés au sein de votre organisation via votre compte de gestion ou un compte d'administrateur délégué. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Marketplace<br><br>Un catalogue numérique compilé qui permet de trouver, acheter, déployer et gérer des logiciels, des données et des services tiers dont vous avez besoin pour créer des solutions personnalisées et pour exercer vos activités. | Vous pouvez partager les licences de vos AWS Marketplace abonnements et achats entre les comptes de votre organisation. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Marketplace Marketplace privée<br><br>Vous fournit un large catalogue de produits disponibles AWS Marketplace, ainsi qu'un contrôle précis de ces produits. | Vous permet de créer plusieurs expériences de marché privées associées à l'ensemble de votre organisation OUs, à un ou plusieurs comptes de votre organisation, chacun avec son propre ensemble de produits approuvés. Vos AWS administr | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | ateurs peuvent également appliquer l'image de marque de l'entreprise à chaque expérience de marché privée avec le logo, le message et la palette de couleurs de votre entreprise ou de votre équipe. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Marketplace tableau de bord des informations sur les<br><br>Vous permet de consulter les contrats et les données d'analyse des coûts pour tous vos AWS Marketplace achats sur les AWS comptes de votre organisation. | AWS Marketplace le tableau de bord des informations sur les achats écoute les modifications apportées à l'organisation, par exemple l'adhésion d'un compte à l'organisation, et agrège les données relatives aux accords correspondants afin de créer ses | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | tableaux de bord. | | | |
| AWS Network Manager<br><br>Vous permet de gérer de manière centralisée votre réseau central AWS Cloud WAN et votre réseau AWS Transit Gateway sur l'ensemble AWS des comptes, des régions et des sites sur site. | Vous pouvez gérer et surveiller de manière centralisée vos réseaux mondiaux grâce aux passerelles de transport et aux ressources associées sur plusieurs AWS comptes au sein de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon Q Developer<br><br>Amazon Q Developer est un assistant conversationnel génératif basé sur l'IA qui peut vous aider à comprendre, créer, étendre et exploiter AWS des applications. | La version d'abonnement payant d'Amazon Q Developer nécessite l'intégration d'Organizations. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Resource Access Manager<br><br>Partagez AWS des ressources spécifiques que vous possédez avec d'autres comptes. | Vous pouvez partager des ressources au sein de votre organisation sans avoir à échanger des invitations supplémentaires. Les ressources que vous pouvez partager incluent des règles de résolveur Route 53, des réservations de capacité | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | à la demande, etc.<br><br>Pour plus d'informations sur les réservations de capacité partagée, consultez le guide de l'utilisateur Amazon EC2 ou le guide de l'utilisateur Amazon EC2.<br><br>Pour obtenir la liste des ressources partageab | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | les, consultez Ressources partageables dans le Guide de l'utilisateur AWS RAM . | | | |
| Explorateur de ressources AWS<br><br>Explorez vos ressources à l'aide d'une expérience semblable à celle d'un moteur de recherche Internet. | Activez la recherche multi-comptes. | ✓Oui<br><br>En savoir plus | ✓Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Security Hub CSPM<br><br>Consultez l'état de votre sécurité AWS et vérifiez que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. | Vous pouvez activer automatiquement le Security Hub CSPM pour tous les comptes de votre organisation, y compris les nouveaux comptes au fur et à mesure de leur ajout. Cela augmente la couverture des contrôles et des conclusio | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | ns du Security Hub CSPM, ce qui fournit une image plus précise de votre niveau de sécurité global. | | | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon S3 Storage Lens<br><br>Obtenez une visibilité de vos métriques d'utilisation et d'activité de stockage Amazon S3 avec des recommandations pratiques pour optimiser le stockage. | Configurez Amazon S3 Storage Lens pour obtenir une visibilité accrue des tendances d'utilisation et d'activité de stockage Amazon S3, ainsi que des recommandations pour tous les comptes membres de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Réponse aux incidents de sécurité<br><br>AWS service de sécurité qui fournit une assistance en direct 24 heures sur 24 et 7 jours sur 7 en cas d'incident de sécurité assisté par un humain afin d'aider les clients à réagir rapidement aux incidents de cybersécurité tels que le vol d'informations d'identification et les attaques par ransomware. | Couverture de sécurité pour l'ensemble de l'organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon Security Lake<br><br>Amazon Security Lake centralise les données de sécurité provenant de sources cloud, sur site et personnalisées dans un lac de données qui est stocké dans votre compte. | Créez un lac de données qui collecte les journaux et les événements de l'ensemble de vos comptes. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Service Catalog<br><br>Créez et gérez des catalogues des services informatiques dont l'utilisation est approuvée sur AWS. | Vous pouvez partager des portefeuilles et copier des produits entre comptes plus facilement, sans partager de portefeuille IDs. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Service Quotas<br><br>Affichez et gérez vos quotas de service, également appelés limites, à partir d'un emplacement centralisé. | Vous pouvez créer un modèle de demande de quotas pour demander automatiquement une augmentation des quotas lorsque les comptes de votre organisation sont créés. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS IAM Identity Center<br><br>Fournissez un accès d'authentification unique pour l'ensemble de vos comptes et de vos applications cloud. | Les utilisateurs peuvent se connecter au portail d' AWS accès à l'aide de leurs informations d'identification professionnelles et accéder aux ressources du compte de gestion ou des comptes membres qui leur ont été attribués. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Systems M<br><br>Améliorez la visibilité et le contrôle de vos AWS ressources. | Vous pouvez synchroniser les données d'exploitation Comptes AV dans l'ensemble de votre organisation à l'aide de Systems Manager Explorer.<br><br>Vous pouvez gérer les modèles, approbations et rapports de changement pour tous les comptes membres | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| | de votre organisation à partir d'un compte d'administrateur délégué à l'aide de Systems Manager Change Manager. | | | |
| Notifications des utilisateurs AWS<br><br>Un emplacement central pour vos AWS notifications. | Vous pouvez configurer et consulter les notifications de manière centralisée pour tous les comptes de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Stratégies de balises<br><br>Utilisez des balises standardisées dans toutes les ressources des comptes de votre organisation. | Vous pouvez créer des politiques de balises pour définir les règles de balisage de ressources et types de ressources spécifiques et les attacher à des unités d'organisation et des comptes afin de contraindre l'application de ces règles. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Trusted Advisor<br><br>Trusted Advisor inspecte votre AWS environnement et émet des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. | Effectuez Trusted Advisor des vérifications pour tous les Comptes AV membres de votre organisation. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| AWS Well-Architected Tool<br><br>Il vous AWS Well-Architected Tool aide à documenter l'état de vos charges de travail et à les comparer aux meilleures pratiques AWS architecturales les plus récentes. | Permet aux clients de Both AWS WA Tool et Organizations de simplifier le processus de partage AWS WA Tool des ressources avec les autres membres de leur organisation. | Oui<br><br>En savoir plus | Non | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Amazon VPC IP Address Manager (IPAM)<br><br>L'IPAM est une fonctionnalité VPC qui vous permet de planifier, de suivre et de surveiller plus facilement les adresses IP pour AWS vos charges de travail. | Contrôlez l'utilisation des adresses IP à l'échelle de votre organisation et partagez des groupes d'adresses IP entre les comptes membres. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

| AWS service | Avantages de l'utilisation avec AWS Organizations | Prise en charge de l'accès approuvé | Prise en charge de l'administrateur délégué | |
|---|---|---|---|---|
| Analyseur d'accessibilité Amazon VPC<br><br>Reachability Analyzer est un outil d'analyse de configuration qui vous permet d'effectuer des tests de connectivité entre une ressource source et une ressource de destination dans vos clouds privés virtuels (). VPCs | Tracez les chemins entre les comptes de vos organisations. | Oui<br><br>En savoir plus | Oui<br><br>En savoir plus | |

## Gestion de compte AWS et AWS Organizations

Gestion de compte AWS vous aide à gérer les informations de compte et les métadonnées pour tous les Comptes AWS membres de votre organisation. Vous pouvez définir, modifier ou supprimer les autres informations de contact pour chaque compte membre de votre organisation. Pour plus

d'informations, consultez Utilisation d' Gestion de compte AWS dans votre organisation dans le Guide de l'utilisateur Gestion de compte AWS .

Utilisez les informations suivantes pour vous aider Gestion de compte AWS à intégrer AWS Organizations.

## Pour activer l'accès approuvé à Account Management

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

La gestion des comptes nécessite un accès AWS Organizations sécurisé pour que vous puissiez désigner un compte de membre comme administrateur délégué de ce service pour votre organisation.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Gestion de compte AWSdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de Gestion de compte AWS dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le Gestion de compte AWS qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer Gestion de compte AWS en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Pour désactiver l'accès approuvé auprès d'Account Manager

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec Gestion de compte AWS.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Gestion de compte AWSdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).

5. Dans la boîte de Gestion de compte AWS dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le Gestion de compte AWS qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver Gestion de compte AWS en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte administrateur délégué pour Account Management

Lorsque vous désignez un compte membre comme administrateur délégué de l'organisation, les utilisateurs et les rôles du compte désigné peuvent gérer les métadonnées Compte AWS pour les autres comptes membres de l'organisation. Si vous n'activez pas de compte administrateur délégué, seul le compte de gestion de l'organisation peut effectuer ces tâches. Cela vous permet de séparer la gestion de l'organisation de celle des détails de votre compte.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre comme administrateur délégué pour Account Management dans l'organisation.

Pour des instructions générales sur la configuration d'une politique de délégation, consultez la rubrique Créez une politique de délégation basée sur les ressources avec AWS Organizations.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

## AWS Application Migration Service (Service de migration d'applications) et AWS Organizations

AWS Application Migration Service simplifie, accélère et réduit le coût de la migration des applications vers. AWS En intégrant Organizations, vous pouvez utiliser la fonctionnalité de vue globale pour gérer des migrations à grande échelle sur plusieurs comptes. Pour plus d'informations, consultez la section Configuration de votre application AWS Organizations dans le guide de l'utilisateur du service de migration des applications.

Utilisez les informations suivantes pour vous aider AWS Application Migration Service à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet au service de migration d'applications d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Application Migration Service et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForApplicationMigrationService`

## Principaux de service utilisés par le service de migration d'applications

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés au service utilisés par le service de migration d'applications accordent l'accès aux principaux de service suivants :

- `mgn.amazonaws.com`

## Permettre un accès fiable avec le service de migration d'applications

Lorsque vous activez l'accès sécurisé avec Application Migration Service, vous pouvez utiliser la fonction d'affichage global, qui vous permet de gérer des migrations à grande échelle sur plusieurs comptes. La vue globale offre de la visibilité et la possibilité d'effectuer des actions spécifiques sur les serveurs sources, les applications et les vagues de différents AWS comptes. Pour plus d'informations, consultez la section Configuration de vos AWS Organisations dans le guide de AWS Application Migration Service l'utilisateur.

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Application Migration Service console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Application Migration Service console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Application Migration Service d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Application Migration Service. Pour plus d'informations, consultez cette note.

Si vous activez l'accès sécurisé à l'aide de la AWS Application Migration Service console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Application Migration Servicedans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Application Migration Service dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Application Migration Service qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Application Migration Service en tant que service fiable auprès des Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal mgn.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactivation de l'accès sécurisé avec le service de migration d'applications

Seul un administrateur du compte de gestion des Organizations peut désactiver l'accès sécurisé avec Application Migration Service.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils AWS Application Migration Service ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Application Migration Service console ou les outils pour désactiver l'intégration avec Organizations. Cela permet AWS Application Migration Service d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Application Migration Service.
> Si vous désactivez l'accès sécurisé à l'aide de la AWS Application Migration Service console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Application Migration Servicedans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).

5. Dans la boîte de AWS Application Migration Service dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Application Migration Service qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Application Migration Service en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour le service de migration d'applications

Lorsque vous désignez un compte membre en tant qu'administrateur délégué de l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Application Migration Service qui, autrement, ne peuvent être effectuées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous permet de séparer la gestion de l'organisation de la gestion du service de migration des applications. Pour plus d'informations, consultez la section Configuration de votre application AWS Organizations dans le guide de l'utilisateur du service de migration des applications.

> **Autorisations minimales**
>
> Seul un utilisateur ou un rôle dans le compte de gestion des Organisations peut configurer un compte membre en tant qu'administrateur délégué pour le service de migration d'applications dans l'organisation

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le service du compte `mgn.amazonaws.com` sous forme de paramètres.

### Désactivation d'un administrateur délégué pour le service de migration d'applications

Seul un administrateur du compte de gestion des Organizations peut supprimer un administrateur délégué pour Application Migration Service. Vous pouvez supprimer l'administrateur délégué à l'aide de l'opération CLI ou SDK Organizations `DeregisterDelegatedAdministrator`.

## AWS Artifact et AWS Organizations

AWS Artifact est un service qui vous permet de télécharger des rapports AWS de conformité en matière de sécurité tels que les rapports ISO et PCI. Grâce à AWS Artifact cette option, un utilisateur du compte de gestion de l'organisation peut automatiquement accepter des accords au nom de tous les comptes membres d'une organisation, même lorsque de nouveaux rapports et comptes sont ajoutés. Les utilisateurs des comptes membres peuvent afficher et télécharger des accords. Pour plus d'informations, consultez la section Gestion d'un accord pour plusieurs comptes dans AWS Artifact dans le guide de l'AWS Artifact utilisateur.

Utilisez les informations suivantes pour vous aider AWS Artifact à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' AWS Artifact effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre AWS Artifact et Organizations, ou si vous supprimez le compte membre de l'organisation.

Même si vous avez la possibilité de supprimer ou de modifier ce rôle dans le cas où vous retirez le compte membre de l'organisation, cela est déconseillé.

La modification du rôle est déconseillée, car elle peut provoquer des problèmes de sécurité tels que le député confus entre services. Pour en savoir plus sur la protection contre le député confus, consultez Prévention du député confus entre services dans le Guide de l'utilisateur AWS Artifact .

- `AWSServiceRoleForArtifact`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par AWS Artifact accordent l'accès aux principaux de service suivants :

- `artifact.amazonaws.com`

## Permettre un accès fiable avec AWS Artifact

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Artifactdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Artifact dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Artifact qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Artifact en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AWS Artifact

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec AWS Artifact.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

AWS Artifact nécessite un accès fiable AWS Organizations pour travailler avec les accords d'organisation. Si vous désactivez l'accès sécurisé AWS Organizations pendant que vous l'utilisez AWS Artifact pour des accords d'organisation, il cesse de fonctionner car il ne peut pas accéder à l'organisation. Tous les accords d'organisation que vous acceptez AWS Artifact sont conservés, mais ne sont pas accessibles AWS Artifact. Le AWS Artifact rôle qui AWS Artifact crée demeure. Si vous réactivez ensuite l'accès approuvé, AWS Artifact continue de fonctionner comme avant, sans qu'il soit nécessaire de reconfigurer le service.

Un compte autonome qui est supprimé d'une organisation n'a plus accès aux accords de l'organisation.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Artifactdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS Artifact dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.

6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Artifact qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Artifact en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## AWS Audit Manager et AWS Organizations

AWS Audit Manager vous aide à auditer en permanence votre AWS utilisation afin de simplifier la façon dont vous évaluez les risques et la conformité aux réglementations et aux normes du secteur. Audit Manager automatise la collecte de preuves pour faciliter l'évaluation de l'efficacité de vos politiques, procédures et activités. Lorsqu'il est temps d'effectuer un audit, Audit Manager vous aide à gérer les examens de vos contrôles par les parties prenantes et vous aide à créer des rapports prêts à être vérifiés avec beaucoup moins d'effort manuel.

Lorsque vous intégrez Audit Manager à Audit Manager AWS Organizations, vous pouvez recueillir des preuves auprès d'une source plus large en incluant plusieurs éléments Comptes AWS provenant de votre organisation dans le cadre de vos évaluations.

Pour plus d'informations, consultez la section Enable AWS Organizations dans le guide de l'utilisateur d'Audit Manager.

Utilisez les informations suivantes pour vous aider AWS Audit Manager à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Audit Manager d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Audit Manager et Organizations, ou si vous supprimez le compte membre de l'organisation.

Pour en savoir plus sur la manière dont Audit Manager utilise ce rôle, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur AWS Audit Manager .

- `AWSServiceRoleForAuditManager`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Audit Manager autorisent l'accès aux mandataires de service suivants :

- `auditmanager.amazonaws.com`

## Pour activer l'accès approuvé avec Audit Manager

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Audit Manager a besoin d'un accès sécurisé pour AWS Organizations que vous puissiez désigner un compte membre comme administrateur délégué de votre organisation.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Audit Manager console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Audit Manager console ou les outils pour permettre l'intégration avec Organizations. Cela permet

AWS Audit Manager d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Audit Manager. Pour plus d'informations, consultez cette note.
Si vous activez l'accès sécurisé à l'aide de la AWS Audit Manager console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console Audit Manager

Pour obtenir des instructions sur l'activation de l'accès approuvé, consultez Configuration dans le Guide de l'utilisateur AWS Audit Manager .

> **Note**
>
> Si vous configurez un administrateur délégué à l'aide de la AWS Audit Manager console, l'accès sécurisé est AWS Audit Manager automatiquement activé pour vous.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Audit Manager en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

### Pour désactiver l'accès approuvé avec Audit Manager

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec AWS Audit Manager.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Audit Manager en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte administrateur délégué pour Audit Manager

Lorsque vous désignez un compte de membre comme administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Audit Manager qui, autrement, ne peuvent être effectuées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion d'Audit Manager.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations disposant de l'autorisation suivante peuvent configurer un compte membre en tant qu'administrateur délégué pour Audit Manager dans l'organisation : `audit-manager:RegisterAccount`

Pour obtenir des instructions sur l'activation d'un compte administrateur délégué pour Audit Manager, consultez Configuration dans le Guide de l'utilisateur AWS Audit Manager .

Si vous configurez un administrateur délégué à l'aide de la AWS Audit Manager console, Audit Manager active automatiquement un accès sécurisé pour vous.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK : appelez l'`RegisterAccount`opération et indiquez `delegatedAdminAccount` en paramètre pour déléguer le compte administrateur.

## AWS Backup et AWS Organizations

AWS Backup est un service qui vous permet de gérer et de suivre les AWS Backup emplois au sein de votre organisation. Si vous vous connectez en AWS Backup tant qu'utilisateur dans le compte de gestion de l'organisation, vous pouvez activer la protection et la surveillance des sauvegardes à l'échelle de l'organisation. Il vous aide à garantir la conformité en utilisant des politiques de sauvegarde pour appliquer de manière centralisée des AWS Backup plans aux ressources de tous les comptes de votre organisation. Lorsque vous utilisez les deux AWS Backup et AWS Organizations ensemble, vous pouvez bénéficier des avantages suivants :

Protection

Vous pouvez activer le type de stratégie de sauvegarde dans votre organisation, puis créer des politiques de sauvegarde à associer à la racine ou aux comptes de l'organisation. OUs Une politique de sauvegarde combine un AWS Backup plan avec les autres informations requises pour appliquer le plan automatiquement à vos comptes. Les politiques directement associées à un compte sont fusionnées avec les politiques héritées de la racine de l'organisation et de tout parent OUs afin de créer une politique efficace qui s'applique au compte. La politique inclut l'ID d'un rôle IAM autorisé à s'exécuter AWS Backup sur les ressources de vos comptes. AWS Backup utilise le rôle IAM pour effectuer la sauvegarde en votre nom, comme indiqué par le plan de sauvegarde dans la politique effective.

Surveillance

Lorsque vous activez l'accès approuvé pour AWS Backup dans votre organisation, vous pouvez utiliser la console AWS Backup pour afficher des détails sur les tâches de sauvegarde, de restauration et de copie dans n'importe quel compte de votre organisation. Pour plus d'informations, consultez Surveiller vos tâches de sauvegarde dans le Manuel du développeur AWS Backup .

Pour plus d'informations à ce sujet AWS Backup, consultez le guide du AWS Backup développeur.

Utilisez les informations suivantes pour vous aider AWS Backup à intégrer AWS Organizations.

## Permettre un accès fiable avec AWS Backup

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Backup console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Backup console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Backup d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Backup. Pour plus d'informations, consultez cette note.

Si vous activez l'accès sécurisé à l'aide de la AWS Backup console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé en utilisant AWS Backup, consultez la section Activation de la sauvegarde multiple Comptes AWS dans le guide du AWS Backup développeur.

## Désactiver l'accès sécurisé avec AWS Backup

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

AWS Backup nécessite un accès fiable AWS Organizations pour permettre la surveillance des tâches de sauvegarde, de restauration et de copie sur les comptes de votre entreprise. Si vous désactivez l'accès sécurisé AWS Backup, vous ne pouvez plus consulter les offres d'emploi en dehors du compte courant. Le AWS Backup rôle qui AWS Backup crée demeure. Si vous réactivez ultérieurement l'accès sécurisé, il AWS Backup continue de fonctionner comme avant, sans que vous ayez à reconfigurer le service.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Backup en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte d'administrateur délégué pour AWS Backup

Reportez-vous à la section Administrateur délégué dans le Guide du développeur AWS Backup .

## AWS Billing and Cost Management et AWS Organizations

AWS Billing and Cost Management fournit une suite de fonctionnalités pour vous aider à configurer votre facturation, à récupérer et à payer les factures, ainsi qu'à analyser, organiser, planifier et optimiser vos coûts. Lorsque vous utilisez Billing and Cost Management, AWS Organizations vous autorisez les données de répartition des coûts fractionnés à récupérer des AWS Organizations informations, le cas échéant, et à collecter des données de télémétrie pour les services de données de répartition des coûts partagés auxquels vous avez souscrit.

Utilisez les informations suivantes pour vous aider AWS Billing and Cost Management à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Billing and Cost Management d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Billing and Cost Management et Organizations, ou si vous supprimez le compte membre de l'organisation.

Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service pour Billing and Cost Management dans le guide de l'utilisateur de Billing and Cost Management.

- `AWSServiceRoleForSplitCostAllocationData`

### Principes de service utilisés par Billing and Cost Management

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Billing and Cost Management donnent accès aux principaux de service suivants :

Billing and Cost Management utilise le `billing-cost-management.amazonaws.com` service principal.

## Permettre un accès fiable grâce à Billing and Cost Management

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Grâce à l'accès sécurisé activé via un compte de gestion, les clients peuvent tirer parti de la fonctionnalité de répartition des coûts partagée dans Billing and Cost Management. Lorsque les clients activent les données de répartition des coûts partagés pour Amazon Elastic Kubernetes Service avec Amazon Managed Service for Prometheus, un accès sécurisé est invoqué pour créer des rôles liés aux services pour tous les comptes membres de l'organisation. Cela permet de répartir les données de répartition des coûts afin de collecter des données télémétriques auprès des espaces de travail Amazon Managed Service for Prometheus des clients et d'effectuer une répartition des coûts en fonction de ces indicateurs.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Billing and Cost Management en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

### Désactiver l'accès sécurisé

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Billing and Cost Management en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## AWS CloudFormation StackSets et AWS Organizations

CloudFormation StackSets vous permet de créer, de mettre à jour ou de supprimer des piles sur plusieurs piles Comptes AWS Régions AWS en une seule opération. StackSets l'intégration avec vous AWS Organizations permet de créer des ensembles de piles avec des autorisations gérées par le service, en utilisant un rôle lié au service disposant de l'autorisation appropriée dans chaque compte membre. Cela vous permet de déployer des instances de piles sur tous les comptes de votre organisation. Vous n'êtes pas obligé de créer les Gestion des identités et des accès AWS rôles nécessaires ; StackSets crée le rôle IAM dans chaque compte membre en votre nom.

Vous pouvez également choisir d'activer les déploiements automatiques sur les comptes qui sont ajoutés ultérieurement à votre organisation. Lorsque le déploiement automatique est activé, les rôles

et le déploiement des instances de l'ensemble de piles associées sont automatiquement ajoutés à tous les comptes ajoutés à l'avenir à cette unité d'organisation.

Lorsque l'accès sécurisé entre StackSets organisations est activé, le compte de gestion est autorisé à créer et à gérer des ensembles de piles pour votre organisation. Le compte de gestion peut enregistrer jusqu'à cinq comptes membres en tant qu'administrateurs délégués. Lorsque l'accès approuvé est activé, les administrateurs délégués disposent également des autorisations pour créer et gérer des ensembles de piles pour votre organisation. Les ensembles de piles dotés d'autorisations gérées par le service sont créés dans le compte de gestion, y compris les ensembles de piles créés par des administrateurs délégués.

> **Important**
>
> Les administrateurs délégués disposent des autorisations complètes pour un déploiement dans les comptes de votre organisation. Le compte de gestion ne peut pas limiter les autorisations d'administrateur déléguées pour effectuer des OUs déploiements ou des opérations spécifiques sur des ensembles de piles spécifiques.

Pour plus d'informations sur l'intégration StackSets à Organizations, voir Working with AWS CloudFormation StackSets dans le guide de AWS CloudFormation l'utilisateur.

Utilisez les informations suivantes pour vous aider AWS CloudFormation StackSets à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à CloudFormation Stacksets d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre CloudFormation StackSets et Organizations, ou si vous supprimez le compte membre de l'organisation.

- Compte de gestion : `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Pour créer le rôle lié à un service `AWSServiceRoleForCloudFormationStackSetsOrgMember` pour les comptes membres de votre organisation, vous devez d'abord créer un ensemble de piles dans le compte de gestion. Cela crée une instance d'ensemble de piles, qui crée ensuite le rôle dans les comptes membres.

- Comptes membres : `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Pour plus de détails sur la création d'ensembles de piles, consultez la section AWS CloudFormation StackSets Utilisation du guide de AWS CloudFormation l'utilisateur.

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par les CloudFormation Stacksets donnent accès aux principaux de service suivants :

- Compte de gestion : `stacksets.cloudformation.amazonaws.com`

  Vous pouvez modifier ou supprimer ce rôle uniquement si vous avez désactivé l'accès sécurisé entre StackSets et Organizations.
- Comptes membres : `member.org.stacksets.cloudformation.amazonaws.com`

  Vous pouvez modifier ou supprimer ce rôle d'un compte uniquement si vous désactivez d'abord l'accès sécurisé entre StackSets et Organizations, ou si vous supprimez d'abord le compte de l'organisation ou de l'unité organisationnelle (UO) cible.

## Permettre un accès fiable avec CloudFormation Stacksets

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Seul un administrateur du compte de gestion des Organisations est autorisé à activer un accès sécurisé avec un autre AWS service. Vous pouvez activer l'accès approuvé à l'aide de la console CloudFormation ou de la console Organizations.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide de AWS CloudFormation StackSets.

Pour activer l'accès sécurisé à l'aide de la console CloudFormation Stacksets, voir Activer l'accès sécurisé avec AWS Organizations dans le guide de l' AWS CloudFormation utilisateur.

## Désactiver l'accès sécurisé avec Stacksets CloudFormation

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur d'un compte de gestion d'Organizations est autorisé à désactiver l'accès sécurisé à un autre AWS service. Vous pouvez désactiver l'accès approuvé uniquement avec la console Organizations. Si vous désactivez l'accès sécurisé auprès d'Organizations pendant que vous l'utilisez StackSets, toutes les instances de pile créées précédemment sont conservées. Toutefois, les ensembles de piles déployés à l'aide des autorisations du rôle lié à un service ne peuvent plus effectuer de déploiements sur des comptes gérés par Organizations.

Vous pouvez désactiver l'accès sécurisé à l'aide de la CloudFormation console ou de la console Organizations.

> **Important**
>
> Si vous désactivez l'accès sécurisé par programmation (par exemple avec AWS CLI ou avec une API), sachez que cela supprimera l'autorisation. Il est préférable de désactiver l'accès sécurisé avec la CloudFormation console.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS CloudFormation StackSetsdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS CloudFormation StackSets dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.

6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS CloudFormation StackSets qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS CloudFormation StackSets en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

### Activation d'un compte d'administrateur délégué pour les CloudFormation Stacksets

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour CloudFormation Stacksets qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous permet de séparer la gestion de l'organisation de la gestion des CloudFormation Stacksets.

Pour obtenir des instructions sur la façon de désigner un compte membre en tant qu'administrateur délégué d' CloudFormation StackSets dans l'organisation, consultez Enregistrer un administrateur délégué dans le Guide de l'utilisateur AWS CloudFormation .

## AWS CloudTrail et AWS Organizations

AWS CloudTrail est un AWS service qui vous aide à garantir la gouvernance, la conformité, ainsi que l'audit opérationnel et des risques de votre entreprise Compte AWS. En utilisant AWS CloudTrail, un utilisateur d'un compte de gestion peut créer un journal d'organisation qui enregistre tous les

événements pour tous Comptes AWS les membres de cette organisation. Les journaux d'activité d'organisation sont automatiquement appliqués à tous les comptes membres de l'organisation. Les comptes membres peuvent voir le journal d'activité de l'organisation, mais ne peuvent ni le modifier ni le supprimer. Par défaut, les comptes membres n'ont pas accès aux fichiers journaux correspondant au journal d'activité de l'organisation dans le compartiment Amazon S3. Cela vous aide à appliquer et faire respecter de manière uniforme votre politique de journalisation des événements dans tous les comptes de votre organisation.

Pour plus d'informations, consultez Création d'un journal d'activité pour une organisation dans le Guide de l'utilisateur AWS CloudTrail .

Utilisez les informations suivantes pour vous aider AWS CloudTrail à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' CloudTrail effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre CloudTrail et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForCloudTrail`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par CloudTrail accordent l'accès aux principaux de service suivants :

- `cloudtrail.amazonaws.com`

## Permettre un accès fiable avec CloudTrail

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Si vous activez l'accès sécurisé en créant une trace depuis la AWS CloudTrail console, l'accès sécurisé est configuré automatiquement pour vous (recommandé). Vous pouvez également activer

l'accès sécurisé à l'aide de la AWS Organizations console. Vous devez vous connecter avec votre compte AWS Organizations de gestion pour créer un suivi de l'organisation.

Si vous choisissez de créer un journal d'organisation à l'aide de l'API AWS CLI ou de l' AWS API, vous devez configurer manuellement l'accès sécurisé. Pour plus d'informations, consultez la section Activation en CloudTrail tant que service de confiance AWS Organizations dans le guide de AWS CloudTrail l'utilisateur.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS CloudTrail console ou les outils pour permettre l'intégration avec Organizations.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS CloudTrail en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec CloudTrail

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

AWS CloudTrail nécessite un accès fiable AWS Organizations pour utiliser les traces des organisations et les banques de données sur les événements de l'organisation. Si vous désactivez l'accès sécurisé AWS Organizations pendant que vous l'utilisez AWS CloudTrail, toutes les traces d'organisation relatives aux comptes des membres sont supprimées car il est CloudTrail impossible d'accéder à l'organisation. Toutes les traces d'organisation des comptes de gestion et les magasins de données sur les événements de l'organisation sont convertis en traces au niveau du compte et en magasins de données d'événements. Le `AWSServiceRoleForCloudTrail` rôle créé pour l'intégration entre CloudTrail et AWS Organizations reste dans le compte. Si vous réactivez l'accès sécurisé, aucune action ne CloudTrail sera entreprise sur les sentiers et les magasins de données d'événements existants. Le compte de gestion doit mettre à jour les traces et les banques de données d'événements au niveau du compte pour les appliquer à l'organisation.

Pour convertir un magasin de données de suivi ou d'événement au niveau du compte en un journal d'organisation ou un magasin de données d'événements d'organisation, procédez comme suit :

- Depuis la CloudTrail console, mettez à jour le magasin de données de suivi ou d'événement et choisissez l'option Activer pour tous les comptes de mon organisation.
- À partir de AWS CLI, procédez comme suit :
  - Pour mettre à jour un historique, exécutez la update-trailcommande et incluez le `--is-organization-trail` paramètre.
  - Pour mettre à jour un magasin de données d'événements, exécutez la update-event-data-storecommande et incluez le `--organization-enabled` paramètre.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec AWS CloudTrail. Vous pouvez désactiver l'accès sécurisé uniquement avec les outils Organizations, en utilisant la AWS Organizations console, en exécutant une commande Organizations AWS CLI ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

### AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS CloudTraildans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS CloudTrail dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS CloudTrail qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

### AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS CloudTrail en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte d'administrateur délégué pour CloudTrail

Lorsque vous utilisez CloudTrail Organizations, vous pouvez enregistrer n'importe quel compte au sein de l'organisation pour agir en tant qu'administrateur CloudTrail délégué chargé de gérer les traces et les banques de données d'événements de l'organisation pour le compte de l'organisation. Un administrateur délégué est un compte membre d'une organisation qui peut effectuer les mêmes tâches administratives CloudTrail que le compte de gestion.

> **Autorisations minimales**
>
> Seul un administrateur du compte de gestion des Organizations peut enregistrer un administrateur délégué pour CloudTrail.

Vous pouvez enregistrer un compte d'administrateur délégué à l'aide de la CloudTrail console, de la `RegisterDelegatedAdministrator` CLI ou du SDK Organizations. Pour enregistrer un administrateur délégué à l'aide de la CloudTrail console, voir Ajouter un administrateur CloudTrail délégué.

### Désactivation d'un administrateur délégué pour CloudTrail

Seul un administrateur du compte de gestion des Organizations peut supprimer un administrateur délégué pour CloudTrail. Vous pouvez supprimer l'administrateur délégué à l'aide de la CloudTrail console, de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations. Pour plus d'informations sur la procédure de suppression d'un administrateur délégué à l'aide de la CloudTrail console, voir Supprimer un administrateur CloudTrail délégué.

## Amazon CloudWatch et AWS Organizations

Vous pouvez utiliser Amazon AWS Organizations CloudWatch pour les cas d'utilisation suivants :

- Découvrez et comprenez l'état de la configuration télémétrique de vos AWS ressources à partir d'une vue centrale dans la CloudWatch console. Cela simplifie le processus d'audit de vos configurations de collecte de données télémétriques pour plusieurs types de ressources au sein de votre organisation ou de votre AWS compte. Vous devez activer l'accès sécurisé pour utiliser la configuration de télémétrie au sein de votre organisation.

  Pour plus d'informations, consultez la section Audit des configurations de CloudWatch télémétrie dans le guide de  CloudWatch l'utilisateur Amazon.

- Travaillez avec plusieurs comptes dans Network Flow Monitor, une fonctionnalité d'Amazon CloudWatch Network Monitoring. Network Flow Monitor fournit une visibilité en temps quasi réel sur les performances du réseau pour le trafic entre les instances Amazon EC2. Après avoir activé l'accès sécurisé pour l'intégration à Organizations, vous pouvez créer un moniteur pour visualiser les détails des performances du réseau sur plusieurs comptes.

  Pour plus d'informations, consultez Initialize Network Flow Monitor pour la surveillance multi-comptes dans le guide de  CloudWatch l'utilisateur Amazon.

Utilisez les informations suivantes pour vous aider à intégrer Amazon CloudWatch à AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Créez le rôle lié au service suivant dans le compte de gestion de votre organisation. Le rôle lié au service est automatiquement créé dans les comptes des membres lorsque vous activez l'accès sécurisé. Ce rôle permet d' CloudWatch effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation. Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre CloudWatch et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForObservabilityAdmin`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par CloudWatch accordent l'accès aux principaux de service suivants :

- `observabilityadmin.amazonaws.com`
- `networkflowmonitor.amazonaws.com`
- `topology.networkflowmonitor.amazonaws.com`

## Permettre un accès fiable avec CloudWatch

Pour plus d'informations sur les autorisations dont vous avez besoin pour activer l'accès sécurisé, consultezAutorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la CloudWatch console Amazon ou de la AWS Organizations console.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la CloudWatch console ou les outils Amazon pour permettre l'intégration avec Organizations. Cela permet à Amazon CloudWatch d'effectuer toutes les configurations nécessaires, telles que la création des ressources nécessaires au service. Procédez comme suit uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par Amazon CloudWatch. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la CloudWatch console ou des outils Amazon, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la CloudWatch console

Consultez la section Activation de l'audit CloudWatch télémétrique dans le guide de CloudWatch l'utilisateur Amazon.

Lorsque vous activez l'accès sécurisé CloudWatch, vous activez l'audit télémétrique et vous pouvez travailler avec plusieurs comptes dans Network Flow Monitor.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Amazon CloudWatch dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de CloudWatch dialogue Activer l'accès sécurisé pour Amazon, tapez activer pour confirmer, puis sélectionnez Activer l'accès sécurisé.

6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon CloudWatch qu'il peut désormais activer ce service pour qu'il fonctionne avec la console AWS Organizations de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer Amazon CloudWatch en tant que service de confiance auprès d'Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal observabilityadmin.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactivez l'accès sécurisé avec CloudWatch

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous pouvez désactiver l'accès sécurisé à l'aide d'Amazon CloudWatch ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la CloudWatch console ou les outils Amazon pour désactiver l'intégration avec Organizations. Cela permet à Amazon CloudWatch d'effectuer tous les nettoyages nécessaires, tels que la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par Amazon CloudWatch.

Si vous désactivez l'accès sécurisé à l'aide de la CloudWatch console ou des outils Amazon, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès sécurisé à l'aide de la CloudWatch console

Consultez la section Désactivation de l'audit CloudWatch télémétrique dans le guide de l'utilisateur Amazon CloudWatch

Lorsque vous désactivez l'accès sécurisé dans CloudWatch, l'audit télémétrique n'est plus actif et vous ne pouvez plus travailler avec plusieurs comptes dans Network Flow Monitor.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver Amazon CloudWatch en tant que service de confiance auprès d'Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal observabilityadmin.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Enregistrement d'un compte d'administrateur délégué pour CloudWatch

Lorsque vous enregistrez un compte membre en tant que compte d'administrateur délégué pour l'organisation, les utilisateurs et les rôles associés à ce compte peuvent effectuer des actions administratives CloudWatch qui, sinon, ne peuvent être effectuées que par des utilisateurs ou des rôles connectés avec le compte de gestion de l'organisation. L'utilisation d'un compte d'administrateur

délégué vous permet de séparer la gestion de l'organisation de la gestion des fonctionnalités dans CloudWatch.

> **Autorisations minimales**
>
> Seul un administrateur du compte de gestion des Organisations peut enregistrer un compte membre en tant que compte d'administrateur délégué pour CloudWatch l'organisation.

Vous pouvez enregistrer un compte d'administrateur délégué à l'aide de la CloudWatch console ou à l'aide de l'opération Organizations `RegisterDelegatedAdministrator` API avec le AWS Command Line Interface ou un SDK.

Pour plus d'informations sur la procédure d'enregistrement d'un compte d'administrateur délégué à l'aide de la CloudWatch console, consultez la section Activation de l'audit CloudWatch télémétrique dans le guide de  CloudWatch l'utilisateur Amazon.

Lorsque vous enregistrez un compte d'administrateur délégué CloudWatch, vous pouvez l'utiliser pour des opérations de gestion avec un audit télémétrique et avec Network Flow Monitor.

## Désenregistrer un administrateur délégué pour CloudWatch

> **Autorisations minimales**
>
> Seul un administrateur connecté avec le compte de gestion des Organizations peut annuler l'enregistrement d'un compte d'administrateur délégué CloudWatch au sein de l'organisation.

Vous pouvez désenregistrer le compte d'administrateur délégué à l'aide de la CloudWatch console ou à l'aide de l'opération Organizations `DeregisterDelegatedAdministrator` API avec le AWS Command Line Interface ou un SDK. Pour plus d'informations, consultez la section Désenregistrement d'un compte d'administrateur délégué dans le guide de l'utilisateur Amazon CloudWatch .

Lorsque vous désenregistrez un compte d'administrateur délégué dans CloudWatch, vous ne pouvez plus l'utiliser pour les opérations de gestion avec l'audit télémétrique et avec Network Flow Monitor.

# Optimiseur de calcul AWS et AWS Organizations

Optimiseur de calcul AWS est un service qui analyse les paramètres de configuration et d'utilisation de vos AWS ressources. Ces ressources sont par exemple des instances Amazon Elastic Compute Cloud (Amazon EC2) ou des groupes Auto Scaling. Compute Optimizer indique si vos ressources sont optimales et génère des recommandations d'optimisation afin de réduire les coûts et d'améliorer les performances de vos charges de travail. Pour plus d'informations sur Compute Optimizer, consultez le Guide de l'utilisateur Optimiseur de calcul AWS.

Utilisez les informations suivantes pour vous aider Optimiseur de calcul AWS à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Compute Optimizer d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Compute Optimizer et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForComputeOptimizer`
- `AWSServiceRoleForComputeOptimizerAutomation`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Compute Optimizer autorisent l'accès aux mandataires de service suivants :

- `compute-optimizer.amazonaws.com`

## Activation de l'accès approuvé avec Compute Optimizer

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la Optimiseur de calcul AWS console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la Optimiseur de calcul AWS console ou les outils pour permettre l'intégration avec Organizations. Cela permet Optimiseur de calcul AWS d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par Optimiseur de calcul AWS. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la Optimiseur de calcul AWS console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console Compute Optimizer

Vous devez vous connecter à la console Compute Optimizer à l'aide du compte de gestion de votre organisation. Inscrivez-vous au nom de votre organisation en suivant les instructions de la rubrique Inscription à votre compte dans le Guide de l'utilisateur Optimiseur de calcul AWS .

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Optimiseur de calcul AWSdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de Optimiseur de calcul AWS dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le Optimiseur de calcul AWS qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer Optimiseur de calcul AWS en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactivation de l'accès approuvé avec Compute Optimizer

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec Optimiseur de calcul AWS.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver Optimiseur de calcul AWS en tant que service sécurisé auprès des Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal compute-optimizer.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour Compute Optimizer

Lorsque vous désignez un compte membre comme administrateur délégué de l'organisation, les utilisateurs et les rôles du compte désigné peuvent gérer les métadonnées Compte AWS pour les autres comptes membres de l'organisation. Si vous n'activez pas de compte administrateur délégué, seul le compte de gestion de l'organisation peut effectuer ces tâches. Cela vous permet de séparer la gestion de l'organisation de celle des détails de votre compte.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué de Compute Optimizer dans l'organisation.

Pour obtenir des instructions sur l'activation d'un compte d'administrateur délégué pour Compute Optimizer, consultez https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.htmldans le Optimiseur de calcul AWS Guide de l'utilisateur.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

### Désactivation d'un administrateur délégué pour Compute Optimizer

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Compute Optimizer.

Pour désactiver le compte administrateur délégué de Compute Optimizer à l'aide de la console Compute Optimizer, consultez https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html dans leOptimiseur de calcul AWS Guide de l'utilisateur.

Pour supprimer un administrateur délégué à l'aide du AWS AWS CLI, reportez-vous deregister-delegated-administratorà la référence des AWS AWS CLI commandes.

## AWS Config et AWS Organizations

L'agrégation de données multicomptes et multirégions vous AWS Config permet d'agréger AWS Config les données de plusieurs comptes Régions AWS en un seul compte. Le regroupement de données multi-comptes et multi-régions est utile pour les administrateurs de l'informatique centrale pour la surveillance de la conformité de plusieurs Comptes AWS au sein de l'entreprise. Un agrégateur est un type de ressource AWS Config qui collecte des AWS Config données provenant de plusieurs comptes sources et régions. Créez un agrégateur dans la région où vous souhaitez voir les AWS Config données agrégées. Lors de la création d'un agrégateur, vous pouvez choisir d'ajouter un compte individuel IDs ou votre organisation. Pour plus d'informations à ce sujet AWS Config, consultez le guide du AWS Config développeur.

Vous pouvez également l'utiliser AWS Config APIspour gérer les AWS Config règles dans l'ensemble Comptes AWS de votre organisation. Pour plus d'informations, consultez la section Activation des AWS Config règles pour tous les comptes de votre organisation dans le guide du AWS Config développeur.

Utilisez les informations suivantes pour vous aider AWS Config à intégrer AWS Organizations.

### Rôles liés à un service

Le rôle lié au service suivant permet d' AWS Config effectuer des opérations prises en charge dans les comptes de votre organisation.

- `AWSServiceRoleForConfig`

Pour en savoir plus sur la création de ce rôle, consultez la section Permissions pour le rôle IAM attribué AWS Config dans le guide du AWS Config développeur

Pour en savoir plus sur l' AWS Config utilisation des rôles liés à un service, consultez la section Utilisation des rôles liés à un service dans le manuel du développeur AWS ConfigAWS Config

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre AWS Config et Organizations, ou si vous supprimez le compte membre de l'organisation.

## Permettre un accès fiable avec AWS Config

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Config console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Config console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Config d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Config. Pour plus d'informations, consultez cette note. Si vous activez l'accès sécurisé à l'aide de la AWS Config console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la AWS Config console

Pour permettre un accès fiable à AWS Organizations l'utilisation AWS Config, créez un agrégateur multi-comptes et ajoutez l'organisation. Pour plus d'informations sur la configuration d'un agrégateur multi-comptes, consultez la section Création d'agrégateurs dans le guide du AWS Config développeur.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Configdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Config dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Config qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Config en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

### Désactiver l'accès sécurisé avec AWS Config

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Config en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Hub d'optimisation des coûts AWS et AWS Organizations

Hub d'optimisation des coûts AWS est une fonctionnalité AWS de Billing and Cost Management qui vous aide à consolider et à hiérarchiser les recommandations d'optimisation des coûts pour l'ensemble de vos AWS comptes et de vos AWS régions, afin que vous puissiez tirer le meilleur parti de vos AWS dépenses. Lorsque vous utilisez Cost Optimization Hub, AWS Organizations vous pouvez facilement identifier, filtrer et agréger les recommandations d'optimisation des AWS coûts sur les comptes membres et les AWS régions de votre Organisation.

Pour plus d'informations, voir Cost Optimization Hub dans le guide de AWS Cost Management l'utilisateur.

Utilisez les informations suivantes pour vous aider Hub d'optimisation des coûts AWS à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Cost Optimization Hub d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Cost Optimization Hub et Organizations, ou si vous supprimez le compte membre de l'organisation.

Pour plus d'informations, consultez la section Autorisations de rôle liées à un service pour Cost Optimization Hub dans le guide de l'AWS Cost Management utilisateur.

- `AWSServiceRoleForCostOptimizationHub`

## Principes de service utilisés par le Cost Optimization Hub

Le hub d'optimisation des coûts utilise le principal `cost-optimization-hub.bcm.amazonaws.com` de service.

## Permettre un accès fiable avec Cost Optimization Hub

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Lorsque vous choisissez d'utiliser le compte de gestion de votre organisation et que vous incluez tous les comptes membres de l'organisation, l'accès sécurisé au Cost Optimization Hub est automatiquement activé dans le compte de votre organisation.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Hub d'optimisation des coûts AWSdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de Hub d'optimisation des coûts AWS dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le Hub d'optimisation des coûts AWS qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer Hub d'optimisation des coûts AWS en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

> **Important**
>
> Si vous désactivez l'accès sécurisé au Cost Optimization Hub après vous être inscrit, le Cost Optimization Hub refuse l'accès aux recommandations relatives aux comptes membres de votre organisation. De plus, les comptes des membres de l'organisation ne sont pas intégrés au Cost Optimization Hub. Pour en savoir plus, consultez Cost Optimization Hub et Organizations trusted access dans le guide de AWS Cost Management l'utilisateur.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver Hub d'optimisation des coûts AWS en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte d'administrateur délégué pour Cost Optimization Hub

Lorsque vous désignez un compte membre comme administrateur délégué de l'organisation, le compte désigné peut récupérer les recommandations du Cost Optimization Hub pour tous les comptes de votre organisation et gérer les préférences du Cost Optimization Hub, ce qui vous donne une plus grande flexibilité pour identifier de manière centralisée les opportunités d'optimisation des ressources.

> **Autorisations minimales**
>
> Seul un utilisateur ou un rôle du compte de gestion des Organisations disposant de l'autorisation suivante peut configurer un compte membre en tant qu'administrateur délégué du Cost Optimization Hub au sein de l'organisation :

Pour obtenir des instructions sur l'activation d'un compte administrateur délégué pour Cost Optimization Hub, voir Déléguer un compte administrateur dans le guide de AWS Cost Management l'utilisateur.

### Désactivation d'un administrateur délégué pour Cost Optimization Hub

Seul un administrateur du compte de gestion des Organizations peut supprimer un administrateur délégué pour Cost Optimization Hub.

Pour désactiver le compte administrateur délégué Cost Optimization Hub à l'aide de la console Cost Optimization Hub, voir Déléguer un compte administrateur dans le guide de AWS Cost Management l'utilisateur.

Pour supprimer un administrateur délégué à l'aide de la AWS CLI, consultez `deregister-delegated-administrator`la référence de la AWS Config CLI.

## AWS Control Tower et AWS Organizations

AWS Control Tower propose un moyen simple de configurer et de gérer un environnement AWS multi-comptes, en suivant les meilleures pratiques prescriptives. AWS Control Tower l'orchestration étend les capacités de. AWS Organizations AWS Control Tower applique des contrôles préventifs et de détection (garde-fous) pour empêcher que vos organisations et vos comptes ne s'écartent des meilleures pratiques (dérive).

AWS Control Tower l'orchestration étend les capacités de. AWS Organizations

Pour plus d'informations, consultez le guide de AWS Control Tower l'utilisateur.

Utilisez les informations suivantes pour vous aider AWS Control Tower à intégrer AWS Organizations.

## Rôles nécessaires à l'intégration

Le rôle `AWSControlTowerExecution` doit être présent dans tous les comptes inscrits. Il permet AWS Control Tower de gérer vos comptes individuels et de communiquer des informations les concernant à vos comptes d'audit et d'archivage des journaux.

Pour en savoir plus sur les rôles utilisés par AWS Control Tower, consultez Comment AWS Control Tower fonctionne avec les rôles pour créer et gérer des comptes et Utiliser des politiques basées sur l'identité (politiques IAM) pour. AWS Control Tower

## Principes de service utilisés par AWS Control Tower

AWS Control Tower utilise le principal `controltower.amazonaws.com` de service.

## Permettre un accès fiable avec AWS Control Tower

AWS Control Tower utilise un accès sécurisé pour détecter les dérives à des fins de contrôles préventifs et pour suivre les modifications des comptes et des unités d'organisation qui sont à l'origine de cette dérive.

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Pour activer l'accès de confiance à partir de la console Organizations, choisissez **`Enable access`** à côté de AWS Control Tower.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Control Tower en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AWS Control Tower

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

> **Important**
>
> La désactivation AWS Control Tower de l'accès sécurisé entraîne une dérive dans votre zone AWS Control Tower d'atterrissage. La seule façon de corriger la dérive est d'utiliser le service de réparation de zone de destination de AWS Control Tower. La réactivation de l'accès sécurisé dans les organisations ne corrige pas le problème. Pour en savoir plus sur les problèmes de dérive, consultez le Guide de l'utilisateur AWS Control Tower .

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Control Tower en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Amazon Detective et AWS Organizations

Amazon Detective utilise vos données de journal pour générer des visualisations qui vous autorisent à analyser, examiner et identifier la cause racine des résultats de sécurité ou des activités suspectes.

L'utilisation vous AWS Organizations permet de vous assurer que votre graphe de comportement de Detective fournit une visibilité sur l'activité de tous les comptes de votre organisation.

Lorsque vous accordez un accès approuvé à Detective, le service Detective peut réagir automatiquement aux modifications de l'appartenance à l'organisation. L'administrateur délégué peut activer n'importe quel compte d'organisation comme compte membre dans le graphique de comportement. Detective peut également activer automatiquement de nouveaux comptes d'organisation comme comptes membres. Les comptes d'organisation ne peuvent pas se dissocier du graphique de comportement.

Pour plus d'informations, consultez Utilisation d'Amazon Detective dans votre organisation dans le Guide d'administration Amazon Detective.

Utilisez les informations suivantes pour vous aider à intégrer Amazon Detective à AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Detective d'effectuer les opérations prises en charge dans les comptes de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Detective et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForDetective`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Detective accordent l'accès aux principaux de service suivants :

- `detective.amazonaws.com`

## Pour activer l'accès approuvé avec Detective

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

> **Note**
>
> Lorsque vous désignez un administrateur délégué pour Amazon Detective, il active automatiquement l'accès approuvé pour Detective pour votre organisation.
> Detective a besoin d' AWS Organizations un accès sécurisé pour que vous puissiez désigner un compte membre en tant qu'administrateur délégué de ce service pour votre organisation.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Organizations console.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.

3. Choisissez Amazon Detective dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour Amazon Detective, tapez enable pour le confirmer, puis choisissez Enable trusted access.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon Detective qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

## Pour désactiver l'accès approuvé avec Detective

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte de AWS Organizations gestion peut désactiver l'accès sécurisé avec Amazon Detective.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé à l'aide de la AWS Organizations console.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Amazon Detective dans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de dialogue Désactiver l'accès sécurisé pour Amazon Detective, tapez Disable pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon Detective qu'il peut désormais désactiver ce service à l' AWS Organizations aide de la console de service ou des outils ;

## Activation d'un compte administrateur délégué pour Detective

Le compte d'administrateur délégué pour Detective est celui d'un graphique de comportement de Detective. L'administrateur délégué détermine les comptes d'organisation à activer et à désactiver comme comptes membres dans ce graphique de comportement. L'administrateur délégué peut configurer Detective pour qu'il active automatiquement les nouveaux comptes d'organisation comme comptes membres à mesure qu'ils sont ajoutés à l'organisation. Pour plus d'informations sur la manière dont un administrateur délégué gère les comptes d'organisation, consultez Gestion des comptes d'organisation comme comptes membres dans le Guide d'administration Amazon Detective.

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Detective.

Vous pouvez spécifier un compte d'administrateur délégué à partir de l'API ou de la console Detective, ou en utilisant la CLI d'Organizations ou l'opération SDK.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre comme administrateur délégué de Detective dans l'organisation.

Pour configurer un administrateur délégué à l'aide de l'API ou de la console Detective, consultez Désignation d'un compte d'administrateur Detective pour une organisation dans le Guide d'administration Amazon Detective.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

### Désactivation d'un administrateur délégué pour Detective

Vous pouvez supprimer l'administrateur délégué à l'aide de l'API ou de la console Detective, ou à l'aide de la CLI Organizations `DeregisterDelegatedAdministrator` ou de l'opération SDK. Pour plus d'informations sur la suppression d'un administrateur délégué à l'aide de l'API ou de la console Detective, ou de l'API Organizations, consultez Désignation d'un compte d'administrateur Detective pour une organisation dans le Guide d'administration Amazon Detective.

## Amazon DevOps Guru et AWS Organizations

Amazon DevOps Guru analyse les données opérationnelles ainsi que les indicateurs et événements liés aux applications afin d'identifier les comportements qui s'écartent des modèles de fonctionnement normaux. Les utilisateurs sont avertis lorsque DevOps Guru détecte un problème ou un risque opérationnel.

L'utilisation de DevOps Guru permet une assistance multi-comptes AWS Organizations, ce qui vous permet de désigner un compte membre pour gérer les informations sur l'ensemble de votre organisation. Cet administrateur délégué peut ensuite afficher, trier et filtrer les informations de tous les comptes de votre organisation afin de développer une vue globale de l'état de toutes les applications contrôlées dans votre organisation sans avoir besoin d'une personnalisation supplémentaire.

Pour plus d'informations, consultez la section Surveiller les comptes au sein de votre organisation dans le guide de l'utilisateur Amazon DevOps Guru.

Utilisez les informations suivantes pour vous aider à intégrer Amazon DevOps Guru à AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à DevOps Guru d'effectuer des opérations prises en charge sur les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre DevOps Guru et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForDevOpsGuru`

### Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par DevOps Guru donnent accès aux principaux de service suivants :

- `devops-guru.amazonaws.com`

Pour plus d'informations, consultez la section Utilisation de rôles liés à un service pour DevOps Guru dans le guide de l'utilisateur Amazon DevOps Guru.

### Pour permettre un accès sécurisé avec DevOps Guru

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

> **Note**
>
> Lorsque vous désignez un administrateur délégué pour Amazon DevOps Guru, DevOps Guru autorise automatiquement un accès sécurisé à DevOps Guru pour votre organisation. DevOpsGuru a besoin d' AWS Organizations un accès sécurisé pour que vous puissiez désigner un compte membre comme administrateur délégué de ce service pour votre organisation.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils Amazon DevOps Guru pour permettre l'intégration avec Organizations. Cela permet à Amazon DevOps Guru d'effectuer toutes les configurations nécessaires, telles que la création des ressources nécessaires au service. Procédez comme suit uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par Amazon DevOps Guru. Pour plus d'informations, consultez cette note.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Organizations console ou de la console DevOps Guru.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Services, recherchez la ligne correspondant à Amazon DevOps Guru, choisissez le nom du service, puis sélectionnez Activer l'accès sécurisé.
3. Dans la boîte de dialogue de confirmation, activez Show the option to enable trusted access (Afficher l'option pour activer l'accès approuvé), saisissez **`enable`** dans la zone, puis choisissez Enable trusted access (Activer l'accès approuvé).
4. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon DevOps Guru qu'il peut désormais activer ce service à l'aide de sa console AWS Organizations.

DevOps Guru console

Pour activer un accès fiable aux services à l'aide de la console DevOps Guru

1. Connectez-vous en tant qu'administrateur sur le compte de gestion et ouvrez la console DevOps Guru : console Amazon DevOps Guru
2. Choisissez Enable trusted access (Activer l'accès approuvé).

## Pour désactiver l'accès sécurisé avec DevOps Guru

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé à Amazon DevOps Guru.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé à l'aide de la AWS Organizations console.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Amazon DevOps Guru dans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de dialogue Désactiver l'accès sécurisé pour Amazon DevOps Guru, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon DevOps Guru qu'il peut désormais désactiver ce service à l' AWS Organizations aide de la console de service ou des outils ;

## Activation d'un compte d'administrateur délégué pour DevOps Guru

Le compte administrateur délégué de DevOps Guru peut consulter les données d'information de tous les comptes membres intégrés à DevOps Guru par l'organisation. Pour plus d'informations sur la façon dont un administrateur délégué gère les comptes de l'organisation, consultez la section Surveiller les comptes au sein de votre organisation dans le guide de l'utilisateur Amazon DevOps Guru.

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour DevOps Guru.

Vous pouvez spécifier un compte d'administrateur délégué depuis la console DevOps Guru, ou en utilisant la `RegisterDelegatedAdministrator` CLI ou le SDK Organizations.

> **Autorisations minimales**
>
> Seul un utilisateur ou un rôle dans le compte de gestion de l'organisation peut configurer un compte membre en tant qu'administrateur délégué de DevOps Guru au sein de l'organisation

DevOps Guru console

Pour configurer un administrateur délégué dans la console DevOps Guru

1. Connectez-vous en tant qu'administrateur sur le compte de gestion et ouvrez la console DevOps Guru : console Amazon DevOps Guru
2. Choisissez Register delegated administrator (Enregistrer l'administrateur délégué). Vous pouvez choisir un compte de gestion ou n'importe compte membre comme administrateur délégué.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

### Désactiver un administrateur délégué pour Guru DevOps

Vous pouvez supprimer l'administrateur délégué à l'aide de la console DevOps Guru, de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations. Pour savoir comment supprimer un administrateur délégué à l'aide de la console DevOps Guru, consultez la section Surveiller les comptes au sein de votre organisation dans le guide de l'utilisateur Amazon DevOps Guru.

## AWS Directory Service et AWS Organizations

AWS Directory Service pour Microsoft Active Directory AWS Managed Microsoft AD, ou vous permet d'exécuter Microsoft Active Directory (AD) en tant que service géré. AWS Directory Service facilite la configuration et l'exécution d'annuaires dans le AWS cloud ou la connexion de vos AWS ressources

à un répertoire Microsoft Active Directory existant sur site. AWS Managed Microsoft AD s'intègre également étroitement AWS Organizations pour permettre un partage de répertoires fluide entre plusieurs VPC Comptes AWS et n'importe quel VPC d'une région. Pour plus d'informations, consultez le Guide d'administration AWS Directory Service.

Pour partager un fichier Directory Service au sein d'une organisation, toutes les fonctionnalités de l'organisation doivent être activées et le répertoire doit se trouver dans le compte de gestion de l'organisation.

Utilisez les informations suivantes pour vous aider AWS Directory Service à intégrer AWS Organizations.

## Permettre un accès fiable avec Directory Service

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Directory Service console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Directory Service console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Directory Service d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Directory Service. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la AWS Directory Service console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la Directory Service console

Pour partager un annuaire, ce qui active automatiquement l'accès approuvé, consultez Partager votre annuaire dans le Guide d'administration AWS Directory Service . Pour step-by-step obtenir des instructions, voir Tutoriel : Partage de votre annuaire Microsoft AD AWS géré.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Organizations console.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Directory Servicedans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Directory Service dialogue Activer l'accès sécurisé pour, tapez enable pour le confirmer, puis choisissez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Directory Service qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

## Désactiver l'accès sécurisé avec Directory Service

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Si vous désactivez l'accès sécurisé AWS Organizations pendant que vous l'utilisez Directory Service, tous les répertoires précédemment partagés continuent de fonctionner normalement. Toutefois, vous ne pouvez plus partager de nouveaux annuaires au sein de l'organisation tant que vous n'avez pas réactivé l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé à l'aide de la AWS Organizations console.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.

3. Choisissez AWS Directory Servicedans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS Directory Service dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez l'administrateur AWS Directory Service qu'il peut désormais désactiver le fonctionnement de ce service à AWS Organizations l'aide de la console de service ou des outils ;.

## Amazon Elastic Compute Cloud et AWS Organizations

Amazon Elastic Compute Cloud fournit une capacité de calcul évolutive à la demande dans le AWS cloud. Lorsque vous utilisez Amazon EC2 avec des organisations, vous permettez à l'administrateur des organisations de créer un rapport indiquant la configuration existante des comptes au sein de leur organisation après avoir utilisé la fonctionnalité Declarative Policies d'Amazon EC2.

Utilisez les informations suivantes pour vous aider à intégrer Amazon Elastic Compute Cloud à AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Amazon EC2 d'effectuer des opérations prises en charge au sein des comptes de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Amazon EC2 et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

### Principaux de service utilisés par Amazon EC2

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Amazon EC2 accordent l'accès aux principaux de service suivants :

- `ec2.amazonaws.com`

## Permettre un accès fiable avec Amazon EC2

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Pour permettre à l'administrateur des Organisations de créer un rapport indiquant la configuration existante des comptes au sein de son organisation, vous devez activer l'accès sécurisé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Declarative Policy for EC2 dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour la politique déclarative pour EC2, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon Elastic Compute Cloud qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

Exécutez la commande suivante pour activer Amazon Elastic Compute Cloud en tant que service fiable auprès des Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal ec2.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver Amazon Elastic Compute Cloud en tant que service de confiance auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ec2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

# Gestionnaire de capacité EC2 et AWS Organizations

EC2 Capacity Manager est une nouvelle interface utilisateur associée à des API qui vous permettent d'agréger, de visualiser, d'analyser et de gérer l'utilisation de vos capacités dans le cadre des réservations EC2 On-Demand, Spot et Capacity. Lorsque vous accordez un accès sécurisé à EC2 Capacity Manager à votre AWS organisation, le service obtient l'autorisation de lire les informations relatives aux membres de l'organisation sur tous les comptes des membres. Plus précisément, Capacity Manager effectue les actions suivantes sur les comptes membres : il collecte les données d'utilisation d'EC2 (y compris les instances à la demande, les instances ponctuelles et les réservations de capacité) auprès de tous les comptes membres pour les agréger dans des rapports de capacité et des tableaux de bord à l'échelle de l'organisation. Le service ne modifie pas les ressources ni les configurations des comptes des membres. Il ne lit que les données de télémétrie d'utilisation déjà collectées par. AWS Cela permet aux administrateurs de l'organisation de visualiser l'utilisation consolidée des capacités, de prévoir les besoins futurs et d'optimiser l'allocation des ressources dans l'ensemble de leur organisation à partir d'un tableau de bord unique. Pour plus d'informations, consultez EC2 Capacity Manager dans le guide de l'utilisateur Amazon EC2.

Utilisez les informations suivantes pour vous aider à intégrer EC2 Capacity Manager à AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à EC2 Capacity Manager d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre EC2 Capacity Manager et Organizations, ou si vous supprimez le compte membre de l'organisation.

Le rôle lié au service suivant est créé dans le compte de gestion lorsque vous activez l'accès sécurisé. Ce rôle permet à EC2 Capacity Manager d'effectuer des tâches au sein de votre organisation et de ses comptes en votre nom.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre EC2 Capacity Manager et AWS Organizations, ou si vous supprimez le compte membre de l'organisation. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour EC2 Capacity Manager et politique AWS gérée : AWSEC2 CapacityManagerServiceRolePolicy dans le guide de l'utilisateur Amazon EC2.

- `AWSServiceRoleForEC2CapacityManager`— Permet à EC2 Capacity Manager d'accéder aux AWS services et aux ressources utilisés ou gérés par EC2 Capacity Manager en votre nom.

## Principaux de service utilisés par EC2 Capacity Manager

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par EC2 Capacity Manager accordent l'accès aux principaux de service suivants :

- `ec2.capacitymanager.amazonaws.com`

## Permettre un accès fiable avec EC2 Capacity Manager

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Lorsque vous accordez un accès sécurisé à EC2 Capacity Manager à votre AWS organisation, le service obtient l'autorisation de lire les informations relatives aux membres de l'organisation sur tous les comptes des membres. Cela permet aux administrateurs de l'organisation de visualiser l'utilisation consolidée des capacités, de prévoir les besoins futurs et d'optimiser l'allocation des ressources dans l'ensemble de leur organisation à partir d'un tableau de bord unique.

Vous pouvez activer l'accès sécurisé à l'aide de la console EC2 Capacity Manager ou de la AWS Organizations console.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils EC2 Capacity Manager pour permettre l'intégration avec Organizations. Cela permet à EC2 Capacity Manager d'effectuer toutes les configurations requises, telles que la création des ressources nécessaires au service. Procédez comme suit uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par EC2 Capacity Manager. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la console ou des outils EC2 Capacity Manager, vous n'avez pas besoin de suivre ces étapes.

Pour activer un accès sécurisé depuis la console EC2 Capacity Manager, connectez-vous en tant qu'administrateur au compte de gestion et ouvrez la console Amazon EC2. Accédez à Capacity Manager, puis à l'onglet Paramètres. Dans la section Accès sécurisé, choisissez Gérer l'accès sécurisé pour l'activer.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez EC2 Capacity Manager dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour EC2 Capacity Manager, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'EC2 Capacity Manager qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer EC2 Capacity Manager en tant que service fiable auprès des Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal ec2.capacitymanager.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Pour désactiver l'accès sécurisé depuis la console EC2 Capacity Manager, accédez à l'onglet Paramètres d'Amazon EC2 Capacity Manager. Dans la section Accès sécurisé, choisissez Gérer l'accès sécurisé pour le désactiver. Remarque : Tous les administrateurs délégués doivent être supprimés avant de désactiver l'accès sécurisé.

Vous pouvez désactiver l'accès sécurisé à l'aide du gestionnaire de capacités EC2 ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils EC2 Capacity Manager pour désactiver l'intégration avec Organizations. Cela permet à EC2 Capacity Manager d'effectuer tout nettoyage dont il a besoin, par exemple en supprimant des ressources ou en accédant à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par EC2 Capacity Manager.
> Si vous désactivez l'accès sécurisé à l'aide de la console ou des outils EC2 Capacity Manager, vous n'avez pas besoin de suivre ces étapes.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

Exécutez la commande suivante pour désactiver EC2 Capacity Manager en tant que service fiable auprès des Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ec2.capacitymanager.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour EC2 Capacity Manager

Un administrateur délégué d'EC2 Capacity Manager peut gérer Capacity Manager pour votre organisation sans utiliser le compte de gestion. Les administrateurs délégués ont la capacité d'activer la gestion des capacités au niveau de l'organisation, de consulter les données de capacité de tous les comptes membres, de modifier les paramètres entre le niveau du compte et celui de l'organisation, et de gérer les prévisions de capacité pour l'ensemble de l'organisation. Pour plus d'informations, consultez la section Administrateurs délégués pour EC2 Capacity Manager dans le guide de l'utilisateur Amazon EC2.

> **Autorisations minimales**
>
> Seul un administrateur du compte de gestion des Organizations peut configurer un administrateur délégué pour EC2 Capacity Manager.

Vous pouvez spécifier un compte d'administrateur délégué à l'aide de la console EC2 Capacity Manager en accédant à Paramètres et en gérant les administrateurs délégués, ou en utilisant la `RegisterDelegatedAdministrator` CLI ou le SDK Organizations. Pour configurer un administrateur délégué à l'aide de la console EC2 Capacity Manager, consultez la section Ajouter un administrateur délégué dans le guide de l'utilisateur Amazon EC2.

AWS CLI, AWS API

Vous pouvez enregistrer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des options AWS SDKs suivantes :

- AWS CLI: register-delegated-administrator

```
$ aws organizations register-delegated-administrator \
    --account-id ACCOUNT_ID \
    --service-principal ec2.capacitymanager.amazonaws.com
```

- AWS API : RegisterDelegatedAdministrator

### Désactivation d'un compte d'administrateur délégué pour EC2 Capacity Manager

Seul un administrateur du compte de gestion des Organisations ou du compte administrateur délégué d'EC2 Capacity Manager peut supprimer un compte d'administrateur délégué de l'organisation. Vous pouvez supprimer un administrateur délégué à l'aide de la console EC2 Capacity Manager en choisissant Supprimer l'administrateur délégué dans l'onglet Paramètres, ou en utilisant la `DeregisterDelegatedAdministrator` CLI ou le SDK Organizations. Pour supprimer un administrateur délégué à l'aide de la console EC2 Capacity Manager, consultez la section Supprimer un administrateur délégué dans le guide de l'utilisateur Amazon EC2.

AWS CLI, AWS API

Vous pouvez supprimer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des options AWS SDKs suivantes :

- AWS CLI: deregister-delegated-administrator

```
$ aws organizations deregister-delegated-administrator \
    --account-id ACCOUNT_ID \
    --service-principal ec2.capacitymanager.amazonaws.com
```

- AWS API : DeregisterDelegatedAdministrator

## Amazon Elastic Kubernetes Service et AWS Organizations

Le tableau de bord Amazon Elastic Kubernetes Service est un tableau de bord consolidé que vous pouvez utiliser pour surveiller, gérer et améliorer la visibilité de vos clusters Kubernetes dans plusieurs régions et comptes. AWS AWS Le tableau de bord EKS vous fournit un contrôle complet et des informations sur votre infrastructure Amazon EKS via une interface centralisée.

Le tableau de bord Amazon Elastic Kubernetes Service vous permet de suivre les clusters dont les mises à niveau sont planifiées, les coûts du plan de contrôle du projet, de consulter les informations

relatives aux clusters et de surveiller la distribution des groupes de nœuds au sein de votre organisation. Vos AWS administrateurs peuvent consulter les données agrégées sur les ressources du cluster, notamment l'état de santé, la distribution des versions et les configurations des modules complémentaires via différentes options de visualisation, notamment des graphiques, des listes de ressources et des cartes géographiques. Le tableau de bord s'intègre aux AWS Organizations pour fournir une visibilité sécurisée entre comptes et entre régions de vos ressources EKS.

Utilisez les informations suivantes pour vous aider à intégrer Amazon Elastic Kubernetes Service à. AWS Organizations

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié au service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès sécurisé à l'aide de la console Amazon Elastic Kubernetes Service. Ce rôle permet à Amazon EKS d'effectuer des opérations prises en charge sur les comptes de votre organisation au sein de votre organisation. Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Amazon Elastic Kubernetes Service et Organizations.

Si vous activez l'accès sécurisé directement depuis la console Organizations, la CLI ou le SDK, le rôle lié au service n'est pas créé automatiquement.

- `AWSServiceRoleForAmazonEKSDashboard`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Amazon EKS donnent accès aux principaux de service suivants :

- `dashboard.eks.amazonaws.com`

## Permettre un accès fiable avec Amazon EKS

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Pour activer un accès sécurisé à l'aide de la console Amazon EKS

Consultez la section Activer l'accès sécurisé dans le guide de l'utilisateur Amazon EKS.

### Désactivation de l'accès sécurisé avec Amazon EKS

Pour désactiver l'accès sécurisé à l'aide de la console Amazon EKS

Consultez la section Désactiver l'accès sécurisé dans le guide de l'utilisateur Amazon EKS.

### Activation d'un compte d'administrateur délégué pour Amazon EKS

L'administrateur du compte de gestion peut déléguer les autorisations administratives Amazon EKS à un compte membre désigné appelé administrateur délégué.

Les comptes de gestion et les comptes d'administrateur délégué peuvent consulter le tableau de bord Amazon EKS.

Pour activer un compte d'administrateur délégué

Consultez la section Activer un compte d'administrateur délégué dans le guide de l'utilisateur Amazon EKS.

### Désactivation d'un administrateur délégué pour Amazon EKS

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Amazon EKS.

Pour désactiver un compte d'administrateur délégué

Consultez la section Désactiver un compte d'administrateur délégué dans le guide de l'utilisateur Amazon EKS.

## AWS Firewall Manager et AWS Organizations

AWS Firewall Manager est un service de gestion de la sécurité que vous utilisez pour configurer et gérer de manière centralisée les règles de pare-feu et autres protections au Comptes AWS sein des applications de votre entreprise. À l'aide de Firewall Manager, vous pouvez déployer des AWS WAF règles, créer AWS Shield Advanced des protections, configurer et auditer les groupes de sécurité Amazon Virtual Private Cloud (Amazon VPC) et déployer AWS Network Firewall des Utilisez Firewall Manager pour configurer vos protections une seule fois et les appliquer automatiquement à l'ensemble des comptes et des ressources de votre organisation, même lorsque de nouvelles

ressources et de nouveaux comptes sont ajoutés. Pour plus d'informations à ce sujet AWS Firewall Manager, consultez le guide du AWS Firewall Manager développeur.

Utilisez les informations suivantes pour vous aider AWS Firewall Manager à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Firewall Manager d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Firewall Manager et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForFMS`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Firewall Manager autorisent l'accès aux mandataires de service suivants :

- `fms.amazonaws.com`

## Activation de l'accès approuvé avec Firewall Manager

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Firewall Manager console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Firewall Manager console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Firewall Manager d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer

l'intégration à l'aide des outils fournis par AWS Firewall Manager. Pour plus d'informations, consultez cette note.
Si vous activez l'accès sécurisé à l'aide de la AWS Firewall Manager console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Vous devez vous connecter avec votre compte AWS Organizations de gestion et configurer un compte au sein de l'organisation en tant que compte AWS Firewall Manager administrateur. Pour de plus amples informations, consultez Définir le compte administrateur AWS Firewall Manager dans le Guide développeur AWS Firewall Manager .

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Firewall Managerdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Firewall Manager dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Firewall Manager qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

Exécutez la commande suivante pour l'activer AWS Firewall Manager en tant que service fiable auprès des Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal fms.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactivation de l'accès approuvé avec Firewall Manager

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils AWS Firewall Manager ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Firewall Manager console ou les outils pour désactiver l'intégration avec Organizations. Cela permet AWS Firewall Manager d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Firewall Manager.
>
> Si vous désactivez l'accès sécurisé à l'aide de la AWS Firewall Manager console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès approuvé à l'aide de la console Firewall Manager

Vous pouvez modifier ou révoquer le compte AWS Firewall Manager administrateur en suivant les instructions de la section Désignation d'un autre compte comme compte AWS Firewall Manager administrateur dans le guide du AWS Firewall Manager développeur.

Si vous révoquez le compte administrateur, vous devez vous connecter au compte AWS Organizations de gestion et créer un nouveau compte administrateur pour AWS Firewall Manager.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Firewall Managerdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS Firewall Manager dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Firewall Manager qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Firewall Manager en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte administrateur délégué pour Firewall Manager

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Firewall Manager qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de Firewall Manager.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué pour Firewall Manager dans l'organisation.

Pour savoir comment désigner un compte membre en tant qu'administrateur de Firewall Manager pour l'organisation, consultez la section Définir le compte AWS Firewall Manager administrateur dans le Guide du AWS Firewall Manager développeur.

## Amazon GuardDuty et AWS Organizations

Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite diverses sources de données, en utilisant des flux de renseignements sur les menaces et l'apprentissage automatique pour identifier les activités inattendues, potentiellement non autorisées et malveillantes au sein de votre AWS environnement. Cela peut inclure des problèmes tels que l'augmentation des privilèges, l'utilisation d'informations d'identification divulguées, la communication avec des adresses IP ou des domaines malveillants URLs, ou la présence de logiciels malveillants sur vos instances Amazon Elastic Compute Cloud et vos charges de travail de conteneur.

Vous pouvez contribuer à simplifier la gestion en GuardDuty utilisant Organizations pour gérer GuardDuty tous les comptes de votre organisation.

Pour plus d'informations, consultez la section Gestion GuardDuty des comptes AWS Organizations dans le guide de GuardDuty l'utilisateur Amazon

Utilisez les informations suivantes pour vous aider à intégrer Amazon GuardDuty à AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Les rôles liés à un service suivant sont automatiquement créés dans le compte de gestion de votre organisation lorsque vous activez l'accès de confiance. Ces rôles permettent d' GuardDuty effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation. Vous ne pouvez supprimer un rôle que si vous désactivez l'accès sécurisé entre GuardDuty et Organizations, ou si vous supprimez le compte membre de l'organisation.

- Le rôle `AWSServiceRoleForAmazonGuardDuty` lié à un service est automatiquement créé dans les comptes intégrés à GuardDuty Organizations. Pour plus d'informations, consultez la section Gestion des GuardDuty comptes auprès d'Organizations dans le guide de GuardDuty l'utilisateur Amazon
- Le rôle `AmazonGuardDutyMalwareProtectionServiceRolePolicy` lié au service est automatiquement créé dans les comptes qui ont activé la protection contre les GuardDuty programmes malveillants. Pour plus d'informations, consultez la section Autorisations de rôle liées à un service pour la protection contre les GuardDuty logiciels malveillants dans le guide de l'utilisateur Amazon GuardDuty

## Principaux de service utilisés par les rôles liés à un service

- `guardduty.amazonaws.com`, utilisé par le rôle lié à un service `AWSServiceRoleForAmazonGuardDuty`.
- `malware-protection.guardduty.amazonaws.com`, utilisé par le rôle lié à un service `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

## Permettre un accès fiable avec GuardDuty

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide d'Amazon GuardDuty.

Amazon a GuardDuty besoin d'un AWS Organizations accès sécurisé pour que vous puissiez désigner un compte membre comme GuardDuty administrateur de votre organisation. Si vous configurez un administrateur délégué à l'aide de la GuardDuty console, l'accès sécurisé est GuardDuty automatiquement activé pour vous.

Toutefois, si vous souhaitez configurer un compte d'administrateur délégué à l'aide du AWS CLI ou de l'un des AWS SDKs, vous devez appeler explicitement l'opération Enable AWSService Access et fournir le principal de service en tant que paramètre. Ensuite, vous pouvez appeler EnableOrganizationAdminAccountpour déléguer le compte GuardDuty administrateur.

## Désactiver l'accès sécurisé avec GuardDuty

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver Amazon GuardDuty en tant que service de confiance auprès d'Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour GuardDuty

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour GuardDuty qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de GuardDuty.

Autorisations minimales

Pour plus d'informations sur les autorisations requises pour désigner un compte membre en tant qu'administrateur délégué, consultez la section Autorisations requises pour désigner un administrateur délégué dans le guide de GuardDuty l'utilisateur Amazon

Pour désigner un compte membre en tant qu'administrateur délégué pour GuardDuty

Consultez Désigner un administrateur délégué et ajouter des comptes membres (console) et Désigner un administrateur délégué et ajouter des comptes membres (API)

## AWS Health et AWS Organizations

AWS Health fournit une visibilité continue sur les performances de vos ressources et sur la disponibilité de vos comptes Services AWS et de vos comptes. AWS Health organise des événements lorsque vos AWS ressources et services sont affectés par un problème ou seront affectés par des modifications à venir. Une fois que vous avez activé la vue organisationnelle, un utilisateur du compte de gestion de l'organisation peut agréger les AWS Health événements de tous les comptes de l'organisation. La vue organisationnelle affiche uniquement AWS Health les événements diffusés après l'activation de la fonctionnalité et les conserve pendant 90 jours.

Vous pouvez activer la vue organisationnelle à l'aide de la AWS Health console, du AWS Command Line Interface (AWS CLI) ou de l' AWS Health API.

Pour plus d'informations, consultez la section Agrégation d' AWS Health événements dans le guide de l'AWS Health utilisateur.

Utilisez les informations suivantes pour vous aider AWS Health à intégrer AWS Organizations.

### Rôles liés aux services pour l'intégration

Le rôle `AWSServiceRoleForHealth_Organizations` lié à un service permet d' AWS Health effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Ce rôle est créé automatiquement dans le compte de gestion de votre organisation lorsque vous activez l'accès sécurisé en appelant l'opération EnableHealthServiceAccessForOrganizationAPI.

Sinon, créez le rôle à l'aide de la AWS Health console, de l'API ou de la CLI, comme décrit dans la section Création d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre AWS Health et Organizations, ou si vous supprimez le compte membre de l'organisation.

### Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par AWS Health accordent l'accès aux principaux de service suivants :

- `health.amazonaws.com`

## Permettre un accès fiable avec AWS Health

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Lorsque vous activez la fonctionnalité d'affichage organisationnel pour AWS Health, l'accès sécurisé est également activé automatiquement pour vous.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Health console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Health console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Health d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Health. Pour plus d'informations, consultez cette note. Si vous activez l'accès sécurisé à l'aide de la AWS Health console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la AWS Health console

Vous pouvez activer l'accès sécurisé AWS Health en utilisant l'une des options suivantes :

- Utilisez la AWS Health console. Pour de plus amples informations, consultez Vue organisationnelle (console) dans le Guide de l'utilisateur AWS Health .
- Utilisez la AWS CLI. Pour de plus amples informations, consultez Vue organisationnelle (CLI) dans le Guide de l'utilisateur AWS Health .
- Appelez l'opération de l'API EnableHealthServiceAccessForOrganization.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Health en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AWS Health

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Une fois que vous avez désactivé la fonctionnalité d'affichage organisationnel, AWS Health arrête d'agréger les événements pour tous les autres comptes de votre organisation. Cela désactive également automatiquement l'accès approuvé pour vous.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils AWS Health ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Health console ou les outils pour désactiver l'intégration avec Organizations. Cela permet AWS Health d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Health.
> Si vous désactivez l'accès sécurisé à l'aide de la AWS Health console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès sécurisé à l'aide de la AWS Health console

Vous pouvez désactiver l'accès approuvé à l'aide de l'une des options suivantes :

- Utilisez la AWS Health console. Pour de plus amples informations, consultez Désactivation de la vue organisationnelle (console) dans le Guide de l'utilisateur AWS Health .
- Utilisez l' AWS CLI. Pour de plus amples informations, consultez Désactivation de la vue organisationnelle (CLI) dans le Guide de l'utilisateur AWS Health .
- Appelez l'opération de l'API DisableHealthServiceAccessForOrganization.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Health en tant que service sécurisé auprès des Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal health.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte d'administrateur délégué pour AWS Health

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour AWS Health qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de AWS Health.

Pour désigner un compte membre en tant qu'administrateur délégué pour AWS Health

Consultez Enregistrer un administrateur délégué pour votre vue organisationnelle

Pour supprimer un administrateur délégué pour AWS Health

Consultez Supprimer un administrateur délégué de votre vue organisationnelle

## Gestion des identités et des accès AWS et AWS Organizations

Gestion des identités et des accès AWS est un service Web permettant de contrôler de manière sécurisée l'accès aux AWS services.

Vous pouvez utiliser les données sur les services consultés en dernier dans IAM pour vous aider à mieux comprendre les activités AWS au sein de votre organisation. Vous pouvez utiliser ces données pour créer et mettre à jour des politiques de contrôle des services (SCPs) qui limitent l'accès aux seuls AWS services utilisés par les comptes de votre organisation.

Pour obtenir un exemple, consultez Utilisation des données pour affiner les autorisations d'une unité d'organisation dans le Guide de l'utilisateur IAM.

IAM vous permet de gérer de manière centralisée les informations d'identification des utilisateurs root et d'effectuer des tâches privilégiées sur les comptes des membres. Une fois que vous avez activé la gestion de l'accès root, qui permet un accès sécurisé pour IAM in AWS Organizations, vous pouvez sécuriser de manière centralisée les informations d'identification de l'utilisateur root des comptes membres. Les comptes membres ne peuvent pas se connecter à leur utilisateur racine ni récupérer le mot de passe de leur utilisateur racine. Le compte de gestion ou un compte d'administrateur délégué

pour IAM peut également effectuer certaines tâches privilégiées sur les comptes des membres en utilisant un accès root à court terme. Les sessions privilégiées de courte durée vous fournissent des informations d'identification temporaires que vous pouvez définir pour effectuer des actions privilégiées sur un compte membre de votre organisation.

Pour plus d'informations, consultez Gestion centralisée de l'accès racine pour les comptes membres dans le Guide de l'utilisateur  IAM.

Utilisez les informations suivantes pour vous aider Gestion des identités et des accès AWS à intégrer AWS Organizations.

## Permettre un accès fiable avec IAM

Lorsque vous activez la gestion de l'accès root, l'accès sécurisé est activé pour IAM in AWS Organizations.

## Désactivation de l'accès sécurisé avec IAM

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec Gestion des identités et des accès AWS.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Gestion des identités et des accès AWSdans la liste des services.

4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de Gestion des identités et des accès AWS dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le Gestion des identités et des accès AWS qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver Gestion des identités et des accès AWS en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal iam.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour IAM

Lorsque vous désignez un compte membre en tant qu'administrateur délégué de l'organisation, les utilisateurs et les rôles associés à ce compte peuvent effectuer des tâches privilégiées sur les comptes membres qui, autrement, ne peuvent être effectuées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Pour plus d'informations, voir Exécuter une tâche privilégiée sur le compte d'un membre d'une Organisation dans le Guide de l'utilisateur d'IAM.

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour IAM.

Vous pouvez spécifier un compte d'administrateur délégué à partir de la console IAM ou de l'API, ou à l'aide de la CLI ou du SDK Organizations.

### Désactivation d'un administrateur délégué pour IAM

Seul un administrateur du compte de gestion Organizations ou du compte d'administrateur délégué IAM peut supprimer un compte d'administrateur délégué de l'organisation. Vous pouvez désactiver l'administration déléguée à l'aide de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations.

## Amazon Inspector et AWS Organizations

Amazon Inspector est un service automatisé de gestion des vulnérabilités qui analyse continuellement les charges de travail Amazon EC2 et de conteneur pour détecter les vulnérabilités logicielles et l'exposition involontaire au réseau.

À l'aide d'Amazon Inspector, vous pouvez gérer plusieurs comptes associés en AWS Organizations déléguant simplement un compte administrateur à Amazon Inspector. L'administrateur délégué gère Amazon Inspector pour l'organisation et dispose d'autorisations spéciales pour effectuer des tâches pour le compte de votre organisation, par exemple :

- Activer ou désactiver les analyses pour les comptes membres
- Afficher les données de résultats agrégées de l'ensemble de l'organisation
- Créer et gérer les règles de suppression

Pour plus d'informations, consultez Gestion de plusieurs comptes avec AWS Organizations dans le Guide de l'utilisateur Amazon Inspector.

Utilisez les informations suivantes pour vous aider à intégrer Amazon Inspector à AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Amazon Inspector d'effectuer les opérations prises en charge dans les comptes de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Amazon Inspector et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForAmazonInspector2`

Pour plus d'informations, consultez Utilisation des rôles liés à un service avec Amazon Inspector dans le Guide de l'utilisateur Amazon Inspector.

### Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Amazon Inspector accordent l'accès aux principaux de service suivants :

- `inspector2.amazonaws.com`

### Pour activer l'accès approuvé avec Amazon Inspector

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Amazon Inspector a besoin d'un AWS Organizations accès sécurisé pour que vous puissiez désigner un compte membre en tant qu'administrateur délégué de ce service pour votre organisation.

Lorsque vous désignez un administrateur délégué pour Amazon Inspector, il active automatiquement l'accès approuvé pour Amazon Inspector pour votre organisation.

Toutefois, si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous devez appeler explicitement l'`EnableAWSServiceAccess`opération et fournir le principal de service en tant que paramètre. Vous pouvez ensuite appeler `EnableDelegatedAdminAccount` pour déléguer le compte administrateur Inspector.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

Exécutez la commande suivante pour activer Amazon Inspector en tant que service fiable auprès d'Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

> **Note**
>
> Si vous utilisez l'API `EnableAWSServiceAccess`, vous devez également appeler `EnableDelegatedAdminAccount` pour déléguer le compte administrateur Inspector.

## Pour désactiver l'accès approuvé avec Amazon Inspector

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec Amazon Inspector.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver Amazon Inspector en tant que service de confiance auprès d'Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte administrateur délégué pour Amazon Inspector

Avec Amazon Inspector, vous pouvez gérer plusieurs comptes au sein d'une organisation à l'aide d'un administrateur délégué avec AWS Organizations service.

Le compte AWS Organizations de gestion désigne un compte au sein de l'organisation en tant que compte d'administrateur délégué pour Amazon Inspector. L'administrateur délégué gère Amazon Inspector pour l'organisation et dispose d'autorisations spéciales pour effectuer des tâches pour le compte de votre organisation, par exemple : activer ou désactiver les analyses des comptes membres, afficher les données de résultats agrégées de l'ensemble de l'organisation, puis créer et gérer des règles de suppression

Pour plus d'informations sur la manière dont un administrateur délégué gère les comptes d'organisation, consultez Présentation de la relation entre les comptes administrateur et membres dans le Guide de l'utilisateur Amazon Inspector.

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Amazon Inspector.

Vous pouvez spécifier un compte d'administrateur délégué à partir de l'API ou de la console Amazon Inspector ou en utilisant la CLI Organizations ou l'opération SDK.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué d'Amazon Inspector dans l'organisation.

Pour configurer un administrateur délégué à l'aide de la console Amazon Inspector, consultez Étape 1 : Activer Amazon Inspector - Environnement à plusieurs-comptes dans le Guide de l'utilisateur Amazon Inspector.

> **Note**
>
> Vous devez appeler `inspector2:enableDelegatedAdminAccount` dans chaque région où vous utilisez Amazon Inspector.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

### Désactivation d'un administrateur délégué pour Amazon Inspector

Seul un administrateur du compte AWS Organizations de gestion peut supprimer un compte d'administrateur délégué de l'organisation.

Vous pouvez supprimer l'administrateur délégué à l'aide de l'API ou de la console Amazon Inspector, ou à l'aide de la CLI `DeregisterDelegatedAdministrator` Organizations ou de l'opération SDK. Pour supprimer un administrateur délégué à l'aide de la console Amazon Inspector, consultez Suppression d'un administrateur délégué dans le Guide de l'utilisateur Amazon Inspector.

## AWS License Manager et AWS Organizations

AWS License Manager rationalise le processus de transfert des licences des fournisseurs de logiciels vers le cloud. Au fur et à mesure que vous développez une infrastructure cloud AWS, vous pouvez réduire les coûts en utilisant les opportunités bring-your-own-license (BYOL), c'est-à-dire en réaffectant votre inventaire de licences existant pour l'utiliser avec les ressources du cloud. En appliquant des commandes à base de règles à la consommation des licences, les administrateurs

peuvent définir des limites flexibles ou strictes pour les déploiements cloud nouveaux ou existants, afin d'arrêter d'avance toute utilisation non conforme du serveur.

Pour plus d'informations sur License Manager, consultez le Guide de l'utilisateur License Manager.

En associant License Manager à AWS Organizations, vous pouvez :

- autoriser la découverte entre comptes de ressources de calcul dans l'ensemble de votre organisation ;
- afficher et gérer les abonnements Linux commerciaux que vous possédez et que vous exécutez sur AWS. Pour plus d'informations, consultez la section Abonnements Linux dans AWS License Manager.

Utilisez les informations suivantes pour vous aider AWS License Manager à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Les rôles liés à un service suivant sont automatiquement créés dans le compte de gestion de votre organisation lorsque vous activez l'accès de confiance. Ces rôles permettent à License Manager d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous ne pouvez supprimer ou modifier ces rôles que si vous désactivez l'accès approuvé entre License Manager et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Pour plus d'informations, consultez les sections License Manager : rôle du compte de gestion, License Manager : rôle du compte membre et License Manager : rôle des abonnements Linux.

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par License Manager autorisent l'accès aux mandataires de service suivants :

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

## Activation de l'accès approuvé avec License Manager

Vous ne pouvez activer l'accès sécurisé qu'à l'aide de AWS License Manager.

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Pour activer l'accès approuvé avec License Manager

Vous devez vous connecter à la console License Manager à l'aide de votre compte de AWS Organizations gestion et l'associer à votre compte License Manager. Pour plus d'informations, consultez la section Paramètres dans AWS License Manager.

## Désactivation de l'accès approuvé avec License Manager

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour la désactiver AWS License Manager en tant que service sécurisé auprès des Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal license-manager.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

Pour désactiver l'accès approuvé des abonnements Linux, utilisez :

```
$  aws organizations disable-aws-service-access \
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- AWS API : Désactiver AWSService l'accès

### Activation d'un compte administrateur délégué pour License Manager

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour License Manager qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de License Manager.

Pour déléguer un compte membre comme administrateur pour License Manager, procédez de la manière décrite sous Enregistrer un administrateur délégué dans le Guide de l'utilisateur License Manager.

## AWS Managed Services (AMS), génération de rapports en libre-service (SSR) et AWS Organizations

AWS Managed Services (AMS) Self-Service Reporting (SSR) collecte des données provenant de divers AWS services natifs et donne accès à des rapports sur les principales offres AMS. Le SSR fournit les informations que vous pouvez utiliser pour soutenir les opérations, la gestion des configurations, la gestion des actifs, la gestion de la sécurité et la conformité.

Après avoir intégré AWS Organizations, vous pouvez activer les rapports agrégés en libre-service (SSR). Il s'agit d'une fonctionnalité AMS qui permet aux clients d'Advanced et d'Accelerate de consulter leurs rapports en libre-service existants agrégés au niveau de l'organisation, entre comptes. Cela vous donne une visibilité sur les indicateurs opérationnels clés tels que la conformité des correctifs, la couverture des sauvegardes et les incidents sur tous les comptes gérés par AMS. AWS Organizations

Utilisez les informations suivantes pour vous aider à intégrer AWS Managed Services (AMS) le reporting en libre-service (SSR) à. AWS Organizations

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à AMS d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre AMS et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par AMS donnent accès aux principaux de service suivants :

- `selfservicereporting.managedservices.amazonaws.com`

## Permettre un accès fiable avec AMS

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer AWS Managed Services (AMS) Self-Service Reporting (SSR) en tant que service fiable auprès des Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal selfservicereporting.managedservices.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AMS

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver AWS Managed Services (AMS) Self-Service Reporting (SSR) en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal selfservicereporting.managedservices.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour AMS

Les comptes d'administrateur délégué peuvent consulter les rapports AMS (tels que les correctifs et les sauvegardes) de tous les comptes dans une vue agrégée unique dans la console AMS.

Vous pouvez ajouter un administrateur délégué à l'aide de la console AMS ou de l'API, ou à l'aide de la `RegisterDelegatedAdministrator` CLI ou du SDK Organizations.

### Désactivation d'un administrateur délégué pour AMS

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour AMS.

Vous pouvez supprimer l'administrateur délégué à l'aide de la console AMS ou de l'API, ou à l'aide de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations.

## Amazon Macie et AWS Organizations

Amazon Macie est un service totalement géré de sécurité et de confidentialité des données qui utilise le machine learning et la correspondance de modèles pour identifier, surveiller et protéger vos données sensibles dans Amazon Simple Storage Service (Amazon S3). Macie automatise la découverte de données sensibles, notamment les informations d'identification personnelle et la propriété intellectuelle, afin de vous fournir une meilleure compréhension des données stockées par votre organisation dans Amazon S3.

Pour plus d'informations, consultez Gestion des comptes Amazon Macie avec AWS Organizations dans le Guide de l'utilisateur Amazon Macie.

Utilisez les informations suivantes pour vous aider à intégrer Amazon Macie à. AWS Organizations

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service ci-dessous est automatiquement créé pour le compte administrateur Macie délégué de l'organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Macie d'effectuer les opérations prises en charge pour les comptes de votre organisation.

Vous ne pouvez supprimer ce rôle que si vous désactivez l'accès approuvé entre Macie et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleRorAmazonMacie`

### Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Macie autorisent l'accès aux mandataires de service suivants :

- `macie.amazonaws.com`

## Activation de l'accès approuvé avec Macie

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès approuvé à l'aide de la console Amazon Macie ou de la console AWS Organizations .

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils d'Amazon Macie pour activer l'intégration à Organizations. Cela permet à Amazon Macie d'effectuer toute configuration nécessaire, par exemple la création des ressources nécessaires au service. Exécutez ces étapes uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par Amazon Macie. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'Amazon Macie, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console Macie

Amazon Macie a besoin d'un accès sécurisé AWS Organizations pour désigner un compte membre en tant qu'administrateur Macie de votre organisation. Si vous configurez un administrateur délégué à l'aide de la console de gestion de Macie, le service active automatiquement l'accès approuvé pour vous.

Pour plus d'informations, consultez Intégration et configuration d'une organisation dans Amazon Macie dans le Guide de l'utilisateur Amazon Macie.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer Amazon Macie en tant que service de confiance auprès d'Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Activation d'un compte administrateur délégué pour Macie

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Macie qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de Macie.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations disposant de l'autorisation suivante peuvent configurer un compte membre en tant qu'administrateur délégué pour Macie dans l'organisation :
>
> - `organizations:EnableAWSServiceAccess`
> - `macie:EnableOrganizationAdminAccount`

Pour désigner un compte membre comme administrateur délégué pour Macie

Amazon Macie a besoin d'un accès sécurisé AWS Organizations pour désigner un compte membre en tant qu'administrateur Macie de votre organisation. Si vous configurez un administrateur délégué à l'aide de la console de gestion de Macie, le service active automatiquement l'accès approuvé pour vous.

Pour de plus amples informations, veuillez consulter https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin.

# AWS Marketplace et AWS Organizations

AWS Marketplace est un catalogue numérique organisé que vous pouvez utiliser pour trouver, acheter, déployer et gérer les logiciels, données et services tiers dont vous avez besoin pour créer des solutions et gérer votre entreprise.

AWS Marketplace crée et gère les licences utilisées AWS License Manager pour vos achats dans AWS Marketplace. Lorsque vous partagez (accordez l'accès à) vos licences avec d'autres comptes de votre organisation, AWS Marketplace crée et gère de nouvelles licences pour ces comptes.

Pour de plus amples informations, consultez Rôles liés à un service pour AWS Marketplace dans le Guide de l'acheteur AWS Marketplace .

Utilisez les informations suivantes pour vous aider AWS Marketplace à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' AWS Marketplace effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre AWS Marketplace et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForMarketplaceLicenseManagement`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par AWS Marketplace accordent l'accès aux principaux de service suivants :

- `license-management.marketplace.amazonaws.com`

## Permettre un accès fiable avec AWS Marketplace

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Marketplace console ou de la AWS Organizations console.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Marketplace console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Marketplace d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Marketplace. Pour plus d'informations, consultez cette note.
>
> Si vous activez l'accès sécurisé à l'aide de la AWS Marketplace console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la AWS Marketplace console

Consultez Création d'un rôle lié à un service pour AWS Marketplace dans le Guide de l'acheteur AWS Marketplace .

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Marketplacedans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Marketplace dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Marketplace qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Marketplace en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AWS Marketplace

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Marketplace en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal license-management.marketplace.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## AWS Marketplace Private Marketplace et AWS Organizations

AWS Marketplace est un catalogue numérique organisé que vous pouvez utiliser pour trouver, acheter, déployer et gérer les logiciels, données et services tiers dont vous avez besoin pour créer des solutions et gérer votre entreprise. Un marché privé vous fournit un large catalogue de produits disponibles AWS Marketplace, ainsi qu'un contrôle précis de ces produits.

AWS Marketplace Private Marketplace vous permet de créer plusieurs expériences de marché privées associées à l'ensemble de votre organisation OUs, à un ou plusieurs comptes de votre organisation, chacun avec son propre ensemble de produits approuvés. Vos AWS administrateurs peuvent également appliquer l'image de marque de l'entreprise à chaque expérience de marché privée avec le logo, le message et la palette de couleurs de votre entreprise ou de votre équipe.

Pour plus d'informations, consultez la section Utilisation des rôles pour configurer Private Marketplace AWS Marketplace dans le Guide de AWS Marketplace l'acheteur.

Utilisez les informations suivantes pour vous aider à intégrer AWS Marketplace Private Marketplace à AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié au service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès sécurisé à l'aide de la console Private AWS Marketplace Marketplace. Ce rôle permet à Private Marketplace d'effectuer des opérations prises en charge sur les comptes de votre organisation au sein de votre organisation. Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre AWS Marketplace Private Marketplace et Organizations et si vous dissociez toutes les expériences de marché privé au sein de votre organisation.

Si vous activez l'accès sécurisé directement depuis la console Organizations, la CLI ou le SDK, le rôle lié au service n'est pas créé automatiquement.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Private Marketplace donnent accès aux principaux de service suivants :

- `private-marketplace.marketplace.amazonaws.com`

## Permettre un accès fiable avec Private Marketplace

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la console AWS Marketplace Private Marketplace ou de la AWS Organizations console.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils AWS Marketplace Private Marketplace pour permettre l'intégration avec Organizations. Cela permet à AWS Marketplace Private Marketplace d'effectuer toutes les configurations nécessaires, telles que la création des ressources nécessaires au service. Procédez comme suit uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Marketplace Private Marketplace. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la console ou des outils AWS Marketplace Private Marketplace, vous n'avez pas besoin de suivre ces étapes.

Pour activer un accès sécurisé à l'aide de la console Private Marketplace

Consultez Getting started with Private Marketplace dans le guide d'AWS Marketplace achat.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Marketplace Private Marketplace dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour AWS Marketplace Private Marketplace, tapez enable pour confirmer, puis choisissez Enable trusted access.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur de AWS Marketplace Private Marketplace qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer AWS Marketplace Private Marketplace en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec Private Marketplace

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver AWS Marketplace Private Marketplace en tant que service de confiance auprès d'Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour Private Marketplace

L'administrateur du compte de gestion peut déléguer les autorisations administratives de Private Marketplace à un compte membre désigné appelé administrateur délégué. Pour enregistrer un compte en tant qu'administrateur délégué pour le marché privé, l'administrateur du compte de gestion doit s'assurer que l'accès sécurisé et le rôle lié au service sont activés, choisir Enregistrer un nouvel administrateur, fournir le numéro de AWS compte à 12 chiffres et choisir Soumettre.

Les comptes de gestion et les comptes d'administrateur délégué peuvent effectuer des tâches administratives de Private Marketplace, telles que la création d'expériences, la mise à jour des paramètres de marque, l'association ou la dissociation d'audiences, l'ajout ou la suppression de produits, ainsi que l'approbation ou le refus des demandes en attente.

Pour configurer un administrateur délégué à l'aide de la console Private Marketplace, consultez la section Création et gestion d'un marché privé dans le Guide de AWS Marketplace l'acheteur.

Vous pouvez également configurer un administrateur délégué à l'aide de l'`RegisterDelegatedAdministrator`API Organizations. Pour plus d'informations, reportez-vous RegisterDelegatedAdministratorà la section Organizations Command Reference.

### Désactiver un administrateur délégué pour Private Marketplace

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Private Marketplace.

Vous pouvez supprimer l'administrateur délégué à l'aide de la console ou de l'API Private Marketplace, ou à l'aide de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations.

Pour désactiver le compte Private Marketplace de l'administrateur délégué à l'aide de la console Private Marketplace, consultez la section Création et gestion d'une place de marché privée dans le Guide de AWS Marketplace l'acheteur.

## AWS Marketplace tableau de bord des informations sur les achats et AWS Organizations

Vous utilisez le tableau de bord des informations sur les AWS Marketplace achats pour consulter les accords et les données d'analyse des coûts pour tous les AWS comptes de votre organisation. Lorsqu'il est intégré à Organizations, le tableau de bord des informations sur les AWS Marketplace achats prend en compte les modifications apportées à l'organisation, par exemple l'adhésion d'un compte à l'organisation, et agrège les données relatives aux accords correspondants afin de créer leurs tableaux de bord.

Pour plus d'informations, consultez la section Informations sur les achats dans le Guide de AWS Marketplace l'acheteur.

Utilisez les informations suivantes pour vous aider à intégrer le tableau de bord des informations sur les AWS Marketplace achats à AWS Organizations.

## Rôles liés aux services et politiques gérées créés lorsque vous activez l'intégration

Lorsque vous activez le tableau de bord des informations sur les AWS Marketplace achats, le rôle `AWSServiceRoleForProcurementInsightsPolicy` lié au service et la politique `AWSServiceRoleForProcurementInsightsPolicy` AWS gérée sont créés.

## Permettre un accès fiable grâce à des informations sur les AWS Marketplace achats

L'activation d'un accès fiable permet au tableau de bord des informations sur les AWS Marketplace achats de s'intégrer au service Organizations du client. AWS Marketplace le tableau de bord des informations sur les achats écoute les modifications apportées à l'organisation, par exemple l'adhésion d'un compte à l'organisation, et agrège les données relatives aux accords correspondants afin de créer ses tableaux de bord.

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer un accès fiable à l'aide de la console du tableau de bord des informations sur les AWS Marketplace achats ou de la AWS Organizations console.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils du tableau de bord des informations sur les AWS Marketplace achats pour permettre l'intégration avec les Organizations. Cela permet au tableau de bord des informations sur les AWS Marketplace achats d'effectuer toutes les configurations requises, telles que la création des ressources nécessaires au service. Procédez comme suit uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par le tableau de bord des informations sur les AWS Marketplace achats. Pour plus d'informations, consultez cette note.
> Si vous activez un accès fiable à l'aide de la console ou des outils du tableau de bord des informations sur les AWS Marketplace achats, vous n'avez pas besoin de suivre ces étapes.

Pour permettre un accès fiable en activant le tableau de bord AWS Marketplace des informations sur les achats

Consultez la section Activation du tableau de bord des informations sur les AWS Marketplace achats dans le Guide de AWS Marketplace l'acheteur.

Pour permettre un accès sécurisé à l'aide des outils Organizations

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez le tableau de bord des informations sur les AWS Marketplace achats dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour le tableau de bord des informations sur les AWS Marketplace achats, tapez activer pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, indiquez à l'administrateur du tableau de bord des informations sur les AWS Marketplace achats qu'il peut désormais activer ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer le tableau de bord des informations sur les AWS Marketplace achats en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès fiable grâce à des informations sur les AWS Marketplace achats

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver le tableau de bord des informations sur les AWS Marketplace achats en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour obtenir des informations sur les AWS Marketplace achats

Pour configurer un administrateur délégué dans la console AWS Marketplace Procurement Insights, consultez la section Enregistrement des administrateurs délégués > dans le Guide de l'AWS Marketplace acheteur.

Vous pouvez également configurer un administrateur délégué à l'aide de l'`RegisterDelegatedAdministrator`API Organizations. Pour plus d'informations, reportez-vous RegisterDelegatedAdministratorà la section Organizations Command Reference.

### Désactiver un administrateur délégué pour obtenir des informations sur les AWS Marketplace achats

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour obtenir des informations sur les AWS Marketplace achats.

Pour supprimer un administrateur délégué via la console AWS Marketplace Procurement Insights, consultez la section Désenregistrement des administrateurs délégués dans le Guide de l'AWS Marketplace acheteur.

Vous pouvez également supprimer l'administrateur délégué à l'aide de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations.

## AWS Gestionnaire de réseau et AWS Organizations

Network Manager vous permet de gérer de manière centralisée votre réseau central AWS Cloud WAN et votre réseau AWS Transit Gateway sur l'ensemble AWS des comptes, des régions et des sites sur site. Grâce à la prise en charge de plusieurs comptes, vous pouvez créer un réseau mondial unique pour n'importe lequel de vos AWS comptes et enregistrer des passerelles de transit entre plusieurs comptes et le réseau mondial à l'aide de la console Network Manager.

Lorsque l'accès sécurisé entre Network Manager et les Organizations est activé, les administrateurs délégués enregistrés et les comptes de gestion peuvent tirer parti du rôle lié au service déployé dans les comptes membres pour décrire les ressources attachées à vos réseaux mondiaux. À partir de la console Network Manager, les administrateurs délégués enregistrés et les comptes de gestion peuvent assumer les rôles IAM personnalisés déployés dans les comptes membres : `CloudWatch-CrossAccountSharingRole` pour la surveillance et la gestion des événements multi-comptes, et `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` pour l'accès au rôle de commutateur de console pour afficher et gérer des ressources multi-comptes)

**Important**

- Nous vous recommandons vivement d'utiliser la console Network Manager pour gérer les paramètres multi-comptes (administrateurs enable/disable trusted access and register/deregister délégués). La gestion de ces paramètres à partir de la console déploie et gère automatiquement tous les rôles liés au service requis et les rôles IAM personnalisés vers les comptes membres nécessaires à l'accès multi-comptes.

- Lorsque vous activez l'accès sécurisé pour Network Manager dans la console Network Manager, la console active également le CloudFormation StackSets service. Network Manager est utilisé StackSets pour déployer les rôles IAM personnalisés nécessaires à la gestion multi-comptes.

Pour plus d'informations sur l'intégration de Network Manager avec Organizations, consultez Gérer plusieurs comptes dans Network Manager AWS Organizations dans le Guide de l'utilisateur Amazon VPC.

Utilisez les informations suivantes pour vous aider à intégrer AWS Network Manager à AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Les rôles liés à un service suivant sont automatiquement créés dans le compte de l'organisation répertorié lorsque vous activez l'accès sécurisé. Ces rôles permettent à Network Manager d'effectuer les opérations prises en charge dans les comptes de votre organisation. Si vous désactivez l'accès sécurisé, Network Manager ne supprimera pas ces rôles des comptes de votre organisation. Vous pouvez les supprimer manuellement à l'aide de la console IAM.

Compte de gestion

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Comptes de membres

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Lorsque vous enregistrez un compte membre en tant qu'administrateur délégué, le rôle supplémentaire suivant est automatiquement créé dans le compte d'administrateur délégué :

- `AWSServiceRoleForCloudWatchCrossAccount`

## Principaux de service utilisés par les rôles liés à un service

Les rôles liés à un service ne peuvent être assumés que par les principaux de service autorisés par les relations d'approbation définies pour le rôle.

- Pour le rôle `AWSServiceRoleForNetworkManager service-linked`, `networkmanager.amazonaws.com` est le seul principal de service à y avoir accès.
- Pour le rôle lié à un service `AWSServiceRoleForCloudFormationStackSetsOrgMember`, `member.org.stacksets.cloudformation.amazonaws.com` est le seul principal de service à y avoir accès.
- Pour le rôle lié à un service `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`, `stacksets.cloudformation.amazonaws.com` est le seul principal de service à y avoir accès.
- Pour le rôle lié à un service `AWSServiceRoleForCloudWatchCrossAccount`, `cloudwatch-crossaccount.amazonaws.com` est le seul principal de service à y avoir accès.

La suppression de ces rôles compromettra la fonctionnalité multi-comptes pour Network Manager.

## Activation de l'accès sécurisé avec Firewall Manager

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Seul un administrateur du compte de gestion des Organisations est autorisé à activer un accès sécurisé avec un autre AWS service. Assurez-vous d'utiliser la console Network Manager pour activer l'accès sécurisé, afin d'éviter les problèmes d'autorisations. Pour de plus amples informations, consultez Gestion de plusieurs comptes dans Network Manager avec AWS Organizations dans le Guide de l'utilisateur Amazon VPC.

## Désactivation de l'accès sécurisé avec Network Manager

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur d'un compte de gestion d'Organizations est autorisé à désactiver l'accès sécurisé à un autre AWS service.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console Network Manager pour désactiver l'accès sécurisé. Si vous désactivez l'accès sécurisé d'une autre manière, par exemple en utilisant AWS CLI, avec une API ou avec la CloudFormation console, les rôles IAM déployés CloudFormation StackSets et personnalisés risquent de ne pas être correctement nettoyés. Pour désactiver l'accès sécurisé, connectez-vous à la console Network Manager.

### Activation d'un compte administrateur délégué pour Network Manager

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Network Manager qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de Network Manager.

Pour obtenir des instructions sur la façon de désigner un compte membre en tant qu'administrateur délégué de Network Manager dans l'organisation, consultez Enregistrer un administrateur délégué dans le Guide de l'utilisateur Amazon VPC.

## Développeur Amazon Q et AWS Organizations

Amazon Q Developer est un assistant conversationnel génératif basé sur l'IA qui peut vous aider à comprendre, créer, étendre et exploiter AWS des applications. Il s'agit également d'un générateur de code à usage général basé sur l'apprentissage automatique qui vous fournit des recommandations de code en temps réel. La version payante d'Amazon Q Developer nécessite l'intégration d'Organizations. Pour plus d'informations, consultez la section Configuration du compte, du centre d'identité IAM et des organisations dans le guide de l'utilisateur d'Amazon Q.

Utilisez les informations suivantes pour vous aider à intégrer Amazon Q Developer à AWS Organizations.

### Rôles liés à un service

Le rôle `AWSServiceRoleForAmazonQDeveloper` lié au service permet à Amazon Q Developer d'effectuer des opérations prises en charge au sein de votre organisation. Créez le rôle à l'aide de la console, de l'API ou de la CLI Amazon Q Developer, comme décrit dans la section Création d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Si vous utilisez un compte membre, vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Amazon Q Developer et Organizations, ou si vous supprimez le compte membre de l'organisation.

## Principes de service utilisés par Amazon Q Developer

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Amazon Q Developer donnent accès aux principaux de service suivants :

- `q.amazonaws.com`

## Permettre un accès fiable avec Amazon Q Developer

Amazon Q Developer Pro utilise un accès sécurisé pour partager les paramètres définis dans le compte de gestion des Organizations avec les comptes membres de la même organisation.

Par exemple, l'administrateur Amazon Q Developer Pro, qui travaille dans le compte de gestion des Organizations, peut autoriser les suggestions avec des références de code. Si l'accès sécurisé est activé, les suggestions avec des références de code seront également activées pour tous les comptes membres de cette organisation.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide d'Amazon Q Developer.

Pour activer l'accès sécurisé pour Amazon Q Developer, suivez cette procédure.

1. Sur la page Amazon Q Developer Settings, sous Paramètres du compte membre, sélectionnez Modifier.
2. Dans la fenêtre contextuelle, sélectionnez Activé.
3. Choisissez Enregistrer.

Pour plus d'informations, consultez la section Activation de l'accès sécurisé dans le guide de l'utilisateur Amazon Q Developer.

## Désactiver l'accès sécurisé avec Amazon Q Developer

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Amazon Q Developer.

Pour désactiver l'accès sécurisé pour Amazon Q Developer, suivez cette procédure.

1. Sur la page Amazon Q Developer Settings, sous Paramètres du compte membre, sélectionnez Modifier.
2. Dans la fenêtre contextuelle, sélectionnez Désactivé.
3. Choisissez Enregistrer.

Pour plus d'informations, consultez la section Activation de l'accès sécurisé dans le guide de l'utilisateur Amazon Q Developer.

## AWS Resource Access Manager et AWS Organizations

AWS Resource Access Manager (AWS RAM) vous permet de partager AWS des ressources spécifiques que vous possédez avec d'autres Comptes AWS. Il s'agit d'un service centralisé qui fournit une expérience cohérente pour le partage de différents types de AWS ressources entre plusieurs comptes.

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

Utilisez les informations suivantes pour vous aider AWS Resource Access Manager à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' AWS RAM effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre AWS RAM et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForResourceAccessManager`

### Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par AWS RAM accordent l'accès aux principaux de service suivants :

- `ram.amazonaws.com`

## Permettre un accès fiable avec AWS RAM

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Resource Access Manager console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Resource Access Manager console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Resource Access Manager d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Resource Access Manager. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la AWS Resource Access Manager console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la AWS RAM console ou de la CLI

Consultez Activer le partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Resource Access Managerdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Resource Access Manager dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.

6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Resource Access Manager qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Resource Access Manager en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AWS RAM

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils AWS Resource Access Manager ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Resource Access Manager console ou les outils pour désactiver l'intégration avec Organizations. Cela permet AWS Resource Access Manager d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Resource Access Manager.

Si vous désactivez l'accès sécurisé à l'aide de la AWS Resource Access Manager console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès sécurisé à l'aide de la AWS Resource Access Manager console ou de la CLI

Consultez Activer le partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Resource Access Managerdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS Resource Access Manager dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Resource Access Manager qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Resource Access Manager en tant que service sécurisé auprès des Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ram.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Explorateur de ressources AWS et AWS Organizations

Explorateur de ressources AWS est un service de recherche et de découverte de ressources. Avec Resource Explorer, vous pouvez explorer vos ressources, telles que les instances Amazon Elastic Compute Cloud, Amazon Kinesis Data Streams ou les tables Amazon DynamoDB, en utilisant une expérience similaire à celle d'un moteur de recherche sur Internet. Vous pouvez rechercher vos ressources à l'aide de métadonnées telles que les noms, les balises et IDs. L'explorateur de ressources fonctionne dans toutes AWS les régions de votre compte afin de simplifier vos charges de travail interrégionales.

Lorsque vous intégrez Resource Explorer à AWS Organizations, vous pouvez recueillir des preuves auprès d'une source plus large en incluant plusieurs éléments Comptes AWS provenant de votre organisation dans le cadre de vos évaluations.

Utilisez les informations suivantes pour vous aider Explorateur de ressources AWS à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Resource Explorer d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Resource Explorer et Organizations, ou si vous supprimez le compte membre de l'organisation.

Pour en savoir plus sur la manière dont Resource Explorer utilise ce rôle, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur Explorateur de ressources AWS .

- `AWSServiceRoleForResourceExplorer`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Resource Explorer accordent l'accès aux principaux de service suivants :

- `resource-explorer-2.amazonaws.com`

## Pour permettre un accès sécurisé avec Explorateur de ressources AWS

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Resource Explorer nécessite un accès AWS Organizations sécurisé pour que vous puissiez désigner un compte membre comme administrateur délégué de votre organisation.

Vous pouvez activer l'accès approuvé à l'aide de la console Resource Explorer ou de la console Organizations. Nous vous recommandons vivement d'utiliser la console ou les outils de Resource Explorer pour activer l'intégration à Organizations. Cela permet Explorateur de ressources AWS d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service.

Pour activer l'accès approuvé à l'aide de la console Resource Explorer

Pour obtenir des instructions sur l'activation de l'accès sécurisé, consultez la section Conditions préalables à l'utilisation de Resource Explorer dans le Guide de l'utilisateur Explorateur de ressources AWS .

> **Note**
>
> Si vous configurez un administrateur délégué à l'aide de la Explorateur de ressources AWS console, l'accès sécurisé est Explorateur de ressources AWS automatiquement activé pour vous.

Vous pouvez activer l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer Explorateur de ressources AWS en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

### Pour désactiver l'accès approuvé avec Resource Explorer

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte AWS Organizations de gestion peut désactiver l'accès sécurisé avec Explorateur de ressources AWS.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils Explorateur de ressources AWS ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la Explorateur de ressources AWS console ou les outils pour désactiver l'intégration avec Organizations. Cela permet Explorateur de ressources AWS d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par Explorateur de ressources AWS.
> Si vous désactivez l'accès sécurisé à l'aide de la Explorateur de ressources AWS console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver Explorateur de ressources AWS en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activer un compte administrateur délégué pour Resource Explorer

Utilisez votre compte d'administrateur délégué pour créer des vues de ressources multi-comptes et les étendre à une unité organisationnelle ou à l'ensemble de votre organisation. Vous pouvez partager des vues multi-comptes avec n'importe quel compte de votre organisation en AWS Resource Access Manager créant des partages de ressources.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion de Organizations disposant de l'autorisation suivante peuvent configurer un compte membre en tant qu'administrateur délégué pour Resource Explorer dans l'organisation : `resource-explorer:RegisterAccount`

Pour obtenir des instructions sur l'activation d'un compte administrateur délégué pour Resource Explorer, consultez Configuration dans le Guide de l'utilisateur Explorateur de ressources AWS .

Si vous configurez un administrateur délégué à l'aide de la Explorateur de ressources AWS console, Resource Explorer active automatiquement un accès sécurisé pour vous.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le service du compte `resource-explorer-2.amazonaws.com` sous forme de paramètres.

### Désactiver un administrateur délégué pour Resource Explorer

Seul un administrateur du compte de gestion Organizations ou du compte d'administrateur délégué Resource Explorer peut supprimer un administrateur délégué de Resource Explorer. Vous pouvez désactiver l'accès approuvé à l'aide de Organizations `DeregisterDelegatedAdministrator` CLI ou de l'opération SDK.

## AWS Security Hub CSPM et AWS Organizations

AWS Security Hub CSPM vous fournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.

Security Hub CSPM collecte des données de sécurité provenant de vos produits partenaires Comptes AWS, de ceux Services AWS que vous utilisez et de ceux pris en charge par des partenaires tiers. Il vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité prioritaires.

Lorsque vous utilisez Security Hub CSPM et AWS Organizations conjointement, vous pouvez activer automatiquement Security Hub CSPM pour tous vos comptes, y compris les nouveaux comptes au fur et à mesure de leur ajout. Cela augmente la couverture des contrôles et des conclusions du Security Hub CSPM, ce qui fournit une image plus complète et plus précise de votre niveau de sécurité global.

Pour plus d'informations sur Security Hub CSPM, consultez le guide de l'AWS Security Hub utilisateur.

Utilisez les informations suivantes pour vous aider AWS Security Hub CSPM à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Security Hub CSPM d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Security Hub CSPM et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForSecurityHub`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Security Hub CSPM donnent accès aux principaux de service suivants :

- `securityhub.amazonaws.com`

## Permettre un accès sécurisé avec Security Hub CSPM

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Lorsque vous désignez un administrateur délégué pour Security Hub CSPM, Security Hub CSPM active automatiquement un accès sécurisé pour Security Hub au sein de votre organisation.

## Désactivation de l'accès sécurisé avec Security Hub CSPM

Pour plus d'informations sur les autorisations nécessaires pour désactiver l'accès sécurisé, consultez la section Autorisations requises pour désactiver l'accès sécurisé dans le Guide de AWS Organizations l'utilisateur.

Avant de désactiver l'accès sécurisé, nous vous recommandons de contacter l'administrateur délégué de votre organisation afin de désactiver le Security Hub CSPM dans les comptes membres et de nettoyer les ressources Security Hub CSPM de ces comptes.

Vous pouvez désactiver l'accès sécurisé à l'aide de la AWS Organizations console, de l'API Organizations ou du AWS CLI. Seul un administrateur du compte de gestion des Organizations peut désactiver l'accès sécurisé avec Security Hub CSPM.

Pour obtenir des instructions sur la désactivation de l'accès sécurisé avec Security Hub CSPM, consultez la section Désactivation de l'intégration de Security Hub CSPM avec. AWS Organizations

## Activation d'un administrateur délégué pour Security Hub CSPM

Lorsque vous désignez un compte membre en tant qu'administrateur délégué de l'organisation, les utilisateurs et les rôles associés à ce compte peuvent effectuer des actions administratives pour Security Hub CSPM qui, autrement, ne peuvent être effectuées que par les utilisateurs ou les rôles du compte de gestion de l'organisation. Cela vous permet de séparer la gestion de l'organisation de la gestion du Security Hub CSPM.

Pour plus d'informations, consultez la section Désignation d'un compte administrateur Security Hub CSPM dans le guide de l'utilisateur.AWS Security Hub

Pour désigner un compte membre en tant qu'administrateur délégué pour Security Hub CSPM

1. Connectez-vous au compte de gestion Organizations.
2. Effectuez l'une des actions suivantes :
   - Si Security Hub CSPM n'est pas activé sur votre compte de gestion, choisissez Go to Security Hub CSPM sur la console Security Hub CSPM.
   - Si Security Hub CSPM est activé sur votre compte de gestion, sur la console Security Hub CSPM, sous Général, choisissez Paramètres.
3. Sous Administrateur délégué, saisissez l'ID du compte.

## Désactivation d'un administrateur délégué pour Security Hub CSPM

Seul le compte de gestion de l'organisation peut supprimer le compte administrateur délégué du Security Hub CSPM.

Pour modifier l'administrateur délégué du Security Hub CSPM, vous devez d'abord supprimer le compte administrateur délégué actuel, puis en désigner un nouveau.

Si vous utilisez la console Security Hub CSPM pour supprimer l'administrateur délégué dans une région, il est automatiquement supprimé dans toutes les régions.

L'API Security Hub CSPM supprime uniquement le compte administrateur Security Hub CSPM délégué de la région dans laquelle l'appel ou la commande d'API est émis. Vous devez répéter l'action dans les autres régions.

Si vous utilisez l'API Organizations pour supprimer le compte administrateur délégué de Security Hub CSPM, celui-ci est automatiquement supprimé dans toutes les régions.

Pour obtenir des instructions sur la désactivation de l'administrateur délégué du Security Hub CSPM, consultez Supprimer ou modifier l'administrateur délégué.

## Lentille de stockage Amazon S3 et AWS Organizations

En donnant à Amazon S3 Storage Lens un accès fiable à votre organisation, vous lui permettez de collecter et d'agréger des métriques sur l' Comptes AWS ensemble de votre organisation. Pour ce faire, S3 Storage Lens accède à la liste des comptes appartenant à votre organisation et collecte et analyse les métriques de stockage, d'utilisation et d'activité pour chacun d'entre eux.

Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon S3 Storage Lens dans le Guide de l'utilisateur Amazon S3 Storage Lens.

Utilisez les informations suivantes pour vous aider à intégrer Amazon S3 Storage Lens à AWS Organizations.

### Création d'un rôle lié à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans votre compte administrateur délégué de l'organisation lorsque vous activez l'accès sécurisé et que la configuration de Storage Lens a été appliquée à votre organisation. Ce rôle permet à Amazon S3 Storage Lens d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Amazon S3 Storage Lens et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForS3StorageLens`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Amazon S3 Storage Lens autorisent l'accès aux mandataires de service suivants :

- `storage-lens.s3.amazonaws.com`

## Activation de l'accès approuvé pour Amazon S3 Storage Lens

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès approuvé à l'aide de la console Amazon S3 Storage Lens ou de la console AWS Organizations .

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils d'Amazon S3 Storage Lens pour activer l'intégration à Organizations. Cela permet à Amazon S3 Storage Lens d'effectuer toute configuration nécessaire, par exemple la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par Amazon S3 Storage Lens. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'Amazon S3 Storage Lens, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console Amazon S3

Consultez la section Activation de l'accès sécurisé pour S3 Storage Lens dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Amazon S3 Storage Lens dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour Amazon S3 Storage Lens, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon S3 Storage Lens qu'il peut désormais activer ce service pour qu'il fonctionne avec la console AWS Organizations de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer Amazon S3 Storage Lens en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactivation de l'accès approuvé pour Amazon S3 Storage Lens

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Amazon S3 Storage Lens.

Vous pouvez désactiver l'accès sécurisé à l'aide de la console Amazon S3, du AWS CLI ou de l'un des AWS SDKs.

Pour désactiver l'accès approuvé à l'aide de la console Amazon S3

Consultez la section Désactivation de l'accès sécurisé pour S3 Storage Lens dans le guide de l'utilisateur d'Amazon Simple Storage Service.

## Activation d'un administrateur délégué pour Amazon S3 Storage Lens

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Amazon S3 Storage Lens qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion d'Amazon S3 Storage Lens.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations disposant de l'autorisation suivante peuvent configurer un compte membre en tant qu'administrateur délégué pour Amazon S3 Storage Lens dans l'organisation : `organizations:RegisterDelegatedAdministrator` `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens prend en charge un maximum de 5 comptes d'administrateur délégués dans votre organisation.

Pour désigner un compte membre comme administrateur délégué pour Amazon S3 Storage Lens

Vous pouvez enregistrer un administrateur délégué à l'aide de la console Amazon S3, du AWS CLI ou de l'un des AWS SDKs. Pour enregistrer un compte membre en tant que compte

d'administrateur délégué pour votre organisation à l'aide de la console Amazon S3, consultez la section Enregistrement d'un administrateur délégué pour S3 Storage Lens dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour annuler l'enregistrement d'un administrateur délégué pour Amazon S3 Storage Lens

Vous pouvez désenregistrer un administrateur délégué à l'aide de la console Amazon S3, du AWS CLI ou de l'un des. AWS SDKs Pour annuler l'enregistrement d'un administrateur délégué à l'aide de la console Amazon S3, consultez la section Désenregistrer un administrateur délégué pour S3 Storage Lens dans le guide de l'utilisateur d'Amazon Simple Storage Service.

## AWS Réponse aux incidents de sécurité et AWS Organizations

AWS Security Incident Response est un service de sécurité qui fournit une assistance en direct, 24 heures sur 24, 7 jours sur 7, pour aider les clients à réagir rapidement aux incidents de cybersécurité tels que le vol d'informations d'identification et les attaques par ransomware. En intégrant Organizations, vous offrez une couverture de sécurité à l'ensemble de votre organisation. Pour plus d'informations, consultez la section Gestion des comptes AWS de réponse aux incidents de sécurité AWS Organizations dans le Guide de l'utilisateur de réponse aux incidents de sécurité.

Utilisez les informations suivantes pour vous aider à intégrer AWS la réponse aux incidents de sécurité à AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Les rôles liés à un service suivant sont automatiquement créés dans le compte de gestion de votre organisation lorsque vous activez l'accès de confiance.

- `AWSServiceRoleForSecurityIncidentResponse`- utilisé pour créer un abonnement Security Incident Response - votre abonnement au service via AWS Organizations.
- `AWSServiceRoleForSecurityIncidentResponse_Triage`- utilisé uniquement lorsque vous activez la fonction de triage lors de l'inscription.

### Principes de service utilisés par Security Incident Response

Les rôles liés au service décrits dans la section précédente ne peuvent être assumés que par les principaux de service autorisés par les relations de confiance définies pour le rôle. Les rôles liés au service utilisés par Security Incident Response accordent l'accès au principal de service suivant :

- `security-ir.amazonaws.com`

## Permettre un accès fiable à la réponse aux incidents de sécurité

L'activation d'un accès fiable à Security Incident Response permet au service de suivre la structure de votre organisation et de garantir que tous les comptes de l'organisation bénéficient d'une couverture active en cas d'incident de sécurité. Cela permet également au service d'utiliser un rôle lié au service dans les comptes des membres pour les fonctionnalités de tri lorsque vous activez la fonctionnalité de triage.

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la console AWS Security Incident Response ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la console ou les outils de réponse aux incidents de AWS sécurité pour permettre l'intégration avec les Organizations. Cela permet à AWS Security Incident Response d'effectuer toutes les configurations requises, telles que la création des ressources nécessaires au service. Procédez comme suit uniquement si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Security Incident Response. Pour plus d'informations, consultez cette note.
>
> Si vous activez l'accès sécurisé à l'aide de la console ou des outils de réponse aux incidents de AWS sécurité, vous n'avez pas besoin de suivre ces étapes.

Organizations active automatiquement l'accès sécurisé des Organizations lorsque vous utilisez la console Security Incident Response pour la configuration et la gestion. Si vous utilisez la réponse aux incidents de sécurité CLI/SDK , vous devez activer manuellement l'accès sécurisé à l'aide de l'API Enable AWSService Access. Pour savoir comment activer un accès sécurisé via la console Security Incident Response, voir Activer l'accès sécurisé pour la gestion des AWS comptes dans le Guide de l'utilisateur de Security Incident Response.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Security Incident Response dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour AWS la réponse aux incidents de sécurité, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur de AWS Security Incident Response qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer AWS Security Incident Response en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal security-ir.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactivation de l'accès sécurisé avec Security Incident Response

Seul un administrateur du compte de gestion des Organizations peut désactiver l'accès sécurisé avec Security Incident Response.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Security Incident Response dans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de dialogue Désactiver l'accès sécurisé pour la réponse aux incidents de AWS sécurité, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur de AWS Security Incident Response qu'il peut désormais désactiver ce service à l' AWS Organizations aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver AWS Security Incident Response en tant que service fiable auprès des Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal security-ir.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour la réponse aux incidents de sécurité

Lorsque vous désignez un compte membre en tant qu'administrateur délégué de l'organisation, les utilisateurs et les rôles associés à ce compte peuvent effectuer des actions administratives pour la réponse aux incidents de sécurité qui, autrement, ne peuvent être effectuées que par les utilisateurs ou les rôles du compte de gestion de l'organisation. Cela vous permet de séparer la gestion de l'organisation de la gestion de la réponse aux incidents de sécurité. Pour plus d'informations, consultez la section Gestion des comptes AWS de réponse aux incidents de sécurité AWS Organizations dans le Guide de l'utilisateur de réponse aux incidents de sécurité.

> **Autorisations minimales**
>
> Seul un utilisateur ou un rôle dans le compte de gestion des Organisations peut configurer un compte membre en tant qu'administrateur délégué pour la réponse aux incidents de sécurité dans l'organisation.

Pour savoir comment configurer un administrateur délégué via la console Security Incident Response, voir Désignation d'un compte administrateur délégué de réponse aux incidents de sécurité dans le Guide de l'utilisateur de Security Incident Response.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
```

```
    --account-id 123456789012 \
    --service-principal security-ir.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le service du compte `security-ir.amazonaws.com` sous forme de paramètres.

### Désactivation d'un administrateur délégué pour la réponse aux incidents de sécurité

> **Important**
>
> Si l'adhésion a été créée à partir du compte d'administrateur délégué, la désinscription de l'administrateur délégué est une action destructrice et entraînera une interruption du service. Pour réenregistrer DA :
>
> 1. Connectez-vous à la console Security Incident Response à l'adresse https://console.aws.amazon.com/security-ir/ home#/membership/settings
> 2. Annulez l'adhésion depuis la console de service. L'adhésion reste active jusqu'à la fin du cycle de facturation.
> 3. Une fois l'adhésion annulée, désactivez l'accès au service via la console Organizations, la CLI ou le SDK.

Seul un administrateur du compte de gestion des Organizations peut supprimer un administrateur délégué pour Security Incident Response. Vous pouvez supprimer l'administrateur délégué à l'aide de l'opération CLI ou SDK Organizations `DeregisterDelegatedAdministrator`.

## Amazon Security Lake et AWS Organizations

Amazon Security Lake centralise les données de sécurité provenant de sources cloud, sur site et personnalisées dans un lac de données qui est stocké dans votre compte. Grâce à l'intégration avec Organizations, vous pouvez créer un lac de données qui collecte les journaux et les événements de l'ensemble de vos comptes. Pour plus d'informations, consultez Gestion de plusieurs comptes avec AWS Organizations (français non garanti) dans le Guide de l'utilisateur Amazon Security Lake (français non garanti).

Utilisez les informations suivantes pour vous aider à intégrer Amazon Security Lake à AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié au service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous appelez l'RegisterDataLakeDelegatedAdministratorAPI. Ce rôle permet à Amazon Security Lake d'effectuer des opérations prises en charge au sein des comptes de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès sécurisé entre Amazon Security Lake et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForSecurityLake`

> ⚠ Recommandation : utilisez l' RegisterDataLakeDelegatedAdministrator API de Security Lake pour autoriser Security Lake à accéder à votre organisation et pour enregistrer l'administrateur délégué de l'organisation
>
> Si vous utilisez « Organisations » APIs pour enregistrer un administrateur délégué, les rôles liés aux services pour les organisations risquent de ne pas être créés correctement. Pour garantir une fonctionnalité complète, utilisez le Security Lake APIs.

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Amazon Security Lake donnent accès aux principaux de service suivants :

- `securitylake.amazonaws.com`

## Permettre un accès fiable avec Amazon Security Lake

Lorsque vous activez l'accès approuvé avec Security Lake, il peut réagir automatiquement aux changements dans l'appartenance à l'organisation. L'administrateur délégué peut activer la collecte de AWS journaux à partir des services pris en charge dans n'importe quel compte d'organisation. Pour plus d'informations, consultez la section Rôle lié à un service pour Amazon Security Lake (français non garanti) dans le guide de l'utilisateur Amazon Security Lake (français non garanti).

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Amazon Security Lake dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour Amazon Security Lake, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon Security Lake qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer Amazon Security Lake en tant que service fiable auprès d'Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal securitylake.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec Amazon Security Lake

Seul un administrateur du compte de gestion des Organizations peut désactiver l'accès sécurisé à Amazon Security Lake.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez Amazon Security Lake dans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de dialogue Désactiver l'accès sécurisé pour Amazon Security Lake, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur d'Amazon Security Lake qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver Amazon Security Lake en tant que service de confiance auprès d'Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour Amazon Security Lake

L'administrateur délégué d'Amazon Security Lake ajoute d'autres comptes au sein de l'organisation en tant que comptes de membres. L'administrateur délégué peut activer Amazon Security Lake et configurer les paramètres Amazon Security Lake pour les comptes des membres. L'administrateur délégué peut collecter des journaux au sein d'une organisation dans toutes les AWS régions où Amazon Security Lake est activé (quel que soit le point de terminaison régional que vous utilisez actuellement).

Vous pouvez également configurer l'administrateur délégué de manière à ce qu'il ajoute automatiquement les nouveaux comptes dans l'organisation en tant que membres. L'administrateur délégué d'Amazon Security Lake a accès aux journaux et aux événements des comptes membres associés. Par conséquent, vous pouvez configurer Amazon Security Lake pour collecter les données détenues par les comptes membres associés. Vous pouvez également accorder aux abonnés l'autorisation de consommer des données appartenant à des comptes membres associés.

Pour plus d'informations, consultez Gestion de plusieurs comptes avec AWS Organizations (français non garanti) dans le Guide de l'utilisateur Amazon Security Lake (français non garanti).

> **Autorisations minimales**
>
> Seul un administrateur du compte de gestion de l'organisation peut configurer un compte membre en tant qu'administrateur délégué pour Amazon Security Lake au sein de l'organisation.

Vous pouvez spécifier un compte d'administrateur délégué à l'aide de la console Amazon Security Lake, de l'opération d'`CreateDatalakeDelegatedAdmin`API Amazon Security Lake ou de la commande `create-datalake-delegated-admin` CLI. Vous pouvez également utiliser l'opération CLI ou SDK d'Organisations `RegisterDelegatedAdministrator`. Pour obtenir des instructions sur l'activation d'un compte d'administrateur délégué pour Amazon Security Lake, consultez la section Désignation de l'administrateur délégué de Security Lake et ajout de comptes membres dans le guide de l'utilisateur d'Amazon Security Lake.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

### Désactivation d'un administrateur délégué pour Amazon Security Lake

Seul un administrateur du compte de gestion des Organizations ou du compte d'administrateur délégué Amazon Security Lake peut supprimer un compte d'administrateur délégué de l'organisation.

Vous pouvez supprimer le compte d'administrateur délégué à l'aide de l'opération d'`DeregisterDataLakeDelegatedAdministrator`API Amazon Security Lake, de la commande `deregister-data-lake-delegated-administrator` CLI, ou en utilisant l'opération Organizations `DeregisterDelegatedAdministrator` CLI ou SDK. Pour supprimer un administrateur délégué à l'aide d'Amazon Security Lake, consultez la section Suppression de l'administrateur délégué Amazon Security Lake dans le guide de l'utilisateur d'Amazon Security Lake.

## AWS Service Catalog et AWS Organizations

Service Catalog vous permet de créer et gérer des catalogues de services informatiques qui sont approuvés pour être utilisés sur AWS.

L'intégration de Service Catalog AWS Organizations simplifie le partage de portefeuilles et la copie de produits au sein d'une organisation. Les administrateurs de Service Catalog peuvent faire référence à une organisation existante AWS Organizations lorsqu'ils partagent un portefeuille, et ils peuvent partager le portefeuille avec n'importe quelle unité organisationnelle (UO) fiable dans l'arborescence de l'organisation. Il n'est donc plus nécessaire de partager le portefeuille IDs et le compte destinataire n'a plus à faire référence manuellement à l'identifiant du portefeuille lors de l'importation du portefeuille. Les portefeuilles partagés via cette méthode sont répertoriés dans le compte de réception dans la vue Imported Portfolio (Portefeuille importé) de l'administrateur dans Service Catalog.

Pour obtenir plus d'informations sur Service Catalog, consultez le Guide de l'administrateur de Service Catalog.

Utilisez les informations suivantes pour vous aider AWS Service Catalog à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

AWS Service Catalog ne crée aucun rôle lié à un service dans le cadre de l'activation d'un accès sécurisé.

## Mandataires de service utilisés pour accorder des autorisations

Pour activer l'accès approuvé, vous devez spécifier le principal de service suivant :

- `servicecatalog.amazonaws.com`

## Activation de l'accès approuvé avec Service Catalog

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Service Catalog console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Service Catalog console ou les outils pour permettre l'intégration avec Organizations. Cela permet

AWS Service Catalog d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Service Catalog. Pour plus d'informations, consultez cette note.
Si vous activez l'accès sécurisé à l'aide de la AWS Service Catalog console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer un accès sécurisé à l'aide de la CLI ou du AWS SDK Service Catalog

Appelez l'une des commandes ou opérations suivantes :

- AWS CLI: catalogue de services aws enable-aws-organizations-access
- AWS SDKs: AWSServiceCatalog : :Activer AWSOrganizations l'accès

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Service Catalogdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Service Catalog dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Service Catalog qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Service Catalog en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactivation de l'accès approuvé avec Service Catalog

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Si vous désactivez l'accès sécurisé AWS Organizations pendant que vous utilisez Service Catalog, cela ne supprime pas vos partages actuels, mais vous empêche d'en créer de nouveaux au sein de votre organisation. Les partages actuels ne seront pas synchronisés avec la structure de votre organisation si elle change après l'appel de cette action.

Pour désactiver l'accès sécurisé à l'aide de la CLI ou du AWS SDK Service Catalog

Appelez l'une des commandes ou opérations suivantes :

- AWS CLI: catalogue de services aws disable-aws-organizations-access
- AWS SDKs: Désactiver AWSOrganizations l'accès

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

### AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Service Catalogdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS Service Catalog dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Service Catalog qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

### AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Service Catalog en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

# Service Quotas et AWS Organizations

Service Quotas est un AWS service qui vous permet de consulter et de gérer vos quotas à partir d'un emplacement central. Les quotas, également appelés limites, sont la valeur maximale pour vos ressources, actions et éléments de votre Compte AWS.

Lorsque Service Quotas est associé à AWS Organizations, vous pouvez créer un modèle de demande de quota pour demander automatiquement des augmentations de quotas lors de la création de comptes.

Pour plus d'informations sur Service Quotas, consultez le Guide de l'utilisateur Service Quotas.

Utilisez les informations suivantes pour vous aider à intégrer les Quotas de Service à AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Service Quotas d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Service Quotas et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForServiceQuotas`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Service Quotas autorisent l'accès aux mandataires de service suivants :

- `servicequotas.amazonaws.com`

## Activation de l'accès approuvé avec Service Quotas

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des Service Quotas.

Vous pouvez activer l'accès sécurisé à l'aide de la console Service Quotas, AWS CLI ou SDK :

- Pour activer l'accès approuvé à l'aide de la console Service Quotas

  Connectez-vous avec votre compte AWS Organizations de gestion, puis configurez le modèle sur la console Service Quotas. Pour plus d'informations, consultez Utilisation du modèle Service Quotas dans le Guide de l'utilisateur Service Quotas.
- Pour activer un accès sécurisé à l'aide du Service Quotas AWS CLI ou du SDK

  Appelez la commande ou l'opération suivante :
  - AWS CLI: quotas de service AWS associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

## AWS IAM Identity Center et AWS Organizations

AWS IAM Identity Center fournit un accès par authentification unique pour toutes vos applications Comptes AWS et celles du cloud. Il se connecte à Microsoft Active Directory AWS Directory Service pour permettre aux utilisateurs de cet annuaire de se connecter à un portail d' AWS accès personnalisé en utilisant leurs noms d'utilisateur et mots de passe Active Directory existants. À partir du portail AWS d'accès, les utilisateurs ont accès à toutes Comptes AWS les applications cloud pour lesquelles ils sont autorisés.

Pour plus d'informations sur IAM Identity Center, consultez le Guide de l'utilisateur AWS IAM Identity Center.

Utilisez les informations suivantes pour vous aider AWS IAM Identity Center à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à IAM Identity Center d'effectuer des opérations prises en charge dans les comptes de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès de confiance entre IAM Identity Center et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForSSO`

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par IAM Identity Center accordent l'accès aux principaux de service suivants :

- `sso.amazonaws.com`

## Activation de l'accès de confiance avec IAM Identity Center

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS IAM Identity Center console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS IAM Identity Center console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS IAM Identity Center d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS IAM Identity Center. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la AWS IAM Identity Center console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour fonctionner, IAM Identity Center a besoin d'un AWS Organizations accès sécurisé. L'accès de confiance est activé lorsque vous configurez IAM Identity Center. Pour plus d'informations, consultez Démarrez - Étape 1 : Activer AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

### AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS IAM Identity Centerdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS IAM Identity Center dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS IAM Identity Center qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

### AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS IAM Identity Center en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Désactivation de l'accès de confiance avec IAM Identity Center

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Pour fonctionner, IAM Identity Center a besoin d'un AWS Organizations accès fiable. Si vous désactivez l'accès sécurisé AWS Organizations pendant que vous utilisez IAM Identity Center, celui-ci cesse de fonctionner car il ne peut pas accéder à l'organisation. Les utilisateurs ne peuvent pas utiliser IAM Identity Center pour accéder aux comptes. Les rôles créés par IAM Identity Center sont conservés, mais le service IAM Identity Center ne peut pas y accéder. Les rôles liés au service IAM Identity Center sont conservés. Si vous réactivez l'accès de confiance, IAM Identity Center continue de fonctionner comme avant, sans que vous ayez à reconfigurer le service.

Si vous supprimez un compte de votre organisation, IAM Identity Center nettoie automatiquement toutes les métadonnées et ressources, telles que son rôle lié au service. Un compte autonome qui est supprimé d'une organisation cesse de fonctionner avec IAM Identity Center.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS IAM Identity Centerdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS IAM Identity Center dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS IAM Identity Center qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS IAM Identity Center en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte administrateur délégué pour IAM Identity Center

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour IAM Identity Center qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion d'IAM Identity Center.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué IAM Identity Center dans l'organisation.

Pour obtenir des instructions sur la façon d'activer un compte administrateur délégué pour IAM Identity Center, consultez Administration déléguée dans le Guide de l'utilisateur AWS IAM Identity Center .

# AWS Systems Manager et AWS Organizations

AWS Systems Manager est un ensemble de fonctionnalités qui permettent la visibilité et le contrôle de vos AWS ressources. Les fonctionnalités suivantes de Systems Manager fonctionnent avec Organizations sur l'ensemble des Comptes AWS de votre organisation :

- Systems Manager Explorer est un tableau de bord des opérations personnalisable qui fournit des informations sur vos AWS ressources. Vous pouvez synchroniser les données opérationnelles Comptes AWS dans l'ensemble de votre organisation à l'aide de Organizations and Systems Manager Explorer. Pour plus d'informations, consultez Systems Manager Explorer dans le Guide de l'utilisateur AWS Systems Manager .
- Systems Manager Change Manager est une structure de gestion des changements d'entreprise qui permet de demander, d'approuver, de mettre en œuvre et de générer des rapports sur les modifications opérationnelles apportées à la configuration et à l'infrastructure de votre application. Pour plus d'informations, consultez AWS Systems Manager Change Manager dans le Guide de l'utilisateur AWS Systems Manager .
- Systems Manager OpsCenter fournit un emplacement central où les ingénieurs des opérations et les professionnels de l'informatique peuvent consulter, étudier et résoudre les éléments de travail opérationnels (OpsItems) liés aux AWS ressources. Lorsque vous l'utilisez OpsCenter avec Organizations, il permet de travailler OpsItems depuis un compte de gestion (soit un compte de gestion Organizations, soit un compte administrateur délégué de Systems Manager) et un autre compte au cours d'une seule session. Une fois la configuration terminée, les utilisateurs peuvent effectuer les types d'actions suivants :
  - Créez, consultez et mettez à jour OpsItems dans un autre compte.
  - Afficher des informations détaillées sur les AWS ressources spécifiées OpsItems dans un autre compte.
  - Démarrez les runbooks de Systems Manager Automation pour résoudre les problèmes liés aux AWS ressources d'un autre compte.

  Pour plus d'informations, consultez AWS Systems Manager OpsCenter dans le Guide de l'utilisateur AWS Systems Manager .
- Utilisez la configuration rapide pour configurer rapidement les AWS services et fonctionnalités fréquemment utilisés conformément aux meilleures pratiques recommandées. Pour plus d'informations, consultez AWS Systems Manager Quick Setup dans le Guide de l'utilisateur AWS Systems Manager .

Lorsque vous enregistrez un compte d'administrateur AWS Organizations délégué pour Systems Manager, vous pouvez créer, mettre à jour, afficher et supprimer les gestionnaires de configuration Quick Setup qui ciblent les unités organisationnelles d'une organisation. Pour en savoir plus, consultez la section Utilisation d'un administrateur délégué pour la configuration rapide dans le guide de AWS Systems Manager l'utilisateur.

- Lorsque vous configurez la console intégrée pour Systems Manager, vous entrez un compte d'administrateur délégué. Ce compte est utilisé pour enregistrer des comptes d'administrateur AWS Organizations délégué avec Quick Setup CloudFormation StackSets, Explorer et Resource Explorer. Pour en savoir plus, consultez le guide d'AWS Systems Manager utilisation de la console intégrée de Systems Manager pour une entreprise.

Utilisez les informations suivantes pour vous aider AWS Systems Manager à intégrer AWS Organizations.

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Systems Manager d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Systems Manager et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

## Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Systems Manager autorisent l'accès aux mandataires de service suivants :

- `ssm.amazonaws.com`

## Activation de l'accès approuvé avec Systems Manager

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Systems Managerdans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Systems Manager dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Systems Manager qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Systems Manager en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactivation de l'accès approuvé avec Systems Manager

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Systems Manager a besoin d'un accès fiable AWS Organizations pour synchroniser les données opérationnelles au Comptes AWS sein de votre organisation. Si vous désactivez l'accès approuvé, Systems Manager ne parvient pas à synchroniser les données opérationnelles et signale une erreur.

Vous ne pouvez désactiver l'accès sécurisé qu'à l'aide des outils Organizations.

Vous pouvez désactiver l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez AWS Systems Managerdans la liste des services.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Dans la boîte de AWS Systems Manager dialogue Désactiver l'accès sécurisé pour, tapez désactiver pour confirmer, puis choisissez Désactiver l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Systems Manager qu'il peut désormais désactiver ce service à AWS Organizations l'aide de la console de service ou des outils.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Systems Manager en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte administrateur délégué pour Systems Manager

Lorsque vous désignez un compte membre en tant qu'administrateur délégué pour l'organisation, les utilisateurs et les rôles de ce compte peuvent effectuer des actions administratives pour Systems Manager qui, autrement, ne peuvent être exécutées que par des utilisateurs ou des rôles dans le compte de gestion de l'organisation. Cela vous aide à séparer la gestion de l'organisation de la gestion de Systems Manager.

Si vous utilisez Change Manager dans une organisation, vous utilisez un compte administrateur délégué. Il s'agit du compte Compte AWS qui a été désigné pour gérer les modèles de modification, les demandes de modification, les livrets de modifications et les flux de travail d'approbation dans Change Manager. Le compte délégué gère les activités de modification dans l'ensemble de votre organisation. Lorsque vous configurez votre organisation pour l'utiliser avec Change Manager, vous spécifiez lequel de vos comptes est utilisé dans ce rôle. Ce n'est pas nécessairement le compte de gestion de l'organisation. Le compte administrateur délégué n'est pas obligatoire si vous utilisez Change Manager avec un seul compte.

Pour désigner un compte de membre comme administrateur délégué, consultez les rubriques suivantes du Guide de l'utilisateur AWS Systems Manager :

- Pour Explorer et OpsCenter, voir Configuration d'un administrateur délégué.
- Pour Change Manager, consultez Configuration d'une organisation et d'un compte délégué pour Change Manager.
- Pour la configuration rapide, voir Enregistrer un administrateur délégué pour la configuration rapide.

### Désactivation d'un compte d'administrateur délégué pour Systems Manager

Pour annuler l'enregistrement d'un administrateur délégué, consultez les rubriques suivantes du guide de l'AWS Systems Manager utilisateur :

- Pour Explorer et OpsCenter, voir Désenregistrer un administrateur délégué d'Explorer.
- Pour Change Manager, consultez Configuration d'une organisation et d'un compte délégué pour Change Manager.
- Pour la configuration rapide, voir Désenregistrer un administrateur délégué pour la configuration rapide.

## Notifications des utilisateurs AWS et AWS Organizations

Notifications des utilisateurs AWSest un emplacement central pour vos AWS notifications.

Après l'intégration AWS Organizations, vous pouvez configurer et consulter les notifications de manière centralisée pour tous les comptes de votre organisation.

Utilisez les informations suivantes pour vous aider Notifications des utilisateurs AWS à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' Notifications des utilisateurs effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Notifications des utilisateurs et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForAWSUserNotifications`

Pour plus d'informations, consultez la section Utilisation des rôles liés à un service dans le guide de l'Notifications des utilisateurs AWS utilisateur.

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Notifications des utilisateurs accordent l'accès aux principaux de service suivants :

- `notifications.amazon.com`

## Permettre un accès fiable avec Notifications des utilisateurs

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'en utilisant Notifications des utilisateurs AWS.

Pour activer l'accès sécurisé à l'aide de la Notifications des utilisateurs console, consultez la section Activation AWS OrganizationsNotifications des utilisateurs AWS dans le guide de Notifications des utilisateurs l'utilisateur.

## Désactiver l'accès sécurisé avec Notifications des utilisateurs

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'en utilisant Notifications des utilisateurs AWS.

Pour désactiver l'accès sécurisé à l'aide de la Notifications des utilisateurs console, consultez la section Activation AWS OrganizationsNotifications des utilisateurs AWS dans le guide de Notifications des utilisateurs l'utilisateur.

## Activation d'un compte d'administrateur délégué pour Notifications des utilisateurs

L'administrateur du compte de gestion peut déléguer des autorisations Notifications des utilisateurs administratives à un compte de membre désigné appelé administrateur délégué. Pour enregistrer un compte en tant qu'administrateur délégué pour le marché privé, l'administrateur du compte de gestion doit s'assurer que l'accès sécurisé et le rôle lié au service sont activés, choisir Enregistrer un nouvel administrateur, fournir le numéro de AWS compte à 12 chiffres et choisir Soumettre.

Les comptes de gestion et les comptes d'administrateur délégué peuvent effectuer des tâches Notifications des utilisateurs administratives, telles que la création d'expériences, la mise à jour des

paramètres de marque, l'association ou la dissociation d'audiences, l'ajout ou la suppression de produits, ainsi que l'approbation ou le refus des demandes en attente.

Pour configurer un administrateur délégué à l'aide de la Notifications des utilisateurs console, consultez la section Enregistrement des administrateurs délégués Notifications des utilisateurs AWS dans le Guide de Notifications des utilisateurs l'utilisateur.

Vous pouvez également configurer un administrateur délégué à l'aide de l'`RegisterDelegatedAdministrator`API Organizations. Pour plus d'informations, reportez-vous RegisterDelegatedAdministratorà la section Organizations Command Reference.

### Désactivation d'un administrateur délégué pour Notifications des utilisateurs

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Notifications des utilisateurs.

Vous pouvez supprimer l'administrateur délégué à l'aide de la Notifications des utilisateurs console ou de l'API, ou à l'aide de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations.

Pour désactiver le Notifications des utilisateurs compte d'administrateur délégué à l'aide de la Notifications des utilisateurs console, voir Supprimer les administrateurs délégués Notifications des utilisateurs AWS dans le Guide de Notifications des utilisateurs l'utilisateur.

## Politiques relatives aux tags et AWS Organizations

Les politiques de balises sont un type de politique AWS Organizations qui peut vous aider à standardiser les balises entre les ressources des comptes de votre organisation. Pour de plus amples informations sur les politiques de balises, consultez Politiques de balises.

Utilisez les informations suivantes pour vous aider à intégrer les politiques de balises à AWS Organizations.

### Principaux de service utilisés par les rôles liés à un service

Organizations interagit avec les balises attachées à vos ressources à l'aide du mandataire de service suivant.

- `tagpolicies.tag.amazonaws.com`

## Activation de l'accès approuvé pour les politiques de balises

Vous pouvez activer l'accès sécurisé soit en activant les politiques de balises dans l'organisation, soit en utilisant la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement d'activer l'accès approuvé en activant des politiques de balises. Cela permet à Organizations d'effectuer les tâches de configuration requises.

Vous pouvez activer l'accès approuvé pour les politiques de balises en activant le type de politique de balises dans la console AWS Organizations . Pour de plus amples informations, veuillez consulter Désactivation d'un type de politique.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.
3. Choisissez les politiques relatives aux balises dans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de dialogue Activer l'accès sécurisé pour les politiques de balises, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, indiquez à l'administrateur des politiques de balises qu'il peut désormais permettre à ce service de fonctionner avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour activer les politiques de balises en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

### Désactivation de l'accès approuvé avec les politiques de balises

Vous pouvez désactiver l'accès sécurisé pour les politiques de balises en désactivant le type de politique de balise dans la AWS Organizations console. Pour de plus amples informations, veuillez consulter Désactivation d'un type de politique.

## AWS Trusted Advisor et AWS Organizations

AWS Trusted Advisor inspecte votre AWS environnement et émet des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Une fois intégré à Organizations, vous pouvez recevoir les résultats des Trusted Advisor contrôles pour tous les comptes de votre organisation et télécharger des rapports pour consulter les résumés de vos contrôles et des ressources concernées.

Pour de plus amples informations, consultez Vue organisationnelle pour AWS Trusted Advisor dans le Guide de l'utilisateur AWS Support .

Utilisez les informations suivantes pour vous aider AWS Trusted Advisor à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' Trusted Advisor effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Trusted Advisor et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForTrustedAdvisorReporting`

### Mandataires de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par Trusted Advisor accordent l'accès aux principaux de service suivants :

- `reporting.trustedadvisor.amazonaws.com`

### Permettre un accès fiable avec Trusted Advisor

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous ne pouvez activer l'accès sécurisé qu'à l'aide de AWS Trusted Advisor.

Pour activer l'accès sécurisé à l'aide de la Trusted Advisor console

Consultez Activer la vue organisationnelle dans le Guide de l'utilisateur AWS Support .

### Désactiver l'accès sécurisé avec Trusted Advisor

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Une fois cette fonctionnalité désactivée, l'enregistrement des informations relatives aux chèques pour tous les autres comptes de votre organisation Trusted Advisor cesse d'être enregistré. Vous ne pouvez pas afficher ou télécharger des rapports existants ou créer de nouveaux rapports.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils AWS Trusted Advisor ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Trusted Advisor console ou les outils pour désactiver l'intégration avec Organizations. Cela permet AWS Trusted Advisor d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Trusted Advisor.
> Si vous désactivez l'accès sécurisé à l'aide de la AWS Trusted Advisor console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès sécurisé à l'aide de la Trusted Advisor console

Consultez Désactiver la vue organisationnelle dans le Guide de l'utilisateur AWS Support .

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Trusted Advisor en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Activation d'un compte d'administrateur délégué pour Trusted Advisor

Lorsque vous désignez un compte membre comme administrateur délégué de l'organisation, les utilisateurs et les rôles du compte désigné peuvent gérer les métadonnées Compte AWS pour les autres comptes membres de l'organisation. Si vous n'activez pas de compte administrateur délégué, seul le compte de gestion de l'organisation peut effectuer ces tâches. Cela vous permet de séparer la gestion de l'organisation de celle des détails de votre compte.

> **Autorisations minimales**
>
> Seul un utilisateur ou un rôle dans le compte de gestion des Organisations peut configurer un compte membre Trusted Advisor en tant qu'administrateur délégué pour l'organisation.

Pour obtenir des instructions sur l'activation d'un compte d'administrateur délégué pour Trusted Advisor, voir Enregistrer les administrateurs délégués dans le guide de Support l'utilisateur.

AWS CLI, AWS API

Si vous souhaitez configurer un compte d'administrateur délégué à l'aide de la AWS CLI ou de l'une des interfaces de ligne de commande AWS SDKs, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK : appelez le `RegisterDelegatedAdministrator` service Organizations et le numéro d'identification du compte membre et identifiez le principal du service du compte `account.amazonaws.com` sous forme de paramètres.

## Désactivation d'un administrateur délégué pour Trusted Advisor

Vous pouvez supprimer l'administrateur délégué à l'aide de la Trusted Advisor console, de la `DeregisterDelegatedAdministrator` CLI ou du SDK Organizations. Pour plus d'informations sur la façon de désactiver le Trusted Advisor compte d'administrateur délégué à l'aide de la Trusted

Advisor console, voir Désenregistrer les administrateurs délégués dans le guide de l'Support utilisateur.

## AWS Well-Architected Tool et AWS Organizations

Il vous AWS Well-Architected Tool aide à documenter l'état de vos charges de travail et à les comparer aux meilleures pratiques AWS architecturales les plus récentes.

L'utilisation de AWS Well-Architected Tool with Organizations permet à AWS Well-Architected Tool Both et aux clients d'Organizations de simplifier le processus de partage AWS Well-Architected Tool des ressources avec les autres membres de leur organisation.

Pour plus d'informations, consultez Partage de vos ressources AWS Well-Architected Tool dans le Guide de l'utilisateur AWS Well-Architected Tool .

Utilisez les informations suivantes pour vous aider AWS Well-Architected Tool à intégrer AWS Organizations.

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet d' AWS WA Tool effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre AWS WA Tool et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForWellArchitected`

La politique de fonction du service est `AWSWellArchitectedOrganizationsServiceRolePolicy`

### Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés aux services utilisés par AWS WA Tool accordent l'accès aux principaux de service suivants :

- `wellarchitected.amazonaws.com`

## Permettre un accès fiable avec AWS WA Tool

Permet la mise à jour de AWS WA Tool pour refléter les changements hiérarchiques au sein d'une organisation.

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Vous pouvez activer l'accès sécurisé à l'aide de la AWS Well-Architected Tool console ou de la AWS Organizations console.

> **Important**
>
> Nous vous recommandons vivement, dans la mesure du possible, d'utiliser la AWS Well-Architected Tool console ou les outils pour permettre l'intégration avec Organizations. Cela permet AWS Well-Architected Tool d'effectuer toute configuration requise, telle que la création des ressources nécessaires au service. N'effectuez ces étapes que si vous ne pouvez pas activer l'intégration à l'aide des outils fournis par AWS Well-Architected Tool. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès sécurisé à l'aide de la AWS Well-Architected Tool console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès sécurisé à l'aide de la AWS WA Tool console

Consultez la section Partage de vos AWS Well-Architected Tool ressources dans le guide de AWS Well-Architected Tool l'utilisateur.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation, choisissez Services.

3. Choisissez AWS Well-Architected Tooldans la liste des services.
4. Choisissez Enable trusted access (Activer l'accès approuvé).
5. Dans la boîte de AWS Well-Architected Tool dialogue Activer l'accès sécurisé pour, tapez enable pour confirmer, puis sélectionnez Activer l'accès sécurisé.
6. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Well-Architected Tool qu'il peut désormais activer ce service pour qu'il fonctionne avec ce service AWS Organizations depuis la console de service.

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour activer l'accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Exécutez la commande suivante pour l'activer AWS Well-Architected Tool en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSService l'accès

## Désactiver l'accès sécurisé avec AWS WA Tool

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous pouvez désactiver l'accès sécurisé à l'aide des outils AWS Well-Architected Tool ou des AWS Organizations outils.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la AWS Well-Architected Tool console ou les outils pour désactiver l'intégration avec Organizations.

Cela permet AWS Well-Architected Tool d'effectuer tout nettoyage nécessaire, comme la suppression de ressources ou l'accès à des rôles dont le service n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Well-Architected Tool.
Si vous désactivez l'accès sécurisé à l'aide de la AWS Well-Architected Tool console ou des outils, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès sécurisé à l'aide de la AWS WA Tool console

Consultez la section Partage de vos AWS Well-Architected Tool ressources dans le guide de AWS Well-Architected Tool l'utilisateur.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour le désactiver AWS Well-Architected Tool en tant que service sécurisé auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Désactiver AWSService l'accès

## Gestionnaire d'adresses IP Amazon VPC (IPAM) et AWS Organizations

Amazon VPC IP Address Manager (IPAM) est une fonctionnalité VPC qui vous permet de planifier, suivre et surveiller plus facilement les adresses IP pour vos charges de travail. AWS

L'utilisation vous AWS Organizations permet de surveiller l'utilisation des adresses IP dans l'ensemble de votre organisation et de partager des pools d'adresses IP entre les comptes des membres.

Pour plus d'informations, consultez Intégration d'IPAM à AWS Organizations dans le Guide de l'utilisateur Amazon VPC IPAM.

Utilisez les informations suivantes pour vous aider à intégrer Amazon VPC IP Address Manager (IPAM) à. AWS Organizations

## Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service ci-dessous est automatiquement créé dans le compte de gestion de votre organisation et dans chaque compte membre au moment où vous intégrez IPAM à AWS Organizations à partir de la console IPAM ou de l'API `EnableIpamOrganizationAdminAccount` d'IPAM.

- `AWSServiceRoleForIPAM`

Pour plus d'informations, consultez Rôles lié à un service pour IPAMdans le Guide de l'utilisateur Amazon VPC IPAM.

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par IPAM accordent l'accès aux principaux de service suivants :

- `ipam.amazonaws.com`

## Pour activer l'accès approuvé auprès d'IPAM

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

> **Note**
>
> Lorsque vous désignez un administrateur délégué pour IPAM, il active automatiquement l'accès approuvé pour IPAM pour votre organisation.

L'IPAM a besoin d'un AWS Organizations accès sécurisé pour que vous puissiez désigner un compte membre en tant qu'administrateur délégué de ce service pour votre organisation.

Vous ne pouvez activer l'accès sécurisé qu'à partir des outils Amazon VPC IP Address Manager (IPAM).

Si vous intégrez IPAM à AWS Organizations l'aide de la console IPAM ou de l'`EnableIpamOrganizationAdminAccount`API IPAM, vous accordez automatiquement un accès sécurisé à IPAM. L'octroi d'un accès approuvé a pour effet de créer le rôle lié à un service `AWS ServiceRoleForIPAM`dans le compte de gestion et dans tous les comptes membres de l'organisation. IPAM utilise le rôle lié à un service pour surveiller les CIDR associés aux ressources réseau EC2 de votre organisation et pour stocker les métriques relatives à l'IPAM sur Amazon. CloudWatch Pour plus d'informations, consultez Rôles lié à un service pour IPAMdans le Guide de l'utilisateur Amazon VPC IPAM.

Pour savoir comment activer l'accès approuvé, consultez Intégration d'IPAM à AWS Organizations dans le Guide de l'utilisateur Amazon VPC IPAM.

Note

Vous ne pouvez pas activer l'accès sécurisé avec IPAM à l'aide de la AWS Organizations console ou de l'`EnableAWSServiceAccess`API.

## Pour désactiver l'accès approuvé auprès d'IPAM

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur du compte de AWS Organizations gestion peut désactiver l'accès sécurisé avec IPAM à l'aide de l' AWS Organizations `disable-aws-service-access`API.

Pour en savoir plus sur la désactivation des autorisations de compte IPAM et sur la suppression du rôle lié à un service, consultez Rôles lié à un service pour IPAM dans le Guide de l'utilisateur Amazon VPC IPAM.

Vous pouvez désactiver l'accès sécurisé en exécutant une AWS CLI commande Organizations ou en appelant une opération d'API Organizations dans l'un des AWS SDKs.

AWS CLI, AWS API

Pour désactiver l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Utilisez les AWS CLI commandes ou les opérations d'API suivantes pour désactiver l'accès aux services sécurisés :

- AWS CLI: disable-aws-service-access

  Exécutez la commande suivante pour désactiver Amazon VPC IP Address Manager (IPAM) en tant que service fiable auprès des Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSService l'accès

## Activation d'un compte administrateur délégué pour IPAM

Le compte administrateur délégué pour IPAM est responsable de la création des groupes d'adresses IP et IPAM, de la gestion et du contrôle de l'utilisation des adresses IP dans l'organisation et du partage des groupes d'adresses IP entre les comptes membres. Pour plus d'informations, consultez Intégration d'IPAM à AWS Organizations dans le Guide de l'utilisateur Amazon VPC IPAM.

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour IPAM.

Vous pouvez spécifier un compte d'administrateur délégué à partir de la console IPAM ou à l'aide de l'API `enable-ipam-organization-admin-account`. Pour plus d'informations, consultez enable-ipam-organization-admin-account dans le manuel de référence des AWS AWS CLI commandes.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué d'IPAM dans l'organisation.

Pour configurer un administrateur délégué à l'aide de la console IPAM, consultez Intégrer IPAM à AWS Organizations dans le Guide de l'utilisateur Amazon VPC IPAM.

### Désactivation d'un administrateur délégué pour IPAM

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour IPAM.

Pour supprimer un administrateur délégué à l'aide de AWS AWS CLI, consultez disable-ipam-organization-admin-account dans le manuel de référence des AWS AWS CLI commandes.

Pour désactiver le compte IPAM d'administrateur délégué à l'aide de la console IPAM, consultez Intégrer PAM à AWS Organizations dans le Guide de l'utilisateur Amazon VPC IPAM.

## Analyseur de reachabilité Amazon VPC et AWS Organizations

Reachability Analyzer est un outil d'analyse de configuration qui vous permet d'effectuer des tests de connectivité entre une ressource source et une ressource de destination dans vos clouds privés virtuels (). VPCs

L'utilisation AWS Organizations de Reachability Analyzer vous permet de suivre les parcours entre les comptes de votre organisation.

Pour plus d'informations, consultez la section Gérer les comptes d'administrateurs délégués dans Reachability Analyzer dans le guide de l'utilisateur de Reachability Analyzer.

Utilisez les informations suivantes pour vous aider à intégrer Reachability Analyzer à. AWS Organizations

### Création de rôles liés à un service lors de l'activation de l'intégration

Le rôle lié à un service suivant est automatiquement créé dans le compte de gestion de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à Reachability Analyzer d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé entre Reachability Analyzer et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForReachabilityAnalyzer`

Pour plus d'informations, voir Analyses entre comptes pour Reachability Analyzer dans le Guide de l'utilisateur de Reachability Analyzer.

## Principaux de service utilisés par les rôles liés à un service

Le rôle lié à un service dans la section précédente ne peut être assumé que par les principaux de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Reachability Analyzer autorisent l'accès aux principaux de service suivants :

- `reachabilityanalyzer.networkinsights.amazonaws.com`

## Pour activer l'accès approuvé pour Reachability Analyzer

Pour en savoir plus sur les autorisations requises pour activer l'accès approuvé, consultez Autorisations requises pour activer l'accès approuvé.

Lorsque vous désignez un administrateur délégué pour Reachability Analyzer, il active automatiquement l'accès approuvé pour Reachability Analyzer pour votre organisation.

Reachability Analyzer nécessite un accès sécurisé AWS Organizations pour que vous puissiez désigner un compte de membre en tant qu'administrateur délégué de ce service pour votre organisation.

⚠ Important

- Vous pouvez activer l'accès approuvé à l'aide de la console Reachability Analyzer ou de la console Organizations. Nous vous recommandons vivement d'utiliser la console Reachability Analyzer ou l'API `EnableMultiAccountAnalysisForAwsOrganization` pour activer l'intégration à Organizations. Cela permet à Reachability Analyzer d'effectuer toute configuration nécessaire, par exemple la création des ressources nécessaires au service.
- L'octroi d'un accès approuvé a pour effet de créer le rôle lié à un service `AWSServiceRoleForReachabilityAnalyzer`dans le compte de gestion et dans tous les comptes membres de l'organisation. Reachability Analyzer utilise le rôle lié au service pour permettre à la direction et à l'administrateur délégué d'exécuter des analyses de connectivité entre toutes les ressources de l'organisation. Reachability Analyzer est capable de prendre des instantanés des éléments réseau des comptes d'une organisation afin de répondre aux demandes de connectivité.

- Pour obtenir plus d'informations et des conseils sur l'activation d'un accès approuvé par Reachability Analyzer, consultez Analyses entre comptes pour Reachability Analyzer dans le Guide de l'utilisateur de Reachability Analyzer.

Vous pouvez activer l'accès sécurisé en utilisant la AWS Organizations console, en exécutant une AWS CLI commande ou en appelant une opération d'API dans l'un des AWS SDKs.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter en tant qu'utilisateur IAM, assumer un rôle IAM ou vous connecter en tant qu'utilisateur racine (non recommandé) dans le compte de gestion de l'organisation.
2. Sur la page Services, recherchez la ligne correspondant à Analyseur d'accessibilité VPC, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Show the option to enable trusted access (Afficher l'option pour activer l'accès approuvé), saisissez **`enable`** dans la zone, puis choisissez Enable trusted access (Activer l'accès approuvé).
4. Si vous êtes l'administrateur de Only AWS Organizations, dites à l'administrateur de Reachability Analyzer qu'il peut désormais activer ce service à l'aide de sa console. AWS Organizations

AWS CLI, AWS API

Pour activer l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les AWS CLI commandes ou les opérations d'API suivantes pour activer un accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer Reachability Analyzer en tant que service approuvé pour Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS API : Activer AWSService l'accès

## Pour désactiver l'accès approuvé pour Reachability Analyzer

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Vous pouvez désactiver l'accès approuvé à l'aide de la console Reachability Analyzer (recommandé) ou de la console Organizations. Pour désactiver l'accès approuvé à l'aide de la console Reachability Analyzer, consultez la section Analyses entre comptes pour Reachability Analyzer dans le Guide de l'utilisateur de Reachability Analyzer.

## Activation d'un compte administrateur délégué pour Reachability Analyzer

Le compte administrateur délégué permet d'exécuter des analyses de connectivité sur toutes les ressources de l'organisation. Pour plus d'informations, voir Intégrer Reachability Analyzer à AWS Organizations dans le Guide de l'utilisateur de Reachability Analyzer.

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Reachability Analyzer.

Vous pouvez spécifier un compte d'administrateur délégué à partir de la console Reachability Analyzer ou à l'aide de l'API `RegisterDelegatedAdministrator`. Pour plus d'informations, reportez-vous RegisterDelegatedAdministratorà la section Organizations Command Reference.

> **Autorisations minimales**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué de Reachability Analyzer dans l'organisation.

Pour configurer un administrateur délégué à l'aide de la console Reachability Analyzer, consultez Intégrer Reachability Analyzer à AWS Organizations dans le Guide de l'utilisateur de Reachability Analyzer.

### Désactiver un administrateur délégué pour Reachability Analyzer

Seul un administrateur du compte de gestion de l'organisation peut configurer un administrateur délégué pour Reachability Analyzer.

Vous pouvez supprimer l'administrateur délégué en utilisant soit l'API ou la console Reachability Analyzer, soit la CLI `DeregisterDelegatedAdministrator` Organizations ou l'opération SDK.

Pour désactiver le compte Reachability Analyzer de l'administrateur délégué à l'aide de la console Reachability Analyzer, consultez la section Analyses entre comptes pour Reachability Analyzer dans le Guide de l'utilisateur de Reachability Analyzer.

## Administrateur délégué pour Services AWS ce travail avec les Organizations

Nous vous recommandons d'utiliser le compte AWS Organizations de gestion, ses utilisateurs et ses rôles uniquement pour les tâches qui doivent être effectuées par ce compte. Nous vous recommandons également de stocker vos AWS ressources dans d'autres comptes membres de l'organisation et de les garder hors du compte de gestion. Cela est dû au fait que les fonctionnalités de sécurité telles que les politiques de contrôle des services des Organisations (SCPs) ne limitent pas les utilisateurs ou les rôles dans le compte de gestion. Le fait de séparer vos ressources de votre compte de gestion peut également vous aider à comprendre les frais figurant sur vos factures.

Beaucoup de Services AWS ceux qui s'intègrent à Organizations vous permettent de réduire l'utilisation du compte de gestion. Ces services vous permettent d'enregistrer un ou plusieurs comptes membres en tant qu'administrateurs pouvant gérer tous les comptes de l'organisation utilisés dans le service. Ces comptes sont appelés administrateurs délégués pour ce service spécifique. En enregistrant un compte membre en tant qu'administrateur délégué pour un service AWS , vous permettez à ce compte de disposer de certaines autorisations administratives pour ce service, ainsi que d'autorisations pour les actions en lecture seule d'Organizations.

Avant d'enregistrer un compte en tant qu'administrateur délégué pour un service :

- Vérifiez que le service prend en charge les administrateurs délégués. Consultez le tableau dans Services AWS que vous pouvez utiliser avec AWS Organizations pour savoir quels services prennent en charge les administrateurs délégués.
- Activez l'accès approuvé pour ce service.

> **Note**
>
> Pour savoir comment activer un administrateur délégué pour un service, consultez le tableau dans Services AWS que vous pouvez utiliser avec AWS Organizations et sélectionnez le lien En savoir plus dans la colonne Prend en charge l'administrateur délégué pour ce service.

## Autorisations accordées aux comptes d'administrateur délégué

Chaque compte d'administrateur délégué spécifique à un service dispose d'autorisations accordées par ce service. Pour savoir plus, consultez le tableau dans Services AWS que vous pouvez utiliser avec AWS Organizations et sélectionnez le lien En savoir plus dans la colonne Prend en charge l'administrateur délégué pour ce service.

Un compte d'administrateur délégué dispose également des autorisations en lecture seule :

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`

- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

Ces autorisations vous permettent d'afficher, mais pas de modifier ces éléments de la console :

- Structure de l'organisation, tous les comptes et OUs politiques de l'organisation
- Membres
- Tous les comptes et OUs.
- Politiques organisationnelles

# Sécurité dans AWS Organizations

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui fonctionne 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 conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Organizations, consultez Services AWS la section Portée par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Organizations. Les rubriques suivantes vous montrent comment configurer Organizations pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres outils Services AWS qui vous aident à surveiller et à sécuriser les ressources de votre Organisation.

Rubriques

# AWS PrivateLink pour AWS Organizations

Avec AWS PrivateLink for AWS Organizations, vous pouvez accéder au AWS Organizations service depuis le Virtual Private Cloud (VPC) sans avoir à passer par l'Internet public.

Amazon VPC vous permet de lancer AWS des ressources dans un réseau virtuel personnalisé. Vous pouvez utiliser un VPC pour contrôler vos paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau. Pour plus d'informations VPCs, consultez le guide de l'utilisateur Amazon VPC.

Pour connecter votre Amazon VPC à AWS Organizations, vous devez d'abord définir un point de terminaison VPC d'interface (points de terminaison d'interface). Les points de terminaison d'interface sont représentés par une ou plusieurs interfaces réseau élastiques (ENIs) auxquelles sont attribuées des adresses IP privées provenant de sous-réseaux de votre VPC. Les demandes de votre VPC destinées à des points de terminaison AWS Organizations via une interface restent sur le réseau Amazon.

Pour obtenir des informations générales sur les points de terminaison d'interface, consultez la section Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Rubriques

- Limites et restrictions du AWS PrivateLink pour AWS Organizations
- Création d'un point de terminaison VPC pour AWS Organizations
- Création d'une politique de point de terminaison VPC pour AWS Organizations

## Limites et restrictions du AWS PrivateLink pour AWS Organizations

Les limites du VPC s'appliquent à. AWS PrivateLink AWS Organizations Pour plus d'informations, consultez la section Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface et de AWS PrivateLink quotas dans le guide de l'utilisateur Amazon VPC. En outre, les restrictions suivantes s'appliquent :

- Disponible uniquement dans la `us-east-1` région
- Ne prend pas en charge le protocole TLS (Transport Layer Security) 1.1

# Création d'un point de terminaison VPC pour AWS Organizations

Vous pouvez créer un AWS Organizations point de terminaison dans votre VPC à l'aide de la console Amazon VPC, du AWS Command Line Interface () ou.AWS CLI CloudFormation

Pour plus d'informations sur la création et la configuration d'un point de terminaison à l'aide de la console Amazon VPC ou du AWS CLI, consultez la section Créer un point de terminaison VPC dans le guide de l'utilisateur Amazon VPC. Pour plus d'informations sur la création et la configuration d'un point de terminaison à l'aide de CloudFormation, consultez la VPCEndpoint ressource AWS : :EC2 : : dans le guide de l'AWS CloudFormation utilisateur.

Lorsque vous créez un AWS Organizations point de terminaison, utilisez le nom de service suivant :

```
com.amazonaws.us-east-1.organizations
```

Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour y accéder AWS, utilisez le nom de service FIPS suivant : AWS Organizations

```
com.amazonaws.us-east-1.organizations-fips
```

# Création d'une politique de point de terminaison VPC pour AWS Organizations

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès aux Organizations. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux points de terminaison d'un VPC à l'aide de politiques de point de terminaison dans le Guide de l'utilisateur Amazon VPC.

## Exemple : politique de point de terminaison VPC pour les actions AWS Organizations

```
{
   "Statement":[
```

```
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

# Identity and Access Management pour AWS Organizations

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 des Organizations. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques



## 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 AWS Organizations d'identité et d'accès)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment AWS Organizations fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Exemples de politiques basées sur l'identité pour AWS Organizations)

## 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 utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS 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.

## Comment AWS Organizations fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès aux Organizations, découvrez quelles fonctionnalités IAM sont disponibles pour les Organizations.

| Fonctionnalité IAM | Organisations de soutien |
|---|---|
| Politiques basées sur l'identité | Oui |
| Politiques basées sur les ressources | Oui |
| Actions de politique | Oui |
| Ressources de politique | Oui |
| Clés de condition de politique (spécifiques au service) | Oui |
| ACLs | Non |

| Fonctionnalité IAM | Organisations de soutien |
| --- | --- |
| ABAC (étiquettes dans les politiques) | Oui |
| Informations d'identification temporaires | Non |
| Transmission des sessions d'accès (FAS) | Oui |
| Rôles de service | Oui |
| Rôles liés à un service | Oui |

Pour obtenir une vue d'ensemble de la façon dont les Organizations et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

## Politiques basées sur l'identité pour les Organisations

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 les Organisations

Pour consulter des exemples de politiques basées sur l'identité des Organisations, consultez. Exemples de politiques basées sur l'identité pour AWS Organizations

## Politiques basées sur les ressources au sein des Organizations

Prend en charge les politiques basées sur les ressources : oui

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.

Le service Organizations ne prend en charge qu'un seul type de stratégie basée sur les ressources, appelée stratégie de délégation basée sur les ressources, qui spécifie quels comptes membres peuvent effectuer des actions sur les politiques. Vous pouvez ajouter plusieurs déclarations dans la politique pour indiquer un ensemble d'autorisations différent pour les comptes membres.

Pour de plus amples informations, veuillez consulter Administrateur délégué pour AWS Organizations.

Exemples de politiques basées sur les ressources au sein des Organizations

Pour consulter des exemples de politiques basées sur les ressources des Organisations, voir Exemples de politiques basées sur les ressources pour AWS Organizations

## Actions politiques pour les Organisations

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 des Organizations, reportez-vous à la section Actions définies par AWS Organizations dans le Service Authorization Reference.

Les actions stratégiques dans Organizations utilisent le préfixe suivant avant l'action :

```
organizations
```

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

```
"Action": [
      "organizations:action1",
      "organizations:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité des Organisations, consultez. Exemples de politiques basées sur l'identité pour AWS Organizations

## Ressources relatives aux politiques pour les Organisations

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 des Organizations et leurs caractéristiques ARNs, consultez la section Ressources définies par AWS Organizations dans le Service Authorization Reference. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Organizations.

Pour consulter des exemples de politiques basées sur l'identité des Organisations, consultez. Exemples de politiques basées sur l'identité pour AWS Organizations

## Clés de conditions de politique pour les Organisations

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 des Organisations, reportez-vous à la section Clés de condition correspondantes AWS Organizations dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Organizations.

Pour consulter des exemples de politiques basées sur l'identité des Organisations, consultez. Exemples de politiques basées sur l'identité pour AWS Organizations

## ACLs dans Organizations

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 Organizations

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

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 auprès d'Organizations

Supporte les informations d'identification temporaires : Non

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.

## Sessions d'accès transféré pour les Organisations

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 les Organisations

Prend en charge les rôles de service : oui

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 des Organisations. Modifiez les rôles de service uniquement lorsque Organizations fournit des instructions à cet effet.

### Rôles liés aux services pour les Organisations

Prend en charge les rôles liés à un service : oui

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.

## Gestion des autorisations d'accès pour une organisation avec AWS Organizations

Toutes les AWS ressources, y compris les racines OUs, les comptes et les politiques d'une organisation, appartiennent à un Compte AWS, et les autorisations de création ou d'accès à une ressource sont régies par des politiques d'autorisation. Le compte de gestion d'une organisation possède toutes les ressources. Un administrateur de compte peut contrôler l'accès aux AWS ressources en associant des politiques d'autorisation aux identités IAM (utilisateurs, groupes et rôles).

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté d'autorisations d'administrateur. Pour plus d'informations, consultez la section Meilleures pratiques en matière de sécurité dans IAM dans le Guide de Gestion de compte AWS référence.

Lorsque vous accordez des autorisations, vous décidez qui doit les obtenir, à quelles ressources ces autorisations s'appliquent et les actions spécifiques que vous souhaitez autoriser sur ces ressources.

Par défaut, les utilisateurs, groupes et rôles IAM ne disposent d'aucune autorisation. En tant qu'administrateur du compte de gestion d'une organisation, vous pouvez exécuter des tâches administratives ou déléguer des autorisations d'administrateur à d'autres utilisateurs ou rôles IAM du compte de gestion. Pour ce faire, vous attachez une politique d'autorisation IAM à un utilisateur, groupe ou rôle IAM. Par défaut, un utilisateur ne dispose d'aucune autorisation. C'est ce que l'on appelle un refus implicite. La politique remplace le refus implicite par une autorisation explicite qui spécifie les actions que l'utilisateur peut exécuter et les ressources sur lesquelles il peut les exécuter. Si les autorisations sont accordées à un rôle, les utilisateurs dans d'autres comptes de l'organisation peuvent assumer ce rôle.

## AWS Organizations ressources et opérations

Cette section explique comment les AWS Organizations concepts correspondent à leurs concepts équivalents à l'IAM.

### Ressources

Dans AWS Organizations, vous pouvez contrôler l'accès aux ressources suivantes :

- Les racines et les OUs éléments qui constituent la structure hiérarchique d'une organisation
- Les comptes qui sont membres de l'organisation
- Les politiques que vous attachez aux entités de l'organisation
- Les handshakes que vous utilisez pour modifier l'état de l'organisation

Chacune de ces ressources possède un nom Amazon Resource Name (ARN) associé unique. Vous contrôlez l'accès à une ressource en spécifiant son ARN dans l'élément `Resource` d'une politique d'autorisation IAM. Pour une liste complète des formats ARN pour les ressources utilisées AWS Organizations, voir Types de ressources définis par AWS Organizations dans la référence d'autorisation de service.

### Opérations

AWS fournit un ensemble d'opérations permettant de travailler avec les ressources d'une organisation. Ces opérations vous permettent de réaliser des tâches telles que la création, l'énumération et la modification de contenus, ainsi que l'accès aux contenus et la suppression des ressources. La plupart des opérations peuvent être référencées dans l'élément `Action`

d'une politique IAM pour contrôler qui peut utiliser cette opération. Pour obtenir la liste des AWS Organizations opérations pouvant être utilisées comme autorisations dans une politique IAM, consultez la section Actions définies par les organisations dans la référence d'autorisation de service.

Lorsque vous associez un élément `Action` et un élément `Resource` dans une politique d'autorisation `Statement` individuelle, vous contrôlez exactement les ressources sur lesquelles un ensemble particulier d'actions peuvent être utilisées.

Clés de condition

AWS fournit des clés de condition que vous pouvez interroger afin de mieux contrôler certaines actions. Vous pouvez référencer ces clés de condition dans l'élément `Condition` d'une politique IAM pour spécifier les conditions supplémentaires qui doivent être remplies pour que l'instruction soit considérée comme une correspondance.

Les clés de condition suivantes sont particulièrement utiles dans les cas AWS Organizations suivants :

- `aws:PrincipalOrgID` : simplifie la spécification de l'élément `Principal` dans une politique basée sur les ressources. Cette clé globale constitue une alternative à la liste de tous IDs les comptes Comptes AWS d'une organisation. Au lieu de répertorier tous les comptes qui sont membres d'une organisation, vous pouvez spécifier l'ID d'organisation dans l'élément `Condition`.

  > **Note**
  >
  > Cette condition globale s'applique également au compte de gestion d'une organisation.

  Pour plus d'informations, consultez la description des clés AWS contextuelles `PrincipalOrgID` en condition globale dans le guide de l'utilisateur IAM.
- `aws:PrincipalOrgPaths` : utilisez cette clé de condition pour faire correspondre les membres d'une racine d'organisation spécifique, d'une unité d'organisation ou de ses enfants. La clé de condition `aws:PrincipalOrgPaths` renvoie true lorsque le principal (utilisateur racine, utilisateur IAM ou rôle) qui effectue la demande figure dans le chemin d'organisation spécifié. Un chemin est une représentation textuelle de la structure d'une AWS Organizations entité. Pour plus d'informations sur les chemins, voir Comprendre le chemin de l' AWS Organizations entité dans le Guide de l'utilisateur IAM. Pour plus d'informations sur l'utilisation de cette clé de condition, consultez aws : PrincipalOrgPaths dans le guide de l'utilisateur IAM.

Par exemple, l'élément de condition suivant correspond aux membres de l'une ou OUs l'autre des deux organisations.

```
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:PrincipalOrgPaths": [
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
                    ]
                }
            }
```

- `organizations:PolicyType` : vous pouvez utiliser cette clé de condition pour restreindre les opérations d'API Organizations liées à la politique de sorte qu'elles fonctionnent uniquement sur les politiques Organizations du type spécifié. Vous pouvez appliquer cette clé de condition à toute déclaration de politique qui inclut une action interagissant avec les politiques Organizations.

  Vous pouvez utiliser les valeurs suivantes avec cette clé de condition :

  - `SERVICE_CONTROL_POLICY`
  - `RESOURCE_CONTROL_POLICY`
  - `DECLARATIVE_POLICY_EC2`
  - `BACKUP_POLICY`
  - `TAG_POLICY`
  - `CHATBOT_POLICY`
  - `AISERVICES_OPT_OUT_POLICY`

  L'exemple de politique suivant permet à l'utilisateur d'effectuer n'importe quelle opération Organizations. Toutefois, si l'utilisateur effectue une opération qui prend un argument de politique, l'opération n'est autorisée que si la politique spécifiée est une politique de balisage. L'opération échoue si l'utilisateur spécifie un autre type de politique.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
```

```
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— Disponible à titre conditionnel si vous utilisez les opérations Activer l'AWSServiceaccès ou Désactiver AWSService l'accès pour activer ou désactiver l'accès sécurisé à d'autres AWS services. Vous pouvez utiliser `organizations:ServicePrincipal` pour restreindre les demandes que ces opérations effectuent à une liste de noms de principal de service approuvés.

  Par exemple, la politique suivante permet à l'utilisateur de spécifier uniquement AWS Firewall Manager lors de l'activation et de la désactivation de l'accès sécurisé avec AWS Organizations.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Pour obtenir la liste de toutes les clés de AWS Organizations condition spécifiques qui peuvent être utilisées comme autorisations dans une politique IAM, voir Clés de condition pour AWS Organizations dans la référence d'autorisation de service.

## Présentation de la propriété des ressources

Il Compte AWS est propriétaire des ressources créées dans le compte, quelle que soit la personne qui les a créées. Plus précisément, le propriétaire Compte AWS de la ressource est l'entité principale (c'est-à-dire l'utilisateur root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande de création de ressource. Pour une organisation, il s'agit toujours du compte de gestion. Vous ne pouvez pas appeler la plupart des opérations qui créent ou consultent les ressources de l'organisation à partir des comptes membres. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte racine de votre compte de gestion pour créer une unité d'organisation, votre compte de gestion est le propriétaire de la ressource. (Dans AWS Organizations, la ressource est l'UO).
- Si vous créez un utilisateur IAM dans votre compte de gestion et lui accordez des autorisations pour créer une unité d'organisation, il peut la créer. Toutefois, le compte de gestion, auquel appartient l'utilisateur, détient la ressource de l'unité d'organisation.
- Si vous créez un rôle IAM dans votre compte de gestion avec des autorisations permettant de créer une unité d'organisation, toute personne capable d'assumer le rôle peut créer une unité d'organisation. Le compte de gestion, auquel appartient le rôle (pas l'utilisateur qui l'assume), détient la ressource de l'unité d'organisation.

## Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

> **Note**
>
> Cette section décrit l'utilisation d'IAM dans le contexte de AWS Organizations. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation IAM complète, consultez le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et

les descriptions des politiques IAM, consultez la référence de politique IAM JSON dans le guide de l'utilisateur IAM.

Les politiques qui sont associées à une identité IAM sont appelées des politiques basées sur l'identité (politiques IAM). Les politiques qui sont attachées à une ressource sont appelées politiques basées sur la ressource.

Rubriques

- Politiques d'autorisations basées sur l'identité (politiques IAM)

Politiques d'autorisations basées sur l'identité (politiques IAM)

Vous pouvez associer des politiques aux identités IAM pour permettre à ces identités d'effectuer des opérations sur les AWS ressources. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associer une politique d'autorisations à un utilisateur ou à un groupe de votre compte : pour accorder à un utilisateur l'autorisation de créer une AWS Organizations ressource, telle qu'une politique de contrôle des services (SCP) ou une UO, vous pouvez associer une politique d'autorisations à un utilisateur ou à un groupe auquel l'utilisateur appartient. L'utilisateur ou le groupe doit se trouver dans le compte de gestion de l'organisation.
- Attacher une politique d'autorisations à un rôle (accorder des autorisations intercomptes) : vous pouvez attacher une politique d'autorisations basée sur l'identité à un rôle IAM pour accorder un accès intercompte à une organisation. Par exemple, l'administrateur du compte de gestion peut créer un rôle pour accorder des autorisations intercomptes à un utilisateur d'un compte membre en procédant comme suit :
  1. L'administrateur du compte de gestion crée un rôle IAM et y attache une politique d'autorisations qui accorde des autorisations aux ressources de l'organisation.
  2. L'administrateur du compte de gestion attache une politique d'approbation au rôle qui identifie l'ID de compte membre comme mandataire (`Principal`) pouvant assumer ce rôle.
  3. L'administrateur du compte membre peut ensuite déléguer des autorisations d'assumer le rôle à tous les utilisateurs du compte membre. Cela permet aux utilisateurs du compte membre de créer ou de consulter les ressources du compte de gestion et de l'organisation. Le principal de la politique de confiance peut également être un principal de AWS service si vous souhaitez autoriser un AWS service à assumer ce rôle.

Pour en savoir plus sur l'utilisation d'IAM pour déléguer des autorisations, consultez Gestion des accès dans le Guide de l'utilisateur IAM.

Voici des exemples de politiques autorisant un utilisateur à exécuter l'action `CreateAccount` dans votre organisation.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

Vous pouvez également fournir un ARN partiel dans l'élément `Resource` de la politique pour indiquer le type de ressource.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

Vous pouvez également refuser la création de comptes qui n'incluent pas de balises spécifiques au compte en cours de création.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez la section Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le guide de l'utilisateur IAM.

## Spécification des éléments d'une politique : actions, conditions, effets et ressources

Pour chaque AWS Organizations ressource, le service définit un ensemble d'opérations d'API, ou d'actions, qui peuvent interagir avec cette ressource ou la manipuler d'une manière ou d'une autre. Pour accorder des autorisations pour ces opérations, AWS Organizations définit un ensemble d'actions que vous pouvez spécifier dans une politique. Par exemple, pour la ressource UO, AWS Organizations définit les actions suivantes :

- `AttachPolicy` et `DetachPolicy`
- `CreateOrganizationalUnit` et `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` et `DescribeOrganizationalUnit`

Dans certains cas, l'exécution d'une opération d'API peut exiger des autorisations sur plus d'une action et peut exiger des autorisations sur plus d'une ressource.

Voici la plupart des éléments de base que vous pouvez utiliser dans une politique d'autorisation IAM :

- Action : utilisez ce mot-clé pour identifier les opérations (actions) que vous souhaitez autoriser ou refuser. Par exemple, en fonction de ce qui est spécifié`Effect`, `organizations:CreateAccount` autorise ou refuse à l'utilisateur les autorisations nécessaires pour effectuer l' AWS Organizations `CreateAccount`opération. Pour plus d'informations, voir Éléments de politique IAM JSON : action dans le guide de l'utilisateur IAM.
- Resource : utilisez ce mot-clé pour spécifier l'ARN de la ressource à laquelle l'instruction de politique s'applique. Pour plus d'informations, voir Éléments de politique IAM JSON : ressource dans le guide de l'utilisateur IAM.
- Condition : utilisez ce mot-clé pour spécifier une condition qui doit être remplie pour que l'instruction de politique s'applique. `Condition` spécifie généralement des circonstances supplémentaires qui doivent être vraies pour que la politique corresponde. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Effect : utilisez ce mot-clé pour spécifier si l'instruction de politique autorise ou refuse l'action sur la ressource. Si vous n'accordez pas explicitement l'accès à (autorisez) une ressource, l'accès est implicitement refusé. Vous pouvez également refuser explicitement l'accès à une ressource, pour veiller à ce qu'un utilisateur ne puisse pas exécuter l'action spécifiée sur la ressource spécifiée, même si une politique différente accorde l'accès. Pour plus d'informations, voir Éléments de politique IAM JSON : effet dans le guide de l'utilisateur IAM.
- Principal : dans les politiques basées sur l'identité (politiques IAM), l'utilisateur auquel la politique est attachée devient automatiquement et implicitement le principal. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource).

Pour en savoir plus sur la syntaxe et les descriptions des politiques IAM, consultez la référence de politique IAM JSON dans le guide de l'utilisateur IAM.

## Exemples de politiques basées sur l'identité pour AWS Organizations

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources des Organizations. 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 les Organizations, y compris le format du ARNs pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS Organizations dans le Service Authorization Reference.

Rubriques



## Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Organizations 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.

## Utilisation de la console Organizations

Pour accéder à la AWS Organizations console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources Organizations de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Organizations, associez également les Organizations `AWSOrganizationsFullAccess`ou la politique

AWSOrganizationsReadOnlyAccess AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur 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:ListGroupsForUser",
                "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": "*"
        }
    ]
}
```

## Octroi des autorisations d'administration complètes à un utilisateur

Vous pouvez créer une politique IAM qui accorde des autorisations d' AWS Organizations administrateur complètes à un utilisateur IAM de votre organisation. Vous pouvez effectuer cette opération à l'aide de l'éditeur de politique JSON dans la console IAM.

Pour utiliser l'éditeur de politique JSON afin de créer une politique

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation de gauche, sélectionnez Policies (Politiques).

   Si vous sélectionnez Politiques pour la première fois, la page Bienvenue dans les politiques gérées s'affiche. Sélectionnez Mise en route.
3. En haut de la page, sélectionnez Créer une politique.
4. Dans la section Éditeur de politique, choisissez l'option JSON.
5. Entrez le document de politique JSON suivant :

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*"
    }
}
```

6. Choisissez Suivant.

> **Note**
>
> Vous pouvez basculer à tout moment entre les options des éditeurs visuel et JSON. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, IAM peut restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour plus d'informations, consultez la page Restructuration de politique dans le Guide de l'utilisateur IAM.

7. Sur la page Vérifier et créer, saisissez un Nom de politique et une Description (facultative) pour la politique que vous créez. Vérifiez les Autorisations définies dans cette politique pour voir les autorisations accordées par votre politique.
8. Choisissez Create policy (Créer une politique) pour enregistrer votre nouvelle politique.

Pour en savoir plus sur la création d'une stratégie IAM, consultez la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

## Octroi d'un accès limité par des actions

Si vous souhaitez accorder des autorisations limitées et non des autorisations complètes, vous pouvez créer une politique qui répertorie les autorisations individuelles que vous voulez accorder dans l'élément `Action` de la politique d'autorisations IAM. Comme le montre l'exemple suivant, vous pouvez utiliser des caractères génériques (*) pour accorder uniquement les autorisations `Describe*` et `List*`, en fournissant essentiellement un accès en lecture seule à l'organisation.

> **Note**
>
> Dans une politique de contrôle des services (SCP), le caractère générique (*) figurant dans un élément `Action` peut être utilisé uniquement seul ou à la fin de la chaîne. Il ne peut pas apparaître au début ni au milieu de la chaîne. Par conséquent, `"servicename:action*"` est valide, mais `"servicename:*action"` les deux `"servicename:some*action"` ne sont pas valides dans SCPs.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "organizations:Describe*",
            "organizations:List*"
        ],
        "Resource": "*"
    }
}
```

Pour obtenir la liste de toutes les autorisations pouvant être attribuées dans une politique IAM, consultez la section Actions définies par les AWS Organizations dans le Service Authorization Reference.

## Octroi de l'accès à certaines ressources

En plus de restreindre l'accès à des actions spécifiques, vous pouvez limiter l'accès à certaines entités de votre organisation. Les éléments `Resource` dans les exemples des sections précédentes spécifient le caractère générique (« * »), ce qui signifie « toute ressource à laquelle l'action peut accéder ». Au lieu de cela, vous pouvez remplacer le caractère générique « * » par l'Amazon Resource Name (ARN) d'entités spécifiques auxquelles vous voulez autoriser l'accès.

Exemple : Octroi d'autorisations à une seule unité d'organisation

La première déclaration de la politique suivante accorde à un utilisateur IAM un accès en lecture à l'ensemble de l'organisation, mais la deuxième déclaration autorise l'utilisateur à effectuer des actions administratives AWS Organizations uniquement au sein d'une seule unité d'organisation (UO) spécifiée. Cela ne s'applique à aucun enfant OUs. Aucun accès de facturation n'est accordé. Notez que cela ne vous donne pas d'accès administratif Comptes AWS à l'unité d'organisation. Il accorde uniquement les autorisations nécessaires pour effectuer des AWS Organizations opérations sur les comptes au sein de l'unité d'organisation spécifiée :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*",
                "organizations:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "arn:aws:organizations::123456789012:ou/o-
<organizationId>/ou-<organizationalUnitId>"
```

```
        }
    ]
}
```

Vous pouvez obtenir les IDs informations pour l'unité d'organisation et l'organisation depuis la AWS Organizations console ou en appelant le `List*` APIs. L'utilisateur ou le groupe auquel vous appliquez cette politique peut effectuer n'importe quelle action (`"organizations:*"`) sur toute entité contenue dans l'unité d'organisation. L'unité d'organisation est identifiée par l'Amazon Resource Name (ARN).

Pour plus d'informations sur les ARNs différentes ressources, voir les types de ressources définis par AWS Organizations dans la référence d'autorisation de service.

## Octroi de la possibilité d'activer un accès approuvé à des mandataires de service limités

Vous pouvez utiliser l'élément `Condition` d'une déclaration de politique pour limiter davantage les circonstances dans lesquelles l'instruction de politique correspond.

Exemple : Octroi d'autorisations pour activer un accès approuvé à un service

La déclaration suivante montre comment limiter la possibilité d'activer un accès approuvé aux seuls services que vous spécifiez. Si l'utilisateur essaie d'appeler l'API avec un principal de service différent de celui pour AWS IAM Identity Center, cette politique ne correspond pas et la demande est refusée :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
```

```
    ]
}
```

Pour plus d'informations sur les ARNs différentes ressources, voir les types de ressources définis par AWS Organizations dans la référence d'autorisation de service.

## Exemples de politiques basées sur les ressources pour AWS Organizations

Les exemples de code suivant montrent comment vous pouvez utiliser les politiques de délégation basées sur les ressources. Pour de plus amples informations, veuillez consulter Administrateur délégué pour AWS Organizations.

Rubriques

- Exemple : Afficher l'organisation OUs, les comptes et les politiques
- Exemple : créer, lire, mettre à jour et supprimer des politiques
- Exemple : politiques de balisage et de débalisage
- Exemple : associer des politiques à une seule unité d'organisation ou à un seul compte
- Exemple : autorisations consolidées de gérer les politiques de sauvegarde d'une organisation

### Exemple : Afficher l'organisation OUs, les comptes et les politiques

Avant de déléguer la gestion des politiques, vous devez déléguer les autorisations nécessaires pour naviguer dans la structure d'une organisation et voir les unités organisationnelles (OUs), les comptes et les politiques qui leur sont associés.

Cet exemple montre comment vous pouvez inclure ces autorisations dans votre politique de délégation basée sur les ressources pour le compte membre. *AccountId*

> **Important**
>
> Il est conseillé de n'inclure des autorisations que pour les actions minimales requises, comme indiqué dans l'exemple, bien qu'il soit possible de déléguer n'importe quelle action en lecture seule Organizations à l'aide de cette politique.

Cet exemple de politique de délégation accorde les autorisations nécessaires pour effectuer des actions par programmation à partir de l' AWS API ou. AWS CLI Pour utiliser cette politique de délégation, remplacez le texte AWS réservé *AccountId* par vos propres informations. Ensuite, suivez les instructions dans Administrateur délégué pour AWS Organizations.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

## Exemple : créer, lire, mettre à jour et supprimer des politiques

Vous pouvez créer une politique de délégation basée sur les ressources qui permet au compte de gestion de déléguer`create`, `readupdate`, et des `delete` actions pour n'importe quel type de stratégie. Cet exemple montre comment vous pouvez déléguer ces actions pour les politiques de contrôle des services au compte du membre*`MemberAccountId`*. Les deux ressources présentées dans l'exemple accordent l'accès aux politiques de contrôle des services gérés par le client et aux politiques de contrôle des services AWS gérés respectivement.

> **Important**
>
> Cette politique permet aux administrateurs délégués d'effectuer des actions spécifiques sur les politiques créées par n'importe quel compte de l'organisation, y compris le compte de gestion.
> Il n'autorise pas les administrateurs délégués à joindre ou à détacher des politiques, car il n'inclut pas les autorisations requises pour effectuer `organizations:AttachPolicy` des `organizations:DetachPolicy` actions.

Cet exemple de politique de délégation accorde les autorisations nécessaires pour effectuer des actions par programmation à partir de l' AWS API ou. AWS CLI AWS Remplacez le texte de remplacement pour *`MemberAccountIdManagementAccountId`*, et *`OrganizationId`* par vos propres informations. Ensuite, suivez les instructions dans Administrateur délégué pour AWS Organizations.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingDescribeListActionsWithoutCondition",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
```

```
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DelegatingPolicyActionsWithCondition",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "SERVICE_CONTROL_POLICY"
                }
            }
        },
        {
            "Sid": "DelegatingMinimalActionsForSCPs",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy"
            ],
            "Resource": [
```

```
                "arn:aws:organizations::111122223333:policy/o-OrganizationId/
service_control_policy/*",
                "arn:aws:organizations::aws:policy/service_control_policy/*"
            ]
        }
    ]
}
```

## Exemple : politiques de balisage et de débalisage

Cet exemple montre comment créer une politique de délégation basée sur les ressources qui permet aux administrateurs délégués de baliser ou de débaliser les politiques de sauvegarde. Il accorde les autorisations nécessaires pour effectuer des actions par programmation à partir de l' AWS API ou. AWS CLI

Pour utiliser cette politique de délégation, remplacez le texte AWS réservé pour *MemberAccountIdManagementAccountId*, et *OrganizationId* par vos propres informations. Ensuite, suivez les instructions dans Administrateur délégué pour AWS Organizations.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActionsWithoutCondition",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListTagsForResource"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "DelegatingNecessaryDescribeListActionsWithCondition",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        },
        {
            "Sid": "DelegatingTaggingBackupPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:TagResource",
                "organizations:UntagResource"
            ],
            "Resource": "arn:aws:organizations::111122223333:policy/
o-OrganizationId/backup_policy/*"
        }
    ]
}
```

## Exemple : associer des politiques à une seule unité d'organisation ou à un seul compte

Cet exemple montre comment vous pouvez créer une politique de délégation basée sur les ressources qui autorise les administrateurs à déléguer des politiques aux `attach` `detach` organisations ou à partir d'une unité organisationnelle (UO) ou d'un compte spécifique. Avant de déléguer ces actions, vous devez déléguer les autorisations nécessaires pour naviguer dans la structure d'une organisation et voir les comptes qui s'y trouvent. Pour plus d'informations, consultez Exemple : Afficher l'organisation OUs, les comptes et les politiques.

> **Important**
>
> - Bien que cette politique permette d'associer ou de détacher des politiques à l'unité d'organisation ou au compte spécifié, elle exclut les comptes enfant OUs et les comptes sous-enfants OUs.
> - Cette politique permet aux administrateurs délégués d'effectuer les actions spécifiées sur les politiques créées par n'importe quel compte de l'organisation, y compris le compte de gestion.

Cet exemple de politique de délégation accorde les autorisations nécessaires pour effectuer des actions par programmation à partir de l' AWS API ou. AWS CLI Pour utiliser cette politique de délégation, remplacez le texte AWS réservé pour*`MemberAccountId`*, *`ManagementAccountIdOrganizationId`*, et *`TargetAccountId`* par vos propres informations. Ensuite, suivez les instructions dans Administrateur délégué pour AWS Organizations.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
```

```
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AttachDetachPoliciesSpecifiedAccountOU",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::111122223333:ou/o-OrganizationId/ou-
OUId",
                "arn:aws:organizations::111122223333:account/
o-OrganizationId/TargetAccountId",
                "arn:aws:organizations::111122223333:policy/o-OrganizationId/
backup_policy/*"
            ]
        }
    ]
}
```

Pour déléguer les politiques d'attachement et de détachement à n'importe quelle unité d'organisation ou compte au sein des organisations, remplacez la ressource de l'exemple précédent par les ressources suivantes :

```
"Resource": [
    "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/
*"
]
```

## Exemple : autorisations consolidées de gérer les politiques de sauvegarde d'une organisation

Cet exemple montre comment vous pouvez créer une politique de délégation basée sur les ressources qui permet au compte de gestion de déléguer toutes les autorisations nécessaires à la gestion des politiques de sauvegarde au sein de l'organisation, y compris les actions `create`, `read`, `update` et `delete`, ainsi que les actions de politique `attach` et `detach`.

> **Important**
>
> Cette politique permet aux administrateurs délégués d'effectuer les actions spécifiées sur les politiques créées par n'importe quel compte de l'organisation, y compris le compte de gestion.

Cet exemple de politique de délégation accorde les autorisations nécessaires pour effectuer des actions par programmation à partir de l' AWS API ou. AWS CLI Pour utiliser cette politique de délégation, remplacez le texte AWS réservé pour*MemberAccountId*, *ManagementAccountIdOrganizationId*, et *RootId* par vos propres informations. Ensuite, suivez les instructions dans Administrateur délégué pour AWS Organizations.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
```

```
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        },
        {
            "Sid": "DelegatingAllActionsForBackupPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:CreatePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
```

```
                "organizations:AttachPolicy",
                "organizations:DetachPolicy",
                "organizations:EnablePolicyType",
                "organizations:DisablePolicyType"
            ],
            "Resource": [
                "arn:aws:organizations::111122223333:root/o-OrganizationId/
r-RootId",
                "arn:aws:organizations::111122223333:ou/o-OrganizationId/*",
                "arn:aws:organizations::111122223333:account/o-OrganizationId/*",
                "arn:aws:organizations::111122223333:policy/o-OrganizationId/
backup_policy/*"
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        }
    ]
}
```

## AWS politiques gérées pour AWS Organizations

Cette section identifie les politiques AWS gérées que vous pouvez utiliser pour gérer votre organisation. Vous ne pouvez pas modifier ou supprimer une politique AWS gérée, mais vous pouvez l'associer ou la détacher aux entités de votre organisation selon vos besoins.

### AWS Organizations politiques gérées à utiliser avec Gestion des identités et des accès AWS (IAM)

Une politique gérée IAM est fournie et tenue à jour par AWS. Une politique gérée fournit des autorisations pour les tâches courantes que vous pouvez attribuer à vos utilisateurs en attachant la politique gérée à l'utilisateur ou au rôle IAM approprié. Vous n'êtes pas obligé de rédiger vous-même la politique, et lorsque vous la mettez AWS à jour de manière appropriée pour prendre en charge de nouveaux services, vous bénéficiez automatiquement et immédiatement de la mise à jour.

Vous pouvez voir la liste des politiques gérées AWS dans la page Politiques sur la console IAM. Utilisation du menu déroulant Politiques de filtre pour sélectionner géré par AWS .

Vous pouvez utiliser les politiques gérées suivantes pour accorder des autorisations aux utilisateurs de votre organisation.

AWS politique gérée : AWSOrganizationsFullAccess

Fournit toutes les autorisations nécessaires à la création et à l'administration complète d'une organisation.

Consultez la politique : `AWSOrganizationsFullAccess`.

AWS politique gérée : AWSOrganizationsReadOnlyAccess

Fournit un accès en lecture seule aux informations relatives à l'organisation. Elle ne permet pas à l'utilisateur d'apporter des modifications.

Consultez la politique : `AWSOrganizationsReadOnlyAccess`.

AWS politique gérée : DeclarativePoliciesEC2Report

Cette politique est utilisée par le rôle lié au service AWSServiceRoleForDeclarativePoliciesEC2Report pour lui permettre de décrire les états des attributs de compte pour les comptes membres.

Afficher la politique : DeclarativePoliciesEC2Rapport.

## Mises à jour des politiques AWS gérées par les Organizations

Le tableau suivant détaille les mises à jour apportées aux politiques AWS gérées depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique des documents .

| Modifier | Description | Date |
| --- | --- | --- |
| AWSOrganizationsFullAccess— mis à jour pour autoriser les autorisations d'API de compte requises pour consulter ou modifier le nom d'un compte via la console Organizations. | Ajout de l'`account:GetAccountInformation` action permettant d'autoriser l'accès pour afficher le nom de compte de n'importe quel compte dans une organisation et de l'`account:PutAccountName` action pour permettre l'accès | 22 avril 2025 |

| Modifier | Description | Date |
| --- | --- | --- |
| | pour modifier n'importe quel nom de compte dans une organisation. | |
| DeclarativePoliciesEC2Rapport — Nouvelle politique gérée | Ajout de la `DeclarativePoliciesEC2Report` politique permettant d'activer les fonctionnalités du rôle `AWSServiceRoleForDeclarativePoliciesEC2Report` lié au service. | 22 novembre 2024 |
| AWSOrganizationsReadOnlyAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour consulter l'adresse e-mail d'un utilisateur root et l'. | Ajout de l'`account:GetPrimaryEmail` action permettant d'accéder à l'adresse e-mail de l'utilisateur root (adresse ) pour tout compte membre d'une organisation et de l'`account:GetRegionOptStatus` action permettant d'accéder à l'affichage des régions activées pour tout compte membre d'une organisation. | 6 juin 2024 |
| AWSOrganizationsFullAccess— mis à jour pour inclure `Sid` des éléments décrivant la déclaration de politique. | Ajout `Sid` d'éléments pour la politique `AWSOrganizationsFullAccess` gérée. | 6 février 2024 |
| AWSOrganizationsReadOnlyAccess— mis à jour pour inclure `Sid` des éléments décrivant la déclaration de politique. | Ajout `Sid` d'éléments pour la politique `AWSOrganizationsReadOnlyAccess` gérée. | 6 février 2024 |

| Modifier | Description | Date |
| --- | --- | --- |
| AWSOrganizationsFullAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour les activer ou les désactiver Régions AWS via la console Organizations. | Ajout de l'`account:ListRegions` `account:DisableRegion` action `account:EnableRegion` et à la politique pour activer l'accès en écriture afin d'activer ou de désactiver les régions pour un compte. | 22 décembre 2022 |
| AWSOrganizationsReadOnlyAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour être Régions AWS répertorié via la console Organizations. | L'`account:ListRegions` action a été ajoutée à la politique pour permettre l'accès à l'affichage des régions d'un compte. | 22 décembre 2022 |
| AWSOrganizationsFullAccess— mis à jour pour autoriser les autorisations d'API de compte requises pour ajouter ou modifier les contacts du compte via la console Organizations. | L'`account:PutContactInformation` action `account:GetContactInformation` and a été ajoutée à la politique pour permettre l'accès en écriture afin de modifier les contacts d'un compte. | 21 octobre 2022 |
| AWSOrganizationsReadOnlyAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour consulter les contacts du compte via la console Organizations. | L'`account:GetContactInformation` action a été ajoutée à la politique pour permettre l'accès à l'affichage des contacts d'un compte. | 21 octobre 2022 |

| Modifier | Description | Date |
| --- | --- | --- |
| AWSOrganizationsFullAccess— mis à jour pour permettre la création d'une organisation. | L'`CreateServiceLinkedRole` autorisation a été ajoutée à la politique pour permettre de créer le rôle lié au service requis pour créer une organisation. L'autorisation est limitée à la création d'un rôle qui ne peut être utilisé que par le service `organizations.amazonaws.com` . | 24 août 2022 |
| AWSOrganizationsFullAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour ajouter, modifier ou supprimer des contacts alternatifs via la console Organizations. | Les `account:PutAlternateContact` actions`account:GetAlternateContact` ,`account:DeleteAlternateContact` , ont été ajoutées à la politique pour permettre l'accès en écriture afin de modifier les contacts alternatifs d'un compte. | 7 février 2022 |
| AWSOrganizationsReadOnlyAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour consulter les contacts alternatifs du compte via la console Organizations. | L'`account:GetAlternateContact` action a été ajoutée à la politique pour permettre l'accès aux contacts alternatifs d'un compte. | 7 février 2022 |

## AWS politiques d'autorisation gérées

Les politiques d'autorisation sont similaires aux politiques d'autorisation IAM, mais elles constituent une fonctionnalité d'IAM AWS Organizations plutôt que d'IAM. Vous utilisez des politiques d'autorisation pour configurer et gérer de manière centralisée l'accès des principaux et des ressources dans vos comptes membres.

Vous pouvez consulter la liste des politiques de votre organisation sur la page Politiques de la console Organizations.

| Nom de la politique | Description | ARN |
| --- | --- | --- |
| CompletAWSAccess | Permet d'accéder à toutes les opérations. | arn:aws:organizations : :aws : -Complet policy/service_control_policy/p AWSAccess |
| RCPFullAWSAccess | Permet d'accéder à toutes les ressources. | arn:aws:organizations : :aws : -policy/resource_control_policy/p RCPFull AWSAccess |

## Contrôle d'accès basé sur les attributs avec des balises pour AWS Organizations

Le contrôle d'accès basé sur les attributs vous permet d'utiliser des attributs gérés par l'administrateur, tels que des balises associées à la fois aux AWS ressources et aux AWS identités, pour contrôler l'accès à ces ressources. Par exemple, vous pouvez spécifier qu'un utilisateur peut accéder à une ressource lorsque l'utilisateur et la ressource ont la même valeur pour une balise donnée.

AWS Organizations les ressources balisables incluent Comptes AWS la racine de l'organisation, les unités organisationnelles (OUs) ou les politiques. Lorsque vous attachez des balises à des ressources Organizations, vous pouvez ensuite utiliser ces balises pour contrôler qui peut accéder à ces ressources. Pour ce faire, ajoutez à vos déclarations de politique d'autorisation Gestion des identités et des accès AWS (IAM) des `Condition` éléments qui vérifient si certaines clés et valeurs de balise sont présentes avant d'autoriser l'action. Cela vous permet de créer une politique IAM qui indique efficacement « Autoriser l'utilisateur à gérer uniquement ceux OUs qui ont une balise avec une clé `X` et une valeur `Y` » ou « Autoriser l'utilisateur à gérer uniquement ceux OUs qui sont étiquetés avec une clé ayant la même valeur `Z` que la clé de balise attachée à l'utilisateur »`Z`.

Vous pouvez baser vos tests `Condition` sur différents types de références de balises dans une politique IAM.

- Vérification des balises attachées aux ressources spécifiées dans la demande
- Vérification des balises attachées à l'utilisateur ou au rôle IAM qui effectue la demande
- Vérifiez les balises qui sont incluses en tant que paramètres dans la demande

Pour plus d'informations sur l'utilisation des balises pour le contrôle d'accès dans les politiques, consultez Contrôle de l'accès aux et pour les utilisateurs et rôles IAM à l'aide des balises de ressources. Pour obtenir la syntaxe complète des politiques d'autorisations IAM, consultez la Référence de politique JSON IAM

### Vérification des balises attachées aux ressources spécifiées dans la demande

Lorsque vous faites une demande en utilisant le AWS Management Console, le AWS Command Line Interface (AWS CLI) ou l'un des AWS SDKs, vous spécifiez les ressources auxquelles vous souhaitez accéder avec cette demande. Que vous tentiez de répertorier les ressources disponibles d'un type donné, de lire une ressource ou d'écrire, de modifier ou de mettre à jour une ressource, vous spécifiez la ressource à laquelle accéder en paramètre de la demande. Ces demandes sont contrôlées par les politiques d'autorisations IAM que vous associez à vos utilisateurs et rôles. Dans ces politiques, vous pouvez comparer les balises attachées à la ressource demandée et choisir d'autoriser ou de refuser l'accès en fonction des clés et des valeurs de ces balises.

Pour vérifier une balise attachée à la ressource, vous référencez la balise dans un élément `Condition` en insérant la chaîne suivante en préfixe du nom de la clé de balise : `aws:ResourceTag/`

L'exemple de politique suivant permet à l'utilisateur ou au rôle d'effectuer n'importe quelle opération AWS Organizations sauf si cette ressource a une balise avec la clé `department` et la valeur `security`. Si cette clé et cette valeur sont présentes, la politique refuse explicitement l'opération `UntagResource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" : "organizations:*",
            "Resource" : "*"

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
```

```
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur l'utilisation de cet élément, voir Contrôle de l'accès aux ressources et aws : ResourceTag dans le guide de l'utilisateur IAM.

## Vérification des balises attachées à l'utilisateur ou au rôle IAM qui effectue la demande

Vous pouvez contrôler ce que la personne à l'origine de la demande (le mandataire) est autorisée à faire en fonction des balises qui sont attachées à l'utilisateur ou au rôle IAM de cette personne. Pour ce faire, utilisez la clé de condition `aws:PrincipalTag/`*`key-name`* pour spécifier la balise et la valeur qui doivent être attachées à l'utilisateur ou au rôle de l'appelant.

L'exemple suivant montre comment autoriser une action uniquement lorsque la balise spécifiée (`cost-center`) a la même valeur à la fois chez le mandataire appelant l'opération et sur la ressource à laquelle accède l'opération. Dans cet exemple, l'utilisateur appelant peut démarrer et arrêter une instance Amazon EC2 uniquement si l'instance est balisée avec la même valeur `cost-center` que l'utilisateur.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Pour plus d'informations sur l'utilisation de cet élément, consultez Contrôle de l'accès pour les mandataires IAM et `aws:PrincipalTag` dans le Guide de l'utilisateur IAM.

### Vérifiez les balises qui sont incluses en tant que paramètres dans la demande

Plusieurs opérations vous permettent de spécifier des balises dans le cadre de la demande. Par exemple, lorsque vous créez une ressource, vous pouvez spécifier les balises qui sont attachées à la nouvelle ressource. Vous pouvez spécifier un élément `Condition` qui utilise `aws:TagKeys` pour autoriser ou refuser l'opération en fonction de l'inclusion d'une clé de balise spécifique, ou d'un ensemble de clés, dans la demande. Cet opérateur de comparaison ne se soucie pas de la valeur que contient la balise. Il vérifie uniquement si une balise avec la clé spécifiée est présente.

Pour vérifier la clé de balise, ou la liste de clés, spécifiez un élément `Condition` avec la syntaxe suivante :

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Vous pouvez utiliser `ForAllValues:` avant l'opérateur de comparaison pour vous assurer que toutes les clés de la demande doivent correspondre à l'une des clés spécifiées dans la politique. Par exemple, l'exemple de politique suivant autorise toute opération Organizations uniquement si toutes les balises présentes dans la demande sont un sous-ensemble des trois balises de cette politique.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
```

```
}
```

Vous pouvez également utiliser `ForAnyValue:` avant un opérateur de comparaison pour vous assurer qu'au moins une des clés de la demande doit correspondre à l'une des clés spécifiées dans la politique. Par exemple, la politique suivante autorise une opération Organizations uniquement si au moins une des clés de balise spécifiées est présente dans la demande.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "us-east-1",
                    "domain"
                ]
            }
        }
    }
}
```

Plusieurs opérations vous permettent de spécifier des balises dans la demande. Par exemple, lorsque vous créez une ressource, vous pouvez spécifier les balises qui sont attachées à la nouvelle ressource. Vous pouvez comparer une paire clé/valeur de balise dans la politique avec une paire clé/valeur de balise incluse dans la demande. Pour ce faire, référencez la balise dans un élément `Condition` en faisant précéder le nom de la clé de balise par la chaîne suivante : `aws:RequestTag/`*`key-name`*, puis spécifiez la valeur de balise qui doit être présente.

Par exemple, l'exemple de politique suivant refuse toute demande de l'utilisateur ou du rôle visant à créer un code Compte AWS lorsque la `costcenter` balise est absente de la demande ou fournit à cette balise une valeur autre que `12`, ou`3`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Pour plus d'informations sur l'utilisation de ces éléments, consultez aws : TagKeys et aws : RequestTag dans le guide de l'utilisateur IAM.

## Résolution des problèmes AWS Organizations d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Organizations et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Organizations
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mes Organisations

## Je ne suis pas autorisé à effectuer une action dans Organizations

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 `organizations:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 organizations: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 `organizations:`*`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 Organizations.

Certains vous 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 Organizations. 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 autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mes Organisations

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 Organizations prend en charge ces fonctionnalités, consultezComment AWS Organizations fonctionne 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.

# Connexion et surveillance AWS Organizations

La bonne pratique consiste à surveiller votre organisation pour vous assurer que les modifications sont journalisées. Cela vous permet de vous assurer que tout changement inattendu peut être étudié et que les modifications indésirables peuvent être annulées. AWS Organizations en supporte actuellement deux Services AWS qui vous permettent de surveiller votre organisation et l'activité qui s'y déroule.

Rubriques



## Journalisation des appels d'API avec AWS CloudTrail for AWS Organizations

AWS Organizations est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Organizations. CloudTrail capture tous les appels d'API AWS Organizations sous forme d'événements, y compris les appels depuis la AWS Organizations console et les appels de code vers le AWS Organizations APIs. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS Organizations. 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 AWS Organizations, l'adresse IP à partir de laquelle elle a été faite, qui l'a faite, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

> **Important**
>
> Vous pouvez consulter toutes les CloudTrail informations AWS Organizations uniquement dans la région de l'Est des États-Unis (Virginie du Nord). Si vous ne voyez pas votre AWS Organizations activité dans la CloudTrail console, réglez votre console sur USA Est (Virginie du Nord) à l'aide du menu situé dans le coin supérieur droit. Si vous effectuez CloudTrail une requête à l'aide des outils AWS CLI ou du SDK, dirigez votre requête vers le point de terminaison de l'est des États-Unis (Virginie du Nord).

## AWS Organizations informations dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Organizations, 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 dans votre Compte AWS, y compris les événements pour AWS Organizations, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Lorsque la CloudTrail journalisation est activée dans votre Compte AWS compte, les appels d'API effectués aux AWS Organizations actions sont suivis dans des fichiers CloudTrail journaux, où ils sont écrits avec d'autres enregistrements de AWS service. Vous pouvez en configurer d'autres Services AWS pour analyser et agir de manière plus approfondie sur les données d'événements collectées dans CloudTrail les journaux. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail

Toutes les AWS Organizations actions sont enregistrées CloudTrail et documentées dans la référence de l'AWS Organizations API. Par exemple, les appels à `CreateAccount` (y compris l'`CreateAccountResult`événement)`ListHandshakesForAccount`,`CreatePolicy`, et `InviteAccountToOrganization` génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque entrée du journal contient des informations sur la personne qui a généré la demande. Les informations d'identité de l'utilisateur dans l'entrée de journal permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle IAM ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail.

> **Note**
>
> CloudTrail enregistrera les événements dans le compte qui effectue une action donnée (c'est-à-dire dans le compte du membre plutôt que dans le compte de gestion si le compte du membre a effectué l'action). Par exemple, un compte de membre quittant une organisation sera enregistré dans le journal du compte membre, et un compte de gestion supprimant un compte de membre sera connecté dans le journal du compte de gestion.

## Comprendre les entrées du fichier AWS Organizations journal

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 individuelle à partir d'une source quelconque et comprend des informations sur l'action demandée, sur tous les paramètres, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne sont pas des séries ordonnées retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

Exemples d'entrées de journal : CloseAccount

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`CloseAccount`appel généré lorsque l'API est appelée et que le processus de fermeture du compte commence à être traité en arrière-plan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

L'exemple suivant montre une entrée de CloudTrail journal pour un `CloseAccountResult` appel une fois que le flux de travail en arrière-plan visant à fermer le compte est terminé avec succès.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
```

```
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Exemples d'entrées de journal : CreateAccount

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`CreateAccount`appel généré lorsque l'API est appelée et que le processus de création du compte commence à être traité en arrière-plan.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

L'exemple suivant montre une entrée de CloudTrail journal pour un `CreateAccount` appel une fois que le flux de travail en arrière-plan pour créer le compte est terminé avec succès.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

L'exemple suivant montre une entrée de CloudTrail journal générée lorsqu'un flux de travail en `CreateAccount` arrière-plan n'a pas réussi à créer le compte.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
```

```
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Exemple d'entrée de journal : CreateOrganizationalUnit

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`CreateOrganizationalUnit`appel.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail",
```

```
            "path": "o-aa111bb222/r-a1b2/ou-examplerootid111-exampleouid111/"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Exemple d'entrée de journal : InviteAccountToOrganization

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`InviteAccountToOrganization`appel.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
```

```
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
```

```
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Exemple d'entrée de journal : AttachPolicy

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`AttachPolicy`appel. La réponse indique que l'appel a échoué parce que le type de politique demandé n'est pas activé dans la racine où la demande d'attachement a été lancée.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
```

```
}
```

Exemple d'entrée de journal : politique effective non valide

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`EffectivePolicyValidation`événement. Cet événement est transmis au compte de gestion de l'organisation chaque fois qu'une mise à jour de l'organisation crée une politique effective non valide pour un compte quelconque.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-07-17T14:53:40Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "EffectivePolicyValidation",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "readOnly": true,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
        "accountId": "111111111111",
        "policyType": "BACKUP_POLICY",
        "state": "INVALID",
        "requestTimestamp": "Jul 17, 2025, 2:53:40 PM",
        "info": "All validation errors listed",
        "validationErrors": [
            {
                "accountPath": "o-aa111bb222/r-a1b2/111111111111/",
                "evaluationTimestamp": "Jul 17, 2025, 2:53:40 PM",
                "errorCode": "ELEMENTS_TOO_MANY",
                "errorMessage": "'hourly_rule' exceeds the allowed maximum limit 10",
                "pathToError": "plans/hourly-backup/rules/hourly_rule",
                "contributingPolicies": [
                    "p-examplepolicyid111"
```

```
                ]
            }
        ]
    },
    "eventCategory": "Management"
}
```

Exemple d'entrée de journal : politique effective valide

L'exemple suivant montre une entrée de CloudTrail journal pour un exemple d'`EffectivePolicyValidation`événement. Cet événement est transmis au compte de gestion de l'organisation chaque fois qu'une mise à jour de l'organisation corrige une politique effective sur un compte qui n'était pas valide auparavant.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "111111111111",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-07-17T14:54:40Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "EffectivePolicyValidation",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "readOnly": true,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
        "accountId": "111111111111",
        "policyType": "BACKUP_POLICY",
        "state": "VALID",
        "requestTimestamp": "Jul 17, 2025, 2:54:40 PM",
        "info": "Previous effective policy validation error(s) resolved for this
 account/policyType"
    },
```

```
    "eventCategory": "Management"
}
```

## Amazon EventBridge et AWS Organizations

AWS Organizations peut fonctionner avec Amazon EventBridge, anciennement Amazon CloudWatch Events, pour déclencher des événements lorsque des actions spécifiées par l'administrateur se produisent dans une organisation. Par exemple, en raison de la sensibilité de ces actions, la plupart des administrateurs souhaitent être avertis chaque fois que quelqu'un crée un nouveau compte dans l'organisation ou quand un administrateur d'un compte membre tente de quitter l'organisation. Vous pouvez configurer EventBridge des règles qui recherchent ces actions, puis envoient les événements générés à des cibles définies par l'administrateur. Une cible peut être une rubrique Amazon SNS qui envoie des e-mails ou des SMS à ses abonnés. Vous pouvez également créer une fonction AWS Lambda qui consigne les détails de l'action pour vous permettre de les passer en revue ultérieurement.

Pour consulter un didacticiel expliquant comment EventBridge activer le suivi des principales activités de votre organisation, consultezTutoriel : Surveillez les modifications importantes apportées à votre organisation avec Amazon EventBridge.

> **Important**
>
> Actuellement, AWS Organizations il est hébergé uniquement dans la région de l'est des États-Unis (Virginie du Nord) (même s'il est disponible dans le monde entier). Pour effectuer les étapes de ce didacticiel, vous devez configurer le AWS Management Console pour utiliser cette région.

Pour en savoir plus EventBridge, notamment comment le configurer et l'activer, consultez le guide de EventBridge l'utilisateur Amazon.

# Validation de conformité pour AWS Organizations

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.

## Résilience dans AWS Organizations

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 de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

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

## Sécurité de l'infrastructure dans AWS Organizations

En tant que service géré, AWS Organizations il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre  AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder aux Organisations via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

# Résolution des problèmes AWS Organizations

Si vous rencontrez des problèmes lors de l' AWS Organizations utilisation, consultez les rubriques de cette section.

## Dépannage de problèmes généraux

Utilisez les informations fournies ici pour vous aider à diagnostiquer et à résoudre les problèmes d'accès refusés ou les autres problèmes courants que vous pourriez rencontrer lors de votre utilisation. AWS Organizations

Rubriques



### Je reçois un message « accès refusé » lorsque je fais une demande à AWS Organizations

- Vérifiez que vous êtes autorisé à appeler l'action et la ressource que vous avez demandées. Un administrateur doit accorder les autorisations en attachant une politique IAM à votre utilisateur, groupe ou rôle. Si les déclarations de politique qui accordent ces autorisations incluent des

conditions, telles que time-of-day des restrictions d'adresse IP, vous devez également respecter ces exigences lorsque vous envoyez la demande. Pour plus d'informations sur l'affichage ou la modification de politiques pour un utilisateur, un groupe ou un rôle, consultez Utilisation de politiques dans le Guide de l'utilisateur IAM.

- Si vous signez des demandes d'API manuellement (sans utiliser le AWS SDKs), vérifiez que vous avez correctement signé la demande.

## Je reçois un message « Accès refusé » lorsque j'effectue une demande avec des informations d'identification de sécurité temporaires

- Vérifiez que l'utilisateur ou le rôle que vous utilisez pour effectuer la demande dispose des autorisations appropriées. Les autorisations affectées aux informations d'identification de sécurité temporaires proviennent d'un utilisateur ou d'un rôle. Elles sont donc limitées à celles accordées à l'utilisateur ou au rôle. Pour plus d'informations sur la manière dont les autorisations pour les informations d'identification de sécurité temporaires sont déterminées, consultez Contrôle des autorisations affectées aux informations d'identification de sécurité temporaires dans le Guide de l'utilisateur IAM.
- Vérifiez que vos demandes sont signées correctement et que la demande est correctement formée. Pour plus de détails, consultez la documentation du kit de développement logiciel correspondant au SDK de votre choix ou l'utilisation d'informations d'identification de sécurité temporaires pour demander l'accès aux AWS ressources dans le guide de l'utilisateur IAM.
- Vérifiez que vos informations d'identification de sécurité temporaires ne sont pas arrivées à expiration. Pour plus d'informations, consultez Obtention d'informations d'identification temporaires de sécurité dans le Guide de l'utilisateur IAM.

## J'obtiens un message « Accès refusé » lorsque j'essaie de quitter une organisation en tant que compte membre ou de supprimer un compte membre en tant que compte de gestion

- Vous ne pouvez supprimer un compte membre qu'après avoir activé l'accès utilisateur IAM à la facturation dans le compte membre. Pour plus d'informations, consultez Activation de l'accès à la console de facturation et de gestion des coûts dans le Guide de l'utilisateur AWS Billing .
- Vous ne pouvez supprimer un compte de votre organisation que si le compte possède les informations requises pour pouvoir fonctionner comme compte autonome. Lorsque vous créez

un compte dans une organisation à l'aide de la AWS Organizations console, de l'API ou de AWS CLI commandes, ces informations ne sont pas automatiquement collectées. Pour un compte que vous souhaitez rendre autonome, vous devez accepter le contrat AWS client, choisir un plan d'assistance, fournir et vérifier les informations de contact requises, et fournir un mode de paiement actuel. AWS utilise le mode de paiement pour facturer toute AWS activité facturable (autre que le niveau AWS gratuit) survenant alors que le compte n'est pas rattaché à une organisation. Pour de plus amples informations, veuillez consulter Quitter une organisation depuis un compte membre avec AWS Organizations.

## J'obtiens un message « Quota dépassé » lorsque j'essaie d'ajouter un compte à mon organisation.

Il existe un nombre maximum de comptes que peut avoir une organisation. Les comptes supprimés ou fermés continuent d'être comptabilisés par rapport à ce quota.

Une invitation à rejoindre l'organisation est comptabilisée par rapport au nombre maximum de comptes de votre organisation. Elle est décomptée si le compte invité décline l'invitation, si le compte de gestion annule l'invitation ou si celle-ci expire.

- Avant de fermer ou de supprimer un Compte AWS, supprimez-le de votre organisation afin qu'il ne soit plus pris en compte dans votre quota.
- Pour savoir comment demander une augmentation de quotas, consultez Valeurs minimales et maximales.

## J'obtiens un message « Cette opération nécessite une période d'attente » lors de l'ajout ou de la suppression de comptes

Certaines actions nécessitent une période d'attente en raison des quotas de compte. Par exemple, il est impossible de supprimer immédiatement de nouveaux comptes créés. Réessayez l'action dans quelques jours.

Pour les problèmes liés à l'ajout de comptes, consultez le quota Nombre maximum de comptes par défaut. Pour les problèmes liés à la suppression de comptes, consultez le quota Nombre de comptes que vous pouvez fermer dans un délai de 30 jours.

## J'obtiens un message « Organisation toujours en cours d'initialisation » lorsque j'essaie d'ajouter un compte à mon organisation.

Si vous recevez cette erreur et que vous avez créé l'organisation depuis plus d'une heure, contactez AWS Support.

## Je reçois le message : « Les invitations sont désactivées » lorsque j'essaie d'inviter un compte dans mon organisation.

Cela se produit lorsque vous activez toutes les fonctions de votre organisation. Cette opération peut prendre un certain temps et nécessite que tous les comptes membres répondent. Tant que l'opération n'est pas terminée, vous ne pouvez pas inviter de nouveaux comptes à rejoindre l'organisation.

## Les modifications que j'apporte ne sont pas toujours visibles immédiatement

En tant que service auquel on accède avec des ordinateurs situés dans des centres de données du monde entier, AWS Organizations utilise un modèle d'informatique distribuée appelé cohérence éventuelle. Toute modification que vous apportez AWS Organizations met du temps à être visible depuis tous les points de terminaison possibles. Ce retard est dû en partie au temps nécessaire pour envoyer les données d'un serveur à un autre ou d'une zone de réplication à une autre. AWS Organizations utilise également la mise en cache pour améliorer les performances, mais dans certains cas, cela peut ajouter du temps. La modification peut ne pas être visible tant que les données mises en cache précédemment n'arrivent pas à expiration.

Concevez vos applications globales pour prendre en compte ces retards potentiels et vous assurer qu'elles fonctionnent comme prévu, même lorsqu'une modification effectuée à un emplacement n'est pas visible instantanément à un autre.

Pour plus d'informations sur la manière dont d'autres Services AWS sont affectés par cette situation, consultez les ressources suivantes :

- Gestion de la cohérence des données dans le Guide du développeur de base de données Amazon Redshift
- Modèle de cohérence de données Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.
- Garantir la cohérence lors de l'utilisation d'Amazon S3 et d'Amazon Elastic MapReduce pour les flux de travail ETL dans le AWS cadre du blog Big Data

- Cohérence éventuelle EC2 dans la Référence d'API Amazon EC2

## Je reçois un message « Inscription complète » lorsque j'essaie d'accéder à un compte qui fait déjà partie d'une organisation

- Jusqu'à 48 heures peuvent être nécessaires pour que le compte membre hérite des informations de facturation du compte de gestion.
- Si le problème persiste après 48 heures, vous pouvez ouvrir un dossier d'assistance auprès de l'équipe d'assistance chargée des comptes et de la facturation. Pour plus d’informations, consultez Création d’un dossier de support.

# Appel de l'API à l'aide de demandes de requête HTTP

Cette section contient des informations générales sur l'utilisation de l'API Query pour AWS Organizations. Pour plus d'informations sur le fonctionnement de l'API et les erreurs, consultez la Référence des API AWS Organizations.

> **Note**
>
> Au lieu d'appeler directement l'API AWS Organizations Query, vous pouvez utiliser l'un des AWS SDKs. Il AWS SDKs s'agit de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Ruby, .NET, iOS, Android, etc.). Ils SDKs fournissent un moyen pratique de créer un accès programmatique à AWS Organizations et AWS. Par exemple, ils se SDKs chargent de tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

L'API de requête pour vous AWS Organizations permet d'appeler des actions de service. Les requêtes de l'API de requête sont des requêtes HTTPS qui doivent contenir un `Action` paramètre pour indiquer l'opération à effectuer. AWS Organizations prend en charge les requêtes GET et POST pour toutes les opérations. Autrement dit, l'API ne requiert pas l'utilisation de GET pour certaines actions et de POST pour d'autres. Toutefois, les demandes GET sont soumises aux limitations de taille d'une URL. Bien que cette limite varie en fonction du navigateur, elle est généralement de 2 048 octets. Par conséquent, dans le cas de demandes d'API de requête requérant des tailles plus importantes, il convient d'utiliser une requête POST.

Vous obtenez une réponse sous la forme d'un document XML. Pour plus d'informations sur la réponse, consultez les pages des actions spécifiques dans la Référence des API AWS Organizations.

Rubriques

- Points de terminaison
- HTTPS requis
- Signature des demandes AWS Organizations d'API

# Points de terminaison

AWS Organizations possède un point de terminaison d'API global unique hébergé dans la région USA Est (Virginie du Nord).

Pour plus d'informations sur les AWS points de terminaison et les régions de tous les services, consultez la section Points de terminaison régionaux dans le. Références générales AWS

# HTTPS requis

Dans la mesure où l'API de requête retourne des informations sensibles telles que des informations d'identification de sécurité, vous devez utiliser HTTPS pour chiffrer toutes les demandes d'API.

# Signature des demandes AWS Organizations d'API

Les demandes doivent être signées à l'aide d'un identifiant de la clé d'accès et d'une clé d'accès secrète. Nous vous recommandons vivement de ne pas utiliser vos Utilisateur racine d'un compte AWS informations d'identification pour travailler au quotidien avec AWS Organizations. Vous pouvez utiliser les informations d'identification d'un utilisateur ou d'un rôle.

Pour signer vos demandes d'API, vous devez utiliser AWS Signature Version 4. Pour plus d'informations sur l'utilisation de Signature version 4, consultez la section Signing AWS API du guide de l'utilisateur IAM.

AWS Organizations ne prend pas en charge les versions antérieures, telles que Signature Version 2.

Pour plus d'informations, consultez les ressources suivantes :

- AWS Informations d'identification de sécurité — Fournit des informations générales sur les types d'informations d'identification que vous pouvez utiliser pour accéder AWS.
- Bonnes pratiques de sécurité dans le domaine de l'IAM : propose des suggestions d'utilisation du service IAM afin de sécuriser vos AWS ressources, y compris celles qui se trouvent dans. AWS Organizations
- Informations d'identification de sécurité temporaires dans IAM : décrit comment créer et utiliser des informations d'identification de sécurité temporaires.

# Exemples de code pour les Organisations utilisant AWS SDKs

Les exemples de code suivants montrent comment utiliser Organizations avec un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés.

Les scénarios sont des exemples de code qui vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'un même service ou combinés à d'autres Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Exemples de base pour les Organisations utilisant AWS SDKs
  - Actions pour les Organisations utilisant AWS SDKs
    - Utilisation AttachPolicy avec un AWS SDK ou une CLI
    - Utilisation CreateAccount avec un AWS SDK ou une CLI
    - Utilisation CreateOrganization avec un AWS SDK ou une CLI
    - Utilisation CreateOrganizationalUnit avec un AWS SDK ou une CLI
    - Utilisation CreatePolicy avec un AWS SDK ou une CLI
    - Utilisation DeleteOrganization avec un AWS SDK ou une CLI
    - Utilisation DeleteOrganizationalUnit avec un AWS SDK ou une CLI
    - Utilisation DeletePolicy avec un AWS SDK ou une CLI
    - Utilisation DescribePolicy avec un AWS SDK ou une CLI
    - Utilisation DetachPolicy avec un AWS SDK ou une CLI
    - Utilisation ListAccounts avec un AWS SDK ou une CLI
    - Utilisation ListOrganizationalUnitsForParent avec un AWS SDK ou une CLI

# Exemples de base pour les Organisations utilisant AWS SDKs

Les exemples de code suivants montrent comment utiliser les principes de base de AWS Organizations with AWS SDKs.

Exemples

- Utilisation DescribePolicy avec un AWS SDK ou une CLI
- Utilisation DetachPolicy avec un AWS SDK ou une CLI
- Utilisation ListAccounts avec un AWS SDK ou une CLI
- Utilisation ListOrganizationalUnitsForParent avec un AWS SDK ou une CLI
- Utilisation ListPolicies avec un AWS SDK ou une CLI

## Actions pour les Organisations utilisant AWS SDKs

Les exemples de code suivants montrent comment effectuer des actions individuelles d'Organisations avec AWS SDKs. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Ces extraits appellent l'API Organizations et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Vous pouvez voir les actions dans leur contexte dans Scénarios destinés aux Organisations utilisant AWS SDKs.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, consultez la Référence des API AWS Organizations.

Exemples

- Utilisation AttachPolicy avec un AWS SDK ou une CLI
- Utilisation CreateAccount avec un AWS SDK ou une CLI
- Utilisation CreateOrganization avec un AWS SDK ou une CLI
- Utilisation CreateOrganizationalUnit avec un AWS SDK ou une CLI
- Utilisation CreatePolicy avec un AWS SDK ou une CLI
- Utilisation DeleteOrganization avec un AWS SDK ou une CLI
- Utilisation DeleteOrganizationalUnit avec un AWS SDK ou une CLI
- Utilisation DeletePolicy avec un AWS SDK ou une CLI
- Utilisation DescribePolicy avec un AWS SDK ou une CLI
- Utilisation DetachPolicy avec un AWS SDK ou une CLI
- Utilisation ListAccounts avec un AWS SDK ou une CLI
- Utilisation ListOrganizationalUnitsForParent avec un AWS SDK ou une CLI
- Utilisation ListPolicies avec un AWS SDK ou une CLI

## Utilisation **`AttachPolicy`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `AttachPolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-00000000";
        var targetId = "r-0000";

        var request = new AttachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };
```

```
            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
 Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Pour plus de détails sur l'API, voir AttachPolicyla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour attacher une stratégie à une racine, une unité d'organisation ou un compte

Exemple 1

L'exemple suivant montre comment attacher une politique de contrôle des services (SCP) à une unité d'organisation :

```
aws organizations attach-policy
               --policy-id p-examplepolicyid111
               --target-id ou-examplerootid111-exampleouid111
```

Exemple 2

L'exemple suivant montre comment attacher une politique de contrôle des services directement à un compte :

```
aws organizations attach-policy
               --policy-id p-examplepolicyid111
```

```
                --target-id 333333333333
```

- Pour plus de détails sur l'API, reportez-vous AttachPolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Pour plus de détails sur l'API, consultez AttachPolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
TRY.
    lo_org->attachpolicy(
      iv_policyid = iv_policy_id
      iv_targetid = iv_target_id ).
    MESSAGE 'Policy attached to target.' TYPE 'I'.
  CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to attach the policy.' TYPE 'E'.
  CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
  CATCH /aws1/cx_orgtargetnotfoundex.
    MESSAGE 'The specified target does not exist.' TYPE 'E'.
  CATCH /aws1/cx_orgduplicateplyatta00.
    MESSAGE 'The policy is already attached to the target.' TYPE 'E'.
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous AttachPolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`CreateAccount`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `CreateAccount`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates a new AWS Organizations account.
    /// </summary>
    public class CreateAccount
    {
        /// <summary>
        /// Initializes an Organizations client object and uses it to create
        /// the new account with the name specified in accountName.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
```

```
    }
```

- Pour plus de détails sur l'API, voir CreateAccountla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour créer un compte membre qui fait automatiquement partie de votre organisation

L'exemple suivant montre comment créer un compte membre dans une organisation. Le compte membre est configuré avec le nom Compte de production et l'adresse e-mail susan@example.com. Organizations crée automatiquement un rôle IAM en utilisant le nom par défaut, OrganizationAccountAccessRole car le paramètre RoleName n'est pas spécifié. En outre, le paramètre qui permet aux utilisateurs ou aux rôles IAM disposant d'autorisations suffisantes d'accéder aux données de facturation du compte est défini sur la valeur par défaut ALLOW car le IamUserAccessToBilling paramètre n'est pas spécifié. Organizations envoie automatiquement à Susan un e-mail « Bienvenue à AWS » :

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

La sortie inclut un objet de demande qui indique que l'état est désormais `IN_PROGRESS` :

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Vous pouvez ultérieurement demander l'état actuel de la demande en fournissant la valeur de réponse Id à la describe-create-account-status commande comme valeur du create-account-request-id paramètre.

Pour plus d'informations, consultez la section Création d'un AWS compte dans votre organisation dans le Guide de l'utilisateur AWS des Organizations.

- Pour plus de détails sur l'API, reportez-vous CreateAccountà la section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`CreateOrganization`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `CreateOrganization`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- Pour plus de détails sur l'API, voir CreateOrganizationla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Exemple 1 : pour créer une organisation

Bill souhaite créer une organisation à l'aide des informations d'identification du compte 111111111111. L'exemple suivant montre que le compte devient le compte principal de la nouvelle organisation. Comme il ne spécifie aucun ensemble de fonctionnalités, la nouvelle organisation utilise par défaut toutes les fonctionnalités activées et les politiques de contrôle des services sont activées à la racine.

```
aws organizations create-organization
```

La sortie inclut un objet d'organisation contenant des détails sur la nouvelle organisation :

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
```

```
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Exemple 2 : pour créer une organisation avec uniquement les fonctionnalités de facturation consolidée activées

L'exemple suivant crée une organisation qui prend uniquement en charge les fonctionnalités de facturation consolidée :

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

La sortie inclut un objet d'organisation contenant des détails sur la nouvelle organisation :

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Pour plus d'informations, consultez Création d'une organisation dans le Guide de l'utilisateur AWS  Organizations.

- Pour plus de détails sur l'API, reportez-vous CreateOrganizationà la section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`CreateOrganizationalUnit`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `CreateOrganizationalUnit`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
```

```
                Name = orgUnitName,
                ParentId = "r-0000",
            };

            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- Pour plus de détails sur l'API, voir CreateOrganizationalUnitla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour créer une unité d'organisation dans une unité d'organisation racine ou parente

L'exemple suivant montre comment créer une unité d'organisation nommée AccountingOU :

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

La sortie inclut un objet organizationalUnit contenant des détails sur la nouvelle unité d'organisation :

```
{
```

```
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateOrganizationalUnitàla section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`CreatePolicy`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `CreatePolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates a new AWS Organizations Policy.
    /// </summary>
    public class CreatePolicy
    {
        /// <summary>
```

```
        /// Initializes the AWS Organizations client object, uses it to
        /// create a new Organizations Policy, and then displays information
        /// about the newly created Policy.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyContent = "{" +
                "   \"Version\": \"2012-10-17\"," +
                " \"Statement\" : [{" +
                    " \"Action\" : [\"s3:*\"]," +
                    " \"Effect\" : \"Allow\"," +
                    " \"Resource\" : \"*\"" +
                "}]" +
            "}";

            try
            {
                var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
                {
                    Content = policyContent,
                    Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                    Name = "AllowAllS3Actions",
                    Type = "SERVICE_CONTROL_POLICY",
                });

                Policy policy = response.Policy;
                Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }
    }
```

- Pour plus de détails sur l'API, voir CreatePolicyla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Exemple 1 : pour créer une politique avec un fichier source texte pour la politique JSON

L'exemple suivant vous montre comment créer une politique de contrôle des services (SCP) nommée `AllowAllS3Actions`. Le contenu de la politique est extrait d'un fichier sur l'ordinateur local appelé `policy.json`.

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

La sortie inclut un objet de politique contenant des informations sur la nouvelle politique :

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

Exemple 2 : pour créer une politique avec une politique JSON en tant que paramètre

L'exemple suivant montre comment créer la même SCP, cette fois en intégrant le contenu de la politique sous forme de chaîne JSON dans le paramètre. La chaîne doit être échappée avec des barres obliques inversées avant les guillemets doubles pour qu'ils soient interprétés comme des caractères littéraux dans le paramètre, qui est lui-même entouré de guillemets doubles :

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
```

```
\":[\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

Pour plus d'informations sur la création et l'utilisation de politiques dans votre organisation, consultez Gestion des stratégies d'organisation dans le Guide de l'utilisateur AWS Organizations.

- Pour plus de détails sur l'API, reportez-vous CreatePolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
 before
                    it is sent to AWS. The specific format depends on the policy
 type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
```

```
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- Pour plus de détails sur l'API, consultez CreatePolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

## SAP ABAP

### Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        oo_result = lo_org->createpolicy(       " oo_result is returned for
testing purposes. "
          iv_name        = iv_policy_name
          iv_description = iv_policy_description
          iv_content     = iv_policy_content
          iv_type        = iv_policy_type ).
        MESSAGE 'Policy created.' TYPE 'I'.
      CATCH /aws1/cx_orgaccessdeniedex.
        MESSAGE 'You do not have permission to create a policy.' TYPE 'E'.
      CATCH /aws1/cx_orgduplicatepolicyex.
        MESSAGE 'A policy with this name already exists.' TYPE 'E'.
      CATCH /aws1/cx_orgmalformedplydocex.
        MESSAGE 'The policy content is malformed.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous CreatePolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`DeleteOrganization`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `DeleteOrganization`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Pour plus de détails sur l'API, voir DeleteOrganizationla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour supprimer une organisation

L'exemple suivant montre comment supprimer une organisation. Pour effectuer cette opération, vous devez être administrateur du compte principal de l'organisation. L'exemple suppose que vous avez précédemment supprimé tous les comptes et politiques des membres de l'organisation : OUs

```
aws organizations delete-organization
```

- Pour plus de détails sur l'API, reportez-vous DeleteOrganizationà la section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`DeleteOrganizationalUnit`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `DeleteOrganizationalUnit`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-00000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };

        var response = await client.DeleteOrganizationalUnitAsync(request);
```

```
            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Pour plus de détails sur l'API, voir DeleteOrganizationalUnitla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour supprimer une unité d'organisation

L'exemple suivant montre comment supprimer une unité d'organisation. L'exemple suppose que vous avez précédemment supprimé tous les comptes et autres comptes OUs de l'unité d'organisation :

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Pour plus de détails sur l'API, reportez-vous DeleteOrganizationalUnità la section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`DeletePolicy`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `DeletePolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);
```

```
            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- Pour plus de détails sur l'API, voir DeletePolicyla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour supprimer une politique

L'exemple suivant montre comment supprimer une stratégie d'une organisation. L'exemple suppose que vous avez préalablement détaché la stratégie de toutes les entités :

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Pour plus de détails sur l'API, reportez-vous DeletePolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Pour plus de détails sur l'API, consultez DeletePolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        lo_org->deletepolicy(
          iv_policyid = iv_policy_id ).
        MESSAGE 'Policy deleted.' TYPE 'I'.
      CATCH /aws1/cx_orgaccessdeniedex.
        MESSAGE 'You do not have permission to delete the policy.' TYPE 'E'.
      CATCH /aws1/cx_orgpolicynotfoundex.
        MESSAGE 'The specified policy does not exist.' TYPE 'E'.
      CATCH /aws1/cx_orgpolicyinuseex.
        MESSAGE 'The policy is still attached to one or more targets.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous DeletePolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`DescribePolicy`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `DescribePolicy`.

CLI

AWS CLI

Pour obtenir les informations sur une politique

L'exemple suivant montre comment demander des informations sur une politique :

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

La sortie inclut un objet de politique contenant des informations sur la politique :

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
```

```
}
```

- Pour plus de détails sur l'API, reportez-vous DescribePolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Pour plus de détails sur l'API, consultez DescribePolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       oo_result = lo_org->describepolicy(     " oo_result is returned for
testing purposes. "
         iv_policyid = iv_policy_id ).
       DATA(lo_policy) = oo_result->get_policy( ).
       MESSAGE 'Retrieved policy details.' TYPE 'I'.
     CATCH /aws1/cx_orgaccessdeniedex.
       MESSAGE 'You do not have permission to describe the policy.' TYPE 'E'.
     CATCH /aws1/cx_orgpolicynotfoundex.
       MESSAGE 'The specified policy does not exist.' TYPE 'E'.
   ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous DescribePolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`DetachPolicy`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `DetachPolicy`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };

        var response = await client.DetachPolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
```

```
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Pour plus de détails sur l'API, voir DetachPolicyla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour détacher une stratégie d'une racine, d'une unité d'organisation ou d'un compte

L'exemple suivant indique comment détacher une politique d'une unité d'organisation :

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Pour plus de détails sur l'API, reportez-vous DetachPolicyà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Pour plus de détails sur l'API, consultez DetachPolicyle AWS manuel de référence de l'API SDK for Python (Boto3).

## SAP ABAP

### Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        lo_org->detachpolicy(
          iv_policyid = iv_policy_id
          iv_targetid = iv_target_id ).
        MESSAGE 'Policy detached from target.' TYPE 'I'.
      CATCH /aws1/cx_orgaccessdeniedex.
        MESSAGE 'You do not have permission to detach the policy.' TYPE 'E'.
```

```
    CATCH /aws1/cx_orgpolicynotfoundex.
      MESSAGE 'The specified policy does not exist.' TYPE 'E'.
    CATCH /aws1/cx_orgtargetnotfoundex.
      MESSAGE 'The specified target does not exist.' TYPE 'E'.
    CATCH /aws1/cx_orgpolicynotattex.
      MESSAGE 'The policy is not attached to the target.' TYPE 'E'.
  ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous DetachPolicyà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`ListAccounts`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ListAccounts`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
```

```
        /// <summary>
        /// Creates the Organizations client and then calls its
        /// ListAccountsAsync method.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var request = new ListAccountsRequest
            {
                MaxResults = 5,
            };

            var response = new ListAccountsResponse();
            try
            {
                do
                {
                    response = await client.ListAccountsAsync(request);
                    response.Accounts.ForEach(a => DisplayAccounts(a));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations account.
        /// </summary>
        /// <param name="account">An Organizations account for which to display
        /// information on the console.</param>
        private static void DisplayAccounts(Account account)
        {
            string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";
```

```
            Console.WriteLine(accountInfo);
        }
    }
```

- Pour plus de détails sur l'API, voir ListAccountsla section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour extraire une liste de tous les comptes d'une organisation

L'exemple suivant vous montre comment demander une liste des comptes d'une organisation :

```
aws organizations list-accounts
```

La sortie comprend une liste d'objets de résumé de compte.

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
                        "Status": "ACTIVE"
```

```
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
}
```

- Pour plus de détails sur l'API, reportez-vous ListAccountsà la section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`ListOrganizationalUnitsForParent`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ListOrganizationalUnitsForParent`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Lists the AWS Organizations organizational units that belong to an
/// organization.
/// </summary>
public class ListOrganizationalUnitsForParent
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// call the ListOrganizationalUnitsForParentAsync method to retrieve
    /// the list of organizational units.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var parentId = "r-0000";

        var request = new ListOrganizationalUnitsForParentRequest
        {
            ParentId = parentId,
            MaxResults = 5,
        };

        var response = new ListOrganizationalUnitsForParentResponse();
        try
        {
```

```
                do
                {
                    response = await
client.ListOrganizationalUnitsForParentAsync(request);
                    response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations organizational unit.
        /// </summary>
        /// <param name="unit">The OrganizationalUnit for which to display
        /// information.</param>
        public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
        {
            string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

            Console.WriteLine(accountInfo);
        }
    }
```

- Pour plus de détails sur l'API, voir ListOrganizationalUnitsForParentla section Référence des AWS SDK pour .NET API.

## CLI

### AWS CLI

Pour récupérer une liste des OUs dans une unité d'organisation parent ou racine

L'exemple suivant montre comment obtenir une liste de OUs dans une racine spécifiée :

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

Le résultat indique que la racine spécifiée en contient deux OUs et indique le détail de chacune d'entre elles :

```
{
        "OrganizationalUnits": [
                {
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
        ]
}
```

- Pour plus de détails sur l'API, reportez-vous ListOrganizationalUnitsForParentà la section Référence des AWS CLI commandes.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Utilisation **`ListPolicies`** avec un AWS SDK ou une CLI

Les exemples de code suivants illustrent comment utiliser `ListPolicies`.

.NET

SDK pour .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
            MaxResults = 5,
        };
```

```
            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Pour plus de détails sur l'API, voir ListPolicieslа section Référence des AWS SDK pour .NET API.

CLI

AWS CLI

Pour extraire une liste de toutes les politiques d'une organisation d'un certain type

L'exemple suivant montre comment obtenir une liste de SCPs, comme indiqué par le paramètre de filtre :

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

La sortie inclut une liste des politiques avec des informations récapitulatives :

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- Pour plus de détails sur l'API, reportez-vous ListPoliciesà la section Référence des AWS CLI commandes.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Pour plus de détails sur l'API, consultez ListPolicieslе AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       oo_result = lo_org->listpolicies(       " oo_result is returned for
testing purposes. "
         iv_filter = iv_filter ).
       DATA(lt_policies) = oo_result->get_policies( ).
       MESSAGE 'Retrieved list of policies.' TYPE 'I'.
     CATCH /aws1/cx_orgaccessdeniedex.
       MESSAGE 'You do not have permission to list policies.' TYPE 'E'.
     CATCH /aws1/cx_orgawsorgsnotinuseex.
       MESSAGE 'Your account is not a member of an organization.' TYPE 'E'.
   ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous ListPoliciesà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Scénarios destinés aux Organisations utilisant AWS SDKs

Les exemples de code suivants vous montrent comment implémenter des scénarios courants dans Organizations with AWS SDKs. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'Organizations ou en les combinant avec d'autres Services AWS. Chaque exemple inclut un lien vers le code source complet, où vous trouverez des instructions sur la configuration et l'exécution du code.

Les scénarios ciblent un niveau d'expérience intermédiaire pour vous aider à comprendre les actions de service dans leur contexte.

Exemples

- Permet à la fonction Optimiseur de calcul AWS d'automatisation d'appliquer les actions recommandées
- Politique visant à permettre l'automatisation au sein de votre organisation
- Politique d'activation de l'automatisation pour votre compte
- Politique visant à accorder un accès complet à Compute Optimizer Automation pour un compte de gestion d'une organisation
- Politique visant à accorder un accès complet à Compute Optimizer Automation pour les comptes autonomes AWS
- Politique visant à accorder un accès en lecture seule à Compute Optimizer Automation pour un compte de gestion d'une organisation
- Politique visant à accorder un accès en lecture seule à Compute Optimizer Automation pour les comptes autonomes AWS
- Politique visant à accorder des autorisations de rôle liées à un service pour l'automatisation de l'optimisation du calcul

## Permet à la fonction Optimiseur de calcul AWS d'automatisation d'appliquer les actions recommandées

L'exemple de code suivant montre comment cette politique basée sur les autorisations permet à la fonctionnalité d' Optimiseur de calcul AWS automatisation d'appliquer les actions recommandées

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "aco-automation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Politique visant à permettre l'automatisation au sein de votre organisation

L'exemple de code suivant montre comment cette politique basée sur les autorisations permet l'automatisation au sein de votre organisation

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/aco-
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation",
            "Condition": {"StringLike": {"iam:AWSServiceName": "aco-
automation.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/aco-
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation"
        },
        {
            "Effect": "Allow",
            "Action": "aco-automation:UpdateEnrollmentConfiguration",
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "aco-automation:AssociateAccounts",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "aco-automation:DisassociateAccounts",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "aco-automation:ListAccounts",
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Politique d'activation de l'automatisation pour votre compte

L'exemple de code suivant montre comment cette politique basée sur les autorisations active l'automatisation de votre compte

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/aco-
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation",
            "Condition": {"StringLike": {"iam:AWSServiceName": "aco-
automation.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/aco-
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation"
        },
        {
            "Effect": "Allow",
            "Action": "aco-automation:UpdateEnrollmentConfiguration",
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Politique visant à accorder un accès complet à Compute Optimizer Automation pour un compte de gestion d'une organisation

L'exemple de code suivant montre comment cette politique basée sur les autorisations accorde un accès complet à Compute Optimizer Automation pour un compte de gestion d'une organisation

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "aco-automation:*",
               "ec2:DescribeVolumes",
               "organizations:ListAccounts",
               "organizations:DescribeOrganization",
               "organizations:DescribeAccount",
               "organizations:EnableAWSServiceAccess",
```

```
                "organizations:ListDelegatedAdministrators",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

## Politique visant à accorder un accès complet à Compute Optimizer Automation pour les comptes autonomes AWS

L'exemple de code suivant montre comment cette politique basée sur les autorisations accorde un accès complet à Compute Optimizer Automation pour les comptes autonomes AWS

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aco-automation:*",
            "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

# Politique visant à accorder un accès en lecture seule à Compute Optimizer Automation pour un compte de gestion d'une organisation

L'exemple de code suivant montre comment cette politique basée sur les autorisations accorde un accès en lecture seule à Compute Optimizer Automation pour un compte de gestion d'une organisation

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "aco-automation:GetEnrollmentConfiguration",
               "aco-automation:GetAutomationEvent",
               "aco-automation:GetAutomationRule",
               "aco-automation:ListAccounts",
               "aco-automation:ListAutomationEvents",
               "aco-automation:ListAutomationEventSteps",
               "aco-automation:ListAutomationEventSummaries",
               "aco-automation:ListAutomationRules",
               "aco-automation:ListAutomationRulePreview",
               "aco-automation:ListAutomationRulePreviewSummaries",
               "aco-automation:ListRecommendedActions",
               "aco-automation:ListRecommendedActionSummaries",
               "aco-automation:ListTagsForResource",
               "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

# Politique visant à accorder un accès en lecture seule à Compute Optimizer Automation pour les comptes autonomes AWS

L'exemple de code suivant montre comment cette politique basée sur les autorisations accorde un accès en lecture seule à Compute Optimizer Automation pour les comptes autonomes AWS

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "aco-automation:GetEnrollmentConfiguration",
               "aco-automation:GetAutomationEvent",
               "aco-automation:GetAutomationRule",
               "aco-automation:ListAutomationEvents",
               "aco-automation:ListAutomationEventSteps",
               "aco-automation:ListAutomationEventSummaries",
               "aco-automation:ListAutomationRules",
               "aco-automation:ListAutomationRulePreview",
               "aco-automation:ListAutomationRulePreviewSummaries",
               "aco-automation:ListRecommendedActions",
               "aco-automation:ListRecommendedActionSummaries",
               "aco-automation:ListTagsForResource",
               "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

# Politique visant à accorder des autorisations de rôle liées à un service pour l'automatisation de l'optimisation du calcul

L'exemple de code suivant montre comment cette politique basée sur les autorisations accorde des autorisations de rôle liées au service pour l'automatisation de l'optimisation du calcul

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/aco-
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation",
            "Condition": {"StringLike": {"iam:AWSServiceName": "aco-
automation.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/aco-
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation"
        }
    ]
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Organizations avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

# Historique du document pour AWS Organizations

Le tableau suivant décrit les principales mises à jour de la documentation pour AWS Organizations.

- Version de l'API : 2016-11-28
- Dernière mise à jour de la documentation : 30 mars 2026

| Modification | Description | Date |
| --- | --- | --- |
| Ajout du champ Path aux objets Account et UO | Les objets de compte et d'unité organisationnelle (UO) incluent désormais des informations de chemin dans les réponses de l'API. Le compte APIs (tel que `DescribeAccount` et`ListAccounts` ) et l'OU APIs (tel que`Describe0 rganizationalUnit` ) renvoient un champ de chemin indiquant où se trouvent les entités au sein d'une organisat ion. | 30 mars 2026 |
| Nouveaux services pris en charge dans RCPs | Ajout de services supplémen taires pris en charge par RCPs. | 23 janvier 2026 |
| Nouveau sujet sur les états du compte de surveillance | Ajout de conseils d'utilisa tion AWS Organizations pour surveiller de manière centralis ée l'état des comptes sur tous les comptes de votre organisat ion, tels que les comptes actifs, suspendus ou fermés, à | 9 septembre 2025 |

| | | |
|---|---|---|
| | partir de la console, de la CLI et SDKs. | |
| Politiques Security Hub ajoutées | Vous pouvez utiliser les politiques du Security Hub pour gérer de manière centralisée les configura tions du Security Hub dans votre environnement AWS Organizations. Ces politiques vous aident à activer les fonctionnalités et à maintenir des contrôles de sécurité cohérents sur plusieurs comptes de votre organisation. | 17 juin 2025 |
| Mise à jour de la politique AWSOrganizations FullAccess gérée | Ajout de l'`account:GetAccountInformation` action permettant d'autoriser l'accès pour afficher le nom de compte de n'importe quel compte dans une organisation et de l'`account:PutAccountName` action pour permettre l'accès pour modifier n'importe quel nom de compte dans une organisation. | 22 avril 2025 |
| Organisations : intégration avec Notifications des utilisateurs AWS | Vous pouvez l'intégrer Notifications des utilisateurs AWS Organizations pour configurer et afficher les notifications de manière centralisée sur tous les comptes de votre organisation. | 24 janvier 2025 |

| | | |
|---|---|---|
| Organisations intégrées à AWS Managed Services (AMS) Self-Service Reporting (SSR) | Vous pouvez intégrer AMS SSR AWS Organizations pour activer les rapports agrégés en libre-service (SSR). Il s'agit d'une fonctionnalité AMS qui permet aux clients d'Advanced et d'Accelerate de consulter leurs rapports en libre-service existants agrégés au niveau de l'organisation, entre comptes. | 21 janvier 2025 |
| Politiques déclaratives ajoutées | Vous pouvez utiliser des politiques déclaratives pour déclarer et appliquer de manière centralisée les configurations souhaitées pour une donnée Service AWS à grande échelle au sein d'une organisation. Une fois connectée, la configuration est toujours maintenue lorsque le service ajoute de nouvelles fonctionnalités ou APIs. | 1er décembre 2024 |
| Nouvelle politique AWS gérée | Ajout de la `DeclarativePoliciesEC2Report` politique permettant d'activer les fonctionnalités du rôle lié au declarative-policies-ec service 2.amazonaws.com. | 22 novembre 2024 |

| | | |
|---|---|---|
| Politiques de sauvegarde mises à jour | AWS Backup les politiques ont mis à jour la `selections` clé de `conditions` stratégie pour inclure une clé de stratégie et ont ajouté une nouvelle clé de `resources` stratégie au schéma. Avec le nouveau schéma, vous disposez d'une plus grande flexibilité dans la sélection des ressources pour vos politiques de sauvegarde. | 14 novembre 2024 |
| Gestion centralisée de l'accès root pour les comptes membres | Vous pouvez désormais gérer les informations d'identification des utilisateurs racine privilégiés sur l'ensemble des comptes membres d'AWS Organizations grâce à un accès root centralisé. Sécurisez de manière centralisée les informations d'identification de l'utilisateur root de votre compte Comptes AWS géré AWS Organizations pour supprimer et empêcher la récupération des informations d'identification de l'utilisateur root et l'accès à grande échelle. | 14 novembre 2024 |

| | | |
|---|---|---|
| Politiques de contrôle des ressources ajoutées (RCPs) | Vous pouvez utiliser les politiques de contrôle des ressources (RCPs) pour contrôler le maximum d'autorisations disponibles pour les ressources d'une organisation. | 13 novembre 2024 |
| Règles relatives aux applications de chat ajoutées | Vous pouvez utiliser les politiques des applications de chat pour contrôler l'accès aux comptes de votre organisation à partir d'applications de chat telles que Slack et Microsoft Teams. | 26 septembre 2024 |
| Mises à jour de contenu basées sur des scénarios | La AWS Organizations documentation a été mise à jour pour être davantage axée sur des scénarios tout au long du guide et le contenu a été réorganisé pour améliorer la lisibilité et la découverte. Si vous avez des commentaires sur ces modifications, utilisez le bouton Envoyer des commentaires en bas de page. | 4 septembre 2024 |
| Nouvelle option de désabonnement à tous les services d'IA | Ajout d'une documentation expliquant comment se désinscrire de tous les services d' AWS IA pris en charge. | 16 août 2024 |

| | | |
|---|---|---|
| Organizations prend désormais en charge 10 000 comptes au sein d'une organisation | Vous pouvez désormais gérer jusqu'à 10 000 comptes membres dans une organisation, soit le double de la limite précédente de 5 000 comptes. Si vos exigences et vos besoins commerciaux sont valides, vous pouvez demander et obtenir une approbation pour un quota de 10 000 comptes sans vérification des limites de service auprès des Organizations ou d'autres entités intégrées Services AWS. | 14 août 2024 |
| Nouveau sujet sur la migration des comptes | Ajout de documentation sur la façon de migrer un compte d'une organisation à une autre. | 1er août 2024 |
| Politiques de sauvegarde mises à jour | AWS Backup les politiques prennent désormais en charge les archives instantanées Amazon Elastic Block Store (Amazon EBS). Pour des exemples mis à jour, consultez les sections Mise à jour d'une politique de sauvegarde et Syntaxe et exemples de stratégie de sauvegarde. | 9 juillet 2024 |

| | | |
|---|---|---|
| Mise à jour de la politique AWSOrganizations ReadOnlyAccess gérée | Ajout de l'`account:GetPrimaryEmail` action à la AWSOrganizations ReadOnlyAccess politique qui permet d'accéder à l'adresse e-mail de l'utilisateur root pour n'importe quel compte membre d'une organisation et ajout de l'`account:GetRegionOptStatus` action permettant d'accéder à l'affichage des régions activées pour n'importe quel compte membre d'une organisation. | 6 juin 2024 |
| Nouvelle mise à jour de l'adresse e-mail de l'utilisateur root (rubrique « » ) | Organizations offre désormais la possibilité de mettre à jour de manière centralisée l'adresse e-mail de l'utilisateur root () pour tout compte membre d'une organisation. | 6 juin 2024 |
| Déclarations de politique mises à jour | De nouveaux `Sid` éléments ont été ajoutés aux déclarations de politique AWS Organizations gérées. | 6 février 2024 |
| Nouveau sujet relatif à la fermeture d'un compte de gestion | Ajout de liens vers des considérations et des étapes détaillées expliquant comment fermer un compte de gestion. | 1er février 2024 |
| Mise à jour des bonnes pratiques | De nouvelles informations ont été ajoutées à la section des bonnes pratiques pour faciliter l'alignement sur les bonnes pratiques de l'IAM. | 12 juin 2023 |

| | | |
|---|---|---|
| Politiques mises à jour AWSOrganizations FullAccess et AWSOrganizations ReadOnlyAccess gérées | Les deux stratégies gérées ont été mises à jour pour permettre l'accès en écriture ou en lecture aux coordonnées des comptes. | 21 octobre 2022 |
| Mise à jour de la politique AWSOrganizations FullAccess gérée | La politique gérée a été mise à jour pour permettre la création d'une organisation en ajoutant l'autorisation requise pour créer le rôle lié au service requis par une nouvelle organisation. | 24 août 2022 |
| Organisations clôturant la fonctionnalité des comptes depuis la AWS Organizations console | Les principaux du compte de gestion peuvent clôturer les comptes de membres à partir de la console AWS Organizations , et protégez les comptes membres contre la clôture accidentelle à l'aide de politiques IAM. | 29 mars 2022 |
| Annonce mise à jour pour mettre à jour les contacts alternatifs avec AWS Organizations la console | Organizations permet désormais de mettre à jour les contacts alternatifs pour les comptes de votre organisation à l'aide de la AWS Organizations console. Annoncez une nouvelle fonctionnalité et pointez vers Référence de gestion de comptes pour obtenir des instructions. | 8 février 2022 |

| | | |
|---|---|---|
| Mises à jour de la politique gérée par Organizations : mise à jour d’une politique existante | Mise à jour des politiques AWSOrganizations FullAccess et AWSOrganizations ReadOnlyAccess gestion des politiques afin d'autoriser les autorisations d'API du compte requises pour mettre à jour ou consulter les contacts alternatifs du compte via la AWS Organizations console. | 7 février 2022 |
| Organisations : intégration avec Amazon DevOps Guru | Vous pouvez intégrer Amazon DevOps Guru AWS Organizations pour surveiller l'état des applications de manière globale sur tous les comptes de votre entreprise et obtenir des informations. | 3 janvier 2022 |
| Intégration d’Organizations à Amazon Detective | Vous pouvez intégrer Amazon Detective AWS Organizations pour vous assurer que votre graphe de comportement de Detective fournit une visibilité sur l'activité de tous les comptes de votre organisation. | 16 décembre 2021 |

| | | |
|---|---|---|
| Organizations Integration with AWS Config Now prend en charge l'agrégation de données multi-comptes et multirégions. | Vous pouvez utiliser un compte d'administrateur délégué pour agréger les données de conformité et de configuration des ressources de tous les comptes membres de votre organisation. Pour plus d'informations, consultez Regroupement de données multi-comptes et multi-régions dans le AWS Config Guide du développeur. | 16 juin 2021 |
| Organisations : l'intégration à AWS Firewall Manager Now inclut la prise en charge d'un administrateur délégué | Vous pouvez désormais désigner un compte membre de votre organisation comme administrateur de Firewall Manager pour l'ensemble de l'organisation. Cela permet une meilleure séparation des autorisations du compte de gestion de l'organisation. | 30 avril 2021 |
| Les politiques de sauvegarde d'Organizations prennent désormais en charge la sauvegarde continue. | Vous pouvez utiliser la fonctionnalité de sauvegarde AWS Backup continue avec les politiques de sauvegarde de votre entreprise. | 10 mars 2021 |

| | | |
|---|---|---|
| Organisations : l'intégration à AWS CloudFormation StackSets Now inclut la prise en charge d'un administrateur délégué | Vous pouvez désormais désigner un compte membre de votre organisation comme CloudFormation StackSets administrateur de l'ensemble de l'organisation. Cela permet une meilleure séparation des autorisations du compte de gestion de l'organisation. | 18 février 2021 |
| Continuez à inviter des comptes tout en activant toutes les fonctionnalités | AWS a mis à jour le processus pour activer toutes les fonctionnalités d'une organisation. Vous pouvez maintenant continuer à inviter de nouveaux comptes à rejoindre votre organisation pendant que vous attendez que les comptes existants répondent à leur invitation. | 3 février 2021 |
| Présente la version 2.0 de la AWS Organizations console | AWS a introduit une nouvelle version de la AWS console. Toute la documentation a été mise à jour pour refléter la nouvelle façon d'effectuer les tâches. | 21 janvier 2021 |
| Organizations prend désormais en charge l'intégration avec AWS Marketplace | Vous pouvez désormais AWS Marketplace partager plus facilement vos licences logicielles entre tous les comptes de votre organisation. | 3 décembre 2020 |

| | | |
|---|---|---|
| Organizations prend désormais en charge l'intégration à Amazon S3 Lens | Amazon S3 Lens prend en charge à la fois l'accès sécurisé et un administrateur délégué avec Organizations. Pour plus d'informations, consultez Amazon S3 Storage Lens dans le Guide de l'utilisateur Amazon Simple Storage Service. | 18 novembre 2020 |
| Copies de sauvegarde entre comptes | Lorsque vous utilisez des politiques de sauvegarde pour sauvegarder les ressources de votre organisation, vous pouvez désormais stocker des copies de votre sauvegarde dans un autre Comptes AWS service de l'organisation. | 18 novembre 2020 |
| Régions AWS en Chine, le support AWS Resource Access Manager est désormais un service fiable pour les Organisations | Vous pouvez désormais utiliser les AWS RAM fonctionnalités qui s'intègrent à Organizations en tant que service fiable lorsque vous utilisez Organizations et AWS RAM en Chine. | 18 novembre 2020 |
| Organizations prend désormais en charge l'intégration avec AWS Security Hub CSPM | Vous pouvez activer Security Hub CSPM sur tous les comptes de votre organisation et désigner l'un des comptes membres de votre organisation comme compte d'administrateur délégué pour Security Hub CSPM. | 12 novembre 2020 |

| | | |
|---|---|---|
| Changement de nom du compte principal | AWS Organizations a changé le nom du « compte principal » en « compte de gestion ». Seul le nom a été changé, la fonctionnalité demeure inchangée. | 20 octobre 2020 |
| Nouvelle section et nouvelles rubriques sur les bonnes pratiques | Une section a été ajoutée présentant les bonnes pratiques de AWS Organizations. La nouvelle section comprend des rubriques qui traitent des bonnes pratiques pour les utilisateurs racines du compte de gestion et des comptes membres ainsi que pour la gestion des mots de passe. | 6 octobre 2020 |
| Ajout d'une nouvelle section sur les bonnes pratiques et de deux premières pages | Une nouvelle section présente des sujets relatifs aux bonnes pratiques de AWS Organizations. Cette mise à jour inclut une rubrique sur les bonnes pratiques pour le compte de gestion d'une organisation et une rubrique sur les bonnes pratiques pour les comptes membres. | 2 octobre 2020 |

| | | |
|---|---|---|
| Les politiques de sauvegarde d'Organizations prennent désormais en charge les sauvegardes cohérentes entre applications sur les instances Windows EC2 en utilisant VSS (Volume Shadow Copy Service). | Les politiques de sauvegarde prennent en charge une nouvelle section « `advanced_backup_settings` ». La première entrée de cette nouvelle section est un paramètre de `ec2` appelé `WindowsVSS` que vous pouvez activer ou désactiver. Pour plus d'informations, consultez Création d'une sauvegarde Windows avec VSS dans le AWS Backup Manuel du développeur. | 24 septembre 2020 |
| Organisations : supports tag-on-create et contrôle d'accès basé sur des balises | Vous pouvez ajouter des balises aux ressources Organizations lors de leur création. Vous pouvez utiliser des politiques de balises pour standardiser l'utilisation des balises associées aux ressources Organizations. Vous pouvez utiliser des politiques IAM pour restreindre l'accès aux ressources ayant des clés de balise et des valeurs spécifiées. | 15 septembre 2020 |
| Ajouté AWS Health en tant que service de confiance | Vous pouvez agréger AWS Health les événements entre les comptes de votre organisation. | 4 août 2020 |

| | | |
|---|---|---|
| Politiques de désactivation des services d'intelligence artificielle (IA) | Vous pouvez utiliser les politiques de désinscription des services d' AWS IA pour contrôler si les services d'IA peuvent stocker et utiliser le contenu client traité par ces services (contenu d'IA) pour le développement et l'amélioration continue des services et technologies d' AWS IA. | 8 juillet 2020 |
| Politiques de sauvegarde ajoutées et intégration avec AWS Backup | Vous pouvez utiliser des politiques de sauvegarde pour créer et appliquer des politiques de sauvegarde sur tous les comptes de votre organisation. | 24 juin 2020 |
| Prise en charge de l'administration déléguée pour IAM Access Analyzer | Permet de déléguer l'accès administratif pour Access Analyzer à un compte membre désigné dans votre organisation. | 30 mars 2020 |
| Intégration avec CloudFormation StackSets | Vous pouvez créer un jeu de piles géré par le service pour déployer des instances de pile sur des comptes gérés par AWS Organizations. | 11 février 2020 |
| Intégration à Compute Optimizer | Compute Optimizer a été ajouté en tant que service pouvant fonctionner avec des comptes de votre organisation. | 4 février 2020 |

| | | |
|---|---|---|
| Stratégies de balises | Vous pouvez utiliser des politiques de balises pour vous aider à standardiser les balises entre les ressource s des comptes de votre organisation. | 26 novembre 2019 |
| Intégration à Systems Manager | Vous pouvez synchroniser les données d'exploitation Comptes AWS dans l'ensembl e de votre organisation dans Systems Manager Explorer. | 26 novembre 2019 |
| lois : PrincipalOrgPaths | La nouvelle clé de condition globale vérifie le AWS Organizations chemin de l'utilisateur IAM, du rôle IAM ou de l'utilisateur Compte AWS root qui fait la demande. | 20 novembre 2019 |
| Intégration avec les AWS Config règles | Vous pouvez utiliser les opérations d' AWS Config API pour gérer les AWS Config règles Comptes AWS dans l'ensemble de votre organisat ion. | 8 juillet 2019 |
| Nouveau service pour un accès de confiance | Service Quotas a été ajouté en tant que service pouvant fonctionner avec les comptes de votre organisation. | 24 juin 2019 |
| Intégration à AWS Control Tower | AWS Control Tower a été ajoutée en tant que service pouvant fonctionner avec les comptes de votre organisation. | 24 juin 2019 |

| | | |
|---|---|---|
| Intégration avec Gestion des identités et des accès AWS | IAM fournit les données du dernier accès au service pour les entités de votre organisation (racine de l'organisation et comptes). OUs Vous pouvez utiliser ces données pour restreindre l'accès uniquement à Services AWS ce dont vous avez besoin. | 20 juin 2019 |
| Balisage des comptes | Vous pouvez ajouter et supprimer les balises de comptes de votre organisation et également afficher les balises d'un compte de votre organisation. | 6 juin 2019 |
| Ressources, conditions et `NotAction` élément des politiques de contrôle des services (SCPs) | Vous pouvez désormais spécifier les ressources, les conditions et l'`NotAction` élément dans SCPs lequel refuser l'accès aux comptes de votre organisation ou unité organisationnelle (UO). | 25 mars 2019 |
| Nouveaux services pour un accès de confiance | AWS License Manager et Service Catalog ajoutés en tant que services pouvant fonctionner avec les comptes de votre organisation. | 21 décembre 2018 |
| Nouveaux services pour un accès de confiance | AWS CloudTrail et AWS RAM ajoutés en tant que services compatibles avec les comptes de votre organisation. | 4 décembre 2018 |

| | | |
|---|---|---|
| Nouveau service pour un accès de confiance | Directory Service ajouté en tant que service pouvant fonctionner avec les comptes de votre organisation. | 25 septembre 2018 |
| Vérification de l'adresse e-mail | Vous devez vérifier que vous possédez l'adresse e-mail associée au compte de gestion avant de pouvoir inviter des comptes existants dans votre organisation. | 20 septembre 2018 |
| CreateAccount notifications | `CreateAccount` les notifications sont publiées dans les CloudTrail journaux du compte de gestion. | 28 juin 2018 |
| Nouveau service pour un accès de confiance | AWS Artifact ajouté en tant que service pouvant fonctionner avec les comptes de votre organisation. | le 20 juin 2018 |
| Nouveaux services pour un accès de confiance | AWS Config et AWS Firewall Manager ajoutés en tant que services compatibles avec les comptes de votre organisation. | 18 avril 2018 |
| Accès aux services de confiance | Vous pouvez désormais activer ou désactiver l'accès Services AWS à Select pour qu'il fonctionne dans les comptes de votre organisation. IAM Identity Center est le service de confiance initialement pris en charge. | 29 mars 2018 |

| | | |
|---|---|---|
| La suppression de compte se fait désormais en libre-service | Vous pouvez désormais supprimer des comptes créés de l'intérieur AWS Organizations sans avoir à nous contacter AWS Support. | 19 décembre 2017 |
| Support supplémentaire pour le nouveau service AWS IAM Identity Center | AWS Organizations prend désormais en charge l'intégration avec AWS IAM Identity Center (IAM Identity Center). | 7 décembre 2017 |
| AWS a ajouté un rôle lié à un service à tous les comptes de l'organisation | Un rôle lié à un service nommé `AWSServiceRoleForOrganizations` est ajouté à tous les comptes d'une organisation pour permettre l'intégration entre AWS Organizations eux. Services AWS | 11 octobre 2017 |
| Vous pouvez désormais supprimer les comptes créés | À présent, les clients peuvent supprimer les comptes créés de leur organisation, avec l'aide de AWS Support. | 15 juin 2017 |
| Lancement de service | Version initiale de la AWS Organizations documentation accompagnant le lancement du nouveau service. | 17 février 2017 |

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.