Guide de l’utilisateur

AWS Organizations

AWS Organizations: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'AWS Organizations ?

AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs Comptes AWS en une organisation que vous créez et gérez de façon centralisée. AWS Organizations inclut toutes les fonctions de facturation consolidée et de gestion de comptes, qui vous permettent de mieux répondre aux besoins budgétaires, de sécurité et de conformité de votre entreprise. En tant qu'administrateur d'une organisation, vous pouvez créer des comptes dans votre organisation et inviter des comptes existants à rejoindre l'organisation.

Ce guide de l'utilisateur définit les concepts clés pour AWS Organizations, fournit des didacticiels et explique comment créer et gérer une organisation.

Rubriques

Fonctions d'AWS Organizations

AWS Organizations offre les fonctions suivantes :

Gestion centralisée de tous vos Comptes AWS

> Vous pouvez combiner vos comptes existants en une organisation qui vous permet de gérer les comptes de manière centralisée. Vous pouvez créer des comptes qui font automatiquement partie de votre organisation et inviter d'autres comptes à rejoindre votre organisation. Vous pouvez également attacher des politiques qui concernent tous vos comptes ou certains d'entre eux.

La facturation consolidée pour tous les comptes membres

> La facturation consolidée est une fonction d'AWS Organizations. Vous pouvez utiliser le compte de gestion de votre organisation pour consolider et payer pour tous les comptes membres. Dans la facturation consolidée, les comptes de gestion peuvent également accéder aux informations de facturation, aux informations de compte et à l'activité des comptes membres de leur organisation. Ces informations peuvent être utilisées pour des services tels que Cost Explorer, qui peuvent aider les comptes de gestion à améliorer les performances de coûts de leur organisation.

Le groupement hiérarchique de vos comptes pour répondre à vos besoins budgétaires, de sécurité et de conformité

Vous pouvez regrouper vos comptes en unités d'organisation (UO) et attacher différentes politiques d'accès à chaque unité d'organisation. Par exemple, si vous disposez de comptes qui doivent uniquement accéder aux services AWS répondant à certaines exigences réglementaires, vous pouvez regrouper ces comptes en une unité d'organisation. Vous pouvez ensuite attacher une politique à cette unité d'organisation qui bloque l'accès aux services qui ne répondent pas à ces exigences réglementaires. Vous pouvez imbriquer des unités d'organisation dans d'autres unités d'organisation, à une profondeur de cinq niveaux, ce qui vous permet de profiter d'une certaine flexibilité dans la façon dont vous structurez vos groupes de comptes.

Politiques de centralisation du contrôle des services et actions d'API AWS auxquels chaque compte peut accéder

En tant qu'administrateur du compte de gestion d'une organisation, vous pouvez utiliser des politiques de contrôle des services (SCP) pour spécifier les autorisations maximales des comptes membres de l'organisation. Dans les politiques de contrôle des services, vous pouvez limiter les services, ressources et actions d'API AWS individuels auxquels les utilisateurs et rôles de chaque compte membre peuvent accéder. Vous pouvez également définir des conditions de restriction de l'accès aux services, ressources et actions d'API AWS. Ces restrictions prennent le pas même sur les administrateurs des comptes membres dans l'organisation. Lorsque AWS Organizations bloque l'accès à un service, une ressource ou une action d'API pour un compte membre, un utilisateur ou un rôle de ce compte ne peut pas y accéder. Ce blocage reste actif même si l'administrateur d'un compte membre accorde explicitement de telles autorisations dans une politique IAM.

Pour de plus amples informations, consultez Politiques de contrôle de service (SCP).

Politiques d'uniformisation des balises entre les ressources des comptes de votre organisation

Vous pouvez utiliser des politiques de balises pour maintenir la cohérence des balises, notamment le traitement de la casse privilégié des clés et des valeurs de balise.

Pour plus d'informations, veuillez consulter Politiques de balises

Politiques de contrôle de la façon dont les services d'intelligence artificielle (IA) et de machine learning AWS peuvent collecter et stocker des données.

Vous pouvez utiliser des politiques de désactivation des services IA pour refuser la collecte et le stockage des données pour tout service IA AWS que vous ne souhaitez pas utiliser.

Pour plus d'informations, veuillez consulter Politiques de désactivation des services IA

Politiques configurant des sauvegardes automatiques des ressources des comptes de votre organisation

Vous pouvez utiliser des politiques de sauvegarde pour configurer et appliquer automatiquement des plans AWS Backup aux ressources de tous les comptes de votre organisation.

Pour plus d'informations, veuillez consulter Politiques de sauvegarde

Intégration et prise en charge d'AWS Identity and Access Management (IAM)

IAM fournit un contrôle granulaire des utilisateurs et rôles des comptes individuels. AWS Organizations développe ce contrôle au niveau des comptes en vous permettant de contrôler les actions des utilisateurs et rôles d'un compte ou d'un groupe de comptes. Les autorisations obtenues constituent l'intersection logique de ce qui est autorisé par AWS Organizations au niveau du compte et des autorisations explicitement accordées par IAM au niveau des utilisateurs ou des rôles au sein de ce compte. En d'autres termes, l'utilisateur peut uniquement accéder à ce qui est autorisé à la fois par les politiques AWS Organizations et les politiques IAM. Si l'une ou l'autre bloque une opération, l'utilisateur ne peut pas accéder à cette opération.

Vous pouvez exploiter facilement d'autres services AWS

Vous pouvez tirer parti des services de gestion multicomptes disponibles dans AWS Organizations avec certains services AWS pour réaliser des tâches sur tous les comptes membres d'une organisation. Pour connaître la liste des services et les avantages de l'utilisation de chaque service à l'échelle de l'organisation, consultez AWS services que vous pouvez utiliser avec AWS Organizations.

Lorsque vous activez un service AWS pour exécuter des tâches en votre nom dans les comptes membres de votre organisation, AWS Organizations crée un rôle lié à un service IAM pour ce service dans chaque compte membre. Le rôle lié à un service possède des autorisations IAM prédéfinies qui permettent à l'autre service AWS d'effectuer des tâches spécifiques dans votre organisation et ses comptes. Pour que cela fonctionne, tous les comptes d'une organisation possèdent automatiquement un rôle lié au service. Ce rôle permet au service AWS Organizations de créer les rôles liés au service requis par les services AWS pour lesquels vous activez l'accès approuvé. Ces rôles liés au service supplémentaires sont attachés à des politiques d'autorisation IAM permettant au service spécifié de réaliser uniquement les tâches requises par vos choix de configuration. Pour plus d'informations, consultez Utilisation d'AWS Organizations avec d'autres services AWS.

Accès mondial

AWS Organizations est un service mondial avec un point de terminaison unique qui fonctionne à partir de toutes les Régions AWS. Vous n'avez pas besoin de sélectionner explicitement une région dans laquelle opérer.

Réplication des données qui est finalement cohérente

AWS Organizations, comme beaucoup d'autres services AWS, est cohérent à terme. AWS Organizations garantit une haute disponibilité en répliquant les données sur plusieurs serveurs dans des centres de données AWS de sa région. Si une demande de modification de certaines données aboutit, la modification est validée et stockée en toute sécurité. Toutefois, la modification doit alors être répliquée sur plusieurs serveurs. Pour plus d'informations, consultez Les modifications que j'apporte ne sont pas toujours visibles immédiatement.

Gratuité

AWS Organizations est une fonctionnalité de votre Compte AWS proposée sans frais supplémentaires. Vous payez uniquement lorsque vous accédez à d'autres services AWS à partir des comptes de votre organisation. Pour obtenir des informations sur la tarification d'autres produits AWS, veuillez consulter la page de tarification Amazon Web Services.

Tarification d'AWS Organizations

AWS Organizations est fourni sans frais supplémentaires. Vous payez uniquement pour les ressources AWS que les utilisateurs et rôles de vos comptes membres utilisent. 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 des informations sur la tarification des autres services AWS, consultez Tarification d'AWS.

Accès à AWS Organizations

Vous pouvez utiliser AWS Organizations de l'une des façons suivantes :

AWS Management Console

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

Outils de ligne de commande AWS

Grâce aux outils de ligne de commande AWS, vous pouvez envoyer des commandes à la ligne de commande de votre système afin d'effectuer des tâches AWS Organizations et AWS. 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 jeux d'outils de ligne de commande :

- AWS Command Line Interface (AWS CLI). Pour plus d'informations sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur AWS Command Line Interface.
- AWS Tools for Windows PowerShell. Pour plus d'informations sur l'installation et l'utilisation des outils Tools for Windows PowerShell, consultez le Guide de l'utilisateur AWS Tools for Windows PowerShell.

Kits SDK AWS

Les kits SDK AWS se composent de bibliothèques et d'exemples de code pour différents langages et plateformes de programmation (Java, Python, Ruby, .NET, iOS et Android, par exemple). Ils automatisent les tâches telles que la signature cryptographique des demandes, la gestion des erreurs et les nouvelles tentatives de demande automatiques. Pour de plus amples informations sur les kits SDK AWS, y compris les procédures pour les télécharger et les installer, consultez Outils pour Amazon Web Services.

API de requête HTTPS AWS Organizations

L'API de requête HTTPS AWS Organizations vous donne un accès par programme 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.

Support et commentaires pour AWS Organizations

Nous apprécions vos commentaires. Vous pouvez envoyer vos commentaires à feedback-awsorganizations@amazon.com. Vous pouvez également publier vos commentaires et vos questions sur le forum de support AWS Organizations. Pour de plus amples informations sur les forums de support AWS, consultez l'aide des forums.

Autres ressources AWS

- Formation et cours AWS : des liens vers des formations spécialisées et basées sur les rôles, ainsi que des ateliers d'autoformation pour améliorer vos compétences AWS et acquérir une expérience pratique.
- Outils de développement AWS : des liens vers des outils et ressources de développement qui fournissent une documentation, des exemples de code, des notes de mise à jour et d'autres informations pour vous aider à développer des applications innovantes avec AWS.
- Centre de support AWS Support : hub pour la création et la gestion de vos cas de support AWS. Inclut également des liens vers d'autres ressources utiles, telles que des forums, des FAQ techniques, l'état d'un service et AWS Trusted Advisor.
- Support AWS : principale page Web d'informations à propos du Support AWS, un canal d'assistance technique individuelle rapide pour vous aider à développer et à exécuter des applications dans le cloud.
- Contactez-nous : point de contact central pour toute question relative à la facturation AWS, à votre compte, aux événements, à des abus ou à d'autres problèmes.
- Conditions d'utilisation du site AWS : informations détaillées sur nos droits d'auteur et notre marque, sur votre compte, votre licence et votre accès au site, et sur d'autres sujets.

Démarrer avec AWS Organizations

Les rubriques suivantes fournissent des informations pour vous aider à démarrer l'apprentissage et l'utilisation de AWS Organizations.

En savoir plus sur ...

Terminologie et concepts relatifs à AWS Organizations

Découvrez la terminologie et les concepts fondamentaux nécessaires pour comprendre AWS Organizations. Cette section décrit chacun des composants d'une organisation et les bases de la façon dont ils collaborent pour fournir un nouveau niveau de contrôle sur ce que les utilisateurs de ces comptes peuvent faire.

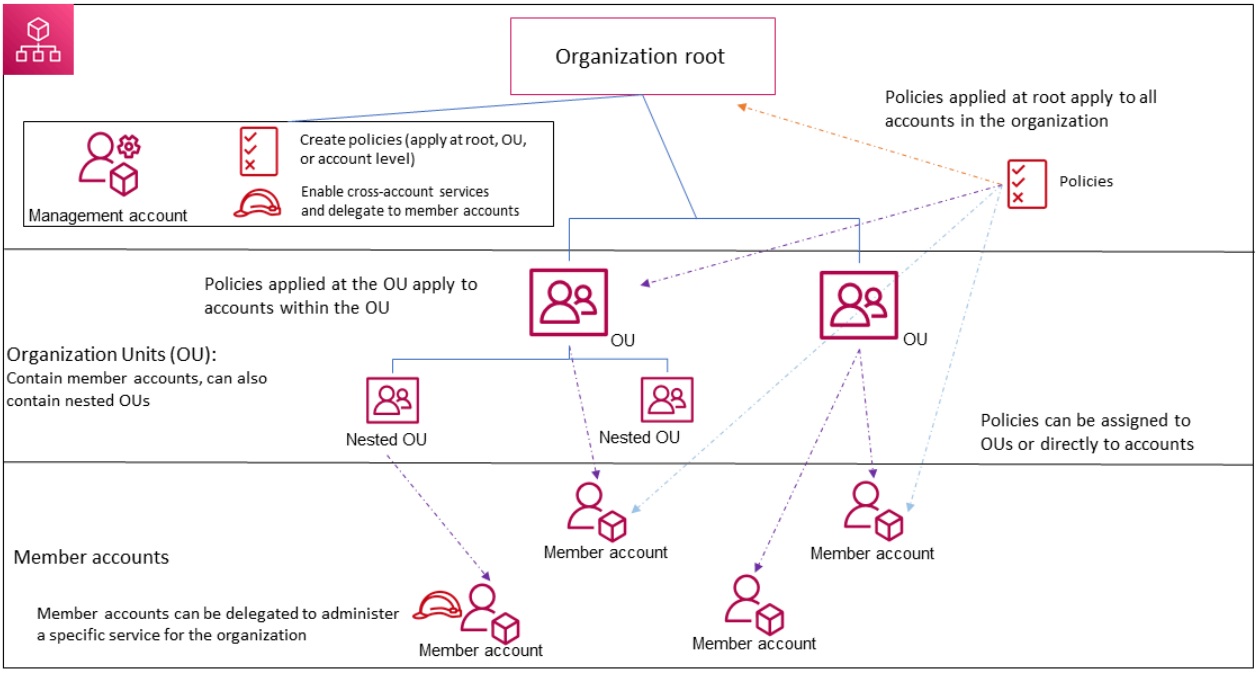
Facturation consolidée pour les organisations

L'une des principales fonctionnalités relatives à AWS Organizations est la consolidation de la facturation de tous les comptes de votre organisation. Découvrez-en plus sur la façon dont la facturation est gérée dans une organisation et sur la manière dont les différentes remises fonctionnent en cas de partage entre plusieurs comptes. Ce contenu se trouve dans le Guide de l'utilisateur AWS Billing.

Terminologie et concepts relatifs à AWS Organizations

Pour vous aider à démarrer avec AWS Organizations, cette rubrique explique certains des concepts clés.

Le diagramme suivant illustre une organisation de base qui comprend cinq comptes organisés en quatre unités d'organisation sous la racine. L'organisation possède également plusieurs politiques attachées à certaines unités d'organisation ou directement aux comptes. Pour une description de chacun de ces éléments, reportez-vous aux définitions de cette rubrique.



Organisation

Une entité que vous créez pour consolider vos comptes AWS de manière à pouvoir les administrer comme une seule unité. Vous pouvez utiliser la console AWS Organizations de façon centralisée pour afficher et gérer tous vos comptes au sein de votre organisation. Une organisation possède un compte de gestion avec zéro ou plusieurs comptes membres. Vous pouvez organiser les comptes dans une structure hiérarchique de type arborescente, avec une racine en haut et des unités d'organisation imbriquées sous la racine. Chaque compte peut se trouver directement dans la racine ou être placé dans l'une des unités d'organisation de la hiérarchie. Une organisation possède la fonctionnalité déterminée par l'ensemble des fonctions que vous activez.

Racine

Le conteneur parent pour tous les comptes de votre organisation. Si vous appliquez une politique à la racine, elle s'applique à toutes les unités d'organisation et à tous les comptes de l'organisation.

> **Note**
>
> Actuellement, vous ne pouvez disposer que d'une seule racine. AWS Organizations la crée automatiquement pour vous lorsque vous créez une organisation.

Unité d'organisation (UO)

Un conteneur pour les comptes au sein d'une racine. Une unité d'organisation peut également contenir d'autres unités d'organisation, ce qui vous permet de créer une hiérarchie semblable à un arbre à l'envers, avec une racine en haut et des branches d'unités d'organisation qui descendent pour se terminer par des comptes qui représentent les feuilles de l'arbre. Lorsque vous attachez une politique à l'un des nœuds de la hiérarchie, elle se transmet en descendant et affecte toutes les branches (unités d'organisation) et les feuilles (comptes) en dessous. Une unité d'organisation peut posséder un seul parent et actuellement chaque compte peut être un membre d'une seule unité d'organisation.

Compte

Un compte dans Organizations est un Compte AWS standard qui contient vos ressources AWS et les identités qui peuvent accéder à ces ressources.

> **Tip**
>
> Un compte AWS n'est pas la même chose qu'un compte d'utilisateur. Un utilisateur AWS est une identité que vous créez avec AWS Identity and Access Management (IAM) et prend la forme d'unutilisateur IAM avec des informations d'identification à long terme ou d'un rôle IAM avec informations d'identification à court terme. Un compte AWS individuel peut contenir et contient généralement 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.

- Le compte de gestion est le compte que vous utilisez pour créer l'organisation. À partir du compte de gestion de l'organisation, vous pouvez effectuer les opérations suivantes :
  - Créer des comptes dans l'organisation
  - Inviter d'autres comptes existants à rejoindre l'organisation
  - Supprimer des comptes de l'organisation

- Désigner des comptes d'administrateur délégué
- Gérer les invitations
- Appliquer des politiques à des entités (racines, unités d'organisation ou comptes) au sein de l'organisation
- Activer l'intégration aux services AWS supportés pour fournir des fonctionnalités de service dans tous les comptes de l'organisation.

Le compte de gestion possède les responsabilités d'un compte souscripteur et est responsable du paiement de tous les frais accumulés par les comptes membres. Vous ne pouvez pas modifier le compte de gestion d'une organisation.

- Les comptes membres constituent tous les autres comptes d'une organisation. Un compte ne peut être membre que d'une seule organisation à la fois. Vous pouvez attacher une politique à un compte pour appliquer des contrôles uniquement à ce compte.

> **Note**
>
> Vous pouvez désigner certains comptes membres comme comptes d'administrateur délégué. Consultez Administrateur délégué ci-dessous.

Administrateur délégué

Nous vous recommandons de n'utiliser le compte de gestion Organizations 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. En effet, les fonctionnalités de sécurité telles que les politiques de contrôle des services (SCP) de l'organisation ne restreignent 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. 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 Organizations : à partir de ces comptes, vous pouvez gérer les politiques d'organisation et les associer à des entités (racines, unités d'organisation ou comptes) au sein de l'organisation. Le compte de gestion peut contrôler les autorisations de délégation à des niveaux granulaires. Pour en savoir plus, consultez Administrateur délégué pour AWS Organizations.

- Administrateur délégué pour un service AWS : à partir de ces comptes, vous pouvez gérer les services AWS qui s'intègrent à 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 en savoir plus, consultez Administrateur délégué pour les services AWS intégrés à Organizations.

Invitation

Processus qui consiste à demander à un autre compte de rejoindre votre organisation. Une invitation ne peut être émise que par le compte de gestion de l'organisation. L'invitation est étendue à l'ID de compte ou à l'adresse e-mail associé(e) au compte invité. Une fois que le compte invité accepte une invitation, il devient un compte membre de l'organisation. Les invitations peuvent également être envoyées à tous les comptes membres actuels lorsque l'organisation a besoin que tous les membres approuvent la modification consistant à passer de la prise en charge des fonctions de facturation consolidée uniquement à la prise en charge de toutes les fonctions de l'organisation. Les invitations fonctionnent par l'échange de handshakes entre les comptes. Vous risquez de ne pas voir les handshakes lorsque vous utilisez la console AWS Organizations. Au contraire, si vous utilisez AWS CLI ou l'API AWS Organizations, vous devez utiliser directement les handshakes.

Handshake

Processus en plusieurs étapes consistant en l'échange d'informations entre deux parties. L'une de ses principales utilisation dans AWS Organizations est de servir d'implémentation sous-jacente pour les invitations. Les messages de handshake sont transmis entre l'initiateur et le destinataire du handshake, qui y répondent. Les messages sont transmis de sorte que les deux parties aient toujours connaissance du statut actuel. Les handshakes sont également utilisés lorsque l'organisation souhaite passer de la prise en charge des fonctions de facturation consolidée uniquement à la prise en charge de toutes les fonctions proposées par AWS Organizations. En général, vous interagissez directement avec des handshakes uniquement si vous utilisez l'API AWS Organizations ou des outils de ligne de commande tels que la AWS CLI.

Ensembles de fonctions disponibles

- Toutes les fonctions : ensemble des fonctions par défaut disponibles pour AWS Organizations. Il inclut toutes les fonctionnalités de facturation consolidée, ainsi que des fonctions avancées qui vous donnent plus de contrôle sur les comptes de votre organisation. Par exemple, lorsque toutes les fonctions sont activées, le compte de gestion de l'organisation dispose d'un contrôle total sur les actions des comptes membres. Le compte de gestion peut appliquer des politiques

de contrôle des services pour limiter les services et les actions auxquels les utilisateurs (y compris l'utilisateur racine) et les rôles d'un compte peuvent accéder. Le compte de gestion peut également empêcher les comptes membres de quitter l'organisation. Vous pouvez également activer l'intégration aux services AWS pris en charge pour permettre à ces services de fournir des fonctionnalités sur tous les comptes de votre organisation.

Vous pouvez créer une organisation avec toutes les fonctions déjà activées ou activer toutes les fonctions d'une organisation qui ne prenait en charge à la base que les seules fonctions 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.

- Facturation consolidée - cet ensemble de fonctions offre une fonctionnalité de facturation partagée, mais n'inclut pas les fonctions plus avancées de AWS Organizations. Par exemple, vous ne pouvez pas permettre à d'autres services AWS de s'intégrer à votre organisation pour opérer sur l'ensemble de ses comptes, ou utiliser des politiques pour restreindre les actions des utilisateurs et des rôles dans les différents comptes. Pour utiliser les fonctions avancées d'AWS Organizations, vous devez activer toutes les fonctions dans votre organisation.

Politique de contrôle des services

Politique qui spécifie les services et les actions que les utilisateurs et les rôles peuvent utiliser dans les comptes concernés par la politique de contrôle des services (SCP). Les SCP sont similaires aux politiques d'autorisation IAM, mais elles n'accordent pas d'autorisations. Au lieu de cela, elles spécifient les autorisations maximales pour une organisation, une unité d'organisation (UO) ou un compte. Lorsque vous attachez une politique de contrôle des services à la racine de votre organisation ou à une unité d'organisation, cette politique limite les autorisations des entités des comptes membres.

Listes d'autorisation et listes de refus

Les listes d'autorisation et les listes de refus sont des politiques complémentaires que vous pouvez utiliser lorsque vous appliquez des politiques de contrôle des services pour filtrer les autorisations disponibles pour les comptes.

- Politique de liste d'autorisation : vous spécifiez explicitement l'accès qui est autorisé. Tous les autres accès sont implicitement bloqués. Par défaut, AWS Organizations attache une politique gérée AWS appelée `FullAWSAccess` à l'ensemble des racines, unités d'organisation et comptes. Cela garantit que lorsque vous créez votre organisation, rien n'est bloqué jusqu'à ce que vous le souhaitiez. En d'autres termes, toutes les autorisations sont accordées par défaut.

Lorsque vous êtes prêt à limiter les autorisations, vous remplacez la politique `FullAWSAccess` par une autre qui autorise uniquement un ensemble plus limité et souhaité d'autorisations. Les utilisateurs et les rôles des comptes concernés ne peuvent alors exercer que ce niveau d'accès, même si leurs politiques IAM permettent toutes les actions. Si vous remplacez la politique par défaut sur la racine, tous les comptes de l'organisation sont concernés par les restrictions. Vous ne pouvez pas rajouter des autorisations à un niveau inférieur de la hiérarchie car une politique de contrôle des services n'accorde jamais d'autorisations ; elle ne fait que les filtrer.

- Stratégie de liste de refus – Vous spécifiez explicitement l'accès qui n'est pas autorisé. Tous les autres accès sont autorisés. Dans ce scénario, toutes les autorisations sont accordées à moins qu'elles soient explicitement bloquées. Il s'agit du comportement par défaut d'AWS Organizations. Par défaut, AWS Organizations attache une politique gérée AWS appelée `FullAWSAccess` à l'ensemble des racines, unités d'organisation et comptes. Cela permet à n'importe quel compte d'accéder à tous les services et opérations sans aucune restriction imposée par AWS Organizations. Contrairement à la technique de liste d'autorisation décrite ci-dessus, lorsque vous utilisez des listes de refus, vous maintenez la politique `FullAWSAccess` par défaut (qui autorise « tous » les accès). Mais vous attachez ensuite des politiques supplémentaires qui refusent explicitement l'accès aux services et aux actions indésirables. À l'instar des politiques d'autorisation IAM, le refus explicite d'une action de service prend le pas sur toute autorisation de cette action.

Politique de désactivation des services d'intelligence artificielle (IA)

Type de politique qui vous aide à standardiser vos paramètres de désactivation pour les services d'intelligence artificielle AWS sur tous les comptes de votre organisation. Certains services d'intelligence artificielle AWS peuvent stocker et utiliser le contenu client traité par ces services pour le développement et l'amélioration continue des services et technologies d'intelligence artificielle d'Amazon. En tant que client d'AWS, vous pouvez utiliser des politiques de désactivation des services d'IA pour choisir de refuser que votre contenu soit stocké ou utilisé à des fins d'amélioration des services.

Politique de sauvegarde

Type de politique qui vous aide à standardiser et à mettre en œuvre une politique de sauvegarde pour les ressources de tous les comptes de votre organisation. Dans une politique de sauvegarde, vous pouvez configurer et déployer des plans de sauvegarde pour vos ressources.

Politique de balises

Type de politique qui vous aide à standardiser les balises entre les ressources de tous les comptes de votre organisation. Dans une politique de balises, vous pouvez spécifier des règles de balisage pour des ressources spécifiques.

Didacticiels AWS Organizations

Utilisez les didacticiels de cette section pour apprendre à effectuer des tâches avec AWS Organizations.

Didacticiel : Création et configuration d'une organisation

Devenez opérationnel avec des instructions détaillées 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.

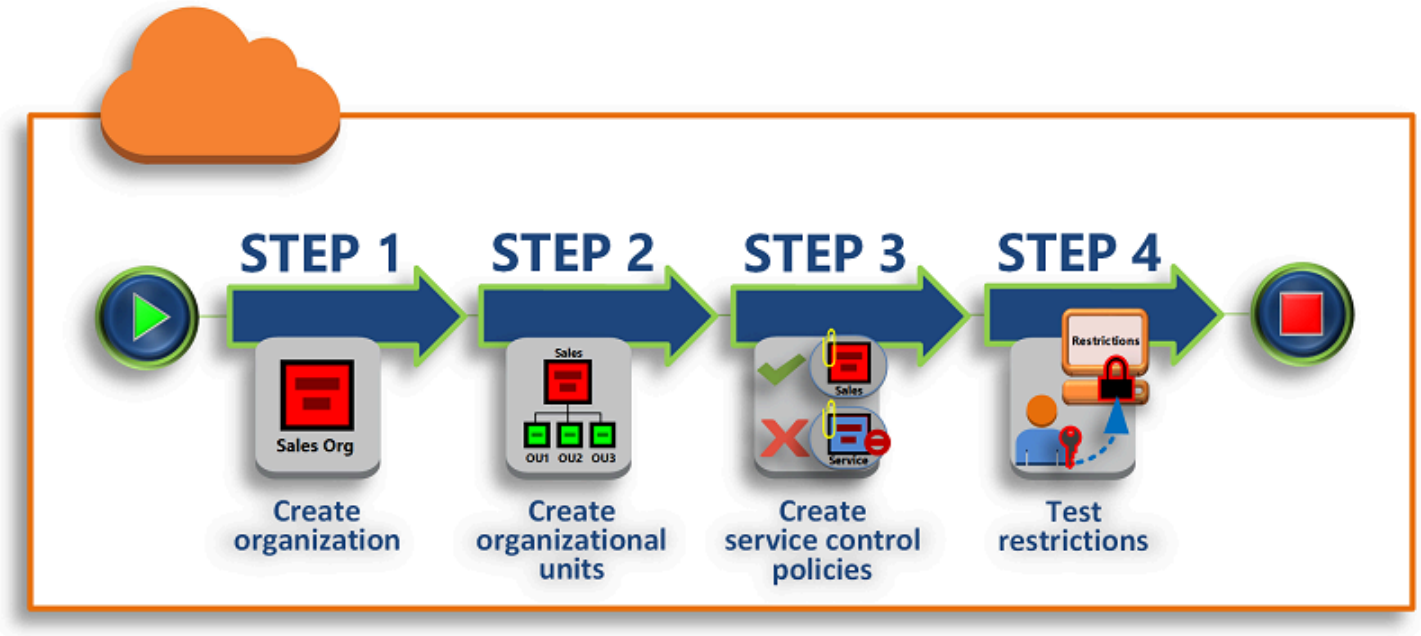
Didacticiel : Surveillance des modifications importantes apportées à votre organisation avec Amazon EventBridge

Contrôlez les modifications clés apportées à votre organisation en configurant Amazon EventBridge pour déclencher une alarme sous la forme d'un e-mail, d'un SMS (message texte) ou d'une entrée de journal lorsque les actions que vous désignez 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.

Didacticiel : Création et configuration d'une organisation

Dans ce didacticiel, vous créez votre organisation et la configurez avec deux comptes membres AWS. 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 introduit par AWS avant d'autoriser son utilisation par une autre personne au sein de votre entreprise. Ainsi, si AWS introduit un nouveau service, celui-ci restera interdit tant qu'un administrateur ne l'aura pas ajouté à la liste d'autorisations dans la politique appropriée. Ce didacticiel vous montre également comment utiliser une liste de refus pour vous assurer qu'aucun utilisateur dans un compte membre ne peut modifier la configuration pour les journaux d'audit qui sont créés par AWS CloudTrail.

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 AWS actuel en tant que compte de gestion. Vous 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

Ensuite, vous créez deux unités d'organisation (UO) dans votre nouvelle organisation et vous placez les comptes membres dans celles-ci.

Étape 3 : Créer les politiques de contrôle des services

Vous pouvez appliquer des restrictions quant aux actions pouvant être déléguées à des utilisateurs et rôles dans les comptes membres à l'aide de politiques de contrôle des services (SCP). Au cours de cette étape, vous créez deux politiques de contrôle des services et vous les attachez aux unités d'organisation de votre organisation.

Étape 4 : Tester les politiques de votre organisation

Vous pouvez vous connecter en tant qu'utilisateur de chacun des comptes de test, afin de voir les effets que les politiques SCP ont sur les comptes.

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

Prerequisites (Prérequis)

Ce didacticiel suppose que vous avez accès à deux Comptes AWS existants (vous en créez un troisième dans le cadre du didacticiel) et que vous pouvez vous connecter à chaque compte 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 à AWS en 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 affiche la page Comptes AWS. 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.

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. Dans la page Ajouter un Compte AWS, choisissez Inviter un Compte AWS existant.
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`**. Alternativement, si vous connaissez le numéro ID du Compte AWS, vous pouvez l'entrer 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 l'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 envoyé par AWS à partir du compte de gestion et choisissez le lien permettant d'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

Dans les étapes de cette section, vous créez un Compte AWS qui devient automatiquement membre de l'organisation. Dans le didacticiel, ce compte identifié 333333333333.

AWS Management Console

Pour créer un compte membre

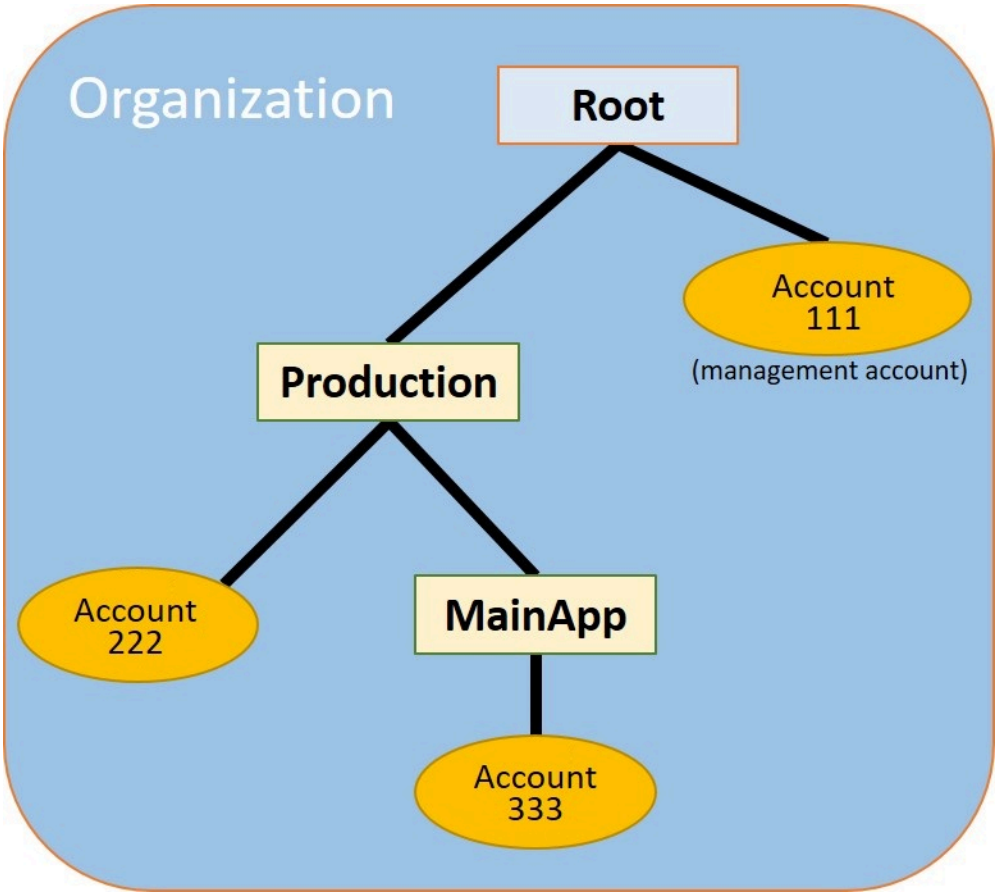
1. Dans la console AWS Organizations, sur la page Comptes AWS, choisissez Ajouter un Compte AWS.
2. Dans la page Ajouter un Compte AWS, choisissez Créer un Compte AWS.

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 un 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

Dans les étapes de cette section, vous créez des unités d'organisation (UO) et y placez vos comptes membres. À la fin, votre hiérarchie ressemble à l'illustration suivante. Le compte de gestion reste dans la racine. Un compte membre est déplacé vers l'unité d'organisation Production et l'autre vers l'unité d'organisation MainApp qui est un enfant de Production.



AWS Management Console

Pour créer et remplir les unités d'organisation

> **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. Dans l'onglet Enfants, choisissez Actions, puis sous Unité d'organisation, choisissez Créer.
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 maintenant déplacer vos comptes membres vers ces unités d'organisation.
8. Revenez à la page Comptes AWS, puis développez l'arborescence sous votre UO Production en choisissant le triangle
   
   en regard de cette UO. Ceci affiche l'UO MainApp 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. Dans la page Déplacer Compte AWS « 333333333333 » choisissez le triangle à côté de Production pour le développer. À côté de MainApp, choisissez le bouton radio
    
    (et non 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. Dans 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 de cette section, vous créez trois politiques de contrôle des services (SCP), puis les attachez à la racine et aux unités d'organisation pour restreindre ce que les utilisateurs peuvent faire dans les comptes de l'organisation. La première politique de contrôle des services empêche les comptes membres de créer ou modifier les journaux AWS CloudTrail que vous configurez. Le compte de gestion n'est pas affecté par une politique de contrôle des services. Ainsi, une fois que vous avez appliqué la politique de contrôle des services CloudTrail, 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 les SCP pour 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 des SCP dans votre organisation.

Créer vos SCP

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 la première politique SCP, qui bloque les actions de configuration de CloudTrail

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 située à droite, sélectionnez CloudTrail pour le service. Choisissez ensuite les actions suivantes : AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging, et UpdateTrail.
5. Toujours dans le volet de droite, choisissez Ajouter une ressource et spécifiez CloudTrail et Toutes les ressources. Choisissez ensuite Ajouter une ressource.

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

```
{
    "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 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.

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

4. Choisissez Créer une politique.

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

AWS Management Console

Pour créer la troisième politique, qui refuse l'accès à des services qui ne peuvent pas être utilisés dans l'UO MainApp

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.

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

5. Choisissez Créer une politique pour enregistrer la SCP.

Attacher les politiques SCP à vos unités d'organisation

Maintenant que les politiques SCP existent et qu'elles sont activées pour votre racine, vous pouvez les attacher à la racine et aux unités d'organisation.

AWS Management Console

Pour attacher les politiques à la racine et aux unités d'organisation

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 attachez la politique à la racine de façon à ce qu'elle affecte tous les comptes membres pour empêcher quiconque de modifier la façon dont vous avez configuré CloudTrail.

Dans la page de détails Racine, l'onglet Politiques indique maintenant que deux politiques SCP sont attachées à la racine : celle que vous venez d'attacher et la politique SCP par défaut `FullAWSAccess`.

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. Choisissez à nouveau l'onglet Politiques pour voir à nouveau que deux politiques SCP sont attachées à l'UO : celle que vous venez d'attacher et la politique SCP par défaut `FullAWSAccess`. 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'UO Production, choisissez la case d'option FullAWSAccess, 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 attacher la politique de contrôle des services nommée `Deny List for MainApp Prohibited services` pour empêcher quiconque dans les comptes de l'unité d'organisation MainApp d'utiliser les services restreints.

    Pour ce faire, accédez à la page Comptes AWS, choisissez l'icône de triangle pour développer la branche de l'UO Production, puis choisissez l'UO MainApp (le nom, pas la case d'option) pour accéder à son contenu.

12. Dans la page de détails MainApp, choisissez l'onglet Politiques.
13. Sous Politiques de contrôle des services, choisissez Attacher, puis, dans la liste des politiques disponibles, choisissez la case d'option en regard de Liste de refus pour les services interdits dans MainApp, puis choisissez Attacher une politique.

Étape 4 : Tester les politiques de votre organisation

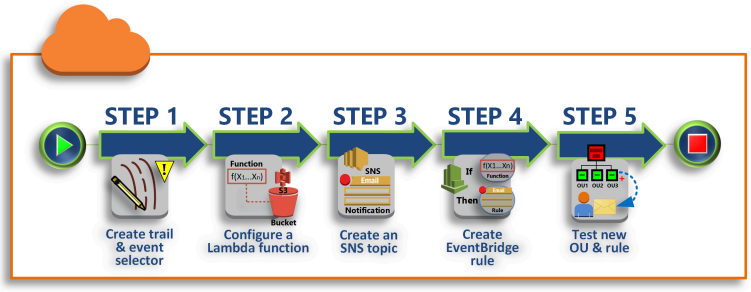
Vous pouvez maintenant vous connecter en tant qu'utilisateur de l'un des comptes membres et essayer d'effectuer différentes actions AWS :

- 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. Les politiques SCP n'affectent pas les utilisateurs et rôles du compte de gestion, quelle que soit la racine ou l'unité d'organisation dans laquelle le compte est situé.
- Si vous vous connectez en tant qu'utilisateur du compte 222222222222, vous pouvez effectuer toutes les actions permises par la liste d'autorisations. AWS Organizations refuse toute tentative d'action dans un service qui ne figure pas dans la liste d'autorisations. De plus, AWS Organizations refuse toute tentative d'exécuter une des actions de configuration de CloudTrail.
- 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. De plus, AWS Organizations refuse toute tentative d'exécuter une des actions de configuration de CloudTrail.

Didacticiel : Surveillance des modifications importantes apportées à votre organisation avec Amazon EventBridge

Ce didacticiel explique comment configurer Amazon EventBridge, anciennement Amazon CloudWatch Events, pour contrôler les modifications apportées à 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 fonction AWS Lambda lorsque la règle est déclenchée et vous configurez Amazon SNS pour envoyer un e-mail avec les détails relatifs à 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 journal d'activité, dans AWS CloudTrail. Vous le configurez pour capturer tous les appels d'API.

Étape 2 : Configuration d'une fonction Lambda

Créez une fonction AWS Lambda qui consigne 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 : Création d'une règle Amazon EventBridge

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

Étape 5 : Test de votre règle Amazon EventBridge

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 de plus amples informations sur l'utilisation de

AWS CloudTrail et Amazon EventBridge avec AWS Organizations, consultez Journalisation et surveillance dans AWS Organizations.

Prerequisites (Prérequis)

Ce didacticiel suppose ce qui suit :

- Vous pouvez vous connecter à la AWS Management Console en tant qu'utilisateur IAM à partir du compte de gestion de votre organisation. L'utilisateur IAM doit être autorisé à créer et configurer un journal dans 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 le journal CloudTrail que vous configurez à l'étape 1.

Important

Actuellement, AWS Organizations est hébergé uniquement dans la région USA Est (Virginie du Nord) (même si ce service est disponible dans le monde entier). Pour effectuer les étapes de ce didacticiel, vous devez configurer la 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 pouvez également configurer un sélecteur d'événements sur le journal de suivi pour capturer tous les appels d'API en lecture/écriture afin de fournir à Amazon EventBridge des appels sur lesquels effectuer des déclenchements.

Pour créer un journal d'activité

1. Connectez-vous à AWS en tant qu'administrateur du compte de gestion de l'organisation, puis ouvrez la console CloudTrail à l'adresse https://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 n'apparaît pas comme option dans les paramètres de configuration d'Amazon EventBridge, et CloudTrail ne capture pas d'informations sur 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. Sélectionnez l'une des options suivantes pour spécifier où CloudTrail doit fournir 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 Next (Suivant).
8. Sur la page Choisir les événements du journal, dans la section Événements de gestion, choisissez Read (Lire) et Write (Écrire).
9. Choisissez Next (Suivant).
10. Passez en revue vos sélections, puis choisissez Create trail (Créer un journal d'activité).

Amazon EventBridge vous permet de choisir parmi différentes méthodes 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 allez créer une fonction Lambda qui consigne l'activité d'API envoyée par la règle Amazon EventBridge que vous configurerez ultérieurement.

Pour créer une fonction Lambda qui consigne des événements Amazon EventBridge

1. Ouvrez la console AWS Lambda à l'adresse https://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. Sélectionnez Create function (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 allez faire de cette rubrique une cible de la règle Amazon EventBridge 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 Create subscription (Créer l'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 : Création d'une règle Amazon EventBridge

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

Pour créer une règle EventBridge

1. Ouvrez la console Amazon EventBridge sur https://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 plus d'informations sur la création de règles, consultez Démarrage avec Amazon EventBridge dans le Guide de l'utilisateur Amazon EventBridge.

Étape 5 : Test de votre règle Amazon EventBridge

Au cours de cette étape, vous créez une unité d'organisation (UO) et observez que la règle Amazon EventBridge génère une entrée de journal et vous envoie un e-mail avec des détails relatifs à l'événement.

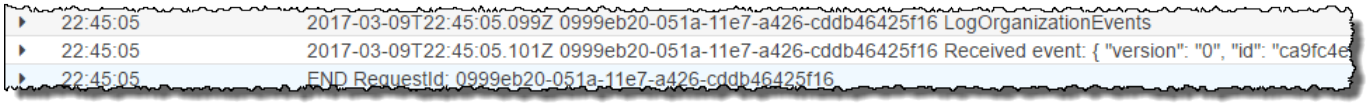
AWS Management Console

Pour créer une unité d'organisation

1. Ouvrez la page Comptes AWS dans la console AWS Organizations.
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 de journal EventBridge

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans la page de navigation, choisissez Logs (Journaux).
3. Sous Log Groups (Groupes de journaux), 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"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
```

```
        "eventType": "AwsApiCall"
    }
}
```

7. Vérifiez dans votre compte de messagerie la présence d'un message d'OrgsCWEvnt (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 de payer des frais, vous devez supprimer toutes les ressources AWS que vous avez créées dans le cadre de ce didacticiel et que vous ne souhaitez pas conserver.

Pour nettoyer votre environnement AWS

1. Utilisez la console CloudTrail pour supprimer le journal d'activité 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 console CloudWatch pour supprimer la règle EventBridge 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 configuré EventBridge pour contrôler les modifications apportées à votre organisation. 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.

Bonnes pratiques pour la gestion des comptes multiples

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

Rubriques

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.

Utilisation d'un mot de passe fort pour l'utilisateur root

Nous vous recommandons d'utiliser un mot de passe fort et unique. De nombreux gestionnaires de mots de passe ainsi que des algorithmes et des outils de génération de mots de passe forts peuvent vous aider à atteindre ces objectifs. Pour plus d'informations, consultez Modification du mot de passe pour le Utilisateur racine d'un compte AWS. Utilisez la politique de sécurité de l'information de votre entreprise pour gérer le stockage à long terme et l'accès au mot de passe de l'utilisateur root. Nous vous recommandons de stocker le mot de passe dans un système de gestion des mots de passe ou un système équivalent qui répond aux exigences de sécurité de votre organisation. Pour éviter de créer une dépendance circulaire, ne stockez pas le mot de passe de l'utilisateur racine avec des outils qui dépendent de services AWS auxquels vous vous connectez avec le compte protégé. Quelle que soit la méthode choisie, nous vous recommandons de donner la priorité à la résilience et d'envisager éventuellement de demander à plusieurs acteurs d'autoriser l'accès à ce coffre-fort pour une protection renforcée. Tout accès au mot de passe ou à son emplacement de stockage doit être consigné et surveillé. Pour des recommandations supplémentaires sur le mot de passe de l'utilisateur root, consultez les Bonnes pratiques d'utilisateur root pour votre Compte AWS.

Documenter les processus d'utilisation des informations d'identification de l'utilisateur root

Documentez l'exécution des processus importants à mesure qu'ils sont effectués afin de veiller à posséder un registre des personnes impliquées dans chaque étape. Pour gérer le mot de passe, nous vous recommandons d'utiliser un gestionnaire de mot de passe sécurisé et chiffré. Il est également important de fournir une documentation sur les exceptions et les événements imprévus qui pourraient survenir. Pour plus d'informations, consultez la rubrique Résolution des problèmes de connexion à la AWS Management Console du Guide de l'utilisateur pour la connexion à AWS et la rubrique Tâches nécessitant des informations d'identification d'utilisateur root du Guide de l'utilisateur IAM.

Au moins une fois par trimestre, testez et confirmez que vous avez toujours accès à l'utilisateur root et que le numéro de téléphone de contact est opérationnel. Cela permet de confirmer à l'entreprise que le processus fonctionne et que vous pouvez conserver l'accès à l'utilisateur root. Cela démontre également que les personnes responsables de l'accès root comprennent les étapes qu'elles doivent suivre pour que le processus réussisse. Pour améliorer le temps de réponse et la réussite, il est important de s'assurer que toutes les personnes impliquées dans un processus comprennent exactement ce qu'elles doivent faire en cas de besoin d'accès.

Activer MFA pour les informations d'identification de votre utilisateur root.

Nous vous recommandons d'activer plusieurs dispositifs d'authentification multifactorielle (MFA) pour l'utilisateur root du Compte AWS et les utilisateurs IAM de vos Comptes AWS. Cela vous permet d'élever la sécurité dans vos Comptes AWS et de simplifier la gestion de l'accès aux utilisateurs hautement privilégiés, tels que l'utilisateur root du Compte AWS. Pour répondre aux différents besoins des clients, AWS prend en charge trois types de dispositifs MFA pour l'IAM, notamment les clés de sécurité FIDO, les applications d'authentification virtuelles et les jetons matériels à mot de passe unique à durée limitée (TOTP).

Chaque type d'authentificateur possède des propriétés physiques et de sécurité légèrement différentes qui conviennent mieux aux différents cas d'utilisation. Les clés de sécurité FIDO2 offrent le niveau d'assurance le plus élevé et résistent au phishing. Toute forme de MFA offre un niveau de sécurité plus élevé que l'authentification par mot de passe uniquement, et nous vous recommandons vivement d'ajouter une forme ou une autre de MFA à votre compte. Choisissez le type de dispositif qui correspond le mieux à vos exigences opérationnelles et de sécurité.

Si vous choisissez un dispositif alimenté par batterie pour votre authentificateur principal, tel qu'un jeton matériel TOTP, envisagez également d'enregistrer un authentificateur qui ne dépend pas de la batterie comme mécanisme de secours. Il est également essentiel de vérifier régulièrement la fonctionnalité du dispositif et de le remplacer avant la date d'expiration pour garantir un accès ininterrompu. Quel que soit le type de dispositif que vous choisissez, nous vous recommandons d'enregistrer au moins deux dispositifs (IAM prend en charge jusqu'à huit dispositifs MFA par utilisateur) afin d'accroître votre résilience en cas de perte ou de défaillance d'un dispositif.

Suivez la politique de sécurité de l'information de votre organisation pour le stockage du dispositif MFA. Nous vous recommandons de stocker le dispositif MFA séparément du mot de passe associé. Cela garantit que l'accès au mot de passe et au dispositif MFA nécessite des ressources différentes (personnes, données et outils). Cette séparation ajoute une couche supplémentaire de protection contre les accès non autorisés. Nous vous recommandons également d'enregistrer et de surveiller tout accès au dispositif MFA ou à son emplacement de stockage. Cela permet de détecter et d'intervenir en cas d'accès non autorisé.

Pour plus d'informations, consultez Sécurisez votre connexion d'utilisateur root avec l'authentification multifactorielle (MFA) dans le Guide de l'utilisateur IAM. Pour obtenir des instructions sur l'activation de l'authentification multifactorielle, consultez Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS et Activation des dispositifs MFA pour les utilisateurs dans AWS.

Appliquer des contrôles pour surveiller l'accès aux informations d'identification de l'utilisateur racine

L'accès aux informations d'identification de l'utilisateur racine doit être un événement rare. Créez des alertes à l'aide d'outils tels qu'Amazon EventBridge pour annoncer la connexion aux informations d'identification de l'utilisateur root du compte de gestion et leur utilisation. Cette alerte doit inclure, sans s'y limiter, l'adresse e-mail utilisée pour l'utilisateur root lui-même. Cette alerte doit être importante et difficile à manquer. Pour obtenir un exemple, consultez Surveiller et notifier l'activité de l'utilisateur racine d'un Compte AWS. Vérifiez que le personnel qui reçoit une telle alerte comprenne comment confirmer que l'accès de l'utilisateur root est attendu et comment remonter l'événement s'il croit qu'un incident de sécurité est en cours. Pour plus d'informations, consultez Signalement d'e-mails suspects ou Signalement des vulnérabilités. Vous pouvez également contacter AWS pour obtenir de l'aide et des conseils supplémentaires.

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 de contact valide et actif qui vous permet de recevoir des messages textuels ou des appels. Nous vous recommandons d'utiliser un numéro de téléphone dédié afin de vous assurer qu'AWS puisse vous contacter à des fins d'assistance et de récupération de votre compte. Vous pouvez facilement afficher et gérer les numéros de téléphone de votre compte via AWS Management Console ou les API de gestion de compte.

Il existe plusieurs façons d'obtenir un numéro de téléphone dédié qui permette à AWS de 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 dans la page de la console Informations de contact AWS, et partagez ses détails avec les équipes spécifiques qui doivent en avoir connaissance 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 AWS doit contacter le propriétaire du compte, par exemple pour confirmer l'accès, l'e-mail 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.

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 et les données de production sous vos unités d'organisation orientées charge de travail de haut niveau. Vos unités d'organisation doivent être basées sur un ensemble commun de contrôles plutôt que de refléter la structure hiérarchique de votre entreprise. Outre les unités d'organisation de production, nous vous recommandons de définir une ou plusieurs unités d'organisation de non-production qui contiennent des comptes et des environnements de charge de travail utilisés pour développer et tester les charges de travail. Pour plus d'informations, consultez Organisation des unités d'organisation orientées vers la charge de travail (français non garanti).

Utiliser plusieurs comptes pour organiser vos charges de travail

Un compte Compte AWS fournit des limites naturelles de sécurité, d'accès et de facturation pour vos ressources AWS. 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 travail de test/développement dans des comptes distincts.

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

En tant que bonne pratique, nous vous recommandons d'activer ou de désactiver tout service avec lequel vous voulez vous intégrer dans l'ensemble des AWS Organizations à l'aide de la console de ce service ou des opérations d'API/commandes CLI équivalentes. Grâce à cette méthode, le service AWS peut effectuer toutes les étapes d'initialisation requises pour votre organisation, telles que la création de toutes les ressources nécessaires et le nettoyage des ressources lors de la désactivation du service. AWS Account Management est le seul service dont l'activation nécessite l'utilisation de la console AWS Organizations ou des API. Pour passer en revue la liste des services intégrés à AWS Organizations, consultez AWS services 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 des balises, suivez les conseils de la section Baliser vos ressources AWS (français non garanti). Outre les ressources, vous pouvez créer des balises sur la racine de l'organisation, les comptes, les unités d'organisation et les politiques. Pour plus d'informations, consultez Créer votre stratégie de balisage (français non garanti).

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 la clé de toutes les tâches administratives mentionnées, telles que la gestion des comptes, les politiques, l'intégration avec d'autres services AWS, 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 tous vos ressources AWS dans d'autres Comptes AWS de l'organisation et gardez-les en dehors du compte de gestion. Une raison importante pour conserver vos ressources dans d'autres comptes est que les politiques de contrôle des services (SCP) d'Organizations 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.

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 les SCP 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, comme AWS Service Catalog pour le partage de logiciels dans l'ensemble de l'organisation, ou AWS CloudFormation StackSets pour la création et le déploiement de piles.

Pour plus d'informations, consultez Architecture de référence de sécurité (français non garanti), Organisation de votre environnement AWS à l'aide de plusieurs comptes (français non garanti), et AWS services que vous pouvez utiliser avec AWS Organizations pour obtenir des suggestions sur l'enregistrement de comptes membres en tant qu'administrateur délégué pour divers services AWS. Pour plus d'informations sur la configuration des administrateurs délégués, consultez Activation d'un compte d'administrateur délégué pour AWS Account Management (français non garanti) et Administrateur délégué pour AWS Organizations.

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

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 de la mise à l'échelle, avant de créer de nouveaux comptes, assurez-vous qu'il n'existe pas déjà des comptes répondant à des besoins similaires, afin d'éviter toute duplication inutile. Les comptes Comptes AWS doivent être basés sur des besoins d'accès communs. 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 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 d'encourir des coûts liés à l'utilisation des ressources et d'atteindre les limites de l'API CloseAccount.

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 de n'importe quel compte membre d'effectuer des appels d'API de service AWS, à l'exception de « Mise à jour d'une politique de compartiment S3 qui a été mal configurée et refuse l'accès à tous les principaux » (l'une des actions qui nécessitent 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.

```
{
 "Version": "2012-10-17",

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
 "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }
```

```
        }

    ]
}
```

Dans la majorité des cas, toutes les tâches administratives peuvent être exécutées par un rôle AWS Identity and Access Management (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 et gestion d'une organisation

Vous pouvez exécuter les tâches suivantes à l'aide de la console AWS Organizations ou en exécutant une commande AWS Command Line Interface (AWS CLI) ou les opérations d'API équivalentes dans les kits SDK AWS :

- Créez une organisation. Créez votre organisation avec votre compte actuel en tant que compte de gestion. Créez des comptes membres au sein de votre organisation et invitez d'autres comptes à la rejoindre.
- Activez toutes les fonctions de votre organisation. L'activation de toutes les fonctions est le meilleur moyen de travailler avec AWS Organizations. Lorsque vous créez une organisation, vous avez la possibilité d'activer toutes les fonctions ou un sous-ensemble de fonctions de facturation consolidée. L'activation de toutes les fonctions est la valeur par défaut et elle comprend des fonctions de facturation consolidée.

  Avec toutes les fonctions activées, vous pouvez utiliser les fonctions de gestion de compte avancées disponibles dans AWS Organizations, telles que les politiques de contrôle des services (SCP). Les politiques de contrôle des services permettent un contrôle centralisé optimal des autorisations disponibles pour tous les comptes de votre organisation, ce qui garantit que vos comptes respectent les directives de contrôle d'accès de votre organisation.
- Affichez les détails de votre organisation. Affichez les détails de votre organisation ainsi que ses racines, unités d'organisation et comptes.
- Supprimez une organisation. Supprimez une organisation lorsque vous n'en avez plus besoin.

> **Note**
>
> Les procédures de cette section spécifient les autorisations minimales nécessaires pour effectuer les tâches. En général, ces dernières s'appliquent à l'API ou accèdent à l'outil de ligne de commande.
> L'exécution d'une tâche dans la console peut exiger des autorisations supplémentaires. Par exemple, vous pouvez accorder des autorisations en lecture seule à tous les utilisateurs de votre organisation, puis accorder d'autres autorisations qui permettent à certains utilisateurs d'exécuter des tâches spécifiques.

Création d'une organisation

Vous pouvez créer une organisation qui démarre avec votre Compte AWS comme compte de gestion. Lorsque vous créez une organisation, vous pouvez choisir si cette dernière prend en charge toutes les fonctions (recommandé) ou seulement les fonctions de facturation consolidée.

Après avoir créé une organisation, vous pouvez lui ajouter des comptes des façons suivantes à partir du compte de gestion :

- Créez d'autres Comptes AWS qui sont automatiquement ajoutés à l'organisation en tant que comptes membres.
- Une fois que vous avez vérifié votre adresse e-mail, invitez des Comptes AWS existants à rejoindre votre organisation en tant que comptes membres.

Créer une organisation.

Vous pouvez créer une organisation avec la AWS Management Console ou à l'aide d'une commande de l'AWS CLI ou de l'une des API du SDK.

> **Autorisations minimales**
>
> Pour créer une organisation avec votre Compte AWS actuel, 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. 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

Pour créer une organisation

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

- AWS CLI : create-organization

L'exemple suivant crée une organisation et fait du Compte AWS actuellement connecté le compte de gestion de l'organisation.

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

- SDK AWS : CreateOrganization

Vous pouvez ensuite ajouter des comptes supplémentaires à votre organisation comme suit :

- Pour créer un Compte AWS qui fait automatiquement partie de votre organisation AWS, consultez Création d'un compte membre dans votre organisation.
- Pour inviter un compte existant à rejoindre votre organisation, consultez Inviter un Compte AWS homme à rejoindre votre organisation.

Vérification de l'adresse e-mail

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 précédemment vérifié, AWS envoie 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.

Dans les 24 heures, suivez les instructions de l'e-mail pour valider votre adresse e-mail.

Si vous ne validez pas votre adresse e-mail dans un délai de 24 heures, vous pouvez renvoyer la demande de vérification afin de pouvoir inviter d'autres comptes Comptes AWS dans 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 Affichage des détails d'une organisation à partir du 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 plus d'informations, consultez Inviter un Compte AWS homme à rejoindre votre organisation.

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. Utilisez la procédure précédente pour renvoyer la demande de vérification. Une fois que vous avez terminé le processus en répondant à l'e-mail, vos comptes invités peuvent accepter les invitations.

Activation de toutes les fonctions de votre organisation

AWS Organizations dispose de deux ensembles de fonctions :

- Toutes les fonctions : cet ensemble de fonctions est le meilleur moyen de travailler avec AWS Organizations et inclut des fonctions de facturation consolidée. Lorsque vous créez une organisation, toutes les fonctions sont activées par défaut. Lorsque toutes les fonctions sont activées, vous pouvez utiliser les fonctions de gestion de compte avancées disponibles dans AWS Organizations telles que l'intégration aux services AWS supportés et les politiques de gestion de l'organisation.
- Fonctions de facturation consolidée : toutes les organisations prennent en charge ce sous-ensemble de fonctions, qui fournit des outils de gestion de base que vous pouvez utiliser pour gérer de façon centralisée les comptes de votre organisation.

Si vous créez une organisation avec uniquement les fonctions de facturation consolidée, vous pouvez ultérieurement activer toutes les fonctions. Cette page décrit le processus d'activation de toutes les fonctions.

Avant d'activer toutes les fonctions

Avant de passer d'une organisation qui prend en charge uniquement les fonctions de facturation consolidée à une organisation qui prend en charge toutes les fonctions, notez les points suivants :

- Lorsque vous lancez le processus d'activation de toutes les fonctions, 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.

- Vous pouvez continuer à inviter des comptes à votre organisation tout en activant toutes les fonctions. 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.
  - 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.
- Vous pouvez également continuer de créer des comptes dans l'organisation. Ce processus n'est pas affecté par cette modification.
- AWS Organizations vérifie également que tous les comptes membres ont 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 d'un compte créé à l'aide d'AWS Organizations, ce compte reçoit une invitation spécifique à recréer ce rôle. Toutes ces invitations doivent être acceptées pour que l'organisation puisse achever le processus d'activation de toutes les fonctions.
- Étant donné que l'activation de toutes les fonctions permet d'utiliser des politiques de contrôle des services, assurez-vous que vos administrateurs de compte comprennent les effets de l'attachement de politiques de contrôle des services à l'organisation, aux unités d'organisation ou aux comptes. Les politiques de contrôle des services peuvent limiter les actions que les utilisateurs et même les administrateurs peuvent effectuer dans les comptes concernés. Le compte de gestion peut, par exemple, appliquer des politiques de contrôle des services qui peuvent empêcher des comptes membres de quitter l'organisation.

- Les politiques de contrôle des services n'ont aucun impact sur le compte de gestion. Vous ne pouvez pas limiter les actions des utilisateurs et des rôles du compte de gestion en appliquant des politiques de contrôle des services. Les politiques de contrôle des services ont uniquement un impact sur les comptes membres.
- 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.
- (Non recommandé) Si seules les fonctions de facturation consolidée sont activées dans votre organisation, les administrateurs des comptes membres peuvent choisir de supprimer le rôle lié à un service nommé `AWSServiceRoleForOrganizations`. Si vous choisissez ultérieurement d'activer toutes les fonctions au sein d'une organisation, ce rôle est requis et est recréé dans tous les comptes dans le cadre de l'acceptation de l'invitation à activer toutes les fonctions. Pour plus d'informations sur la manière dont AWS Organizations utilise ce rôle, consultez AWS Organizations et rôles liés à un service.

Initialisation du processus d'activation de toutes les fonctions

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 d'approbation à chaque compte invité (non créé) de l'organisation pour activer toutes les fonctions de l'organisation. Si vous possédez des comptes créés à l'aide d'AWS Organizations et que l'administrateur du compte membre a supprimé le rôle lié à un service nommé `AWSServiceRoleForOrganizations`, AWS Organizations envoie à ce compte une demande de recréation du 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.

- SDK AWS : 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 Finalisation du processus d'activation de toutes les fonctions.

Approbation de la demande d'activation de toutes les fonctions ou de recréation d'un rôle lié à un service

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, au contraire, votre compte a été créé à l'aide d'AWS Organizations et que vous avez supprimé le rôle lié à un service `AWSServiceRoleForOrganizations`, vous recevez une invitation visant uniquement à 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 fonctions pour votre compte membre, vous devez 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 console AWS Organizations via le lien 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 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"
            }
        ]
    }
}
```

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

Finalisation du processus d'activation de toutes les fonctions

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"
            }
        ]
    }
}
```


- SDK AWS :
  - AcceptHandshake
  - AcceptHandshake

Étapes suivantes :

- Activez les types de politiques que vous souhaitez utiliser. Ensuite, vous pouvez attacher des politiques pour gérer les comptes de votre organisation. Pour de plus amples informations, consultez Gestion des politiques dans AWS Organizations.
- Activez l'intégration aux services supportés Pour de plus amples informations, veuillez consulter Utilisation d'AWS Organizations avec d'autres services AWS.

Affichage de détails sur votre organisation

Vous pouvez exécuter les tâches suivantes pour afficher des détails relatifs aux éléments de votre organisation.

Rubriques

Affichage des détails d'une organisation à partir du 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.

- SDK AWS : DescribeOrganization

Affichage des détails du conteneur racine

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

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 dans la hiérarchie des unités d'organisation (UO) et se comporte généralement comme une UO. Cependant, en tant que conteneur tout en haut de la

hiérarchie, les modifications apportées à la racine affectent toutes les autres unités d'organisation et chaque Compte AWS 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"
                }
            ]
        }
    ]
}
```

- SDK AWS : ListRoots

Affichage des détails d'une unité d'organisation

Lorsque vous vous connectez au compte de gestion de l'organisation dans la console AWS Organizations, vous pouvez afficher les détails des UO de l'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, SDK AWS :
  - 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"
    }
}
```

- SDK AWS :
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Affichage des détails d'un compte

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

> **Autorisations minimales**
>
> Pour afficher 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"
    }
}
```

- SDK AWS :
  - ListAccounts
  - DescribeAccount

Affichage des détails d'une politique

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

> **Autorisations minimales**
>
> Pour afficher les détails d'une politique, vous devez disposer des autorisations suivantes :
>
> - `organizations:DescribePolicy`
> - `organizations:ListPolicies`

AWS Management Console

Pour afficher les détails d'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. Effectuez l'une des actions suivantes :
   - Accédez à la page Politiques, puis choisissez le type de politique correspondant à la politique que vous souhaitez examiner.
   - Accédez à la page Comptes AWS, puis accédez à l'unité d'organisation ou au compte auquel la politique est attachée. Enfin, choisissez l'onglet Politiques pour afficher la liste des politiques attachées.
3. Choisissez le nom de la politique (pas la case d'option).

Dans la page Détails de la politique, vous pouvez afficher toutes les informations sur la politique, y compris le texte de la politique JSON, ainsi que la liste des unités d'organisation et des comptes auxquels la politique est attachée.

AWS CLI & AWS SDKs

Pour afficher les détails d'une politique

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

- AWS CLI:
  - list-policies
  - describe-policy : répertorie uniquement les détails de la politique spécifiée

L'exemple suivant montre comment rechercher l'ID de politique de la politique que vous souhaitez examiner. Vous devez spécifier un type de politique et la commande renvoie toutes les politiques de ce type uniquement.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

La réponse inclut tous les détails à l'exception du document de politique JSON.

L'exemple suivant montre comment récupérer les détails de la politique spécifiée uniquement, y compris le document de politique JSON.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
```

```
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
                  :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                  \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                  My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}"
    ]
}
```


- SDK AWS :
  - ListPolicies
  - DescribePolicy

Suppression d'une organisation

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 AWS autonome qui n'est plus géré par AWS Organizations. Vous avez alors trois possibilités : vous pouvez continuer à l'utiliser en tant que compte autonome, l'utiliser pour créer une autre organisation ou accepter une invitation d'une autre organisation pour rejoindre celle-ci en tant que compte membre.

Important

- 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.

- Vous ne pouvez supprimer une organisation qu'après en avoir supprimé tous les comptes membres. Si vous avez créé certains de vos comptes membres avec AWS Organizations, vous pouvez être empêché de 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 votre compte membre.
- Si vous avez clôturé un compte membre avant de le supprimer de l'organisation, il prend l'état « suspendu » pendant un certain temps et vous ne pouvez pas supprimer le compte de l'organisation tant qu'il n'est pas définitivement clôturé. 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.

Lorsque vous supprimez le compte de gestion d'une organisation en supprimant l'organisation, le compte peut être affecté comme suit :

- 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 a besoin d'une organisation pour fonctionner. Par conséquent, 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 de service (SCP). Aucune modification n'est donc effectuée dans les autorisations une fois que les SCP ne sont plus disponibles.

Rubriques

- Supprimer une organisation

Supprimer une organisation

Utilisez la procédure suivante pour supprimer une organisation qui rétablit 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 Suppression d'un compte membre de votre organisation.
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 Clôture d'un compte membre de votre organisation.

AWS CLI & AWS SDKs

Pour supprimer une organisation

Utilisez l'une des commandes suivantes pour supprimer une organisation :

- AWS CLI : delete-organization

L'exemple suivant supprime l'organisation pour laquelle le Compte AWS dont les informations d'identification sont utilisées est le compte de gestion.

```
$ aws organizations delete-organization
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- SDK AWS : DeleteOrganization

Gestion des Comptes AWS de votre organisation

Une organisation est un ensemble de Comptes AWS que vous gérez ensemble. Vous pouvez exécuter les tâches suivantes pour gérer les comptes qui font partie de votre organisation :

- Affichez les détails des comptes de votre organisation. Vous pouvez afficher l'ID unique du compte, son Amazon Resource Name (ARN) et les politiques qui lui sont attachées.
- Exportez la liste de tous les Comptes AWS de votre organisation. Vous pouvez télécharger un fichier .csv qui contient des informations sur chaque compte de votre organisation.
- Invitez des comptes Comptes AWS existants à rejoindre votre organisation. Créez des invitations, gérez les invitations que vous avez créées, et acceptez ou refusez des invitations.
- Créez un Compte AWS dans votre organisation. Créez et consultez un Compte AWS qui fait automatiquement partie de votre organisation.
- Mettre à jour les autres contacts de votre organisation. Mettre à jour les autres contacts pour vos instances Compte AWS de votre organisation.
- Supprimez un Compte AWS de votre organisation. En tant qu'administrateur du compte de gestion, supprimez de votre organisation les comptes membres que vous ne voulez plus gérer. En tant qu'administrateur d'un compte membre, supprimez votre compte de son organisation. Si le compte de gestion a attaché une politique à votre compte membre, il se peut que vous ne puissiez pas supprimer votre compte.
- Supprimez (clôturez) un Compte AWS. Lorsque vous n'avez plus besoin d'un Compte AWS, vous pouvez le clôturer pour empêcher toute utilisation ou toute augmentation des frais.

Impact de l'appartenance à une organisation

- Quel est l'impact sur un Compte AWS qui rejoint une organisation ?
- Quel est l'impact sur un Compte AWS que vous créez dans une organisation ?

Impact sur un Compte AWS qui rejoint une organisation

Lorsque vous invitez un Compte AWS à rejoindre une organisation et que le propriétaire du compte accepte l'invitation, AWS Organizations apporte automatiquement les modifications de configuration suivantes au nouveau compte membre :

- AWS Organizations crée un rôle lié à un service appelé `AWSServiceRoleForOrganizations`. Le compte doit avoir ce rôle si votre organisation prend en charge toutes les fonctions. Vous pouvez supprimer le rôle si l'organisation prend uniquement en charge les fonctions de facturation consolidée. Si vous supprimez le rôle et que vous activez ultérieurement toutes les fonctions dans votre organisation, AWS Organizations recrée le rôle pour le compte.
- Diverses politiques peuvent être attachées à la racine de l'organisation ou à l'unité d'organisation qui contient le compte. Si tel est le cas, ces politiques s'appliquent immédiatement à tous les utilisateurs et rôles du compte invité.
- Vous pouvez activer l'approbation de service pour un autre service AWS pour 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.

> **Note**
>
> Pour les comptes de membres invités, le rôle OrganizationAccountAccessRoleIAM 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, consultez Création du OrganizationAccountAccessRole dans un compte de membre invité.

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.

Impact sur un Compte AWS que vous créez dans une organisation

Lorsque vous créez un compte Compte AWS dans votre organisation, AWS Organizations apporte immédiatement les modifications suivantes au nouveau compte membre :

- AWS Organizations crée un rôle lié à un service appelé `AWSServiceRoleForOrganizations`. Le compte doit avoir ce rôle si votre organisation prend en charge toutes les fonctions. Vous pouvez supprimer le rôle si l'organisation prend uniquement en charge les fonctions de facturation consolidée. Si vous supprimez le rôle et que vous activez ultérieurement toutes les fonctions dans votre organisation, AWS Organizations recrée le rôle pour le compte.

- AWS Organizationscrée le rôle OrganizationAccountAccessRoleIAM. Ce rôle accorde l'accès du compte de gestion au nouveau compte membre. Ce rôle peut être supprimé, mais nous vous recommandons de ne pas le faire afin qu'il soit disponible comme option de récupération.
- Si vous avez des politiques attachées à la racine de l'arborescence des UO, ces politiques s'appliquent immédiatement à tous les utilisateurs et à tous les rôles du compte créé. Les nouveaux comptes sont ajoutés à l'UO racine par défaut.
- Si vous avez activé l'approbation de service pour un autre service AWS pour votre organisation, 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 votre compte créé.

Inviter un Compte AWS homme à rejoindre votre organisation

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.

Lorsque vous invitez un compte AWS Organizations , envoyez une invitation au propriétaire du compte, qui décide d'accepter ou de refuser l'invitation. Vous pouvez utiliser la AWS Organizations console pour lancer et gérer les invitations que vous envoyez à d'autres comptes. Vous ne pouvez envoyer une invitation à un autre compte qu'à partir du compte de gestion de votre organisation.

> **Note**
>
> L'historique et les rapports de facturation de tous les comptes restent dans le compte de souscripteur d'une organisation. Avant de transférer le compte vers une nouvelle organisation, téléchargez les historiques de facturation et de rapports des comptes membres que vous souhaitez conserver. Il peut s'agir notamment de rapports d'utilisation et de coût, de rapports de facturation détaillés ou de rapports générés par Cost Explorer Service.

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. Votre compte peut rejoindre une seule organisation. Si vous recevez plusieurs invitations, vous ne pouvez donc pas en accepter plus d'une.

Lorsqu'un compte accepte l'invitation à rejoindre une organisation, le compte de gestion de l'organisation devient responsable de tous les frais encourus 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.

Lorsqu'un compte invité rejoint votre organisation et que celle-ci passe en mode Toutes les fonctionnalités, le compte de gestion dispose d'un accès administratif complet et d'un contrôle sur le compte du membre invité. Toutefois, contrairement aux comptes créés, le rôle `OrganizationAccountAccessRole` IAM n'est pas automatiquement créé dans le compte membre avec les autorisations que le compte de gestion peut assumer. Pour le créer et le configurer une fois que le compte invité est devenu membre, suivez les étapes indiquéesCréation du OrganizationAccountAccessRole dans un compte de membre invité.

> **Note**
>
> Lorsque vous créez un compte dans votre organisation au lieu d'inviter un compte existant à le rejoindre, crée AWS Organizations automatiquement un rôle IAM (nommé `OrganizationAccountAccessRole` par défaut) que vous pouvez utiliser pour accorder aux utilisateurs du compte de gestion l'accès administrateur au compte créé.

AWS Organizations crée automatiquement un rôle lié à un service dans les comptes des membres invités afin de faciliter l'intégration entre les services AWS Organizations et les autres AWS . Pour plus d'informations, consultez AWS Organizations et rôles liés à un service.

Pour connaître le nombre d'invitations que vous pouvez envoyer par jour, consultez Valeurs 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. Elle est décomptée si le compte invité refuse, si le compte de gestion annule l'invitation ou l'invitation expire.

Pour créer un compte qui fait automatiquement partie de votre organisation, consultez Création d'un compte membre dans votre organisation.

Important

En raison des contraintes de facturation, vous Comptes AWS ne pouvez inviter que le même AWS vendeur (dans le cas de l' AWS Inde) et le AWS partitionner en tant que compte de gestion.

- Tous les comptes d'une organisation doivent provenir du même vendeur enregistré que le compte de gestion si le compte de gestion de votre organisation a été créé par Amazon Web Services India Private Limited (« AWS Inde ») (anciennement Amazon Internet Services Private Limited). Par exemple, en tant que AWS vendeur en Inde, vous ne pouvez inviter que d'autres comptes AWS indiens à rejoindre votre organisation. Vous ne pouvez pas combiner des comptes AWS en Inde ou ceux d'un autre AWS vendeur.
- 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 possédant des comptes issus de la partition China Regions ou des comptes de la partition AWS GovCloud (US) Regions.

Envoi d'invitations à des Comptes AWS

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 plus d'informations, consultez Vérification de l'adresse e-mail. 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 SDK : InviteAccountToOrganization

Gestion des invitations en attente pour votre organisation

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.

   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 SDK : ListHandshakesForOrganization, CancelHandshake

Acceptation ou refus d'une invitation d'une organisation

Compte AWS Il se peut que vous receviez une invitation à rejoindre une organisation. Vous pouvez accepter ou refuser l'invitation. Pour ce faire, exécutez les étapes suivantes.

> **Note**
>
> Le statut d'un compte auprès d'une organisation a un impact sur les données de coût et d'utilisation qui sont 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.

Note

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 membre, ce compte doit quitter l'organisation actuelle avant d'accepter l'invitation. Si une invitation est envoyée à un compte de gestion qui fait déjà partie d'une AWS Organization, ce compte ne pourra pas accepter l'invitation tant qu'il n'aura pas supprimé tous les comptes membres de son organisation et supprimé l'organisation.

Autorisations minimales

Pour accepter ou refuser une invitation à rejoindre une AWS 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`.
- `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 d'autres AWS services. Pour plus d'informations, consultez AWS Organizations et rôles liés à un service.

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 à un service dans le nouveau compte membre pour faciliter l'intégration entre les services AWS Organizations et les autres AWS . Pour plus d'informations, consultez AWS Organizations et rôles liés à un service.

     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 SDK : AcceptHandshake, DeclineHandshake

Création d'un compte membre dans votre organisation

Cette page décrit comment créer des Comptes AWS au sein de votre organisation dans AWS Organizations. Pour en savoir plus sur la mise en route avec AWS et la création d'un Compte AWS unique, consultez Centre de ressources de mise en route.

Une organisation est un ensemble de Comptes AWS que vous gérez de façon centralisée. Vous pouvez exécuter les procédures suivantes pour gérer les comptes qui font partie de votre organisation :

- Création d'un Compte AWS qui fait partie de votre organisation
- Accès à un compte membre possédant un rôle d'accès au compte de gestion

Important

- Lorsque vous créez un compte membre dans votre organisation, AWS Organizations crée automatiquement un rôle AWS Identity and Access Management (IAM) `OrganizationAccountAccessRole` dans le compte membre qui permet aux utilisateurs et rôles du compte de gestion d'exercer un contrôle administratif total sur le compte membre. Ce rôle est soumis à toutes les politiques de contrôle des services qui s'appliquent au compte membre.

  AWS Organizations ajoute aussi automatiquement une politique gérée avec le `OrganizationAccountAccessRole` rôle au compte membre. Cela permet un contrôle centralisé, de sorte que tous les comptes supplémentaires attachés à la même politique gérée seront automatiquement mis à jour chaque fois que la politique est mise à jour. Auparavant, les nouveaux comptes créés au sein d'une organisation ont été ajoutés à une politique intégrée qui ne s'appliquait qu'à ce compte unique. Pour en savoir plus sur les politiques en ligne, veuillez consulter politiques gérées et politiques en ligne dans le guide de l'utilisateur IAM.

  AWS Organizations crée également automatiquement un rôle lié au service nommé `AWSServiceRoleForOrganizations` et qui permet l'intégration avec une sélection de services AWS. Vous devez configurer les autres services pour permettre l'intégration. Pour de plus amples informations, consultez AWS Organizations et rôles liés à un service.
- Si cette organisation est gérée avecAWS Control Tower, créez vos comptes en utilisant la fonctionnalité AWS Control Tower Account Factory dans la console AWS Control Tower ou des API. Si vous créez un compte dans Organizations, ce compte n'est pas inscrit dans 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 AWS Control Tower.

Note

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

Création d'un Compte AWS qui fait partie de votre organisation

Après vous être connecté au compte de gestion de l'organisation, vous pouvez créer des comptes membres qui font automatiquement partie de votre organisation. Lorsque vous créez un compte à l'aide de la procédure suivante, AWS Organizations copie automatiquement les informations de contact principal suivantes du compte de gestion vers le nouveau compte membre :

- Phone number (Numéro de téléphone)
- Nom de la société
- URL du site Web
- Address

Elle copie également le langage de communication et les informations relatives à la Marketplace (le vendeur du compte dans certaines Régions AWS) à partir du compte de gestion.

> **Note**
>
> AWS ne collecte pas automatiquement toutes les informations nécessaires au fonctionnement d'un compte membre en tant que compte autonome. Si vous souhaitez supprimer un compte membre d'une organisation et en faire un compte autonome, vous devez fournir ces informations pour le compte avant de pouvoir le supprimer. Pour de plus amples informations, veuillez consulter Quitter une organisation depuis votre compte membre.

> **Autorisations minimales**
>
> Pour créer un compte membre dans votre organisation, vous devez disposer des autorisations suivantes :
>
> - `organizations:CreateAccount`
> - `organizations:DescribeOrganization` — requis uniquement si vous utilisez la console Organizations
> - `iam:CreateServiceLinkedRole` (accordé au principal `organizations.amazonaws.com` pour permettre la création du rôle lié à un service requis dans les comptes membres).

AWS Management Console

Pour créer un Compte AWS qui fait automatiquement partie 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, 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 AWSNom 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 un autre Compte AWS, car elle devient l'identification du nom d'utilisateur pour l'utilisateur racine 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 aucun nom, AWS Organizations donne au rôle le nom par défaut `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 un 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 rechercher dans le journal AWS CloudTrail des informations indiquant si la création du compte a réussi. Pour de plus amples informations, veuillez consulter Journalisation et surveillance dans 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 et administration des comptes membres de votre organisation.

> **Note**
>
> Lorsque vous créez un nouveau compte, AWS Organizations attribue initialement à l'utilisateur racine un mot de passe aléatoire, long (64 caractères) et complexe. Vous ne pouvez pas récupérer ce mot de passe initial. Pour accéder au compte en tant qu'utilisateur racine pour la première fois, vous devez suivre le processus de récupération du mot de passe. Pour de plus amples informations, veuillez consulter Accès à un compte membre en tant qu'utilisateur racine.

AWS CLI & AWS SDKs

Pour créer un Compte AWS qui fait automatiquement partie de votre organisation

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

- AWS CLI : create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
```

```
        }
}
```

Vous pouvez ensuite vérifier l'état de la création du compte à l'aide de la commande suivante.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- SDK AWS : CreateAccount

Accès et administration des comptes membres de votre organisation

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 entre tous vos comptes. Dans ce guide, nous utilisons ce nom par défaut pour faire référence au rôle. AWS Organizations ne crée aucun autre utilisateur ou rôle. Pour accéder aux comptes de votre organisation, vous devez utiliser l'une des méthodes suivantes :

- Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur root du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent

de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant les informations d'identification de l'utilisateur root dans le Guide de l'utilisateur IAM. Pour des recommandations supplémentaires de sécurité pour l'utilisateur root, consultez Bonnes pratiques d'utilisateur root pour votre Compte AWS.

- Si vous créez un compte à l'aide des outils fournis avec AWS Organizations, vous pouvez y accéder en utilisant le rôle préconfiguré `OrganizationAccountAccessRole` qui existe dans tous les nouveaux comptes créés de cette manière. Pour plus d'informations, consultez Accès à un compte membre possédant un rôle d'accès au compte de gestion.
- 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 du OrganizationAccountAccessRole dans un compte de membre invité. Après avoir créé le rôle, vous pouvez y accéder grâce à la procédure décrite dans Accès à un compte membre possédant un rôle d'accès au compte de gestion.
- Utilisez AWS IAM Identity Center et activez l'accès de confiance à IAM Identity Center avec AWS Organizations. Cela permet aux utilisateurs de se connecter au portail d'accès AWS avec les informations d'identification de leur entreprise et d'accéder aux ressources dans le compte de gestion qui leur est attribué ou dans les comptes membres.

  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.

> **Autorisations minimales**
>
> Pour accéder à un Compte AWS à partir de n'importe quel autre compte de votre organisation, vous devez disposer de l'autorisation suivante :
>
> - `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.

Accès à un compte membre en tant qu'utilisateur racine

Lorsque vous créez un nouveau compte, AWS Organizations attribue initialement à l'utilisateur racine un mot de passe comportant au moins 64 caractères. Tous les caractères sont générés de façon aléatoire, sans aucune garantie sur l'apparence de certains jeux de caractères. Vous ne pouvez pas récupérer ce mot de passe initial. Pour accéder au compte en tant qu'utilisateur racine pour la première fois, 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.

Remarques

- En tant que bonne pratique, nous vous recommandons de ne pas utiliser l'utilisateur racine pour accéder à votre compte pour des activités autres que la création d'autres utilisateurs et rôles avec des autorisations plus limitées. Ensuite, connectez-vous en tant que l'un de ces utilisateurs ou rôles.
- Nous vous recommandons également d'activer l'authentification multifactorielle (MFA) sur l'utilisateur root. Réinitialisez le mot de passe et attribuez un dispositif MFA à l'utilisateur racine.
- Si vous avez créé un compte membre dans une organisation avec une adresse e-mail incorrecte, vous ne pouvez pas vous connecter au compte en tant qu'utilisateur racine. Contactez AWS Billing and Support pour obtenir de l'aide.

Création du OrganizationAccountAccessRole dans un compte de membre invité

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 membre possédant un rôle d'accès au compte de gestion.

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'administration AWS Organizations dans un compte membre

1. Connectez-vous à la console IAM à l'adresse https://console.aws.amazon.com/iam/. 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 prendre note des points suivants :

   - 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 l'adresse https://console.aws.amazon.com/iam/. 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 des ARN.
14. Entrez le numéro d'ID du compte membre AWS, puis indiquez le nom du rôle que vous avez créé précédemment aux étapes 1 à 8. Choisissez Ajouter des ARN.
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. Choisissez l'onglet Permissions (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 qui sont membres du groupe sélectionné peuvent désormais utiliser les adresses URL 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 membre possédant un rôle d'accès au compte de gestion.

Accès à un compte membre possédant un rôle d'accès au compte de gestion

Lorsque vous créez un compte membre à l'aide de la console AWS Organizations, AWS Organizations crée automatiquement un rôle IAM nommé `OrganizationAccountAccessRole` dans le compte. 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 du OrganizationAccountAccessRole dans un compte de membre invité. 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 à l'adresse https://console.aws.amazon.com/iam/ en tant qu'utilisateur avec des autorisations d'administration 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, tapez **STS** dans la zone de recherche pour filtrer la liste, puis choisissez l'option STS.
4. Dans la section Actions, tapez **assume** dans la zone de recherche pour filtrer la liste, puis choisissez l'AssumeRoleoption.
5. Dans la section Ressources, choisissez Spécifique, choisissez Ajouter des ARN, puis tapez le numéro de compte du membre et le nom du rôle que vous avez créé dans la section précédente (nous vous recommandons de le nommer`OrganizationAccountAccessRole`).
6. Choisissez Ajouter des ARN lorsque la boîte de dialogue affiche le bon ARN.

7. (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.
8. Choisissez Suivant.
9. 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.
10. Choisissez Créer une politique pour enregistrer votre nouvelle politique gérée.
11. 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.
12. Choisissez l'onglet Autorisations, puis Ajouter des autorisations, et enfin Attacher des politiques.
13. (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 10 apparaisse. Vous pouvez également filtrer toutes les politiques AWS gérées en choisissant Tous les types, puis en choisissant Gestion par le client.
14. Cochez la case à côté de votre politique, puis choisissez Joindre des politiques.

Les utilisateurs IAM qui sont membres du groupe disposent désormais d'autorisations pour endosser le nouveau rôle dans la console AWS Organizations en suivant la procédure ci-dessous.

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 console AWS Organizations, choisissez le lien qui contient 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 (celui que vous avez spécifié comme nom d'affichage), puis cliquez sur Retour à. *UserName*

Ressources supplémentaires

- Pour plus d'informations sur l'octroi d'autorisations permettant de changer de rôle, consultez la section Octroi à un utilisateur d'autorisations pour changer de rôle dans le Guide de l'utilisateur IAM.
- Pour plus d'informations sur l'utilisation d'un rôle que vous avez été autorisé à assumer, consultez la section Passer à un rôle (console) dans le guide de l'utilisateur IAM.
- Pour un didacticiel sur l'utilisation des rôles pour l'accès entre comptes, voir Tutoriel : déléguer l'accès à Comptes AWS l'aide de rôles IAM dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la clôture de Comptes AWS, consultez Clôture d'un compte membre de votre organisation.

Exportation des détails de Compte AWS de votre organisation

Avec AWS Organizations, les utilisateurs du compte de gestion et les administrateurs délégués d'une organisation peuvent exporter un fichier .csv contenant les détails de tous les comptes d'une organisation. Par conséquent, les administrateurs de l'organisation peuvent facilement afficher les comptes et filtrer par statut : `ACTIVE`, `SUSPENDED` ou `PENDING`. 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.

Auparavant, la seule façon de consulter les comptes était d'examiner la hiérarchie des comptes ou l'affichage liste dans la AWS Organizationsconsole https://console.aws.amazon.com/organizations/v2.

> **Note**
>
> Seuls les principaux du compte de gestion peuvent télécharger la liste des comptes.

Exportation de la liste de tous les Comptes AWS 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`.
- 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 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.

Suppression d'un compte membre de votre organisation

Une partie de la gestion des comptes d'une organisation consiste à supprimer des comptes membres dont vous n'avez plus besoin. La suppression d'un compte membre ne ferme pas le compte, mais le retire de l'organisation. L'ancien compte membre devient un Compte AWS autonome 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.

Pour en savoir plus sur la suppression du compte de gestion, consultez Suppression d'une organisation.

Rubriques

Éléments à prendre en considération avant de supprimer un compte d'une organisation

Avant de supprimer un compte, il est important de tenir compte des points suivants :

- Vous ne pouvez supprimer un compte de votre organisation que si le compte possède les informations requises pour pouvoir fonctionner comme compte autonome. Quand vous créez un compte dans une organisation avec la console AWS Organizations, l'API ou les commandes AWS CLI, toutes les informations requises pour les comptes autonomes ne sont pas collectées automatiquement. Pour chaque compte que vous souhaitez rendre autonome, vous devez choisir un plan de support, fournir et vérifier les informations de contact nécessaires, puis indiquer un moyen de paiement. AWS utilise ce moyen de paiement pour débiter les frais de toutes les activités AWS facturables (ne faisant pas partie de l'offre gratuite AWS) qui interviennent tant que le compte n'est pas attaché à une organisation. Pour supprimer un compte qui ne possède pas encore ces informations, suivez les étapes de Quitter une organisation depuis votre compte membre.
- Pour supprimer un compte que vous avez créé dans l'organisation, vous devez attendre au moins sept jours après la création du compte. Les comptes invités ne sont pas soumis à cette période d'attente.
- Au moment où le compte quitte avec succès l'organisation, le propriétaire du Compte AWS devient responsable de tous les nouveaux frais AWS encourus et c'est le moyen de paiement du compte qui est utilisé. Le compte de gestion de l'organisation n'est plus responsable.
- Le compte que vous souhaitez supprimer ne peut pas être un compte administrateur délégué pour les services AWS activés 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 administrateur délégué d'un service AWS, consultez la documentation de ce service.
- Même après la suppression des comptes créés (comptes créés à l'aide de la console AWS Organizations ou de l'API `CreateAccount`) d'une organisation, (i) les comptes créés sont régis par les conditions de l'accord du compte de gestion créateur avec nous et (ii) le compte de gestion créateur reste conjointement et séparément responsable des actions prises par les comptes qu'il

a créés. Les accords du client avec nous, ainsi que les droits et obligations issus de ces accords, ne peuvent pas être attribués ni transférés sans notre accord préalable. Pour obtenir notre accord, contactez AWS.

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

Effets de la suppression d'un compte d'une organisation

Lorsque vous supprimez un compte d'une organisation, aucune modification directe n'est effectuée sur le compte. Cependant, les effets indirects suivants ont lieu :

- Le compte est désormais responsable du paiement de ses propres frais et un moyen de paiement valide doit lui être attaché.
- 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 les SCP disparaissent et que les utilisateurs et rôles du compte peuvent disposer de plus d'autorisations qu'avant. Les autres types de politiques d'organisation ne peuvent plus être appliqués ni traités.
- Si vous utilisez la clé de condition `aws:PrincipalOrgID` dans des politiques pour restreindre l'accès aux seuls utilisateurs et rôles des Comptes AWS de votre organisation, vous devez revoir et éventuellement mettre à jour ces politiques avant de supprimer le compte membre. Si vous ne mettez pas à jour les politiques, les utilisateurs et les rôles du compte risquent de perdre l'accès aux ressources lorsque le compte quitte l'organisation.
- L'intégration à d'autres services peut être désactivée. Si vous supprimez un compte d'une organisation qui dispose d'une intégration avec un service AWS, les utilisateurs de ce compte ne peuvent plus utiliser ce service.

Supprimer un compte membre de votre 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.

> **Note**
>
> 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 console AWS Artifact sur la page AWS ArtifactAccords d'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 naviguer dans la hiérarchie des UO ou activer Afficher uniquement les Comptes AWSpour afficher une liste non hiérarchique des comptes sans la structure des unités 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 des unités d'organisation (choisissez l'icône ▶) pour trouver le compte souhaité.
3. Choisissez Actions, puis, sous Compte AWS, choisissez Supprimer de l'organisation.
4. Dans la boîte de dialogue Supprimer le compte « nom-compte » (n°id-compte) de l'organisation ?, choisissez Supprimer le compte.
5. Si AWS Organizations échoue dans la suppression d'un ou plusieurs comptes, la raison est généralement que vous n'avez pas fourni toutes les informations requises pour que le compte puisse opérer 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 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. Après que vous avez réalisé la dernière étape de connexion, AWS redirige automatiquement votre navigateur vers la console AWS Organizations pour le 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.

- SDK AWS : 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 votre compte membre.

Quitter une organisation depuis votre compte membre

Lorsque vous êtes connecté à un compte membre, vous pouvez retirer ce compte de son organisation. Pour ce faire, procédez comme suit : Cette procédure s'applique uniquement aux comptes membres. 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.

Note

Le statut d'un compte auprès d'une organisation a un impact sur les données de coût et d'utilisation qui sont 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.

Important

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 afficher la liste de ces accords d'organisation dans la console AWS Artifact sur la page Accords d'organisation AWS Artifact. 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.

Autorisations minimales

Pour quitter une organisation AWS, 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 console AWS Organizations via le lien 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 un compte membre.

   Par défaut, vous n'avez pas accès au mot de passe de l'utilisateur racine d'un compte membre compte créé avec AWS Organizations. Si nécessaire, récupérez le mot de passe de l'utilisateur racine en suivant les étapes décrites dans Accès à un compte membre en tant qu'utilisateur racine.
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. Vous êtes ensuite redirigé vers la page de démarrage de la console AWS Organizations, depuis laquelle vous pouvez consulter les invitations à rejoindre d'autres organisations en attente.

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.
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 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.
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.

- SDK AWS : 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 en utilisant plutôt remove-account-from-organization. Pour de plus amples informations, veuillez consulter Supprimer un compte membre de votre organisation.

Clôture d'un compte membre de votre organisation

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 section. 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.

Clôture d'un compte 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.
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. Organisations en mode facturation consolidée ne pourront pas voir le bouton Fermer dans la console. Pour

fermer un compte en mode de facturation consolidée, suivez les étapes décrites dans l'onglet Compte autonome de la section Comment fermer votre compte du Guide de gestion de AWS compte.

4. Cochez chaque case pour accuser réception de tous les relevés de clôture de compte requis.
5. Entrez l'identifiant du compte du membre, puis choisissez Fermer le compte.

> **Note**
>
> Tout compte de membre que vous fermez affichera une `SUSPENDED` étiquette à côté de son nom dans la AWS Organizations console.

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 SDK : CloseAccount

Protection des comptes membres contre la clôture

Si vous souhaitez empêcher la clôture accidentelle d'un compte membre, vous pouvez créer une politique IAM pour spécifier les comptes qui n'ont pas besoin d'être clôturés. Aucun compte membre protégé par ces politiques ne peut être clôturé. Cela ne peut pas être réalisé avec un SCP, car ils n'affectent pas les principaux du compte de gestion.

Vous pouvez créer une politique IAM qui empêche la clôture de comptes de deux manières :

- Indiquer explicitement chaque compte que vous souhaitez protéger dans la politique en incluant l'`arn` dans l'élément `Resource`. Vous trouverez un exemple dans Protection des comptes membres répertoriés dans cette politique contre la clôture.
- Étiqueter les comptes individuels pour éviter qu'ils ne soient clôturés. Utilisez la clé de condition globale d'identification `aws:ResourceTag` dans votre politique pour empêcher la clôture de tout compte labelisé. Pour savoir comment étiqueter un compte, consultez Étiquetage des ressources Organizations. Vous trouverez un exemple dans Protection des comptes membres auxquels une balise est associée contre la clôture .

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.

Protection des comptes membres auxquels une balise est associée contre la clôture

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`AccountType`Key et`Critical`valeur de balise.

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

Protection des comptes membres répertoriés dans cette politique contre la clôture

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"
            ]
        }
    ]
}
```

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.

Comment fermer un 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 les sections 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 et assurez-vous que tous les comptes des membres apparaissent à `Suspended` côté de leur nom de compte. Si vous avez un compte membre toujours actif, vous devrez suivre les instructions fournies Clôture d'un compte membre de votre 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, faites défiler la page vers le bas jusqu'à la section Fermer le compte. Lisez le processus de fermeture du compte et assurez-vous de bien le 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 SDK. Vous ne pouvez effectuer cette tâche qu'à l'aide du AWS Management Console.

Mise à jour d'autres contacts de votre organisation

Vous pouvez mettre à jour d'autres contacts pour les comptes de votre organisation à l'aide de la console AWS Organizations ou par programmation à l'aide de la CLI AWS ou des SDK AWS. Pour en savoir plus sur la mise à jour d'autres contacts, consultez Accès à d'autres contacts et mise à jour de ceux-ci dans la Référence de gestion de comptes AWS.

Mettre à jour les coordonnées principales de votre organisation

Vous pouvez mettre à jour d'autres coordonnées pour les comptes de votre organisation à l'aide de la console AWS Organizations ou par programmation à l'aide d'AWS CLI ou des SDK d'AWS. Pour savoir comment mettre à jour les coordonnées principales, consultez la section Accès ou mise à jour des coordonnées principales du compte dans le document Référence de gestion de comptes AWS.

Mise à jour des Régions AWS activées dans votre organisation

Vous pouvez mettre à jour les Régions AWS activées pour des comptes dans votre organisation à l'aide de la console AWS Organizations. Pour savoir comment mettre à jour les Régions AWS activées, consultez la section Spécifier quelles Régions AWS votre compte peut utiliser dans la Référence de gestion des comptes AWS.

Gestion des politiques dans 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.

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 des Comptes AWS de votre organisation.

- Les politiques de contrôle des services (SCP) offrent un contrôle central sur les autorisations maximales disponibles pour tous les comptes de votre organisation.

Politiques de gestion

Les politiques de gestion vous permettent de configurer et de gérer de manière centralisée les AWS services et leurs fonctionnalités.

- Les politiques de désactivation des services d'intelligence artificielle (IA) vous permettent de contrôler la collecte de données pour les services IA d' AWS pour tous les comptes de votre organisation.
- Les politiques de sauvegarde vous permettent de gérer et d'appliquer des plans de sauvegarde de manière centralisée aux AWS ressources des comptes de votre entreprise.
- Les politiques relatives aux balises vous aident à standardiser les balises associées aux AWS ressources des comptes de votre 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 pour AWS Organizations.

Type de stratégie	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	 Non	5	5 120 octets	 Non
Politique de désactivation des services IA	 Oui	5	2 500 caractères	 Oui
Politique de sauvegarde	 Oui	10	10 000 caractères	 Oui
Politique de balises	 Oui	10	10 000 caractères	 Oui

Utilisation de politiques dans votre organisation

- Activation et désactivation des types de politiques
- Obtenir des informations sur les politiques de votre organisation
- Administrateur délégué pour AWS Organizations

- Politiques de gestion
- Politiques de contrôle de service (SCP)

Activation et désactivation des types de politiques

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.

> **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. Dans la page du type de politique, choisissez Activer ***type de politique***.

   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` ».

- SDK AWS : 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 à partir du compte de gestion de l'organisation.

Important

- 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 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 attachements de politiques SCP aux entités sont perdues lorsque les SCP sont désactivées dans l'organisation. Si vous souhaitez réactiver ultérieurement les SCP, vous devez les rattacher à la racine, aux unités d'organisation et aux comptes de l'organisation, selon les nécessités.

Autorisations minimales

Pour désactiver les SCP, vous avez avoir l'autorisation d'effectuer 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. Dans la page du type de politique, choisissez Désactiver ***type de politique***.
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.

- SDK AWS : DisablePolicyType

Obtenir des informations sur les politiques de votre organisation

Cette section décrit différentes méthodes pour obtenir des informations 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.

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 afficher les politiques de votre organisation dans la AWS Management Console ou en utilisant une commande d'AWS Command Line Interface (AWS CLI) ou une opération de SDK AWS.

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

Pour répertorier toutes les politiques de votre organisation

Vous pouvez utiliser l'une des commandes suivantes pour répertorier les politiques d'une organisation :

- AWS CLI : list-policies

  L'exemple suivant montre comment obtenir une liste de toutes les politiques de contrôle des services de votre organisation. Vous devez spécifier le type de politique que vous souhaitez voir. Répétez la commande pour chaque type de politique à inclure.

```
$ aws organizations list-policies \
    --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
        }
    ]
}
```

- SDK AWS : ListPolicies

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. Vous devrez peut-être développer des unités d'organisation (choisissez l'icône ▶) pour trouver l'UO 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
        }
    ]
}
```

- SDK AWS : ListPoliciesForTarget

Liste de l'ensemble des racines, UO et comptes auxquels la 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 l'ensemble des racines, UO et comptes auxquels une stratégie spécifiée 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 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 l'ensemble des racines, UO et comptes auxquels une stratégie spécifiée est attachée

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 tous les attachements à la racine, aux UO et aux comptes de la politique spécifiée.

```
$ 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"
        }
    ]
}
```

- SDK AWS : 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, UO et comptes auxquels la politique est attachée.
   - 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

Pour obtenir des détails sur une politique

Vous pouvez utiliser l'une des commandes suivantes pour obtenir des détails sur une politique :

- AWS CLI : describe-policy

  L'exemple suivant affiche les détails de la politique spécifiée.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "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
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- SDK AWS : DescribePolicy

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. En effet, les fonctionnalités de sécurité telles que les politiques de contrôle des services (SCP) de l'organisation ne restreignent 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.

Création ou mise à jour d'une politique de délégation basée sur les ressources

À partir du compte de gestion, créez ou 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 créer ou mettre à jour la politique de délégation basée sur les ressources, vous devez posséder l'autorisation d'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.

Utilisez l'éditeur de politique JSON afin de créer ou 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. Sélectionnez Settings (Paramètres).
3. Dans la section Administrateur délégué pour AWS Organizations, choisissez Delegate (Déléguer) pour créer la politique de délégation Organizations. Pour mettre à jour une politique de délégation existante, choisissez Edit (Modifier).
4. Composez ou collez un document de politique 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).

Utilisez l'éditeur visuel pour créer ou 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. Sélectionnez Settings (Paramètres).
3. Dans la section Administrateur délégué pour AWS Organizations, choisissez Delegate (Déléguer) pour créer la politique de délégation Organizations. Pour mettre à jour une politique de délégation existante, choisissez Edit (Modifier).
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. Pour de plus amples informations sur la syntaxe, consultez Exemple de politiques de délégation basées sur les ressources.
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 membre délégué peut attacher des politiques à la racine de l'organisation ou aux unités d'organisation, veuillez définir les `Resources`. Vous devez également sélectionner `policy` comme type de ressource. Pour plus de détails, veuillez

consulter Exemple de politiques de délégation basées sur les ressources. 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 ARN des ressources 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 de plus amples informations sur l'utilisation des ARN dans l'élément ressource d'une politique, consultez Éléments de politique JSON IAM : Resource.

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`**. Pour plus de détails, veuillez consulter Exemple de politiques de délégation basées sur les ressources. 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 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.

Afficher une politique de délégation basée sur les ressources

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. Sélectionnez Settings (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

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. Sélectionnez Settings (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

Exemple de politiques de délégation basées sur les ressources

Les exemples de code suivant montrent comment vous pouvez utiliser les politiques de délégation basées sur les ressources.

Exemples

- Exemple : afficher l'organisation, les unités d'organisation, les comptes et les politiques
- Exemple : autorisations consolidées de gérer les politiques de sauvegarde d'une organisation

Exemple : afficher l'organisation, les unités d'organisation, les comptes et les politiques

Avant de déléguer la gestion des politiques, vous devez déléguer les autorisations permettant de naviguer dans la structure d'une organisation et de consulter les unités organisationnelles, les comptes et les politiques qui leur sont attachées.

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 réaliser ces actions de manière programmatique à partir de l'API AWS ou de la AWS CLI. Pour utiliser cette politique de délégation, remplacez l'espace réservé AWS pour *AccountId* par vos propres informations. Ensuite, suivez les instructions dans Administrateur délégué pour AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId: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 : 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`. Pour comprendre la signification de chaque action, ressource et condition, voir Exemple de politiques de délégation basées sur les ressources.

> **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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId: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": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Politiques de gestion

Les politiques de gestion vous permettent de configurer et de gérer de manière centralisée les services AWS et leurs fonctions. La manière dont les politiques affectent les UO et les comptes qui en héritent dépend du type de politique de gestion que vous appliquez dans AWS Organizations. Consultez les rubriques de cette section pour comprendre les termes et concepts pertinents relatifs aux politiques de gestion.

Rubriques

Fonctionnement de l'héritage des politiques de gestion

> **Note**
>
> Les informations contenues dans cette section ne s'appliquent pas aux SCP, car ces dernières gèrent à la fois l'autorisation et le refus des actions IAM. Bien que les SCP soient attachés à la racine, aux UO et aux comptes, l'autorisation des actions nécessite une instruction `allow` explicite dans les SCP à chaque niveau, de la racine via chaque UO sur le chemin d'accès direct au compte (y compris le compte cible lui-même). Pour plus d'informations sur le fonctionnement des SCP dans une hiérarchie AWS Organizations, consultez la rubrique Évaluation du SCP.

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 politique de gestion à la racine de l'organisation, toutes les UO et tous 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.

Cette section explique comment les politiques parentes et les politiques enfants sont traitées dans 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 attacher des politiques à la racine de l'organisation, à des unités d'organisation, 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. Par exemple, les politiques de balises vous permettent d'afficher la politique de balises effective qui s'applique à l'un de vos comptes. Pour de plus amples informations, consultez Affichage des politiques de balises effectives.

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 dont les politiques affectent les UO et les comptes qui en héritent dépend du type de politique de gestion que vous choisissez. Les types de politiques de gestion sont les suivants :

- Politiques de désactivation des services d'intelligence artificielle (IA)
- Stratégies de sauvegarde
- Stratégies de balises

La syntaxe des types de politiques de gestion inclut des Opérateurs d'héritage, qui permettent de spécifier avec précision quels éléments des politiques parentes sont appliqués et quels éléments peuvent être remplacés ou modifiés lorsqu'ils sont hérités par des UO et des comptes enfants.

La politique effective correspond à l'ensemble de règles héritées de la racine de l'organisation et des unités d'organisation, ainsi qu'à celles directement attachées 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 Affichage des politiques de balises effectives.

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 dans la console AWS Organizations, vous pouvez uniquement utiliser l'opérateur `@@assign`. 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.

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.

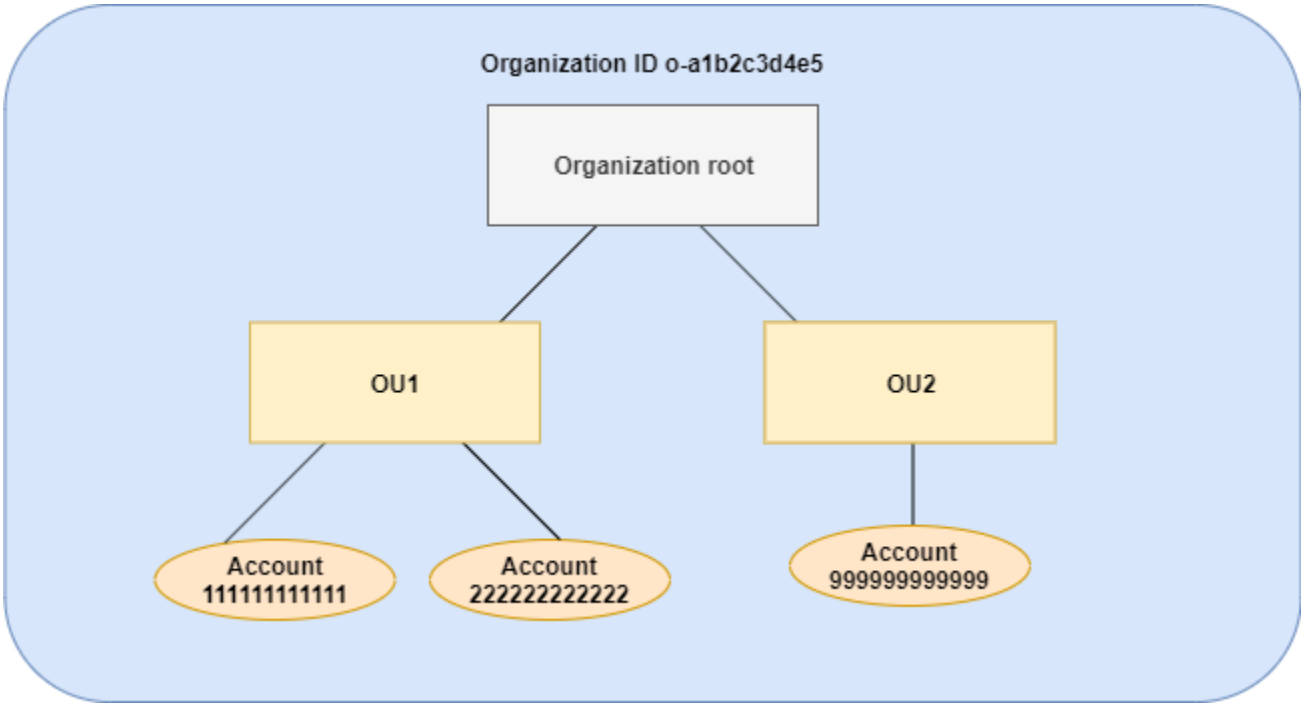
- `"@@operators_allowed_for_child_policies":["@@all"]` : les unités d'organisation et les comptes enfants peuvent utiliser n'importe quel opérateur dans les politiques. Par défaut, tous les opérateurs sont autorisés dans les politiques enfants.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` : les UO et comptes enfants peuvent uniquement utiliser les opérateurs spécifiés dans les politiques enfants. Vous pouvez spécifier un ou plusieurs opérateurs de définition de valeurs dans cet opérateur de contrôle enfant.
- `"@@operators_allowed_for_child_policies":["@@none"]` : les UO et comptes enfants ne peuvent pas utiliser d'opérateur 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 utilisateurs d'OU1 utilisent une valeur de balise différente pour une clé et que vous souhaitiez appliquer la politique de balise à certains types de ressources. 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'opérateur `@@assign` et créer une politique de balises telle que ci-dessous pour l'attacher à OU1.

Politique B : politique d'identifications attachée à l'unité organisationnelle 1

```
{
    "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 illustré dans le diagramme, OU1 comprend 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.

Politique C : politique d'identifications attachée à l'unité organisationnelle 2 pour ajouter des valeurs

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
```

```
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

L'attachement de la politique C à OU2 a les effets suivants lorsque la politique A et la politique C fusionnent pour constituer la politique de balises effective d'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 illustré dans le diagramme, OU2 comprend 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 exécuté tous les exemples précédents, les politiques B, C et D sont des politiques enfants de A. La politique B étant uniquement attachée à OU1, elle n'a 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 ajoutiez d'autres comptes à OU2 ultérieurement, leurs politiques de balises effectives seraient 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"
```

```
            ]
        }
    }
}
```

Politiques de désactivation des services IA

Les services d'intelligence artificielle (IA) d'AWS, notamment Amazon Rekognition, Amazon CodeWhisperer, Amazon Transcribe et Contact Lens for Amazon Connect, peuvent stocker et utiliser le contenu client traité par ces services pour le développement et l'amélioration continue d'autres services AWS. En tant que client AWS, vous pouvez refuser que votre contenu soit stocké ou utilisé à des fins d'amélioration des services.

> **Note**
>
> Les services d'intelligence artificielle (IA) d'AWS pourraient avoir besoin de stocker votre contenu pour fournir les services, même si vous refusez qu'AWS utilise vos données pour l'amélioration des services. Pour plus d'informations, consultez la documentation du service d'IA que vous utilisez.

Au lieu de configurer ce paramètre individuellement pour chaque Compte AWS que votre organisation utilise, vous pouvez configurer une politique d'organisation qui applique votre choix de paramètre à tous les comptes qui sont membres de l'organisation. Vous pouvez choisir de refuser le stockage et l'utilisation du contenu pour un service IA individuel ou pour tous les services couverts en même temps. Vous pouvez interroger la politique effective applicable à chaque compte pour voir les effets de vos choix de paramètres.

> **Important**
>
> - Lorsque vous spécifiez une préférence d'activation ou de désactivation pour un service, ce paramètre est mondial et appliqué à toutes les Régions AWS. Le réglage de la valeur à partir d'une Région AWS se propage dans toutes les autres régions.
> - Lorsque vous désactivez l'utilisation du contenu par un service IA AWS, ce service supprime tout le contenu historique associé qui a été partagé avec AWS avant votre choix d'option. Cette suppression doit être limitée aux données stockées qui ne sont pas requises pour fournir des fonctions de service.

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. Activez les politiques de désactivation des services IA pour votre organisation.
2. Créez une politique de désactivation des services IA.
3. Attachez la politique de désactivation des services IA à la racine, une UO ou un compte de votre organisation.
4. Affichez la politique combinée de désactivation des services IA qui s'applique à un compte.

Pour effectuer toutes ces étapes, vous devez vous connecter en tant qu'utilisateur AWS Identity and Access Management (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

- Découvrir la syntaxe de politique pour les politiques de désactivation des services IA et consulter des exemples de politiques

Création, mise à jour et suppression de politiques de désactivation des services IA

Dans cette rubrique :

- Après avoir activé les politiques de désactivation des services IA pour votre organisation, vous pouvez créer une politique.
- Lorsque vos exigences de désactivation changent, vous pouvez mettre à jour une politique existante.
- Lorsque vous n'avez plus besoin d'une politique et que vous l'avez détachée de toutes les UO et de tous les comptes, vous pouvez la supprimer.

Création d'une politique de désactivation des services 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 Balisage de ressources 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"
        }
    }
}
```

- SDK AWS : CreatePolicy

Suite des opérations

Une fois que vous avez créé une politique de désactivation des services IA, vous pouvez mettre en œuvre vos choix de désactivation. Pour ce faire, vous pouvez attacher la politique à la racine de l'organisation, à des UO, à des Comptes AWS de votre organisation ou à une combinaison de tous ces éléments.

Mise à jour d'une politique de désactivation des services 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"}
}
```

- SDK AWS : UpdatePolicy

Modification des balises attachées à une politique de désactivation des services 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 Balisage de ressources AWS Organizations.

Autorisations minimales

Pour modifier les balises attachées à une politique de désactivation des services IA dans votre organisation AWS, 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
- SDK AWS : TagResource et UntagResource

Suppression d'une politique de désactivation des services IA

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.

> **Autorisations minimales**
>
> Pour supprimer une politique, vous devez avoir l'autorisation d'effectuer l'action suivante :
>
> - `organizations:DescribePolicy` (console uniquement — pour accéder à la politique)
> - `organizations:DeletePolicy`

AWS Management Console

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. La politique à supprimer doit d'abord être détachée de l'ensemble des racines, unités d'organisation et 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 de désactivation des services IA

Vous pouvez utiliser l'une des commandes suivantes pour supprimer une politique :

- AWS CLI : delete-policy

  L'exemple suivant supprime la politique spécifiée. Cela fonctionne uniquement si la politique n'est attachée à aucune racine, aucune UO ni aucun compte.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- SDK AWS : DeletePolicy

Attachement et détachement de politiques de désactivation des services IA

Vous pouvez utiliser des politiques de désactivation des services IA sur l'ensemble d'une organisation ainsi que sur des UO et des comptes individuels. Ce à quoi s'applique la politique de désactivation des services IA dépend de l'élément d'organisation auquel vous l'attachez :

- Lorsque vous attachez une politique de désactivation des services IA à la racine de votre organisation, la politique de sauvegarde s'applique à toutes les UO et tous les comptes membres de cette racine.
- Lorsque vous attachez une politique de désactivation des services IA à une UO, cette politique s'applique aux comptes qui appartiennent à l'UO ou à l'une de ses UO enfants. Ces comptes sont également soumis à toutes les politiques attachées à la racine de l'organisation.
- Lorsque vous attachez une politique de désactivation des services IA à un compte, cette politique s'applique uniquement à ce compte. Le compte est également soumis à toute politique attachée à la racine de l'organisation et aux UO auxquelles le compte appartient.

L'agrégation de toutes les politiques de désactivation des services IA héritées des UO racines et parentes, ainsi que de toutes les politiques directement associées au compte constitue la politique effective. Pour de plus amples informations sur la façon dont les politiques se fusionnent pour former la politique effective, consultez Fonctionnement de l'héritage des politiques de gestion.

> **Autorisations minimales**
>
> Pour attacher des politiques de désactivation des services IA, vous devez avoir l'autorisation d'exécuter l'action suivante :

- `organizations:AttachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône) pour trouver l'UO ou le compte souhaité.
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 des unités d'organisation (choisissez l'icône ) pour trouver l'UO ou le compte souhaité.
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.

AWS CLI & AWS SDKs

Pour attacher une politique de désactivation des services IA à la racine de l'organisation, à une unité d'organisation ou à un compte

Vous pouvez utiliser l'une des commandes suivantes pour attacher une politique de désactivation des services IA :

- AWS CLI : attach-policy

  L'exemple suivant attache une politique à un unité d'organisation.

  ```
  $ aws organizations attach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- SDK AWS : AttachPolicy

La modification de la politique prend effet immédiatement.

Détachement d'une politique de désactivation des services IA

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez détacher une politique de désactivation des services IA de la racine de l'organisation, de l'unité d'organisation ou du compte auquel celle-ci est attachée. Une fois que vous avez détaché une politique de désactivation des services IA d'une entité, cette politique ne s'applique plus à aucun compte qui était affecté par celle-ci. Pour détacher une politique, effectuez les opérations suivantes.

Autorisations minimales

Pour détacher une politique de désactivation des services IA de la racine de l'organisation, de l'unité d'organisation ou du compte, vous devez être autorisé à exécuter l'action suivante :

- `organizations:DetachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône) pour trouver l'UO ou le compte souhaité. 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 des unités d'organisation (choisissez l'icône ▶) pour trouver l'UO ou le compte souhaité.
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.

AWS CLI & AWS SDKs

Pour détacher une politique de désactivation des services IA de la racine de l'organisation, d'une unité organisationnelle ou d'un compte

Vous pouvez utiliser l'une des commandes suivantes pour détacher une désactivation des services IA :

- AWS CLI : detach-policy

  L'exemple suivant détache une politique d'une unité d'organisation.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- SDK AWS : DetachPolicy

La modification de la politique prend effet immédiatement.

Affichage des politiques effectives de désactivation des services IA

Déterminez la politique effective de désactivation des services d'Intelligence artificielle (IA) pour un compte de votre organisation.

Qu'est-ce que la politique effective de désactivation des services IA ?

La politique effective de désactivation des services IA spécifie les règles finales qui s'appliquent à un Compte AWS. Il s'agit de l'agrégation de toutes les politiques de désactivation des services IA héritées par le compte, ainsi que des politiques de désactivation des services IA directement attachées au compte. Lorsque vous attachez une politique de désactivation des services IA à la racine de l'organisation, elle s'applique à tous les comptes de votre organisation. Lorsque vous attachez une politique de désactivation des services IA à une UO, elle s'applique à tous les comptes et UO qui appartiennent à l'UO. Lorsque vous attachez une politique directement à un compte, elle ne s'applique qu'à ce seul Compte AWS.

Par exemple, la politique de désactivation des services IA attachée à la racine de l'organisation peut spécifier que tous les comptes de l'organisation doivent refuser l'utilisation du contenu par tous les services de machine learning AWS. 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. Le résultat est que tous les services AWS sont désactivés pour tous les comptes de l'organisation, à l'exception d'un compte qui accepte Amazon Rekognition.

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.

Comment afficher la politique effective de désactivation des services IA

Vous pouvez afficher la politique effective de désactivation des services IA pour un compte à partir de la AWS Management Console, de l'API AWS ou de l'AWS Command Line Interface.

> **Autorisations minimales**
>
> Pour afficher la politique effective de désactivation des services IA d'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 afficher la politique effective de désactivation des services IA 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. Dans la page Comptes AWS, choisissez le nom du compte dont vous souhaitez afficher la politique effective de désactivation des services IA. Vous devrez peut-être développer des unités d'organisation (choisissez l'icône ▶) pour trouver le compte souhaité.
3. Dans l'onglet Politiques, dans la section Politiques de désactivation des services IA, choisissez Afficher la politique effective de désactivation des services IA pour ce Compte AWS.

   La console affiche la politique effective appliquée au compte spécifié.

   > **Note**
   >
   > Vous ne pouvez pas copier et coller une politique effective et l'utiliser comme le JSON pour une autre politique de désactivation des services IA sans modifications importantes. Les documents de politique de désactivation des services IA doivent inclure les opérateurs d'héritage qui spécifient comment chaque paramètre est fusionné dans la politique effective finale.

AWS CLI & AWS SDKs

Pour afficher la politique effective de désactivation des services IA pour un compte

Vous pouvez utiliser l'une des commandes suivantes pour afficher la politique effective de désactivation des services IA :

- 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"
    }
}
```

- SDK AWS : DescribeEffectivePolicy

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 attacher des politiques enfants à des unités d'organisation ou directement à des comptes pour remplacer ce paramètre pour n'importe quel service IA, 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.
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`
    - `connectamd`
    - `connectoptimization`
    - `contactlens`
    - `datazone`
    - `entityresolution`
    - `frauddetector`
    - `glue`
    - `guardduty`
    - `lex`

- `polly`
- `q`
- `quicksightq`
- `rekognition`
- `securitylake`
- `textract`
- `transcribe`
- `translate`

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 pourraient être affectés par des politiques enfants dans d'autres unités d'organisation ou comptes.

```
{
    "services": {
```

```
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Politiques de sauvegarde

AWS Backup vous permet de créer des plans de sauvegarde qui définissent comment sauvegarder vos ressources AWS. Les règles du plan incluent divers paramètres, notamment la fréquence de sauvegarde, la fenêtre horaire pendant laquelle la sauvegarde a lieu, la Région AWS contenant les ressources à sauvegarder et le coffre-fort dans lequel stocker la sauvegarde. Vous pouvez ensuite appliquer un plan de sauvegarde à des groupes de ressources AWS identifiés à l'aide de balises. Vous devez également identifier un rôle AWS Identity and Access Management (IAM) qui accorde à AWS Backup l'autorisation d'effectuer l'opération de sauvegarde en votre nom.

Les politiques de sauvegarde dans AWS Organizations combinent tous ces éléments dans des documents texte JSON. Vous pouvez attacher une politique de sauvegarde à tous les éléments qui composent la structure de votre organisation, notamment la racine, les unités d'organisation (UO) et les comptes individuels. Organizations applique des règles d'héritage pour combiner les politiques de la racine de l'organisation, de toutes les UO parentes ou attachées au compte. Il en résulte une politique de sauvegarde effective pour chaque compte. Cette politique effective indique à AWS Backup comment sauvegarder automatiquement vos ressources AWS.

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 attacher une politique de sauvegarde aux UO qui remplace la fréquence de sauvegarde en fonction des exigences de chaque UO. 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 attacher ces politiques à différentes parties de l'arborescence de l'organisation, notamment la

racine ou une UO parente, dans le but que ces politiques partielles soient héritées par des UO et des comptes de niveau inférieur. 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. Sinon, AWS Backup considère la politique non valide et ne sauvegarde pas les ressources concernées.

> **Important**
>
> AWS Backup peut uniquement effectuer une sauvegarde réussie s'il est appelé par une politique effective 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 Compte AWS de l'organisation apparaît dans la console AWS Backup comme un plan immuable pour ce compte. Vous pouvez le voir, mais pas le modifier.

Lorsque AWS Backup lance une sauvegarde basée sur un plan de sauvegarde créé par une politique, vous pouvez voir l'état de la tâche de sauvegarde dans la console AWS Backup. 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 au service approuvé avec AWS Backup, un utilisateur du compte de gestion de l'organisation peut voir l'état 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

Conditions préalables et autorisations pour la gestion des politiques de sauvegarde

Cette page décrit les conditions préalables et les autorisations requises pour la gestion des politiques de sauvegarde dans AWS Organizations.

Rubriques

- Conditions préalables pour la gestion des politiques de sauvegarde
- Autorisations pour la gestion des politiques de sauvegarde

Conditions préalables pour la gestion des politiques de sauvegarde

La gestion des politiques de sauvegarde dans une organisation demande ce qui suit :

- Toutes les fonctions doivent être activées pour votre organisation.
- Vous devez être connecté au compte de gestion de votre organisation.
- Votre utilisateur ou rôle AWS Identity and Access Management (IAM) a besoin des autorisations répertoriées dans la section suivante.

Autorisations pour la gestion des politiques de sauvegarde

L'exemple de politique IAM suivant fournit des autorisations pour gérer tous les aspects des politiques de sauvegarde dans une organisation.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "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.

Bonnes pratiques pour l'utilisation des politiques de sauvegarde

AWS recommande les bonnes 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 afficher la politique effective à l'aide de la AWS Management Console, de l'opération d'API GetEffectivePolicy ou de l'une de ses variantes de AWS CLI ou de SDK AWS. 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 Régions AWS et comptes de votre organisation

Pour améliorer votre position de reprise après sinistre, vous pouvez stocker des copies de vos sauvegardes.

- Une région différente : si vous stockez des copies de la sauvegarde dans d'autres Régions AWS, vous contribuez à protéger la sauvegarde contre la corruption ou la 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 compte différent : si vous stockez des copies de la sauvegarde dans d'autres 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 d'ensembles de piles AWS CloudFormation à Organizations pour créer automatiquement les coffres-forts de sauvegarde et les rôles AWS Identity and Access Management (IAM) requis dans chacun des comptes membres de votre organisation. Vous pouvez créer un ensemble de piles qui inclut les ressources dont vous souhaitez qu'elles soient automatiquement disponibles dans chaque Compte AWS 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. Cela va au-delà de l'examen de la politique effective

et garantit que AWS Backup interprète vos politiques et la mise en œuvre des plans de sauvegarde comme vous l'aviez prévu.

Création, mise à jour et suppression de politiques de sauvegarde

Dans cette rubrique :

- Après avoir activé les politiques de sauvegarde pour votre organisation, vous pouvez créer une politique.
- Lorsque vos exigences de sauvegarde changent, vous pouvez mettre à jour une politique existante.
- Lorsque vous n'avez plus besoin d'une politique et que vous l'avez détachée de toutes les UO et de tous les comptes, vous pouvez la supprimer.

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 dans la AWS Management Console de l'une des deux manières suivantes :

- Un éditeur visuel qui vous permet de sélectionner 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 Balisage de ressources 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-fort à l'aide de la console AWS Backup ou de commandes AWS CLI.
- (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'affectation est effectuée en spécifiant des paires de balises que AWS Backup utilise pour trouver et 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" ] }
                        }
                    }
                }
            }
    }
}
```

Cette politique de sauvegarde indique que AWS Backup doit sauvegarder toutes les ressources des Comptes AWS concernés qui se trouvent dans les Régions AWS spécifiées et qui ont la balise `dataType` avec la valeur `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...",
    }
}
```

- SDK AWS : CreatePolicy

Suite des opérations

Après avoir créé une politique de sauvegarde, vous pouvez mettre votre politique en application. Pour ce faire, vous pouvez attacher la politique à la racine de l'organisation, à des unités d'organisation, à des Comptes AWS de votre organisation ou à une combinaison de tous ces éléments.

Mise à jour d'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" }
                    },
                    "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" ] }
                        }
                    }
                }
            }
    }
}
```

```
$ 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\"]}}}}}}"
}
```

- SDK AWS : UpdatePolicy

Modification des balises attachées 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 Balisage de ressources AWS Organizations.

Autorisations minimales

Pour modifier les balises attachées à une politique de sauvegarde dans votre organisation AWS, 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
- SDK AWS : TagResource et UntagResource

Suppression d'une politique de sauvegarde

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.

Autorisations minimales

Pour supprimer une politique, vous devez avoir l'autorisation d'effectuer l'action suivante :

- `organizations:DeletePolicy` avec un élément `Resource` dans la même instruction de politique que celle qui inclut le nom ARN de la politique à supprimer (ou « * »).

AWS Management Console

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 préalablement détacher la politique de sauvegarde à supprimer de l'ensemble des racines, unités d'organisation et 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 de sauvegarde

Vous pouvez utiliser l'une des méthodes suivantes pour supprimer une politique :

- AWS CLI : delete-policy

  L'exemple suivant supprime la politique spécifiée. Cela fonctionne uniquement si la politique n'est attachée à aucune racine, aucune UO ni aucun compte.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- SDK AWS : DeletePolicy

Attachement et détachement de politiques de sauvegarde

Vous pouvez utiliser des politiques de sauvegarde sur l'ensemble d'une organisation ainsi que sur des UO et des comptes individuels. Gardez les points suivants à l'esprit :

- Lorsque vous attachez une politique de sauvegarde à la racine de votre organisation, la politique s'applique à toutes les UO et tous les comptes membres de cette racine.

- Lorsque vous attachez une politique de sauvegarde à une UO, cette politique s'applique aux comptes qui appartiennent à l'UO ou à l'une de ses UO enfants. Ces comptes sont également soumis à toutes les politiques attachées à la racine de l'organisation.
- Lorsque vous attachez une politique de sauvegarde à un compte, cette politique s'applique uniquement à ce compte. Le compte est également soumis à toute politique attachée à la racine de l'organisation et aux UO auxquelles le compte appartient.

L'agrégation de toutes les politiques de sauvegarde que le compte hérite des UO racines et parentes, ainsi que de toutes les politiques directement associées au compte constitue la politique effective. Pour de plus amples informations sur la façon dont les politiques sont fusionnées pour constituer la politique effective, consultez Fonctionnement de l'héritage des politiques de gestion.

Attachement d'une politique de sauvegarde

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez attacher une politique de sauvegarde à la racine, à l'UO ou directement à un compte de l'organisation.

> **Autorisations minimales**
>
> Pour attacher des politiques de sauvegarde, vous devez avoir l'autorisation d'exécuter l'action suivante :
>
> - `organizations:AttachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône ▶) pour trouver l'UO ou le compte souhaité.

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 des unités d'organisation (choisissez l'icône ▶) pour trouver l'UO ou le compte souhaité.
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.

AWS CLI & AWS SDKs

Pour attacher une politique de sauvegarde à la racine de l'organisation, une UO ou à un compte

Vous pouvez utiliser l'une des commandes suivantes pour attacher une politique de sauvegarde :

- AWS CLI : attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
```

```
    --policy-id p-i9j8k7l6m5
```

- SDK AWS : AttachPolicy

La modification de la politique prend effet immédiatement.

Détachement d'une politique de sauvegarde

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez détacher une politique de sauvegarde de la racine de l'organisation, de l'UO ou du compte auquel celle-ci est attachée. Une fois que vous avez détaché une politique de sauvegarde d'une entité, cette politique ne s'applique plus à aucun compte qui était affecté par celle-ci. Pour détacher une politique, effectuez les opérations suivantes.

> **Autorisations minimales**
>
> Pour détacher une politique de sauvegarde de la racine de l'organisation, de l'UO ou du compte, vous devez être autorisé à exécuter l'action suivante :
>
> - `organizations:DetachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône ▶) pour trouver l'UO ou le compte souhaité. 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 des unités d'organisation (choisissez l'icône ▶) pour trouver l'UO ou le compte souhaité.
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.

AWS CLI & AWS SDKs

Pour détacher une politique de sauvegarde de la racine de l'organisation, d'une UO ou d'un compte

Vous pouvez utiliser l'une des commandes suivantes pour détacher une politique de sauvegarde :

- AWS CLI : detach-policy

  L'exemple suivant détache une politique d'une unité d'organisation.

```
$ aws organizations detach-policy \
```

```
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- SDK AWS : DetachPolicy

La modification de la politique prend effet immédiatement.

Affichage des politiques de sauvegarde effectives

Vous pouvez afficher la politique de sauvegarde effective d'un compte à partir de la Console de gestion AWS, d'une API AWS ou de l'interface de ligne de commande (CLI) AWS. La section suivante fournit une brève présentation de la politique de sauvegarde effective, avec un exemple.

Quelle est la politique de sauvegarde effective ?

La politique de sauvegarde effective spécifie les paramètres finaux du plan de sauvegarde qui s'appliquent à un Compte AWS. Il s'agit de l'agrégation de toutes les politiques de sauvegarde héritées par le compte, ainsi que de toute politique de sauvegarde directement attachée au compte. Lorsque vous attachez une politique de sauvegarde à la racine de l'organisation, elle s'applique à tous les comptes de votre organisation. Lorsque vous attachez une politique de sauvegarde à une unité d'organisation (UO), elle s'applique à tous les comptes et UO qui appartiennent à l'UO. Lorsque vous attachez une politique directement à un compte, elle ne s'applique qu'à ce Compte AWS.

Par exemple, la politique de sauvegarde attachée à la racine de l'organisation peut spécifier que tous les comptes de l'organisation doivent sauvegarder toutes les tables Amazon DynamoDB selon 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.

Pour de plus amples informations sur la façon dont les politiques de sauvegarde se combinent pour former la politique effective finale, consultez Fonctionnement de l'héritage des politiques de gestion.

Affichage de la politique de sauvegarde effective

Vous pouvez afficher la politique de sauvegarde effective pour un compte à l'aide de la AWS Management Console, de l'API AWS ou de AWS Command Line Interface.

> **Autorisations minimales**
>
> Pour afficher la politique de sauvegarde effective d'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 afficher la politique de sauvegarde effective d'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, choisissez le nom du compte dont vous souhaitez afficher la politique de sauvegarde effective. Vous devrez peut-être développer des unités d'organisation (choisissez l'icône ▶) pour trouver le compte souhaité.
3. Dans l'onglet Politiques, dans la section Politiques de sauvegarde, choisissez Afficher la politique de sauvegarde effective pour ce Compte AWS.

   La console affiche la politique effective appliquée au compte spécifié.

   > **Note**
   >
   > Vous ne pouvez pas copier et coller une politique effective et l'utiliser comme JSON pour une autre politique de sauvegarde sans modifications importantes. Les documents de politique de sauvegarde doivent inclure les Opérateurs d'héritage qui spécifient comment chaque paramètre se fusionne dans la politique effective finale.

AWS CLI & AWS SDKs

Pour afficher la politique de sauvegarde effective d'un compte

Vous pouvez utiliser l'une des commandes suivantes pour afficher la politique de sauvegarde effective :

- AWS CLI : describe-effective-policy

  L'exemple suivant affiche les détails d'une politique de sauvegarde.

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- SDK AWS : DescribeEffectivePolicy

Utilisation d'événements AWS CloudTrail pour surveiller les politiques de sauvegarde de votre entreprise

Vous pouvez utiliser des événements AWS CloudTrail pour surveiller la création, la mise à jour ou la suppression de politiques de sauvegarde au niveau des comptes de votre organisation AWS, ou si 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 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 de sauvegarde.

L'essentiel d'une politique de sauvegarde est constitué du plan de sauvegarde et de ses règles. La syntaxe du plan de sauvegarde dans une politique de AWS Organizations sauvegarde est structurellement identique à celle utilisée par AWS Backup, mais les noms des clés sont différents. Dans les descriptions des noms de clé de stratégie ci-dessous, chacun inclut le nom de clé de AWS Backup plan équivalent. Pour plus d'informations sur AWS Backup les forfaits, consultez CreateBackupPlanle guide duAWS Backup développeur.

> **Note**
>
> Lors de l'utilisation de JSON, les noms de clé dupliqués seront rejetés. Si vous souhaitez inclure plusieurs plans, règles ou sélections dans une seule politique, assurez-vous que le nom de chaque clé est unique.

Pour être complète et fonctionnelle, une politique de sauvegarde effective doit inclure plus qu'un simple plan de sauvegarde avec son calendrier et ses règles. La politique doit également identifier Régions AWS les ressources à sauvegarder, ainsi que le rôle AWS Identity and Access Management (IAM) qui AWS Backup peut être utilisé pour effectuer la sauvegarde.

La politique fonctionnellement complète suivante montre la syntaxe de la politique de sauvegarde de base. Si cet exemple était attaché directement à un compte, AWS Backup il sauvegarderait toutes les ressources de ce compte dans les `eu-north-1` régions `us-east-1` et dont la balise `dataType` a la valeur `PII` ou`RED`. L'exemple sauvegarde ces ressources tous les jours à 5h00 dans `My_Backup_Vault` et stocke également une copie dans `My_Secondary_Vault`. Ces deux coffres-

forts sont dans le même compte que la ressource. Il stocke également une copie de la sauvegarde dans `My_Tertiary_Vault` dans un autre compte explicitement spécifié. Les coffres-forts doivent déjà exister dans chacun des coffres-forts spécifiés Régions AWS pour chaque Compte AWS personne recevant la politique effective. Si parmi les ressources sauvegardées il y a des instances EC2, la prise en charge de Microsoft Volume Shadow Copy Service (VSS) est activée pour les sauvegardes sur ces instances. La sauvegarde applique la balise `Owner:Backup` à chaque point de restauration.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
```

```
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "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"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
```

```
        }
    }
}
```

La syntaxe d'une politique de sauvegarde inclut les composants suivants :

- Variables `$account` : dans certaines chaînes de texte des politiques, vous pouvez utiliser la variable `$account` pour représenter le Compte AWScourant. Lorsqu'un plan est AWS Backup exécuté dans la stratégie effective, il remplace automatiquement cette variable par le plan actuel Compte AWS dans lequel s'exécutent la politique effective et ses plans.

  > **Important**
  >
  > Vous pouvez utiliser la variable `$account` uniquement dans des éléments de politique pouvant inclure un Amazon Resource Name (ARN), tels que ceux qui spécifient le coffre-fort de sauvegarde dans lequel stocker la sauvegarde ou le rôle IAM disposant des autorisations nécessaires pour effectuer la sauvegarde.

  Par exemple, ce qui suit exige qu'un coffre nommé `My_Vault` existe dans chaque coffre Compte AWS auquel la politique s'applique.

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  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'utilisateurAWS CloudFormation .

- Opérateurs d'héritage : les politiques de sauvegarde peuvent utiliser à la fois les opérateurs de définition de valeur d'héritage et les opérateurs de contrôle enfants.
- `plans`

  Au niveau supérieur, la clé de la politique est la clé `plans`. Une politique de sauvegarde doit toujours commencer avec ce nom de clé fixe en haut du fichier de politique. Sous cette clé, vous pouvez avoir un ou plusieurs plans de sauvegarde.

- Chaque plan sous la clé de niveau supérieur `plans` a un nom de clé qui comprend le nom du plan de sauvegarde attribué par l'utilisateur. Dans l'exemple précédent, le nom du plan de sauvegarde est `PII_Backup_Plan`. Vous pouvez avoir plusieurs plans dans une politique, chacun avec ses propres `rules`, `regions`, `selections` et `tags`.

  Ce nom de clé de plan de sauvegarde dans une politique de sauvegarde correspond à la valeur de la `BackupPlanName` clé dans un AWS Backup plan.

  Chaque plan peut contenir les éléments suivants :

  - `rules` : cette clé contient un ensemble de règles. Chaque règle se traduit par une tâche planifiée, avec une heure de début et une fenêtre dans laquelle sauvegarder les ressources identifiées par les éléments `selections` et `regions` dans la politique de sauvegarde effective.
  - `regions`— Cette clé contient une liste de tableaux des Régions AWS ressources qui peuvent être sauvegardées par cette politique.
  - `selections` : cette clé contient un ou plusieurs ensembles de ressources (dans les `regions` spécifiées) qui sont sauvegardés par les `rules` spécifiées.
  - `advanced_backup_settings` : cette clé contient des paramètres spécifiques aux sauvegardes exécutées sur certaines ressources.
  - `backup_plan_tags` : cet élément spécifie des balises qui sont attachées au plan de sauvegarde lui-même.
- `rules`

  La clé de politique `rules` correspond à la clé `Rules` d'un plan AWS Backup . Vous pouvez avoir une ou plusieurs règles sous la clé `rules`. Chaque règle devient une tâche planifiée pour effectuer une sauvegarde des ressources sélectionnées.

  Chaque règle contient une clé dont le nom est celui de la règle. Dans l'exemple précédent, le nom de la règle est « My_Hourly_Rule ». La valeur de la clé de la règle est l'ensemble suivant d'éléments de règle :

  - `schedule_expression`— Cette clé de politique correspond à la `ScheduleExpression` clé d'un AWS Backup plan.

    Spécifie l'heure de début de la sauvegarde. Cette clé contient l'opérateur de valeur d'`@@assign`héritage et une valeur de chaîne avec une expression CRON qui indique quand AWS Backup lancer une tâche de sauvegarde. Le format général de la chaîne CRON est : « cron( ) ». Chaque paramètre est un chiffre ou un caractère générique. Par exemple, `cron(0 5 ? * 1,3,5 *)` démarre la sauvegarde à 5 heures tous les lundis, mercredis et vendredis.

`cron(0 0/1 ? * * *)` démarre la sauvegarde toutes les heures à l'heure pile, tous les jours de la semaine.

- `target_backup_vault_name`— Cette clé de politique correspond à la `TargetBackupVaultName` clé d'un AWS Backup plan.

  Spécifie le nom du coffre-fort de sauvegarde dans lequel stocker la sauvegarde. Vous créez la valeur en utilisant AWS Backup. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur de chaîne avec un nom de coffre-fort.

  > **Important**
  >
  > Le coffre-fort doit déjà exister lorsque le plan de sauvegarde est lancé pour la première fois. 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'utilisateurAWS CloudFormation .

- `start_backup_window_minutes`— Cette clé de politique correspond à la `StartWindowMinutes` clé d'un AWS Backup plan.

  (Facultatif) Spécifie le nombre de minutes à attendre avant d'annuler une tâche qui ne démarre pas correctement. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur avec un nombre entier de minutes.

- `complete_backup_window_minutes` : cette clé de politique correspond à la clé `CompletionWindowMinutes` d'un plan AWS Backup .

  (Facultatif) Spécifie le nombre de minutes après le démarrage d'une tâche de sauvegarde avant qu'elle doive s'achever ou être annulée par AWS Backup. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur avec un nombre entier de minutes.

- `enable_continuous_backup`— Cette clé de politique correspond à la `EnableContinuousBackup` clé d'un AWS Backup plan.

  (Facultatif) Spécifie s'il AWS Backup crée des sauvegardes continues. `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.

> **Note**
>
> Étant donné que les sauvegardes compatibles PITR peuvent être conservées pendant 35 jours au maximum, vous devez choisir `False` ou ne spécifier aucune valeur si vous définissez l'une des options suivantes :
>
> - Définir `delete_after_days` à une valeur supérieure à 35
> - Définir `move_to_cold_storage_after_days` à n'importe quelle valeur.

Pour plus d'informations sur les sauvegardes continues, consultez P oint-in-time recovery dans le Guide duAWS Backup développeur.

- `lifecycle`— Cette clé de politique correspond à la `Lifecycle` clé d'un AWS Backup plan.

  (Facultatif) Spécifie à AWS Backup quel moment cette sauvegarde passe en stockage à froid et à quel moment elle expire.

  - `move_to_cold_storage_after_days` — Cette clé de politique correspond à la `MoveToColdStorageAfterDays` clé d'un AWS Backup plan.

    Spécifie le nombre de jours après la sauvegarde, avant que AWS Backup déplace le point de restauration vers le stockage à froid. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur avec un nombre entier de jours.

  - `delete_after_days`— Cette clé de politique correspond à la `DeleteAfterDays` clé d'un AWS Backup plan.

    Spécifie le nombre de jours après la sauvegarde, avant que AWS Backup supprime le point de restauration. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur avec un nombre entier de jours. Si vous effectuez la transition d'une sauvegarde vers un stockage à froid, elle doit y rester au moins 90 jours, de sorte que cette valeur doit être supérieure d'au moins 90 jours à la valeur `move_to_cold_storage_after_days`.

- `copy_actions`— Cette clé de politique correspond à la `CopyActions` clé d'un AWS Backup plan.

  (Facultatif) Spécifie qui AWS Backup doit copier la sauvegarde vers un ou plusieurs emplacements supplémentaires. Chaque emplacement de copie de sauvegarde est décrit comme suit :

- Une clé dont le nom identifie de manière unique cette action de copie. Pour l'instant, le nom de la clé doit être l'Amazon Resource Name (ARN) du coffre-fort de sauvegarde. Cette clé contient deux entrées.
  - `target_backup_vault_arn` : cette clé de politique correspond à la clé `DestinationBackupVaultArn` d'un plan AWS Backup .

    (Facultatif) Spécifie le coffre dans lequel est AWS Backup stockée une copie supplémentaire de la sauvegarde. La valeur de cette clé contient l'opérateur de valeur d'héritage `@@assign` et l'ARN du coffre-fort.
    - Pour référencer un coffre dans Compte AWS lequel s'exécute la politique de sauvegarde, utilisez la `$account` variable de l'ARN à la place du numéro d'identification du compte. Lors de l' AWS Backup exécution du plan de sauvegarde, il remplace automatiquement la variable par le numéro d'identification du compte Compte AWS dans lequel la politique est exécutée. Cela permet à la sauvegarde de s'exécuter correctement lorsque la politique de sauvegarde s'applique à plusieurs comptes d'une organisation.
    - Pour référencer un coffre-fort dans un autre Compte AWS de la même organisation, utilisez le numéro d'ID de compte réel dans l'ARN.

    > **Important**
    >
    > - Si cette clé est manquante, une version en minuscules de l'ARN contenu dans le nom de clé parent est utilisée. Étant donné que les ARN sont sensibles à la casse, cette chaîne peut ne pas correspondre à l'ARN réel du coffre-fort et le plan peut donc échouer. C'est pourquoi nous vous recommandons de toujours fournir cette clé et cette valeur.
    > - Le coffre-fort de sauvegarde de destination de la copie doit déjà exister la première fois que vous lancez le plan de sauvegarde. Nous vous recommandons d'utiliser des ensembles de piles AWS CloudFormation et l'intégration de ce service avec 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'utilisateurAWS CloudFormation .
- `lifecycle`— Cette clé de politique correspond à la `Lifecycle` clé située sous la `CopyAction` clé dans un AWS Backup plan.

(Facultatif) Spécifie à AWS Backup quel moment cette copie d'une sauvegarde passe en stockage à froid et à quel moment elle expire.

- `move_to_cold_storage_after_days` : cette clé de politique correspond à la clé `MoveToColdStorageAfterDays` d'un plan AWS Backup .

  Spécifie le nombre de jours après la sauvegarde avant de AWS Backup déplacer le point de restauration vers un stockage à froid. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur avec un nombre entier de jours.

- `delete_after_days` : cette clé de politique correspond à la clé `DeleteAfterDays` d'un plan AWS Backup .

  Spécifie le nombre de jours après la sauvegarde avant de AWS Backup supprimer le point de restauration. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur avec un nombre entier de jours. Si vous effectuez la transition d'une sauvegarde vers un stockage à froid, elle doit y rester au moins 90 jours, de sorte que cette valeur doit être supérieure d'au moins 90 jours à la valeur `move_to_cold_storage_after_days`.

- `recovery_point_tags`— Cette clé de politique correspond à la `RecoveryPointTags` clé d'un AWS Backup plan.

  (Facultatif) Spécifie AWS Backup les balises associées à chaque sauvegarde créée à partir de ce plan. La valeur de cette clé contient un ou plusieurs des éléments suivants :

  - Identifiant de cette paire nom de clé/valeur. Pour chaque élément sous `recovery_point_tags`, ce nom est le nom de la clé de balise en minuscules, même si la `tag_key` a une casse différente. Cet identifiant n'est pas sensible à la casse. Dans l'exemple précédent, cette paire de clés était identifiée par le nom `0wner`. Chaque paire de clés contient les éléments suivants :

    - `tag_key` : spécifie le nom de la clé de balise à attacher au plan de sauvegarde. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur de chaîne. La valeur est sensible à la casse.

    - `tag_value` : spécifie la valeur qui est attachée au plan de sauvegarde et associée à la `tag_key`. Cette clé contient l'un des opérateurs de valeur d'héritage et une ou plusieurs valeurs à remplacer, ajouter ou supprimer de la politique effective. Les valeurs sont sensibles à la casse.

- `regions`

La clé de `regions` stratégie Régions AWS indique laquelle AWS Backup recherche les ressources qui répondent aux conditions de la `selections` clé. Cette clé contient n'importe quel opérateur de valeur d'héritage et une ou plusieurs valeurs de chaîne pour Région AWS les codes, par exemple :`["us-east-1", "eu-north-1"]`.

- `selections`

  La clé de politique `selections` spécifie les ressources qui sont sauvegardées par les règles de plan de cette politique. Cette touche correspond approximativement à l'BackupSelectionobjet dans AWS Backup. Les ressources sont spécifiées par une requête concernant les noms et valeurs de clé de balise correspondants. La clé `selections` contient une clé sous elle : `tags`.

  - `tags` : spécifie les balises qui identifient les ressources et le rôle IAM qui a l'autorisation d'interroger les ressources et de les sauvegarder. La valeur de cette clé contient un ou plusieurs des éléments suivants :
    - Identifiant de cet élément de balise. Cet identifiant sous `tags` est le nom de la clé de balise en minuscules, même si la balise à interroger a une casse différente. Cet identifiant n'est pas sensible à la casse. Dans l'exemple précédent, un élément était identifié par le nom `My_Backup_Assignment`. Chaque identifiant sous `tags` contient les éléments suivants :
      - `iam_role_arn` : spécifie le rôle IAM qui a l'autorisation d'accéder aux ressources identifiées par la requête de balise dans les Régions AWS spécifiées par la clé `regions`. Cette valeur contient l'opérateur de valeur d'`@@assign`héritage et une valeur de chaîne contenant l'ARN du rôle. AWS Backup utilise ce rôle pour rechercher et découvrir les ressources et pour effectuer la sauvegarde.

        Vous pouvez utiliser la variable `$account` dans l'ARN à la place du numéro d'ID de compte. Lorsque le plan de sauvegarde est exécuté par AWS Backup, il remplace automatiquement la variable par le numéro d'identification du compte Compte AWS dans lequel la politique est exécutée.

        > **Important**
        >
        > Le rôle doit déjà exister lorsque vous lancez le plan de sauvegarde pour la première fois. 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'utilisateurAWS CloudFormation .

- `tag_key` : spécifie le nom de la clé de balise à rechercher. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur de chaîne. La valeur est sensible à la casse.
- `tag_value`— Spécifie la valeur qui doit être associée à un nom de clé correspondant`tag_key`. AWS Backup inclut la ressource dans la sauvegarde uniquement si les deux `tag_key` et `tag_value` correspondent. Cette clé contient l'un des opérateurs de valeur d'héritage et une ou plusieurs valeurs à remplacer, ajouter ou supprimer de la politique effective. Les valeurs sont sensibles à la casse.

- `advanced_backup_settings` : spécifie des 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 :
  - Nom de la clé d'objet : chaîne qui spécifie le type de ressource auquel les paramètres avancés suivants s'appliquent.
  - Valeur de l'objet : chaîne d'objet JSON contenant un ou plusieurs paramètres de sauvegarde spécifiques au type de ressource associé.

  À l'heure actuelle, le seul paramètre de sauvegarde avancé pris en charge active les sauvegardes Microsoft VSS (Volume Shadow Copy Service) pour Windows ou SQL Server exécutées sur une instance Amazon EC2. Le nom de la clé doit être le type de ressource `"ec2"` et la valeur spécifie que la prise en charge de `"windows_vss"` est soit `enabled` soit `disabled` pour les sauvegardes effectuées sur ces instances Amazon EC2. Pour plus d'informations sur cette fonction, consultez.Création de sauvegardes Windows VSS dans le Guide du développeurAWS Backup .

  ```
  "advanced_backup_settings": {
      "ec2": {
          "windows_vss": {
              "@@assign": "enabled"
          }
      }
  }
  ```

- `backup_plan_tags` : spécifie les balises qui sont attachées au plan de sauvegarde lui-même. Cela n'affecte en aucune façon les balises spécifiées dans les règles ou sélections.

(Facultatif) Vous pouvez attacher des balises à vos plans de sauvegarde. La valeur de cette clé est un ensemble d'éléments.

Le nom de clé pour chaque élément sous `backup_plan_tags` est le nom de clé de balise en minuscules, même si la balise à interroger a une casse différente. Cet identifiant n'est pas sensible à la casse. La valeur de chacune de ces entrées se compose des clés suivantes :

- `tag_key` : spécifie le nom de la clé de balise à attacher au plan de sauvegarde. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur de chaîne. Cette valeur est sensible à la casse.
- `tag_value` : spécifie la valeur qui est attachée au plan de sauvegarde et associée à la `tag_key`. Cette clé contient l'opérateur de valeur d'héritage `@@assign` et une valeur de chaîne. Cette valeur est sensible à la casse.

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 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"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "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"
                                }
                            }
                        },
                        "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"
                            }
                        }
                    }                   }
            }
        },
        "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",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "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" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
```

```
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$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" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
```

```
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "MonthlyDatatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$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",
                    "lifecycle": {
```

```
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$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": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
```

```
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "30",
                            "to_delete_after_days": "365"
                        }
                    }
                }
            },
            "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"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                                "to_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"
                                }
                            }
                        }
                    }
                },
                "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",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "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"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "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"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

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",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
```

```
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Politiques de balises

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 attributs personnalisés que vous affectez ou qu'AWS affecte aux ressources AWS. 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 Balisage de ressources AWS Organizations.
- Pour plus d'informations sur le balisage des ressources dans d'autres AWS services, 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 d'utiliser 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 AWS Resource Groups 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 service AWS où vous avez créé la ressource.

  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 la gestion des politiques de balises.

> **Important**
>
> Pour commencer à utiliser les politiques de balises, AWS recommande fortement de suivre l'exemple de flux de travail fourni à la section 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.

Conditions préalables et autorisations pour la gestion des politiques de balises

Cette page décrit les conditions préalables et les autorisations requises pour la gestion des politiques de balises dans AWS Organizations.

Rubriques

Conditions préalables pour la gestion des politiques de balises

L'utilisation de politiques de balises exige d'effectuer les actions suivantes :

- Toutes les fonctions doivent être activées pour votre organisation.
- Vous devez être connecté au compte de gestion de votre organisation.
- Vous avez besoin des autorisations répertoriées à la rubrique Autorisations pour la gestion des politiques de balises.

Pour évaluer la conformité aux politiques de balises, utilisez AWS Resource Groups. Pour de plus amples informations sur les conditions requises pour évaluer la conformité, consultez Conditions préalables et autorisations dans le Guide de l'utilisateur AWS Resource Groups.

Autorisations pour la gestion des politiques de balises

L'exemple de politique IAM suivant fournit les autorisations nécessaires pour la gestion des politiques de balises.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Pour plus d'informations sur les politiques et les autorisations IAM, consultez le Guide de l'utilisateur IAM.

Bonnes pratiques pour l'utilisation de politiques de balises

AWS recommande les bonnes pratiques suivantes pour l'utilisation des politiques de 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 pouvez spécifier que lorsqu'une balise `CostCenter` est attachée à des secrets AWS Secrets Manager, elle doit utiliser le traitement de casse 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 sous la rubrique Évaluation de la conformité d'un compte dans le Guide de l'utilisateur AWS Resource Groups. 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 Présentation de l'application de la conformité. Consultez également les flux de travail décrits sous Mise en route avec les politiques de balises.

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 obtenir un exemple de SCP, consultez Exiger une balise sur des ressources créées spécifiées. Pour savoir si un service AWS prend en charge le contrôle d'accès à l'aide de balises, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM. Recherchez les services qui ont Oui dans la colonne 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 de balises implique de travailler avec plusieurs AWS services. 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 la gestion des politiques de balises
- 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.

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. 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. 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

Tâche	Compte auquel vous connecter	AWS console de service à utiliser
		secrets conformes et non conformes.
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. 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. 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. 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
Attacher des stratégies de balises à des comptes ou des unités organisationnelles supplémentaires. 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. Pour voir un exemple, consultez Exiger une balise sur des ressources créées spécifiées.	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 Présentation de l'application de la conformité.

Tâches d'application	Compte auquel vous connecter	AWS console de service à utiliser
Étape 1 : Créez une politique de balises. 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.

Création, mise à jour et suppression de politiques de balises

Dans cette rubrique :

- Après avoir activé les politiques de balises pour votre organisation, vous pouvez créer une politique de balises.
- Lorsque vos exigences de balisage changent, vous pouvez mettre à jour une politique existante.
- Lorsque vous n'avez plus besoin d'une politique et que vous l'avez détachée de toutes les UO et de tous les comptes, vous pouvez la supprimer.

> **Important**
>
> Les ressources non balisées n'apparaissent pas dans les résultats comme étant non conformes.

Création d'une politique 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 de balises dans la AWS Management Console 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.

AWS Management Console

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 Balisage de ressources 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.

   Pour Nouvelle clé de balise 1, spécifiez le nom d'une clé de balise à ajouter.
6. Laissez la case Conformité de la capitalisation de la clé de balise désactivée (par défaut) pour spécifier que la politique de balises parente héritée, si elle existe, doit définir le traitement de la casse 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. Vous pourrez créer

et attacher ultérieurement des politiques de balises supplémentaires à des unités d'organisation ou à des comptes pour créer des règles de balisage supplémentaires.

7. Activez Conformité de la valeur de balise si vous souhaitez ajouter des valeurs autorisées pour cette clé de balise aux valeurs éventuellement héritées d'une politique parente.

   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. Laissez la case Empêcher les opérations non conformes pour cette balise désactivée (par défaut), sauf si vous êtes familiarisé avec l'utilisation de politiques de balises. Veillez à consulter les recommandations de la rubrique Présentation de l'application de la conformité 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 politique comme celle-ci signifie qu'une ressource dont la balise CostCenter est attachée 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\n"
    }
}
```

- SDK AWS : CreatePolicy

Suite des opérations

Après avoir créé une politique de balises, vous pouvez mettre en application vos règles de balisage. Pour ce faire, attachez la politique à la racine de l'organisation, à des unités d'organisation, à des Comptes AWS de votre organisation ou à une combinaison d'entités d'organisation.

Mise à jour d'une politique 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\"]}}}}"
}
```

- SDK AWS : UpdatePolicy

Modification des balises attachées à une politique 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 AWS, 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 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 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
- SDK AWS : TagResource et UntagResource

Suppression d'une politique de balises

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.

> **Autorisations minimales**
>
> Pour supprimer une politique de balises, vous devez avoir l'autorisation d'effectuer l'action suivante :
>
> - `organizations:DeletePolicy`

AWS Management Console

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.
3. Sur la page Politiques de balises, choisissez la politique que vous souhaitez supprimer.
4. La politique à supprimer doit d'abord être détachée de l'ensemble des racines, unités d'organisation et 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.
5. En haut de la page, choisissez Supprimer.
6. Dans la boîte de dialogue de confirmation, saisissez le nom de la politique, puis choisissez Supprimer.

AWS CLI & AWS SDKs

Pour supprimer une politique de balises

Vous pouvez utiliser l'une des méthodes suivantes pour supprimer une politique :

- AWS CLI : delete-policy

  L'exemple suivant supprime la politique spécifiée. Cela fonctionne uniquement si la politique n'est attachée à aucune racine, aucune UO ni aucun compte.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- SDK AWS : DeletePolicy

Attachement et détachement de politiques de balises

Vous pouvez appliquer des politiques de balises à l'ensemble d'une organisation ainsi qu'à des unités d'organisation (UO) et à des comptes individuels.

- Lorsque vous attachez une politique de balises à la racine de votre organisation, la politique de balises s'applique à toutes les unités d'organisation et tous les comptes membres de cette racine.
- Lorsque vous attachez une politique de balises à une unité d'organisation, cette politique de balises s'applique aux comptes qui appartiennent à l'unité d'organisation. Ces comptes sont également soumis à toutes les politiques de balises attachées à la racine de l'organisation.
- Lorsque vous attachez une politique de balises à un compte, cette politique de balises s'applique au compte. En outre, ce compte est soumis à toutes les politiques de balises attachées à la racine de l'organisation, ainsi qu'à toutes celles attachées à une unité d'organisation à laquelle le compte appartient.

L'agrégation de toutes les politiques de balises héritées par le compte, ainsi que de toutes les politiques de balises directement attachées au compte constitue la politique de balises effective. Pour de plus amples informations, veuillez consulter Fonctionnement de l'héritage des politiques de gestion.

> **Important**
>
> Les ressources non balisées n'apparaissent pas dans les résultats comme étant non conformes.

Autorisations minimales

Pour attacher des politiques de balises, vous devez avoir l'autorisation d'exécuter l'action suivante :

- `organizations:AttachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône) pour trouver l'UO ou le compte souhaité.
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 des unités d'organisation (choisissez l'icône ) pour trouver l'UO ou le compte souhaité.
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.

AWS CLI & AWS SDKs

Pour attacher une politique de balises à la racine de l'organisation, à une unité d'organisation ou à un compte

Vous pouvez utiliser l'une des commandes suivantes pour attacher une politique de balises :

- AWS CLI : attach-policy

  La procédure suivante décrit comment attacher la politique de balises que vous venez de créer à un seul compte de test.

  - Attachez la politique de balises à votre compte de test en exécutant la commande suivante :

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    Cette commande n'a pas de sortie si elle réussit.
- SDK AWS : AttachPolicy

La modification de la politique prend effet immédiatement.

Suite des opérations

Après avoir attaché une politique de balises, vous pouvez découvrir le degré de conformité des ressources à cette politique de balises. Pour cela, utilisez la console Resource Groups. Pour de plus amples informations, consultez Évaluation de la conformité d'un compte dans le Guide de l'utilisateur AWS Resource Groups.

Détachement d'une politique de balises

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez détacher une politique de balises de la racine de l'organisation, de l'unité d'organisation ou du compte auquel celle-ci est attachée. Une fois que vous avez détaché une politique de balises d'une entité, cette politique ne s'applique plus à aucun compte qui était affecté par celle-ci. Pour détacher une politique, effectuez les opérations suivantes.

Autorisations minimales

Pour détacher une politique de balises de la racine de l'organisation, d'une unité d'organisation ou d'un compte, vous devez être autorisé à exécuter l'action suivante :

- `organizations:DetachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône ) pour trouver l'UO ou le compte souhaité. 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 des unités d'organisation (choisissez l'icône) pour trouver l'UO ou le compte souhaité.
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.

AWS CLI & AWS SDKs

Pour détacher une politique de balises de la racine de l'organisation, d'une unité d'organisation ou d'un compte

Vous pouvez utiliser l'une des méthodes suivantes pour détacher une politique de balises :

- AWS CLI : detach-policy
- SDK AWS : DetachPolicy

La modification de la politique prend effet immédiatement.

Affichage des politiques de balises effectives

Avant de vérifier le statut de conformité des ressources balisées dans un compte, il s'avère utile de commencer par déterminer la politique de balises effective pour un compte.

Qu'est-ce que la politique de balises effective ?

La politique de balises effective spécifie les règles de balisage qui s'appliquent à un compte. Il s'agit de l'agrégation de toutes les politiques de balises héritées par le compte, ainsi que de toutes les politiques de balises directement attachées au compte. Lorsque vous attachez une politique de balises à la racine de l'organisation, elle s'applique à tous les comptes de votre organisation. Lorsque vous attachez une politique de balises à une unité d'organisation, elle s'applique à tous les comptes et unités d'organisation qui appartiennent à l'unité d'organisation.

Par exemple, la politique de balises attachée à la racine de l'organisation peut définir une balise `CostCenter` comportant 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.

Pour de plus amples informations et pour obtenir des exemples plus avancés de génération des politiques de balises effectives, consultez Fonctionnement de l'héritage des politiques de gestion.

Comment afficher la politique de balises effective

Vous pouvez afficher la politique de balises effective pour un compte à partir de la AWS Management Console, d'une API AWS ou de la AWS Command Line Interface.

> **Autorisations minimales**
>
> Pour afficher la politique de balises effective d'un compte, vous devez être autorisé à exécuter les actions suivantes :
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization`

AWS Management Console

Pour afficher la politique effective d'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, choisissez le nom du compte dont vous souhaitez afficher la politique de balises effective. Vous devrez peut-être développer des unités d'organisation (choisissez l'icône ▶) pour trouver le compte souhaité.
3. Dans l'onglet Politiques, dans la section Politiques de balises, choisissez Afficher la politique de balises effective pour ce Compte AWS.

   La console affiche la politique effective appliquée au compte spécifié.

   > **Note**
   >
   > Vous ne pouvez pas copier et coller une politique effective et l'utiliser comme JSON pour une autre politique de balises sans modifications importantes. Les documents de politique de balises doivent inclure les opérateurs d'héritage, qui spécifient comment chaque paramètre est fusionné dans la politique effective finale.

AWS CLI & AWS SDKs

Pour afficher la politique effective d'un compte

Vous pouvez utiliser l'une des méthodes suivantes pour afficher la politique de balises effective :

- AWS CLI : describe-effective-policy

  Pour déterminer les règles de balisage qui sont héritées par un compte ou qui lui sont attachées, exécutez ce qui suit à partir du compte et enregistrez les résultats dans un fichier :

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
```

```
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

Si une politique de balises est attachée au compte ainsi qu'à la racine ou à des UO, la combinaison des politiques héritées constitue la politique de balises effective du compte. Dans ces cas, l'exécution de `describe-effective-policy` à partir du compte renvoie le contenu fusionné de toutes les politiques de la hiérarchie du compte.

- SDK AWS : DescribeEffectivePolicy

Utilisation de Amazon EventBridge pour contrôler les balises non conformes

Vous pouvez utiliser Amazon EventBridge, anciennement Amazon CloudWatch Events pour contrôler 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 en savoir plus EventBridge, consultez le Guide de l'utilisateur Amazon EventBridge.

Présentation de l'application de la conformité

Une politique de balises permet de spécifier que les opérations de balisage non conformes au niveau des types de ressources définis sont appliquées. En d'autres termes, les demandes de balisage non conformes sur des types de ressources spécifiés ne peuvent pas aboutir.

> **Important**
>
> L'application n'a aucun effet sur les ressources créées sans balises.

Pour appliquer la conformité aux politiques de balises, effectuez l'une des opérations suivantes lorsque vous créez une politique de balises:

- Dans l'onglet Éditeur visuel, sélectionnez Empêcher les opérations non conformes pour cette balise.
- 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.

Suivez ces bonnes pratiques pour appliquer la conformité aux politiques de balises :

- 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 les flux de travail recommandés décrits sous Mise en route avec les politiques de balises. 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.
- 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 AWS services comportent des regroupements de ressources semblables à des conteneurs qui créent automatiquement des ressources pour vous, et les balises peuvent se propager d'une ressource d'un service à l'autre. Par exemple, les balises des groupes Amazon EC2 Auto Scaling et des clusters Amazon EMR

peuvent se propager automatiquement aux instances Amazon EC2 qu'ils contiennent. Certaines politiques de balises pour Amazon EC2 sont plus strictes que pour les groupes Auto Scaling ou les clusters 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.

Recherche de ressources non conformes pour un compte

Vous pouvez obtenir des informations sur les ressources non conformes de chaque compte. Vous devez exécuter cette commande à partir de chaque région dans laquelle le compte possède des ressources.

Pour rechercher des ressources non conformes pour un compte doté d'une politique de balises, exécutez la commande suivante pour enregistrer les résultats dans un fichier :

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

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 AWS Resource Groups TagResourceset pour ajouter des balises conformes à la politique en vigueur ou pour supprimer des balises non conformes.

Recherche et correction d'autres problèmes de non-conformité

La recherche et la correction des problèmes de conformité est un processus itératif. Répétez les étapes des deux sections précédentes jusqu'à ce que les ressources qui vous intéressent soient conformes à votre politique de balises.

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, supposons que vous disposez d'une politique de balises qui définit une nouvelle balise standardisée pour un type de ressources. Les ressources de ce type qui ne possèdent pas cette balise sont affichées comme étant conformes dans le rapport pendant 48 heures 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 get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

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.

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 :

Nom du service	Type de ressource	Syntaxe JSON
Amazon API Gateway	• Clés API • Noms de domaine • Opérations d'API REST • Étapes	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`
AWS Amplify	• Composant • Thème	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Application • Profil de configuration • Déploiement • Stratégie de déploiement • Environnement	• `"appconfig:application"` • `"appconfig:application/configurationprofile"` • `"appconfig:application/environment/deployment"` • `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Tous • Routage de passerelle • Maillage • Acheminement • Passerelle virtuelle • Nœud virtuel • Routeur virtuel	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"`

Nom du service	Type de ressource	Syntaxe JSON
	• Service virtuel	• `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• Tous • WorkGroup	• `"athena:*"` • `"athena:workgroup"`
AWS Audit Manager	• Évaluation • Cadre d'évaluation • Contrôle	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• Plan de sauvegarde • Coffre-fort • Passerelle • Hyperviseur • MV	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`
AWS Batch	• Tâche • Définition de tâche • File d'attente de tâche	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Événement	• `"bugbust:event"`
AWS Certificate Manager	• Tous • Certificats • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Chime	• Instance d'application • Canal • Pipeline multimédia • Réunion • Applications multimédias SIP • Instance d'application utilisateur • Connecteur vocal	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• Collaboration • Tableau configuré • Membres • Association de tableaux configurés	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• Environnement	• `"cloud9:environment"`
Amazon CloudFront	• Tous • Distribution • Distribution en streaming	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distribution"`
AWS CloudTrail	• Tous • Journal d'activité	• `"cloudtrail:*"` • `"cloudtrail:trail"`
Amazon CloudWatch	• Tous • alerte • Règle de Contributor Insights • Flux de métriques	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon CloudWatch Internet Monitor	• Surveiller	• `"internetmonitor:monitor"`
Amazon CloudWatch Logs	• Destination • Groupe de journaux	• `"logs:destination"` • `"logs:log-group"`
Gestionnaire d'accès Amazon CloudWatch Observability	• Lien • Sink	• `"oam:link"` • `"oam:sink"`
AWS CodeBuild	• Tous • Projet	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Connexions	• `"codecatalyst:connections"`
AWS CodeCommit	• Tous • Référentiel.	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Tous • Type d'action • Pipeline • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`
Amazon Cognito Identity	• Tous • Groupe d'identités	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Groupes d'utilisateurs Amazon Cognito	• Tous • Groupe d'utilisateurs	• `"cognito-idp:*"` • `"cognito-idp:userpool"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Comprehend	• Tous • Classificateur de documents • Module de reconnaissance d'entité	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Tous • Autorisation d'agrégation • Module d'agrégation de configuration • Règle de configuration	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Réviseur Amazon	• Association	• `"codeguru-reviewer:association"`
Amazon CodeGuru Security	• Analyser	• `"codeguru-security:scans"`
CodeConnections	• Connexion • Host (Hôte)	• `"codestar-connections:connection"` • `"codestar-connections:host"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Connect	• Flux de contact • Association d'intégration • File d'attente • Connexion rapide • Profil de routage • Utilisateur	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`
Amazon Connect Wisdom	• Assistant • Association • Contenu • Base de connaissances • Session	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Tous • Point de terminaison • ES • Rép • Subgrp • Tâche	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
Amazon Data Lifecycle Manager	• Politique	• `"dlm:policy"`
AWS Diode	• Mappage	• `"diode-messaging:mapping"`

Nom du service	Type de ressource	Syntaxe JSON
AWS Direct Connect	• Tous • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• Tous • Tableau	• `"dynamodb:*"` • `"dynamodb:table"`
Amazon EC2	• Réservation de capacité • Flotte de réservation de capacité • Passerelle transporteur	• `"ec2:capacity-reservation"` • `"ec2:capacity-reservation-fleet"` • `"ec2:carrier-gateway"`
	• Point de terminaison VPN Client • pool CoIP • Passerelle client	• `"ec2:client-vpn-endpoint"` • `"ec2:coip-pool"` • `"ec2:customer-gateway"`
	• Hôte dédié • Options DHCP • Passerelle Internet de sortie uniquement	• `"ec2:dedicated-host"` • `"ec2:dhcp-options"` • `"ec2:egress-only-internet-gateway"`
	• Adresses IP Elastic • Fenêtre d'événements • Flotte	• `"ec2:elastic-ip"` • `"ec2:instance-event-window"` • `"ec2:fleet"`

Nom du service	Type de ressource	Syntaxe JSON
	• Image FPGA • Réservation d'hôte • Image	• `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"`
	• Instance • Passerelle Internet • IP Address Manager	• `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:ipam"`
	• Pool de gestionnaires d'adresses IP • Champ d'application du gestionnaire d'adresses IP • Pool IPv4	• `"ec2:ipam-pool"` • `"ec2:ipam-scope"` • `"ec2:ipv4pool-ec2"`
	• Key Pair (Paire de clés) • Modèle de lancement • Table de routage de passerelle locale	• `"ec2:key-pair"` • `"ec2:launch-template"` • `"ec2:local-gateway-route-table"`
	• Table de routage de passerelle locale, association de groupes d'interfaces virtuelles • Association VPC de table de routage de passerelle locale • Passerelle NAT	• `"ec2:local-gateway-route-table-virtual-interface-group-association"` • `"ec2:local-gateway-route-table-vpc-association"` • `"ec2:natgateway"`

Nom du service	Type de ressource	Syntaxe JSON
	• Réseau ACL • Interface réseau • Étendue d'accès à Network Insights	• `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:network-insights-access-scope"`
	• Analyse de l'étendue d'accès à Network Insights • Analyse des informations sur le réseau • Parcours Network Insights	• `"ec2:network-insights-access-scope-analysis"` • `"ec2:network-insights-analysis"` • `"ec2:network-insights-path"`
	• Groupe de placement • Liste des préfixes • Tâche de remplacement du volume racine	• `"ec2:placement-group"` • `"ec2:prefix-list"` • `"ec2:replace-root-volume-task"`
	• Instances réservées • Table de routage • Groupe de sécurité	• `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"`
	• Instantané • Demande d'instances Spot • Sous-réseau	• `"ec2:snapshot"` • `"ec2:spot-instances-request"` • `"ec2:subnet"`

Nom du service	Type de ressource	Syntaxe JSON
	• Réservation CIDR de sous-réseau • Filtre Traffic mirror • Session Traffic mirror	• `"ec2:subnet-cidr-reservation"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"`
	• Cible Traffic mirror • Passerelle de transit • Pièce jointe Transit Gateway	• `"ec2:traffic-mirror-target"` • `"ec2:transit-gateway"` • `"ec2:transit-gateway-attachment"`
	• Transit Gateway Connect Peer • Domaine de multidiffusion Transit Gateway • Tableau des politiques de Transit Gateway	• `"ec2:transit-gateway-connect-peer"` • `"ec2:transit-gateway-multicast-domain"` • `"ec2:transit-gateway-policy-table"`
	• Table de routage de passerelle de transit • Point de terminaison d'accès vérifié • Groupe d'accès vérifié	• `"ec2:transit-gateway-route-table"` • `"ec2:verified-access-endpoint"` • `"ec2:verified-access-group"`
	• Instance d'accès vérifié • Fournisseur d'accès sécurisé vérifié • Volume	• `"ec2:verified-access-instance"` • `"ec2:verified-access-trust-provider"` • `"ec2:volume"`

Nom du service	Type de ressource	Syntaxe JSON
	• Journal de flux VPC • VPC • Point de terminaison d'un VPC	• `"ec2:vpc-flow-log"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"`
	• Service de point de terminaison d'un VPC • Connexion d'appairage de VPC • Connexion VPN • Passerelle VPN	• `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"` • `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`
Corbeille Amazon EC2	• Règle	• `"rbin:rule"`
AWS Elastic Beanstalk	• Application • Version de l'application • Modèle de configuration • Plateforme	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`
Amazon Elastic Container Registry	• Référentiel.	• `"ecr:repository"`
Amazon Elastic Container Service	• Fournisseur de capacité • Cluster • Service • Définition de tâche • Ensemble de tâches	• `"ecs:capacity-provider"` • `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-definition"` • `"ecs:task-set"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Elastic File System	• Tous • Système de fichiers	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`
Amazon Elastic Inference	• Accélérateur	• `"elastic-inference:elastic-inference-accelerator"`
Amazon Elastic Kubernetes Service	• Cluster	• `"eks:cluster"`
Amazon Elastic Search	• Domaine	• `"es:domain"`
Amazon EMR	• Cluster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon EMR sans serveur	• Application	• `"emr-serverless:applications"`
AWS Résolution de l'entité	• Flux de travail correspondant • Cartographie du schéma	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Cluster	• `"elasticache:cluster"`
Amazon EventBridge	• Tous • Bus d'événement • Règle	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
Amazon EventBridge Pipes	• Barre verticale	• `"pipes:pipe"`
Amazon EventBridge Scheduler	• Groupe de planifications	• `"scheduler:schedule-group"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Fraud Detector	• Détecteur • Version du détecteur • Modèle • Règle • Variable	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Amazon Global Accelerator	• Accélérateur	• `"globalaccelerator:accelerator"`
Elastic Load Balancing	• Tous • Listener • Règle de l'auditeur • Équilibreur de charge • Groupe cible	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:listener"` • `"elasticloadbalancing:listener-rule"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Tous • Sauvegarde • Système de fichiers	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
Amazon GuardDuty	• Détecteur • Filtre • Ensemble d'adresses IP • Ensemble de renseignements sur les menaces	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`

Nom du service	Type de ressource	Syntaxe JSON
AWS HealthLake	• Entrepôt de données	• `"healthlake:datastore "`
AWS HealthOmics	• Magasin d'annotations • Version du magasin d'annotations • Magasin de références • Référence • Exécuter • Groupe d'exécution • Magasin de séquences • Jeu de lecture • Magasin de variantes • Flux de travail	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filtre	• `"inspector2:filter "`
AWS Identity and Access Management	• Profil d'instance • MFA • Fournisseur OIDC • Politique • Fournisseur SAML • Certificat de serveur	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`

Nom du service	Type de ressource	Syntaxe JSON
AWS IoT Analytics	• Tous • Canal • Jeux de données • Entrepôt de données • Pipeline	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`
AWS IoT Events	• Tous • Modèle de détecteur • Entrée	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS IoT Fleet Hub	• Application	• `"iotfleethub:application"`
AWS IoT SiteWise	• Ressource • Modèle de ressource	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`
AWS IoT Greengrass	• Déploiement en bloc • Définition de connecteur • Définition principale • Définition d'appareil • Définition de fonction • Définition d'enregistreur d'activités • Définitions de ressource • Définition d'abonnement	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`

Nom du service	Type de ressource	Syntaxe JSON
AWS Key Management Service	• Tous • Clé	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Tous • Application	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`
Amazon Data Firehose	• Tous • Flux de transmission	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Tous • Fonction	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Identifiant de données personnalisé	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Conteneur	• `"mediastore:container"`
Amazon MQ	• Broker • Configuration	• `"mq:broker"` • `"mq:configuration"`
Amazon Network Firewall	• Pare-feu • Politique de pare-feu • Groupe de règles avec état • Groupe de règles sans état	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon OpenSearch sans serveur	• Collection	• `"aoss:collection"`

Nom du service	Type de ressource	Syntaxe JSON
AWS Organizations	• Compte • Unité d'organisation • Politique • Racine	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`
Amazon Pinpoint SMS Voice V2	• Jeu de configurations • Liste de désinscriptions • Numéro de téléphone • Groupe • Id de l'expéditeur	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon RDS	• Groupe de paramètres du cluster • Point de terminaison de cluster • Abonnement aux événements • Groupe d'options DB • Groupe de paramètres de base de données • Proxy de base de données • Point de terminaison de proxy de base de données • instance de base de données réservée • Groupe de sécurité de base de données • Groupe de sous-réseaux de base de données • Groupe cible	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Redshift	• Tous • Cluster • Groupe de la base de données • Nom de la base de données • Utilisateur de la base de données • Abonnement aux événements • Certificat de client HSM • Configuration HSM • Groupe de paramètres • Instantané • Autorisation de copie d'instantanés • Planification des instantanés • Groupe de sous-réseaux	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
Amazon Redshift sans serveur	• Espace de noms • WorkGroup	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• Tous • Partage de ressources	• `"ram:*"` • `"ram:resource-share"`

Nom du service	Type de ressource	Syntaxe JSON
AWS Resource Groups	• Tous • Groupe	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• Zone hébergée	• `"route53:hostedzone"`
Amazon Route 53 Resolver	• Tous • Point de terminaison du résolveur • Règle du résolveur	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`
Amazon S3	• Compartiment • Cadre de stockage • Groupe de lentilles de rangement	• `"s3:bucket"` • `"s3:storage-lens"` • `"s3:storage-lens-group"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon SageMaker	• Configuration d'image d'application • Artefact • Contexte • Tâche de formation • Tâche de traitement • Groupe de packages de modèles • UI des tâches humaines • Package de modèle • Action • Pipeline • Expérience • Définition de flux • Projet	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• Tous • Secret	• `"secretsmanager:*"` • `"secretsmanager:secret"`
AWS Lac de sécurité	• Lac de données • Subscriber	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• Application • Groupe d'attributs • Portefeuille • Produit (langue française non garantie)	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Simple Notification Service (SNS)	• Rubrique	• `"sns:topic"`
Amazon Simple Queue Service (SQS)	• File d'attente	• `"sqs:queue"`
Amazon States Language	• Tous • Activité • State Machine	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Activité	• `"states:activity"`
AWS Storage Gateway	• Tous • Passerelle • Partage • Bande • Volume	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`
AWS Systems Manager	• Association • Exécution d'automatisation • Document • Maintenance Window • Instance gérée • Élément Ops • Référentiel de correctifs • Session • Contacts	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`

Nom du service	Type de ressource	Syntaxe JSON
Amazon Textract	• Adaptateurs • Versions	• `"textract:adapters"` • `"textract:adapters/versions"`
AWS Transfer Family	• Serveur • Utilisateur • Flux de travail	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Well-Arch itected	• Charge de travail	• `"wellarchitected:workload"`
AWS Wickr	• Réseau	• `"wickr:network"`
Amazon WorkSpaces	• Tous • Alias de connexion • Annuaire • WorkSpace • WorkSpaces offre groupée • WorkSpaces image • WorkSpaces Groupe IP	• `"workspaces:*"` • `"workspaces:connectionalias"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`
Amazon WorkLink	• Flotte	• `"worklink:fleet"`

Syntaxe des politiques de balises et exemples

Cette page décrit la syntaxe des politiques de balises et fournit des exemples.

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"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

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. Contrairement à la clé de balise (décrite ci-après), la valeur de politique n'est pas sensible à la casse.

  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 admises pour la clé de balise `CostCenter` sont `100` et `200`.

- (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 balises indique que toutes les ressources AWS Secrets Manager doivent avoir cette balise.

  > **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 de plus amples informations sur les opérateurs, consultez Opérateurs d'héritage.
- : vous pouvez utiliser le caractère générique `*` dans les valeurs de balise et dans les champs `enforced_for`.
  - Vous pouvez utiliser un caractère générique par valeur de balise. Par exemple, `*@example.com` est autorisé, contrairement à `*@*.com`.
  - Pour `enforced_for`, vous pouvez utiliser `<service>:*` avec certains services pour activer l'application pour toutes les ressources de 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 recommande de suivre cet exemple pour créer une politique de balises 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 de plus amples informations sur l'héritage des politiques, avec des exemples de fonctionnement des opérateurs d'héritage et des exemples de politiques de balises effectives, consultez Fonctionnement 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"
                ]
            }
        }
    }
}
```

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 US East (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
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

Nom de la région	Paramètre de région
Canada-Ouest (Calgary) [2]	`ca-west-1`
Région Canada (Centre)	`ca-central-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 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`

[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
- GetResources
- 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 desAWS comptes. La console Resource Groups n'est pas disponible dans ces régions.

Politiques de contrôle de service (SCP)

Les politiques de contrôle des services (SCP) sont un type de politique d'organisation que vous pouvez utiliser pour gérer les autorisations dans votre organisation. Les SCP offrent un contrôle centralisé sur les autorisations maximales disponibles pour les utilisateurs IAM et les rôles IAM au sein de votre organisation. Les politiques de contrôle des services vous aident à vous assurer que vos comptes respectent les directives de contrôle d'accès de votre organisation. Les politiques de contrôle des services sont disponibles uniquement dans une organisation dont toutes les fonctions sont activées. Les politiques SCP ne sont pas disponibles si votre organisation a activé uniquement les fonctions de facturation consolidée. Pour obtenir des instructions sur l'activation des SCP, consultez Activation et désactivation des types de politiques.

Les SCP n'accordent 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. Les autorisations effectives sont l'intersection logique entre ce qui est autorisé par le SCP et ce qui est autorisé par les politiques basées sur l'identité et les ressources.

> **Important**
>
> Les SCP n'affectent pas les utilisateurs ni les rôles dans le compte de gestion. Elles affectent uniquement les comptes membres de votre organisation.

Rubriques dans cette page

Test des effets des politiques de contrôle des services

AWS vous recommande vivement de ne pas associer de SCP 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 des SCP (politiques de contrôle des services)

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 politiques SCP formatées avec des espaces supplémentaires pour une meilleure 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.

Attachement de SCP à différents niveaux de l'organisation

Pour en savoir plus sur le fonctionnement des SCP, consultez la rubrique Évaluation du SCP.

Effets des SCP sur les autorisations

Les SCP sont similaires aux politiques d'autorisation AWS Identity and Access Management (IAM) et utilisent presque la même syntaxe. Toutefois, une politique de contrôle des services n'accorde jamais d'autorisations. Les SCP sont plutôt des politiques JSON qui spécifient les autorisations maximales 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.

- Les SCP affectent uniquement les utilisateurs et les rôles IAM qui sont gérés par des comptes faisant partie de l'organisation. Les SCP 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 */*.
- Les SCP affectent uniquement les comptes membres de l'organisation. Elles n'ont aucun effet sur les utilisateurs ou les rôles du compte de gestion.
- Les utilisateurs et les rôles doivent toujours se voir attribuer des autorisations avec les politiques d'autorisation IAM appropriées. Un utilisateur sans aucune politique d'autorisation IAM ne bénéficie d'aucun accès, même si les politiques SCP applicables 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 qui est également autorisée par les politiques SCP applicables, 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 qui n'est pas autorisée ou qui est explicitement refusée par les politiques SCP applicables, l'utilisateur ou le rôle ne peut pas exécuter cette action.
- Les politiques SCP affectent tous les utilisateurs et les rôles figurant dans les comptes attachés, y compris l'utilisateur racine. Les seules exceptions sont celles décrites dans Tâches et entités non restreintes par les SCP.
- Les SCP n'affectent pas les rôles liés à un service. Les rôles liés aux services permettent à d'autres AWS services de s'intégrer aux SCP AWS Organizations et ne peuvent pas être restreints par ces derniers.
- Lorsque vous désactivez le type de politique SCP dans une racine, tous les SCP sont automatiquement détachés de toutes les AWS Organizations entités de cette racine. AWS Organizations les entités incluent les unités organisationnelles, les organisations et les comptes.

Si vous activez de nouveau les politiques SCP dans une racine, cette dernière revient uniquement à la politique `FullAWSAccess` par défaut attachée automatiquement à toutes les entités figurant dans la racine. Tous les attachements de politiques SCP à des entités AWS Organizations réalisés avant la désactivation de ces politiques sont perdus et ne sont pas récupérables automatiquement, mais vous pouvez les attacher de nouveau 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.

Utilisation des données d'accès pour améliorer les politiques de contrôle des services (SCP)

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. Elles vous permettent d'identifier toute autorisation non utilisée. Vous pouvez ainsi peaufiner vos SCP afin qu'elles respectent au plus près le principe du moindre privilège.

Par exemple, vous pouvez avoir une liste de refus SCP qui interdit l'accès à trois AWS services. 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 quels AWS services sont autorisés par le SCP mais ne sont jamais utilisés. 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 restreintes par les SCP

Vous ne pouvez pas utiliser des SCP 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
- Modifier le niveau de AWS support en tant qu'utilisateur root
- 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

Création, mise à jour et suppression de politiques de contrôle des services

Une fois connecté au compte de gestion de votre organisation, vous pouvez créer et mettre à jour les politiques de contrôle des services (SCP). Vous créez des politiques SCP en créant des instructions qui refusent ou autorisent l'accès aux services et actions que vous spécifiez.

La configuration par défaut pour travailler avec des SCP consiste à utiliser une politique de « liste de blocage » dans laquelle toutes les actions sont implicitement autorisées à l'exception des actions que vous voulez bloquer en créant des instructions qui refusent l'accès. Avec des instructions de refus, vous pouvez spécifier des ressources et conditions pour l'instruction et utiliser l'élément NotAction. Pour les instructions d'autorisation, vous pouvez spécifier uniquement des services et des actions. Pour plus d'informations sur les instructions qui refusent et autorisent l'accès, consultez Évaluation du SCP.

> **Tip**
>
> Vous pouvez utiliser les dernières informations consultées relatives aux services dans IAM pour mettre à jour vos politiques SCP afin de limiter l'accès uniquement aux 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.

Dans cette rubrique :

- Après avoir activé les politiques de contrôle des services pour votre organisation, vous pouvez créer une politique.
- Lorsque vos exigences de SCP changent, vous pouvez mettre à jour une politique existante.
- Lorsque vous n'avez plus besoin d'une politique et après l'avoir détachée de toutes les unités d'organisation (UO) et de tous les comptes, vous pouvez la supprimer.

Création d'une politique de contrôle des services (SCP)

> **Autorisations minimales**
>
> Pour créer des SCP, vous avez besoin d'une autorisation pour effectuer 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 Balisage de ressources 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 des instructions de `Deny`, vous disposez d'un contrôle supplémentaire, car vous pouvez limiter l'accès à des ressources spécifiques, définir des conditions pour le moment où les politiques de contrôle des services sont en vigueur et utiliser l'élément NotAction. 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 l'instruction de l'éditeur, sous Ajouter des actions, choisissez un service AWS.

      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 services AWS (par exemple, `aws:SourceIp`) ou une clé spécifique à un service pour un seul des services que vous avez sélectionnés pour cette instruction.
- Qualificateur – (Facultatif) Si vous saisissez plusieurs valeurs pour la condition selon la clé de condition spécifiée), vous pouvez spécifier un qualificateur pour tester les demandes par rapport aux valeurs.
  - 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 tous les opérateurs de conditions, sauf le test `Null`, vous pouvez choisir l'option IfExists.
- 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 Éléments de politique JSON IAM : NotAction 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 attacher votre SCP à la racine, aux UO ou aux comptes.

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\":[\"*\"]}]}"
    }
}
```

- SDK AWS : CreatePolicy

> **Note**
>
> Les politiques SCP n'ont pas d'effet sur le compte de gestion et dans quelques autres situations. Pour de plus amples informations, consultez Tâches et entités non restreintes par les SCP.

Mise à jour d'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\":[\"*
\"]}]}"
    }
}
```

- SDK AWS : UpdatePolicy

Pour plus d'informations

Pour plus d'informations sur la création de politiques SCP, consultez les rubriques suivantes :

- Exemples de politiques de contrôle des services
- Syntaxe d'une stratégie de contrôle de service

Modification de balises attachées à une 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 Balisage de ressources AWS Organizations.

Autorisations minimales

Pour modifier les balises attachées à une politique SCP dans votre organisation AWS, 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
- SDK AWS : TagResource et UntagResource

Suppression d'une politique de contrôle des services (SCP)

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.

> **Remarques**
>
> - Avant de supprimer une politique, vous devez d'abord la détacher de toutes les entités attachées.
> - Vous ne pouvez pas supprimer les politiques SCP gérées par AWS, comme celle nommée `FullAWSAccess`.

> **Autorisations minimales**
>
> Pour supprimer une SCP, vous devez être autorisé à effectuer l'action suivante :
>
> - `organizations:DeletePolicy`

AWS Management Console

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. La politique à supprimer doit d'abord être détachée de l'ensemble des racines, unités d'organisation et 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 SCP

Vous pouvez utiliser l'une des commandes suivantes pour supprimer une politique :

- AWS CLI : delete-policy

  L'exemple suivant supprime la SCP spécifiée.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- SDK AWS : DeletePolicy

Attachement et détachement de politiques de contrôle des services

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez attacher une politique de contrôle des services (SCP) que vous avez préalablement créée. Vous pouvez attacher une SCP à la racine de l'organisation, à une unité d'organisation ou directement à un compte. Pour attacher une SCP, procédez comme suit.

Autorisations minimales

Pour attacher une SCP à une racine, une unité d'organisation ou un compte, vous avez besoin de l'autorisation d'effectuer 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

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 des unités d'organisation (choisissez l'icône) pour trouver l'UO ou le compte souhaité.
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 SCP attachées sur l'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 des unités d'organisation (choisissez l'icône) pour trouver l'UO ou le compte souhaité.
5. Choisissez Attacher la politique.

   La liste des SCP attachées sur l'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.

AWS CLI & AWS SDKs

Pour attacher une SCP en accédant à la racine, à l'unité d'organisation ou au compte

Vous pouvez utiliser l'une des commandes suivantes pour attacher une SCP :

- AWS CLI : attach-policy

  L'exemple suivant attache une SCP à une unité d'organisation.

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- AWS SDK : AttachPolicy

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.

Détachement d'une SCP de la racine de l'organisation, d'unités d'organisation ou de comptes

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez détacher une SCP de la racine de l'organisation, de l'unité d'organisation ou du compte auquel celle-ci est attachée. Une fois que vous avez détaché un SCP d'une entité, ce SCP ne s'applique plus aux utilisateurs IAM et aux rôles IAM affectés par l'entité désormais détachée. Pour détacher une SCP, procédez comme suit.

> **Note**
>
> Vous ne pouvez pas détacher la dernière politique SCP d'une racine, d'une unité d'organisation ou d'un compte. Au moins une politique de contrôle des services doit être attachée en permanence à chaque racine, unité d'organisation et compte.

> **Autorisations minimales**
>
> Pour détacher une SCP de la racine, d'une unité d'organisation ou d'un compte, vous avez besoin d'une autorisation pour effectuer l'action suivante :
>
> - `organizations:DetachPolicy`

AWS Management Console

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 des unités d'organisation (choisissez l'icône ) pour trouver l'UO ou le compte souhaité. 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 SCP attachées 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 des unités d'organisation (choisissez l'icône ) pour trouver l'UO ou le compte souhaité.
4. Choisissez Détacher.
5. Dans la boîte de dialogue de confirmation, choisissez Détacher.

La liste des SCP attachées 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.

AWS CLI & AWS SDKs

Pour détacher une SCP d'une racine, d'une unité d'organisation ou d'un compte

Vous pouvez utiliser l'une des commandes suivantes pour détacher une SCP :

- AWS CLI : detach-policy

  L'exemple suivant détache la SCP spécifiée de l'unité d'organisation spécifiée.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS SDK : DetachPolicy

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.

Évaluation du SCP

> **Note**
>
> Les informations de cette section ne s'appliquent pas aux types de politiques de gestion, y compris les politiques de désactivation des services AI, les politiques de sauvegarde ou les politiques de balises. Pour de plus amples informations, veuillez consulter Fonctionnement de l'héritage des politiques de gestion.

Vous pouvez attacher plusieurs politiques de contrôle des services (SCP) à différents niveaux dans AWS Organizations. Comprendre comment les SCP sont évaluées peut ainsi vous aider à définir des SCP de sorte qu'elles produisent les résultats attendus.

Rubriques

Fonctionnement des SCP 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 activez des SCP, AWS Organizations attache une politique SCP AWS gérée nommée FullAWSAccess qui autorise tous les services et toutes les actions. Si cette politique est supprimée et n'est remplacée à aucun niveau de l'organisation, aucune action ne sera possible pour les UO ou les comptes sous-jacents.

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 des SCP obéit à un modèle de refus par défaut selon lequel toutes les autorisations non explicitement autorisées dans les SCP sont refusées. Si aucune instruction Allow n'est présente dans les SCP à quelque niveau que ce soit (à la racine ou au niveau de l'UO de production ou du compte B), l'accès est refusé.

> **Remarques**
>
> - Une instruction `Allow` dans un SCP permet à l'élément `Resource` de ne posséder qu'une entrée `"*"`.
> - Une instruction `Allow` dans une SCP ne peut pas avoir d'élément `Condition` du tout.

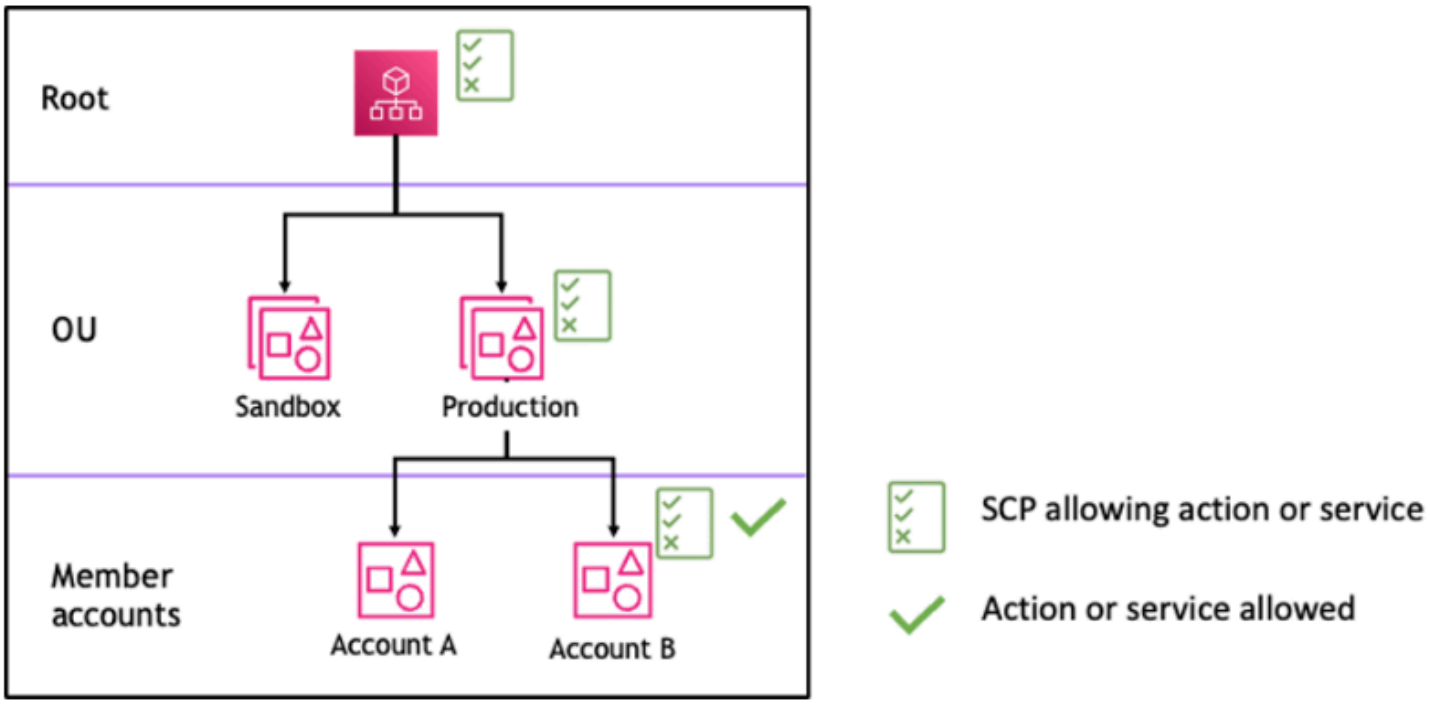


Figure 1 : exemple de structure organisationnelle avec une instruction *Allow* attachée à la racine, à l'UO de production et au compte B

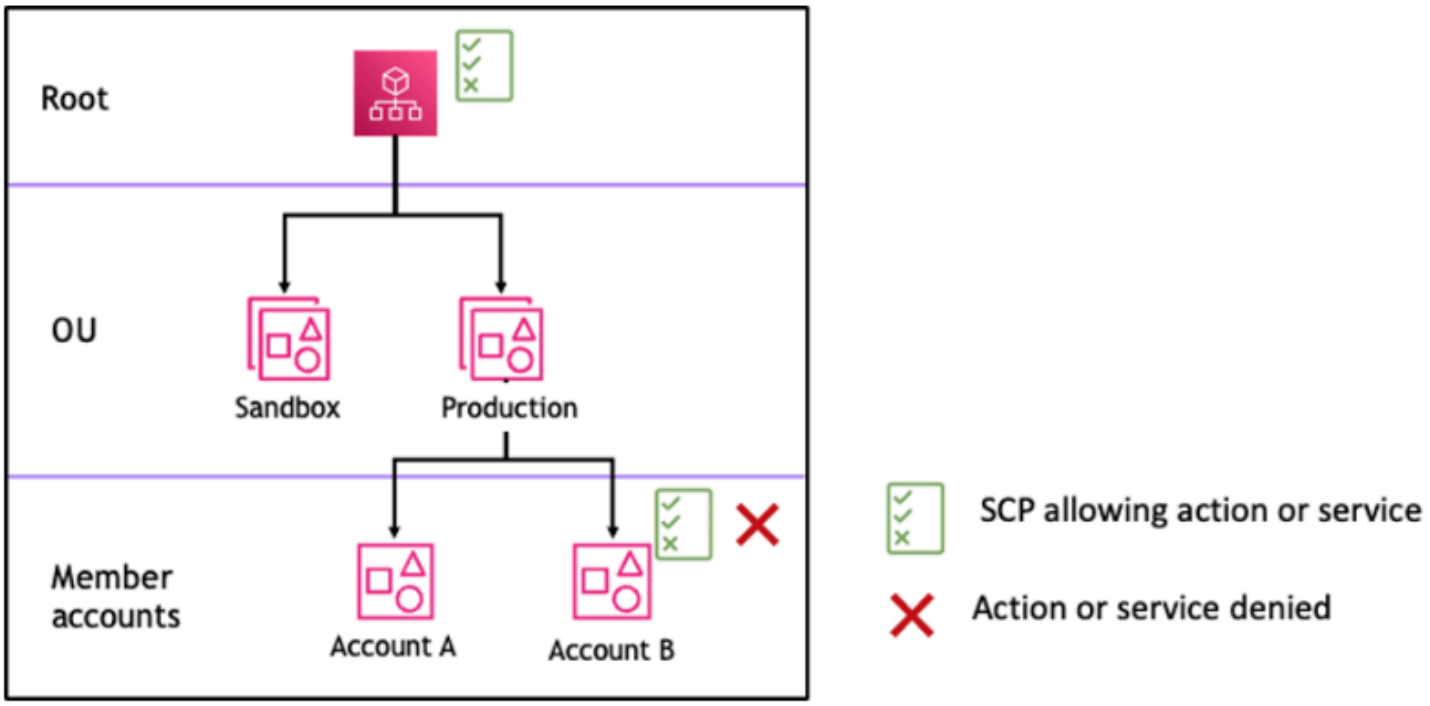


Figure 2 : exemple de structure organisationnelle avec une instruction *Allow* attachée à l'UO de production et impact sur le compte B

Fonctionnement des SCP 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 toutes les UO et tous les comptes membres sous-jacents.

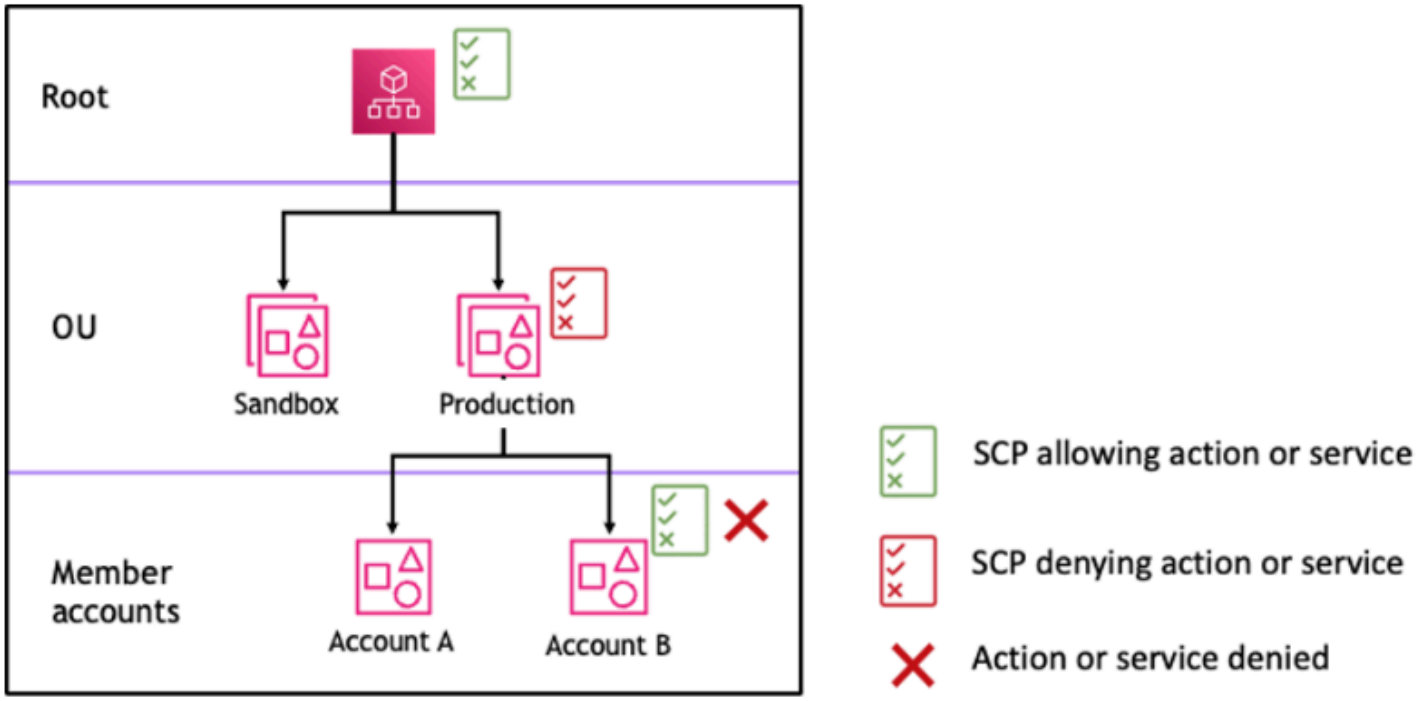


Figure 3 : exemple de structure organisationnelle avec une instruction *`Deny`* attachée à l'UO de production et impact sur le compte B

Stratégie d'utilisation des SCP

Lorsque vous définissez des SCP, vous pouvez utiliser une combinaison d'instructions `Allow` et `Deny` pour autoriser certaines actions et certains services dans votre organisation. Les instructions `Deny` constituent un moyen efficace de mettre en œuvre des restrictions qui s'appliquent à une plus grande partie de votre organisation ou de vos UO, car lorsqu'elles sont appliquées à la racine ou au niveau de l'UO, elles affectent tous les comptes sous-jacents.

Par exemple, vous pouvez mettre en œuvre une politique utilisant Empêcher les comptes membres de quitter l'organisation au niveau de la racine, qui sera effective pour tous les comptes de l'organisation. Les instructions Deny prennent également en charge un élément de condition qui peut être utile pour définir des exceptions.

> **Tip**
>
> Vous pouvez utiliser les dernières informations consultées relatives aux services dans IAM pour mettre à jour vos politiques SCP afin d'en limiter l'accès uniquement aux 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 une SCP gérée par AWS nommée FullAWSAccess à chaque racine, UO et compte lors de sa création. Cette politique autorise tous les services et actions. Vous pouvez remplacer FullAWSAccess par une politique n'autorisant qu'un ensemble défini de services, de sorte que les nouveaux services AWS ne soient pas autorisés à moins d'être explicitement autorisés par une mise à jour des SCP. 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.

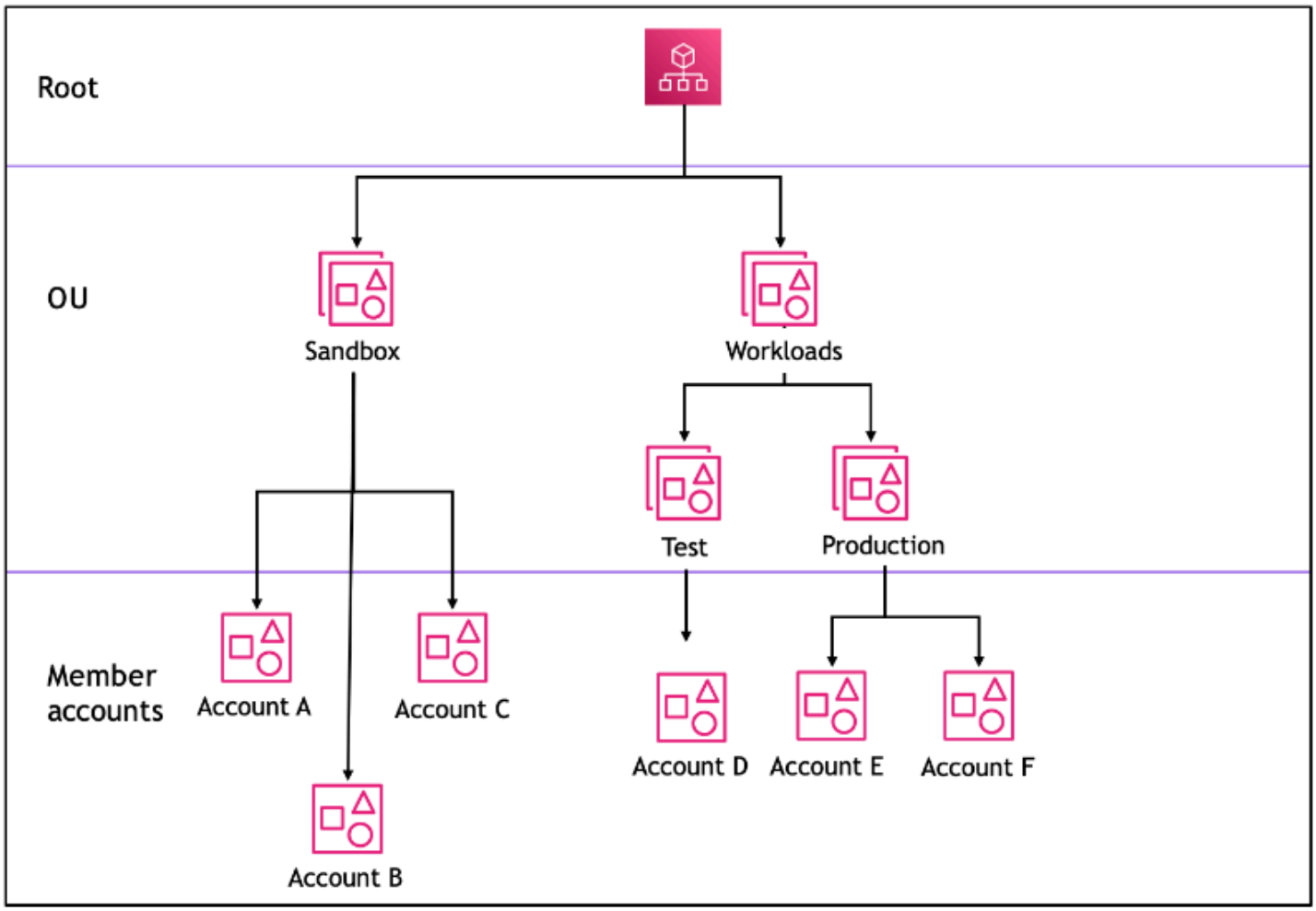
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 politique FullAWSAccess et attacher celle-ci à la place.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Examinons à présent l'exemple de structure organisationnelle suivant pour comprendre comment vous pouvez appliquer plusieurs SCP à différents niveaux d'une organisation.



Le tableau suivant présente les politiques effectives dans l'UO d'environnement de test.

Scénario	SCP attachée à la racine	SCP attachée à l'UO d'environnement de test	SCP attachée au compte A	Politique correspondante attachée au compte A	Politique correspondante attachée au compte B et au compte C
1	Accès complet à AWS	Accès complet à AWS + accès à S3 refusé	Accès complet à AWS + accès à EC2 refusé	Aucun accès à S3 ni EC2	Aucun accès à S3

Scénario	SCP attachée à la racine	SCP attachée à l'UO d'environnement de test	SCP attachée au compte A	Politique correspondante attachée au compte A	Politique correspondante attachée au compte B et au compte C
2	Accès complet à AWS	Accès à Amazon Elastic Compute Cloud (Amazon EC2) autorisé	Accès à EC2 autorisé	Accès autorisé pour EC2 uniquement	Accès autorisé pour EC2 uniquement
3	Accès à S3 refusé	Accès à S3 autorisé	Accès complet à AWS	Aucun accès au service	Aucun accès au service

Le tableau suivant présente les politiques effectives dans l'UO de charge de travail.

Scénario	SCP attachée à la racine	SCP attachée à l'UO de charge de travail	SCP attachée à l'UO de test	Politique correspondante attachée au compte D	Politiques correspondantes attachées à l'UO de production, au compte E et au compte F
1	Accès complet à AWS	Accès complet à AWS	Accès complet à AWS + accès à EC2 refusé	Aucun accès à EC2	Accès complet à AWS

Scénario	SCP attachée à la racine	SCP attachée à l'UO de charge de travail	SCP attachée à l'UO de test	Politique correspondante attachée au compte D	Politiques correspondantes attachées à l'UO de production, au compte E et au compte F
2	Accès complet à AWS	Accès complet à AWS	Accès à EC2 autorisé	Accès à EC2 autorisé	Accès complet à AWS
3	Accès à S3 refusé	Accès complet à AWS	Accès à S3 autorisé	Aucun accès au service	Aucun accès au service

Syntaxe d'une stratégie de contrôle de service

Les politiques de contrôle des services (SCP) utilisent une syntaxe similaire à celle utilisée par les politiques d'autorisation AWS Identity and Access Management (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 politiques SCP formatées avec des espaces supplémentaires pour une meilleure 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 obtenir des informations générales sur les politiques de contrôle des services, consultez Politiques de contrôle de service (SCP).

Récapitulatif des éléments

Le tableau suivant résume les éléments de politique que vous pouvez utiliser dans les politiques de contrôle des services. Certains éléments de politique sont disponibles uniquement dans les politiques de contrôle des services qui refusent des actions. La colonne Effets supportés répertorie le type d'effet que vous pouvez utiliser avec chaque élément de politique dans les politiques de contrôle des services.

Element	Objectif	Effets pris en charge
Version	Spécifie les règles de syntaxe du langage à utiliser pour le traitement de la politique.	`Allow`, `Deny`
Instruction	Sert de conteneur pour les éléments de politique. Vous pouvez avoir plusieurs instructions dans des	`Allow`, `Deny`

Element	Objectif	Effets pris en charge
	politiques de contrôle des services.	
ID d'instruction (Sid)	(Facultatif) Fournit un nom simple pour l'instruction.	`Allow`, `Deny`
Effet	Définit si l'instruction SCP autorise ou refuse l'accès aux utilisateurs et rôles IAM d'un compte.	`Allow`, `Deny`

Element	Objectif	Effets pris en charge
Action	Spécifie le AWS service et les actions que le SCP autorise ou refuse.	`Allow`, `Deny`
NotAction	Spécifie le AWS service et les actions exemptés du SCP. Utilisé au lieu de l'élément `Action`.	`Deny`
Ressource	Spécifie les AWS ressources auxquelles le SCP s'applique.	`Deny`

Element	Objectif	Effets pris en charge
Condition	Spécifie les conditions lorsque l'instruction est vigueur.	`Deny`

Les sections suivantes fournissent davantage d'informations et des exemples sur la façon dont les éléments de politique sont utilisés dans les politiques de contrôle des services.

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.

```
    "Version": "2012-10-17",
```

Pour plus d'informations, consultez Éléments de politique JSON IAM : Version 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 `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. Les SCP agissent plutôt comme des filtres qui spécifient les autorisations maximales pour les utilisateurs IAM et les rôles IAM dans une organisation. 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 où l'élément `Effect` a une valeur de `Deny`, vous pouvez également limiter l'accès à certaines ressources ou définir des conditions pour le moment où les politiques de contrôle des services sont en vigueur.

L'exemple suivant montre la façon d'utiliser une clé de condition dans une instruction de refus.

```
{
```

```
    "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.

Éléments **`Action`** et **`NotAction`**

Chaque instruction doit contenir l'un des éléments suivants :

- Dans les instructions d'autorisation et de refus, un élément `Action`.
- Dans les instructions de refus uniquement (où la valeur de l'élément `Effect` est `Deny`), un «élément `Action` ou `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 sont sensibles à la casse et doivent être saisies comme indiqué dans la documentation de chaque service. En général, elles sont toutes saisies avec chaque mot commençant par une lettre majuscule et le reste en minuscules. 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.

> **Note**
>
> Dans une SPC, les caractères génériques (*) et (?) figurant dans un élément `Action` ou `NotAction` peuvent uniquement être utilisés seuls 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"` et `"servicename:some*action"` sont tous les deux non valides dans des politiques de contrôle des services.

Pour obtenir une liste de tous les services et des actions qu'ils prennent en charge dans les politiques d'autorisation AWS Organizations SCP et 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.

```
{
    "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 :

```
{
    "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.

```
{
  "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 **`Resource`**

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 noms ARN (Amazon Resource Names) de ressources individuelles.

Vous pouvez également utiliser des caractères génériques comme un astérisque (*) ou un point d'interrogation (?) dans l'élément de 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'élément `Effect` a une valeur `Deny`, vous pouvez spécifier des ARN individuels, comme illustré dans l'exemple suivant.

```
{
  "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.

Pour plus d'informations, consultez Éléments de politique JSON IAM : Ressource dans le Guide de l'utilisateur IAM.

Élément **`Condition`**

Vous pouvez spécifier un élément `Condition` dans les instructions de refus d'une SCP.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Cette politique SCP refuse l'accès à toutes les opérations hors des régions `eu-central-1` et `eu-west-1` à l'exception des actions dans les services répertoriés.

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 les politiques de contrôle des services :

- `Principal`
- `NotPrincipal`
- `NotResource`

Exemples de politiques de contrôle des services

Les exemples de politiques de contrôle des services (SCP) affichés dans cette rubrique sont fournis à titre d'information uniquement.

> **Avant d'utiliser ces exemples**
>
> Avant de tenter d'utiliser ces exemples de politiques de contrôle des services dans votre organisation, prenez les précautions suivantes :
>
> - Vérifiez attentivement et personnalisez les SCP en fonction de vos exigences uniques.
> - Testez soigneusement les SCP dans votre environnement avec les services AWS que vous utilisez.
>
> Les exemples de politiques présentés dans cette section illustrent la mise en œuvre et l'utilisation des politiques SCP. 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 à base de refus afin de déterminer si elle répond aux exigences professionnelles de votre environnement. Les politiques de contrôle des services à base de refus peuvent limiter ou bloquer involontairement votre utilisation de services AWS, à moins d'ajouter les exceptions nécessaires à la politique. Pour obtenir un exemple d'exception, consultez le premier exemple qui exempte les services globaux des règles qui bloquent l'accès aux Régions AWS indésirables.

- N'oubliez pas qu'une politique de contrôle des services affecte chaque utilisateur et chaque rôle, y compris l'utilisateur root, dans chaque compte auquel elle est attachée.

> **Tip**
>
> Vous pouvez utiliser les dernières informations consultées relatives aux services dans IAM pour mettre à jour vos politiques SCP afin d'en limiter l'accès uniquement aux 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.

Chacune des politiques suivantes est un exemple de stratégie de politique de liste de refus. Les politiques de liste de refus doivent être attachées avec d'autres politiques qui autorisent les actions approuvées dans les comptes concernés. Par exemple, la politique `FullAWSAccess` par défaut autorise l'utilisation de tous les services d'un compte. Cette politique est attachée par défaut à la racine, à toutes les unités d'organisation et à tous les comptes. Elle n'accorde en fait pas réellement d'autorisations ; aucune politique SCP ne le fait. Au lieu de cela, elle permet aux administrateurs de ce compte de déléguer l'accès à ces actions en attachant des politiques d'autorisations AWS Identity and Access Management (IAM) standard à des utilisateurs, des rôles ou des groupes dans le compte. Chacune de ces politiques de liste de refus remplace toute autre politique en bloquant l'accès aux services ou actions spécifiés.

Exemples

- Exemples généraux
  - Refuser l'accès à AWS en fonction de la Région AWS demandée
  - Empêcher les utilisateurs et les rôles IAM d'apporter certaines modifications
  - Empêcher les utilisateurs et les rôles IAM d'apporter des modifications spécifiées, à l'exception d'un rôle administrateur spécifié
  - Exiger une MFA pour effectuer une action API
  - Bloquer l'accès à des services pour l'utilisateur racine
  - Empêcher les comptes membres de quitter l'organisation
- Exemple de SCP pour Amazon CloudWatch
  - Empêcher les utilisateurs de désactiver CloudWatch ou d'en modifier la configuration
- Exemple de SCP pour AWS Config

Exemples généraux

Refuser l'accès à AWS en fonction de la Région AWS demandée

Cette politique SCP refuse l'accès à toutes les opérations en dehors des régions spécifiées. Remplacez `eu-central-1` et `eu-west-1` par les Régions AWS que vous souhaitez utiliser. La politique prévoit des exemptions pour les opérations dans les services mondiaux approuvés.

Cet exemple montre également comment exempter les demandes faites par l'un des deux rôles d'administrateur spécifiés.

> **Note**
>
> Pour utiliser les Stratégies d'utilisation des politiques de contrôle des services avec AWS Control Tower, consultez Refuser l'accès à AWS en fonction de la Région AWS demandée.

Cette politique utilise l'effet `Deny` pour refuser l'accès à toutes les demandes d'opérations qui ne ciblent pas l'une des deux régions approuvées (`eu-central-1` et `eu-west-1`). L'élément NotAction vous permet de répertorier les services dont les opérations (ou des opérations individuelles) sont exemptées de cette restriction. Étant donné que les services mondiaux ont des points de terminaison hébergés physiquement par la région `us-east-1`, ils doivent être exemptés de cette façon. Avec une politique SCP structurée de cette manière, les demandes adressées aux services mondiaux dans la région `us-east-1` sont autorisées si le service demandé est inclus dans l'élément `NotAction`. Toutes les autres demandes adressées à des services dans la région `us-east-1` sont refusées par cet exemple de politique.

> **Note**
>
> Cet exemple peut ne pas inclure tous les derniers services ou opérations AWS mondiaux. Remplacez la liste des services et opérations par les services mondiaux utilisés par les comptes de votre organisation.
>
> > **Conseil**
> >
> > Vous pouvez afficher les dernières informations consultées relatives aux services dans la console IAM pour déterminer les services mondiaux utilisés par votre organisation. L'onglet Access Advisor de la page de détails d'un utilisateur, d'un groupe ou d'un rôle IAM affiche les services AWS qui ont été utilisés par cette entité, triés en fonction de l'accès le plus récent.

Considérations

- AWS KMS et AWS Certificate Manager prennent en charge les points de terminaison régionaux. Toutefois, si vous souhaitez les utiliser avec un service mondial tel qu'Amazon CloudFront, vous devez les inclure dans la liste d'exclusions de services mondiaux de l'exemple SCP suivant. Un service mondial tel qu'Amazon CloudFront exige généralement l'accès à AWS KMS et ACM dans la même région, qui, pour un service mondial ; est la région USA Est (Virginie du Nord) (`us-east-1`).
- Par défaut, AWS STS est un service mondial et doit être inclus dans la liste d'exclusions de services mondiaux. Cependant, vous pouvez activer AWS STS pour utiliser des points de terminaison régionaux au lieu d'un seul point de terminaison mondial. Si vous faites cela, vous pouvez supprimer STS de la liste d'exemptions de services mondiaux dans l'exemple SCP suivant. Pour plus d'informations, consultez Gestion de AWS STS dans une Région AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
```

```
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
```

```
}
```

Empêcher les utilisateurs et les rôles IAM d'apporter certaines modifications

Cette politique de contrôle des services empêche les utilisateurs et rôles IAM d'apporter des modifications au rôle IAM spécifié que vous avez créé dans tous les comptes de votre organisation.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "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/name-of-role-to-deny"
      ]
    }
  ]
}
```

Empêcher les utilisateurs et les rôles IAM d'apporter des modifications spécifiées, à l'exception d'un rôle administrateur spécifié

Cette politique SCP s'appuie sur l'exemple précédent pour créer une exception pour les administrateurs. Elle 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, à l'exception des administrateurs qui utilisent un rôle spécifié.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "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/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Exiger une MFA pour effectuer une action API

Utilisez une politique SCP telle que ci-dessous pour exiger l'activation de l'authentification multi-facteur (MFA) avant qu'un utilisateur ou un rôle IAM puisse effectuer une action. Dans cet exemple, l'action consiste à arrêter une instance Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Bloquer l'accès à des services pour l'utilisateur racine

La politique suivante limite l'accès à toutes les actions spécifiées pour l'utilisateur racine dans un compte membre. Si vous souhaitez empêcher vos comptes d'utiliser des informations d'identification racine de certaines façons, ajoutez vos propres actions à cette politique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Empêcher les comptes membres de quitter l'organisation

La politique suivante bloque l'utilisation de l'opération d'API `LeaveOrganization` afin que les administrateurs des comptes membres ne puissent pas retirer leurs comptes de l'organisation.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple de SCP pour Amazon CloudWatch

Exemples de cette catégorie

- Empêcher les utilisateurs de désactiver CloudWatch ou d'en modifier la configuration

Empêcher les utilisateurs de désactiver CloudWatch ou d'en modifier la configuration

Un opérateur CloudWatch de niveau inférieur doit surveiller les tableaux de bord et les alarmes. Toutefois, l'opérateur ne doit pas être en mesure de supprimer ni de modifier des tableaux de bord ou des alarmes que ses supérieurs peuvent mettre en place. Cette politique SCP empêche les utilisateurs et les rôles des comptes concernés d'exécuter les commandes CloudWatch qui pourraient supprimer ou modifier vos tableaux de bord ou alarmes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple de SCP pour AWS Config

Exemples de cette catégorie

- Empêcher les utilisateurs de désactiver AWS Config ou d'en modifier les règles

Empêcher les utilisateurs de désactiver AWS Config ou d'en modifier les règles

Cette politique SCP empêche les utilisateurs et les rôles des comptes concernés d'exécuter des opérations AWS Config qui pourraient désactiver AWS Config ou en modifier les règles ou les déclencheurs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemples de SCP pour Amazon Elastic Compute Cloud (Amazon EC2)

Exemples de cette catégorie

- Exiger que les instances Amazon EC2 utilisent un type spécifique
- Empêcher le lancement d'instances EC2 sans IMDSv2
- Empêcher la désactivation du chiffrement Amazon EBS par défaut

Exiger que les instances Amazon EC2 utilisent un type spécifique

Avec cette politique de contrôle des services, tous les lancements d'instances qui n'utilisent pas le type d'instance `t2.micro` sont refusés.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

Empêcher le lancement d'instances EC2 sans IMDSv2

La politique suivante interdit à tous les utilisateurs de lancer des instances EC2 sans IMDSv2.

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
```

```
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

La politique suivante interdit à tous les utilisateurs de lancer des instances EC2 sans IMDSv2, mais autorise des identités IAM spécifiques pour modifier les options de métadonnées d'instance.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
```

```
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

Empêcher la désactivation du chiffrement Amazon EBS par défaut

La politique suivante interdit à tous les utilisateurs de désactiver le chiffrement Amazon EBS par défaut.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Exemples de SCP pour Amazon GuardDuty

Exemples de cette catégorie

- Empêcher les utilisateurs de désactiver GuardDuty et d'en modifier la configuration

Empêcher les utilisateurs de désactiver GuardDuty et d'en modifier la configuration

Cette politique SCP empêche les utilisateurs et les rôles des comptes concernés de désactiver GuardDuty ou d'en modifier la configuration, que ce soit directement sous la forme d'une commande ou via la console. Elle permet d'accéder en lecture seule aux informations et aux ressources GuardDuty.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
```

```
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple de SCP pour AWS Resource Access Manager

Exemples de cette catégorie

- Empêcher le partage externe
- Autoriser des comptes spécifiques à partager uniquement des types de ressources spécifiés
- Empêcher le partage avec des organisations ou des unités d'organisation (UO)
- Autoriser le partage uniquement avec des utilisateurs et des rôles IAM spécifiés

Empêcher le partage externe

L'exemple suivant SCP empêche les utilisateurs de créer des partages de ressources qui autorisent le partage avec des utilisateurs et des rôles IAM qui ne font pas partie de l'organisation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Autoriser des comptes spécifiques à partager uniquement des types de ressources spécifiés

La politique SCP suivante autorise les comptes 111111111111 et 222222222222 à créer des partages de ressources partageant des listes de préfixes et à associer des listes de préfixes à des partages de ressources existants.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Empêcher le partage avec des organisations ou des unités d'organisation (UO)

La politique SCP suivante empêche les utilisateurs de créer des partages de ressources qui partagent des ressources avec un organisation ou des unités d'organisation AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
```

```
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Autoriser le partage uniquement avec des utilisateurs et des rôles IAM spécifiés

L'exemple de SCP suivant permet aux utilisateurs de partager des ressources uniquement avec l'organisation `o-12345abcdef`, l'unité d'organisation `ou-98765fedcba` et le compte `111111111111`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
```

```
            }
        }
    ]
}
```

Exemple des politiques de contrôle des services (SCP) pour Amazon Route 53 Application Recovery Controller

Exemples de cette catégorie

- Empêcher les utilisateurs de mettre à jour les états de contrôle de routage Route 53 ARC

Empêcher les utilisateurs de mettre à jour les états de contrôle de routage Route 53 ARC

Un opérateur Route 53 ARC de niveau inférieur doit surveiller les tableaux de bord et les informations relatives à Route 53 ARC. Toutefois, l'opérateur ne doit pas être en mesure de mettre à jour les commandes de routage pour faire basculer l'application d'une Région AWS à une autre, comme un opérateur expérimenté pourrait être autorisé à le faire. Cette politique SCP empêche les utilisateurs et les rôles des comptes concernés d'exécuter les opérations Route 53 ARC qui mettent à jour les contrôles de routage Route 53 ARC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
```

```
}
```

Exemples de SCP pour Amazon S3

Exemples de cette catégorie

- Empêcher les téléchargements d'objets non chiffrés sur Amazon S3

Empêcher les téléchargements d'objets non chiffrés sur Amazon S3

La politique suivante interdit à tous les utilisateurs de télécharger des objets non chiffrés vers des compartiments S3.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

La politique suivante interdit à tous les utilisateurs de télécharger des objets non chiffrés vers des compartiments S3 et applique également un type de chiffrement spécifique (AES256 ou aws:kms) pour le téléchargement d'objets dans leurs compartiments.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
```

```
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

Exemples de SCP pour le balisage de ressources

Exemples de cette catégorie

- Exiger une balise sur des ressources créées spécifiées
- Empêcher la modification de balises sauf par des mandataires autorisés

Exiger une balise sur des ressources créées spécifiées

La politique SCP suivante empêche les utilisateurs et les rôles IAM des comptes concernés de créer certains types de ressources si la demande n'inclut pas les balises spécifiées.

> **Important**
>
> N'oubliez pas de tester les politiques basées sur Deny avec les services que vous utilisez dans votre environnement. L'exemple suivant est un simple blocage des actions visant à créer des secrets non balisés ou d'exécuter des instances Amazon EC2 non balisées, et ne comporte aucune exception.
>
> L'exemple de politique suivant n'est pas compatible avec AWS CloudFormation tel qu'il est écrit, car ce service crée un secret, puis le balise en deux étapes distinctes. Cet exemple de politique empêche efficacement AWS CloudFormation de créer un secret dans le cadre d'une pile, car une telle action aboutirait, aussi brièvement que ce soit, à un secret qui n'est pas balisé de la manière requise.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
```

```
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
```

```
        }
      }
    }
  ]
}
```

Pour obtenir une liste de tous les services et actions pris en charge à la fois dans les politiques de contrôle des services AWS Organizations et dans les politiques d'autorisation IAM, consultez Actions, ressources et clés de conditions pour les services AWS dans le Guide de l'utilisateur IAM.

Empêcher la modification de balises sauf par des mandataires autorisés

La politique SCP suivante montre comment une politique peut autoriser uniquement les mandataires autorisés à modifier les balises attachées à vos ressources. Ceci est une partie importante de l'utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le cadre de votre politique de sécurité dans le cloud AWS. Cette politique permet à un appelant de modifier les balises uniquement sur les ressources où la balise d'autorisation (dans cet exemple, `access-project`) correspond exactement à la même balise d'autorisation attachée à l'utilisateur ou rôle qui fait la demande. La politique empêche également l'utilisateur autorisé de modifier la valeur de la balise utilisée pour l'autorisation. Le mandataire appelant doit avoir la balise d'autorisation pour pouvoir effectuer des modifications.

Cette politique ne fait qu'empêcher les utilisateurs non autorisés de modifier des balises. Un utilisateur autorisé qui n'est pas bloqué par cette politique doit toujours disposer d'une politique IAM distincte qui accorde explicitement l'autorisation `Allow` sur les API de balisage appropriées. Par exemple, si votre utilisateur dispose d'une politique d'administrateur avec `Allow */*` (autoriser tous les services et toutes les opérations), la combinaison permet à l'utilisateur administrateur de modifier uniquement les balises dont la valeur de balise d'autorisation correspond à la valeur de balise d'autorisation attachée au mandataire de l'utilisateur. En effet, le `Deny` explicite dans cette politique remplace le `Allow` explicite contenu dans la politique d'administrateur.

> **Important**
>
> Il ne s'agit pas d'une solution de politique complète et elle ne doit pas être utilisée comme illustré ici. Cet exemple est destiné uniquement à illustrer une partie d'une politique ABAC et doit être personnalisé et testé pour les environnements de production.
> Pour obtenir la politique complète avec une analyse détaillée de son fonctionnement, consultez Sécurisation des balises de ressources utilisées pour l'autorisation en utilisant une politique de contrôle des services dans AWS Organizations

N'oubliez pas de tester les politiques basées sur Deny avec les services que vous utilisez dans votre environnement.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Exemples de SCP pour Amazon Virtual Private Cloud (Amazon VPC)

Exemples de cette catégorie

- Empêcher les utilisateurs de supprimer des journaux de flux Amazon VPC
- Empêcher tout VPC qui ne dispose pas déjà d'un accès Internet de l'obtenir

Empêcher les utilisateurs de supprimer des journaux de flux Amazon VPC

Cette politique SCP empêche les utilisateurs et les rôles des comptes concernés de supprimer des journaux de flux Amazon Elastic Compute Cloud (Amazon EC2) ou des groupes ou flux de journaux CloudWatch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Empêcher tout VPC qui ne dispose pas déjà d'un accès Internet de l'obtenir

Cette politique SCP empêche les utilisateurs et les rôles des comptes concernés de modifier la configuration de vos clouds privés virtuels (VPC) Amazon EC2 pour leur accorder un accès direct à Internet. Elle ne bloque pas l'accès direct existant ni aucun accès qui passe par votre environnement réseau sur site.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

Gestion des unités d'organisation

Vous pouvez utiliser des unités d'organisation (UO) pour regrouper des 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 créer plusieurs unités d'organisation au sein d'une seule organisation. Vous pouvez également créer des unités d'organisation au sein d'autres unités d'organisation. 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.

> **Note**
>
> Il existe une racine dans l'organisation, qui AWS Organizations crée pour vous lorsque vous configurez votre organisation pour la première fois.

Rubriques

Vous pouvez également examiner toutes les UO de votre organisation. Pour plus d'informations, consultez la rubrique Affichage des détails d'une UO.

Navigation dans la racine et la hiérarchie des unités d'organisation

Pour accéder à différentes unités d'organisation ou à la racine lors du déplacement de comptes ou de l'attachement de stratégies, vous pouvez utiliser la vue « arborescence » affichée par défaut.

AWS Management Console

Pour naviguer dans l'organisation sous la forme d'une arborescence

1. Connectez-vous à la consoleAWS 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. Initialement, l'arborescence présente la racine et n'affiche que le premier niveau des unités d'organisation enfants affichées. 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 voir aucune des unités d'organisation ni manipuler les politiques qui leur sont attachées.

AWS Management Console

Pour afficher l'organisation sous la forme d'une liste non hiérarchique des comptes

1. Connectez-vous à la consoleAWS 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.

Création d'une unité d'organisation

Lorsque que vous êtes connecté au compte de gestion de votre organisation, vous pouvez créer une unité d'organisation dans la racine de l'organisation. Les unités d'organisation peut être imbriquées jusqu'à une profondeur de cinq niveaux. Pour créer une unité d'organisation, procédez comme suit :

Important

Si cette organisation est gérée par AWS Control Tower, créez vos unités d'organisation avec la AWS Control Tower console ou les API. 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 deAWS 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 consoleAWS 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 créé précédemment des unités d'organisation et que vous avez déplacé des comptes vers celles-ci, la console affiche uniquement les unités

d'organisation de niveau supérieur et les comptes que vous n'avez pas encore déplacés vers une unité d'organisation.

3. (Facultatif) Si vous voulez créer une unité d'organisation à l'intérieur d'une unité d'organisation existante, accédez à l'unité d'organisation enfant en choisissant le nom (pas la case à cocher) de l'unité d'organisation enfant ou en choisissant l'icône

en regard de l'unité d'organisation dans l'arborescence jusqu'à voir celle que vous voulez, pis 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 unité d'organisation

Vous pouvez utiliser l'une des commandes suivantes pour créer une unité d'organisation :

- AWS CLI: create-organizational-unit

  Pour créer une unité d'organisation, vous devez d'abord trouver l'identité de la racine ou de l'unité d'organisation que vous souhaitez définir comme unité parente de la nouvelle unité.

  Pour trouver l'identité de la racine, utilisez la commande list-roots. Pour trouver l'identité d'une unité d'organisation, utilisez la commande liste-children pour accéder à l'unité d'organisation souhaitée.

  L'exemple suivant montre comment trouver l'identité de la racine, puis trouver l'identité d'une unité d'organisation sous la racine. La dernière commande indique comment créer une unité d'organisation dans celle que vous avez trouvée.

```
$ 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"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS SDK : CreateOrganizationalUnit

Modification du nom d'une unité d'organisation

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 de votre AWS 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 consoleAWS 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"
    }
}
```

- AWS SDK : UpdateOrganizationalUnit

Modification de balises attachées à une UO

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 associées à une unité organisationnelle au sein d'une racine de votre AWS 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 consoleAWS 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 SDK : TagResourceet UntagResource

Déplacement de comptes vers une unité d'organisation ou entre la racine et des unités d'organisation

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. Lorsque vous placez un compte dans une unité d'organisation, ce compte est soumis à toutes les politiques attachées à l'unité parente et aux autres unités situées dans la chaîne d'unités parentes 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 consoleAWS 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 un compte 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 les ID des 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 SDK : MoveAccount

Suppression d'unités d'organisation

Lorsque vous êtes connecté au compte de gestion de votre organisation, vous pouvez supprimer les unités d'organisation dont vous n'avez plus besoin.

Vous devez d'abord sortir tous les comptes de l'unité d'organisation et des unités d'organisation enfants, après quoi vous pouvez supprimer les unités enfants.

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 consoleAWS 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 les unités d'organisation à supprimer et cochez ☑ en regard du nom de chaque unité.
3. Choisissez Actions, puis, sous Unité d'organisation, choisissez Supprimer.
4. Pour confirmer que vous souhaitez supprimer les unités d'organisation, entrez le nom de l'unité d'organisation (si vous avez choisi d'en supprimer une seule) ou le mot « supprimer » (si vous en avez choisi plusieurs), puis choisissez Supprimer.

   AWS Organizations supprime les UO et les retire de la liste.

AWS CLI & AWS SDKs

Pour supprimer une unité d'organisation

Vous pouvez utiliser l'une des commandes suivantes pour supprimer une unité d'organisation :

- AWS CLI: delete-organizational-unit

  L'exemple suivant montre comment supprimer une unité d'organisation.

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS SDK : DeleteOrganizationalUnit

Balisage de ressources AWS Organizations

Une balise est une étiquette d'attribut personnalisée que vous ajoutez à une ressource AWS 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 les balises pour classer vos ressources par objectif, propriétaire, environnement ou selon 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.

Actuellement, AWS Organizations prend en charge les opérations de balisage suivantes lorsque vous êtes connecté au compte principal :

- Vous pouvez ajouter des balises aux ressources d'organisation suivantes :
  - Comptes AWS
  - Unités d'organisation
  - Racine de l'organisation
  - Politiques

Vous pouvez ajouter des balises 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`.

Vous pouvez afficher les balises sur n'importe quelle ressource balisable dans AWS Organizations en utilisant la console ou en appelant l'opération `ListTagsForResource`.

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 désactivation des services IA
  - Politique de sauvegarde
  - Politique de contrôle des services
  - Politique de balises

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 valeurs de balise sont sensibles à la casse. 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
- AWSSDK : 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
- AWSSDK : UntagResource

Utilisation d'AWS Organizations avec d'autres services AWS

Vous pouvez utiliser l'accès approuvé pour permettre à un service AWS supporté que vous spécifiez, appelé le service approuvé, d'effectuer des tâches dans votre organisation et dans 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

Nous vous recommandons fortement, lorsque l'option est disponible, d'activer et de désactiver l'accès approuvé uniquement en utilisant la console du service approuvé ou ses équivalents via l'AWS CLI ou une 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 AWS services 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 approuvé nécessite des autorisations pour deux services : AWS Organizations et le service approuvé. Pour activer l'accès approuvé, choisissez l'un des scénarios suivants :

- Si vous avez des informations d'identification avec des autorisations dans AWS Organizations et le service approuvé, activez l'accès à l'aide des outils (console ou AWS CLI) disponibles dans le service approuvé. Cela permet au service approuvé d'activer l'accès approuvé dans AWS Organizations en votre nom et de créer toutes les ressources requises par le service pour fonctionner 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, consultez Clés de condition.
  - `organizations:ListAWSServiceAccessForOrganization` : Nécessaire si vous utilisez la console AWS Organizations.
  - 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 dispose d'informations d'identification avec des autorisations dans AWS Organizations mais que quelqu'un d'autre a des informations d'identification avec des autorisations dans le service approuvé, effectuez les étapes suivantes dans l'ordre suivant :

  1. La personne qui dispose des informations d'identification avec des autorisations dans AWS Organizations doit utiliser la console AWS Organizations, l'AWS CLI ou un kit SDK AWS pour activer l'accès approuvé pour le service approuvé. 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 autorisations AWS Organizations minimales sont les suivantes :

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – Nécessaire uniquement si vous utilisez la console AWS Organizations

     Pour les étapes permettant l'activation de l'accès approuvé dans AWS Organizations, consultez Procédure 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 AWS services 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 service AWS, vous pouvez supprimer les autorisations IAM qui accordent cet accès ou vous pouvez utiliser les politiques de contrôle des services (SCP) dans AWS Organizations.

Vous pouvez appliquer des politiques de contrôle de service uniquement aux comptes membres. Les politiques de contrôle de service ne s'appliquent pas au compte de gestion. Nous vous recommandons de ne pas exécuter de services dans le compte de gestion. Au lieu de cela, exécutez-les dans des comptes de membres où vous pouvez contrôler la sécurité à l'aide de SCP.

- Si vous avez des informations d'identification avec des autorisations dans AWS Organizations et le service approuvé, désactivez l'accès à l'aide des outils (console ou AWS CLI) disponibles pour le service approuvé. 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, consultez Clés de condition.
  - `organizations:ListAWSServiceAccessForOrganization` : Nécessaire si vous utilisez la console AWS Organizations.
  - 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 avec des autorisations dans AWS Organizations ne sont pas les informations d'identification avec des autorisations dans le service approuvé, effectuez les étapes suivantes 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 AWS services que vous pouvez utiliser avec AWS Organizations.
  2. La personne dotée d'autorisations dans AWS Organizations peut alors utiliser la console AWS Organizations, AWS CLI ou un kit SDK AWS afin de désactiver l'accès pour le service approuvé. Cela élimine de l'organisation et de ses comptes les autorisations pour le service approuvé.

     Les autorisations AWS Organizations minimales sont les suivantes :

     - `organizations:DisableAWSServiceAccess`

- `organizations:ListAWSServiceAccessForOrganization` – Nécessaire uniquement si vous utilisez la console AWS Organizations

Pour les étapes permettant la désactivation de l'accès approuvé dans AWS Organizations, consultez Procédure 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 approuvé à votre organisation au nom de l'administrateur de l'autre service AWS, utilisez la procédure suivante.

Important

Nous vous recommandons fortement, lorsque l'option est disponible, d'activer et de désactiver l'accès approuvé uniquement en utilisant la console du service approuvé ou ses équivalents via l'AWS CLI ou une 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 AWS services 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.

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, indiquez à l'administrateur de l'autre service AWS qu'il peut désormais permettre à l'autre service de fonctionner avec 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 commandes de la AWS CLI ou les opérations d'API suivantes pour activer ou désactiver l'accès aux services approuvés :

- AWS CLI : AWS organizations enable-aws-service-access
- AWS CLI : AWS organizations disable-aws-service-access
- API AWS : EnableAWSServiceAccess
- API AWS : DisableAWSServiceAccess

AWS Organizations et rôles liés à un service

AWS Organizations utilise les rôles liés à un service IAM pour permettre aux services approuvés d'effectuer des tâches en votre nom dans 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 service AWS Organizations lui-même peut assumer ce rôle. Ce rôle dispose d'autorisations permettant à AWS Organizations de créer des rôles liés à un service pour d'autres 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 à un service, si celui-ci n'existe pas encore.
- 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**
>
> Les politiques SCP d'AWS Organizations n'affectent jamais les rôles liés à un service. Ces rôles sont dispensés de toute restriction SCP.

AWS services 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 AWS des autres services. Vous pouvez tirer parti des services de gestion multicomptes disponibles dans AWS Organizations certains AWS services pour effectuer des tâches sur tous les comptes membres de votre organisation.

Le tableau suivant répertorie les AWS services que vous pouvez utiliser et AWS Organizations les avantages de l'utilisation de chaque service au niveau 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 plus d'informations, consultez Utilisation d'AWS Organizations avec d'autres services AWS.

Administrateur délégué pour les AWS services — 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 plus d'informations, consultez Administrateur délégué pour les services AWS intégrés à Organizations.

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
AWS Account Management Gérez les détails et les métadonnées de l'ensemble Comptes AWS de votre organisation.	Vous pouvez créer, mettre à jour et supprimer les autres informations de contact pour tous les comptes de votre	 Oui En savoir plus	 En savoir plus	Oui

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	organisation.			
AWS Application Migration Service AWS Application Migration Service permet aux entreprises AWS d'lift-and-shift accéder 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 En savoir plus	 Oui 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 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 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 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 En savoir plus	Oui 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 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 dans vos unités d'organisation (UO). Vous pouvez surveiller de manière centralisée les sauvegard	 Oui En savoir plus	 Oui 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 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	 Oui 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	
	partagés auxquels vous avez souscrit. 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 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	 Oui En savoir plus	 Oui 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	
	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 CloudTrail 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	 Oui En savoir plus	 Oui 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	
	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 Compute Optimizer 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. Pour de plus amples informations, consultez Comptes pris en charge par Compute	 Oui En savoir plus	 Oui 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	
	Optimizer dans le Guide de l'utilisateur AWS Compute Optimizer.			

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 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\	 Oui En savoir plus	 Oui En savoir plus : Règles de configuration Packs de conformité 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	
	dans l'ensemble de votre organisation. 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 service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	AWS Organizations. Pour 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 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	 Oui 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	
	réglementations de conformité à l'ensemble de vos activités Comptes A\ 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 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. Pour plus d'informations, voir Cost Optimization Hub	 Oui En savoir plusa	 Non	

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 du Cost Optimization Hub.			

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
Amazon Detective 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 En savoir plus	 Oui 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 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 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	Oui En savoir plus	Oui 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	
	comptes afin d'obtenir l'état de toutes les applications contrôlées à l'échelle de l'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 Directory Service 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 AWS Directory Service un partage d'annuaire fluide entre plusieurs comptes et n'importe quel VPC d'une région.	 Oui 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 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. Pour plus d'informations, consultez la section Envoyer et	 Nor	 Non	

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	recevoir 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	
AWS Firewall Manager 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 En savoir plus	 Oui 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 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	 Oui En savoir plus	 Oui 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. Vous pouvez également automatiser GuardDuty l'activation des nouveaux comptes ajoutés à votre organisation. 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 Bénéficiez d'une visibilité sur les événements susceptibles d'affecter les performances de vos ressources ou les problèmes de disponibilité des AWS services.	Vous pouvez agréger AWS Health les événements entre les comptes de votre organisation.	 Oui En savoir plus	 Oui 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 Identity and Access Management 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 les politiques de	 Nor	 Non	

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	contrôle des services (SCP) qui limitent l'accès uniquement aux services AWS utilisés par les comptes de votre organisation. Pour obtenir un exemple, consultez Utilisation des données pour affiner les autorisations d'une unité d'organis			

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	ation dans le Guide de l'utilisateur IAM.			

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 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. Pour de plus amples informations, consultez Activation d'Access Analyzer dans le Guide de l'utilisateur IAM.	 Oui En savoir plus	 Oui 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 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 les expositions involontaires sur le 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. Pour plus d'informa	 Oui En savoir plus	 Oui 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	
	tions, consultez Gestion de plusieurs comptes avec AWS Organizations dans le Guide de l'utilisateur Amazon Inspector.			

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
AWS License Manager 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 En savoir plus	 Oui 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 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	 Oui En savoir plus	 Oui 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	
	pouvez 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 compartim			

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué
	ents S3 pour l'ensemble de votre organisation.		
AWS Marketplace 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 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 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, à une ou plusieurs unités d'organisation ou à un ou plusieurs comptes de votre organisation, chacun disposant de son propre	 Oui En savoir plus	 Oui 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	
	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			

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	votre équipe.			
AWS 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.	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 En savoir plus	 Oui 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
Développeur Amazon Q Amazon Q Developer est un assistant conversationnel basé sur l'intelligence artificielle générative (IA) qui peut vous aider à comprendre, créer, étendre et exploiter AWS des applications.	La version payante d'Amazon Q Developer nécessite l'intégration d'Organizations.	 Oui 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 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	 Oui 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	
	capacité à la demande, etc. Pour en savoir plus sur le partage des réservations de capacité, consultez le Guide de l'utilisateur Amazon EC2 pour les instances Linux ou le Guide de l'utilisateur Amazon EC2 pour les instances Windows.			

AWS service	Avantages de l'utilisation avec AWS Organizations	Prise en charge de l'accès approuvé	Prise en charge de l'administrateur délégué	
	Pour obtenir la liste des ressources partageables, consultez Ressources partageables dans le Guide de l'utilisateur AWS RAM .			
Explorateur de ressources AWS Explorez vos ressources à l'aide d'une expérience semblable à celle d'un moteur de recherche Internet.	Activez la recherche multi-comptes.	 Oui En savoir plus	 Oui 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 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 Security Hub pour tous les comptes de votre organisation, y compris les nouveaux comptes à mesure qu'ils sont ajoutés. Cela augmente la couverture des vérifications et conclusions de Security	 Oui En savoir plus	 Oui 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	
	Hub, ce qui fournit une image plus précise de votre posture de sécurité globale.			

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 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 En savoir plus	 Oui 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 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 En savoir plus	 Oui 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 Créez et gérez des catalogues des services informatiques dont l'utilisation est approuvée sur AWS.	Vous pouvez partager des portefeuilles et copier des produits sur des comptes plus facilement, sans partager des ID de portefeuilles.	 Oui En savoir plus	 Oui 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 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 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 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	 Oui En savoir plus	 Oui 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	
	ont été attribués.			

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 Manager Améliorez la visibilité et le contrôle de vos AWS ressources.	Vous pouvez synchroniser les données opérationnelles Comptes A\ dans l'ensemble de votre organisation à l'aide de Systems Manager Explorer. Vous pouvez gérer les modèles, approbations et rapports de changement pour tous les comptes	Oui En savoir plus	Oui 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	
	membres de votre organisation à partir d'un compte d'administrateur délégué à l'aide de Systems Manager Change Manager.			

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 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	 Oui 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	
	de ces règles.			
AWS Trusted Advisor 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 A\ membres de votre organisation.	 Oui En savoir plus	 Oui 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 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 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) 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 En savoir plus	 Oui 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 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 (VPC).	Tracez les chemins entre les comptes de vos organisations.	 Oui En savoir plus	 Oui En savoir plus	

AWS Account Management et AWS Organizations

AWS Account Management vous aide à gérer les informations et les métadonnées de compte pour tous les Comptes AWS 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'AWS Account Management dans votre organisation dans le Guide de l'utilisateur AWS Account Management.

Utilisez les informations suivantes pour vous aider à intégrer AWS Account Management à 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.

Account Management a besoin d'un accès approuvé à AWS Organizations pour vous autoriser à désigner un compte membre comme administrateur délégué de ce service pour votre organisation.

Vous pouvez activer l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Account Management, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Account Management qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Account Management en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

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 de gestion AWS Organizations peut désactiver l'accès approuvé avec AWS Account Management.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS Account Management, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.

5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Account Management qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Account Management en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 Création ou mise à jour d'une politique de délégation basée sur les ressources.

AWS CLI, AWS API

Si vous souhaitez configurer un compte administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le principal du service de compte `account.amazonaws.com` en tant que 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 SDK.

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 la page Services, recherchez la ligne correspondant à AWS Application Migration Service, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur de AWS Organizations Only, indiquez-lui AWS Application Migration Service 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 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 AWSServiceAccess

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 AWS Organizations outils AWS Application Migration Service ou.

> **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 SDK.

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. Sur la page Services, recherchez la ligne correspondant à AWS Application Migration Service, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Disable trusted access (Désactiver l'accès approuvé).

5. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Application Migration Service qu'il peut désormais désactiver ce service à l'aide de sa console ou des outils qu'il n'utilise pas AWS Organizations.

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 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 AWSServiceAccess

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'un AWS des SDK, 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`

Activation de l'accès approuvé 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 pouvez activer l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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 la page Services, recherchez la ligne correspondant à AWS Artifact, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur de AWS Organizations Only, indiquez-lui AWS Artifact 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 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 AWSServiceAccess

Désactivation de l'accès approuvé 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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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. Sur la page Services, recherchez la ligne correspondant à AWS Artifact, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS Artifact qu'il peut désormais désactiver ce service à l'aide de sa console ou des outils qu'il n'utilise pas AWS Organizations.

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 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 AWSServiceAccess

AWS Audit Manager et AWS Organizations

AWS Audit Manager vous aide à auditer en continu votre utilisation d'AWS pour simplifier la gestion des 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 AWS Organizations, vous pouvez recueillir des preuves auprès d'une source plus large en incluant plusieurs Comptes AWS de votre organisation dans le cadre de vos évaluations.

Pour de plus amples informations, consultez Activer AWS Organizations dans le Guide de l'utilisateur Audit Manager.

Utilisez les informations suivantes pour vous aider à intégrer AWS Audit 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 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 exige un accès approuvé à AWS Organizations avant que vous puissiez désigner un compte membre comme administrateur délégué pour votre organisation.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Audit Manager ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Audit Manager pour activer l'intégration à Organizations. Cela permet à AWS Audit Manager 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 AWS Audit Manager. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Audit Manager, 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 console AWS Audit Manager, AWS Audit Manager active automatiquement l'accès approuvé pour vous.

Vous pouvez activer l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès approuvé aux services :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Audit Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

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 de gestion AWS Organizations peut désactiver l'accès approuvé avec AWS Audit Manager.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Audit Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

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 console AWS Audit Manager, Audit Manager active automatiquement l'accès approuvé pour vous.

AWS CLI, AWS API

Si vous souhaitez configurer un compte administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- SDK AWS : appelez l'opération `RegisterAccount` et donnez `delegatedAdminAccount` comme paramètre pour déléguer le compte administrateur.

AWS Backup et AWS Organizations

AWS Backup est un service qui vous permet de gérer et de surveiller les tâches AWS Backup de votre organisation. En utilisant AWS Backup, si vous vous connectez en tant qu'utilisateur au compte de gestion de l'organisation, vous pouvez activer la protection et la surveillance des sauvegardes à l'échelle de l'organisation. Cela vous aide à réaliser la conformité au moyen de politiques de sauvegarde pour appliquer de manière centralisée des plans AWS Backup aux ressources de tous les comptes de votre organisation. Lorsque vous utilisez AWS Backup et AWS Organizations ensemble, vous pouvez profiter des avantages suivants :

Protection

Vous pouvez activer le type de politique de sauvegarde dans votre organisation, puis créer des politiques de sauvegarde à associer à la racine, aux UO ou aux comptes de l'organisation. Une politique de sauvegarde combine un plan AWS Backup avec les autres détails nécessaires à l'application automatique du plan à vos comptes. Les politiques directement attachées à un compte sont fusionnées avec celles héritées de la racine de l'organisation et des UO parentes éventuelles afin de créer une politique effective qui s'applique au compte. La politique inclut l'ID d'un rôle IAM qui dispose des autorisations requises pour exécuter AWS Backup sur les ressources de vos comptes. AWS Backup utilise le rôle IAM pour effectuer la sauvegarde en votre nom, comme spécifié 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 sur AWS Backup, consultez le Guide du développeur AWS Backup.

Utilisez les informations suivantes pour vous aider à intégrer AWS Backup à AWS Organizations.

Activation de l'accès approuvé 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 approuvé à l'aide de la console AWS Backup ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Backup pour activer l'intégration à Organizations. Cela permet à AWS Backup 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 AWS Backup. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Backup, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de AWS Backup, consultez Activation de la sauvegarde dans plusieurs Comptes AWS dans le Manuel du développeur AWS Backup.

Désactivation de l'accès approuvé 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 exige un accès approuvé avec AWS Organizations pour activer la surveillance des tâches de sauvegarde, de restauration et de copie dans les comptes de votre organisation. Si vous désactivez l'accès approuvé AWS Backup, vous perdez la possibilité d'afficher les tâches en dehors du compte actuel. Le rôle AWS Backup créé par AWS Backup demeure. Si vous réactivez ensuite l'accès approuvé, AWS Backup continue de fonctionner comme avant, sans qu'il soit nécessaire de reconfigurer le service.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Backup en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

Activation d'un compte 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 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 SDK.

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 la page Services, recherchez la ligne correspondant à AWS Billing and Cost Management, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur de AWS Organizations Only, indiquez-lui AWS Billing and Cost Management 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 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 AWSServiceAccess

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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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 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 AWSServiceAccess

AWS CloudFormation StackSets et AWS Organizations

AWS CloudFormation StackSets vous permet de créer, mettre à jour ou supprimer des piles dans plusieurs Comptes AWS et Régions AWS en une seule opération. L'intégration de StackSets à AWS Organizations vous permet de créer des ensembles de piles avec des autorisations gérées par le service, à l'aide d'un rôle lié à un 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'avez donc pas à créer les rôles AWS Identity and Access Management 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 approuvé entre StackSets et Organizations est activé, le compte de gestion dispose des autorisations nécessaires pour créer et 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 délégué pour le déploiement vers des UO spécifiques ou pour l'exécution d'opérations d'ensembles de piles spécifiques.

Pour en savoir plus sur l'intégration de StackSets à Organizations, consultez Utilisation d'AWS CloudFormation Stacksets dans le Guide de l'utilisateur AWS CloudFormation.

Utilisez les informations suivantes pour vous aider à intégrer AWS CloudFormation StackSets 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 AWS CloudFormation StackSets 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 AWS 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 en savoir plus sur la création d'ensemble de piles, consultez Travailler avec AWS les StackSets CloudFormation dans le AWS CloudFormation guide de 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 mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par AWS CloudFormation StackSets autorisent l'accès aux mandataires de service suivants :

- Compte de gestion : `stacksets.cloudformation.amazonaws.com`

  Vous ne pouvez modifier ou supprimer ce rôle que si vous avez désactivé l'accès approuvé 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 approuvé entre StackSets et Organizations ou si vous supprimez d'abord le compte de l'organisation ou de l'unité organisationnelle cible.

Activation de l'accès approuvé avec AWS 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 dans le compte de gestion Organizations dispose des autorisations nécessaires pour activer l'accès approuvé avec un autre service AWS. Vous pouvez activer l'accès approuvé à l'aide de la console AWS CloudFormation ou de la console Organizations.

Vous pouvez activer l'accès approuvé en utilisant uniquement AWS CloudFormation StackSets.

Pour activer l'accès approuvé à l'aide de la console AWS CloudFormation StackSets, consultez Activer l'accès approuvé avec AWS Organizations dans le Guide de l'utilisateur AWS CloudFormation.

Désactivation de l'accès approuvé avec AWS CloudFormation StackSets

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Seul un administrateur dans un compte de gestion Organizations dispose des autorisations nécessaires pour désactiver l'accès approuvé avec un autre service AWS. Vous pouvez désactiver l'accès approuvé uniquement avec la console Organizations. Si vous désactivez l'accès approuvé avec Organizations pendant que vous utilisez StackSets, toutes les instances de piles 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 approuvé à l'aide de la console AWS CloudFormation ou de la console Organizations.

> **Important**
>
> Si vous désactivez l'accès approuvé par programme (par exemple avec AWS CLI ou avec une API), sachez que cela supprimera l'autorisation. Il est préférable de désactiver l'accès approuvé avec la console AWS CloudFormation.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS CloudFormation StackSets puis choisissez le nom du service.

3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS CloudFormation StackSets qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS CloudFormation StackSets en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

Activation d'un compte administrateur délégué pour AWS 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 AWS 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 aide à séparer la gestion de l'organisation de la gestion d'AWS CloudFormation StackSets.

Pour obtenir des instructions sur la façon de désigner un compte membre en tant qu'administrateur délégué d'AWS 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 et 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'utilisateurAWS 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`

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 CloudTrail accordent l'accès aux principaux de service suivants :

- `cloudtrail.amazonaws.com`

Activation de l'accès approuvé 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 Organizationsdans le guide deAWS 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 SDK.

AWS CLI, AWS API

Pour activer 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 activer un accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Vous pouvez exécuter 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 AWSServiceAccess

Désactivation de l'accès approuvé 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 SDK.

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 SDK.

AWS Management Console

Pour désactiver l'accès approuvé à l'aide de la console Organizations

1. Connectez-vous à la consoleAWS 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 AWS CloudTrail, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Si vous êtes l'administrateur de Only AWS Organizations, informez-le AWS CloudTrail qu'il peut désormais désactiver ce service à l'aide de sa console ou des outils qu'il n'utilise pas AWS Organizations.

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 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 AWSServiceAccess

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.

AWS Compute Optimizer et AWS Organizations

AWS Compute Optimizer est un service qui analyse les mesures de configuration et d'utilisation de vos ressources AWS. 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 AWS Compute Optimizer.

Utilisez les informations suivantes pour vous aider à intégrer AWS Compute Optimizer 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 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`

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 approuvé à l'aide de la console AWS Compute Optimizer ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Compute Optimizer pour activer l'intégration à Organizations. Cela permet à AWS Compute Optimizer 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 AWS Compute Optimizer. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Compute Optimizer, 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 AWS Compute Optimizer.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Compute Optimizer, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Compute Optimizer qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Compute Optimizer en tant que service approuvé pour Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal compute-optimizer.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

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 de gestion AWS Organizations peut désactiver l'accès approuvé avec AWS Compute Optimizer.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Compute Optimizer en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 AWS Compute Optimizer Guide de l'utilisateur.

AWS CLI, AWS API

Si vous souhaitez configurer un compte administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le principal du service de compte `account.amazonaws.com` en tant que 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 leAWS Compute OptimizerGuide de l'utilisateur.

Pour supprimer un administrateur délégué à l'aide de l'AWS AWS CLI, consultez désenregistrement de l'administrateur déléguédans le AWS AWS CLI Référence des commandes.

AWS Config et AWS Organizations

Le regroupement des données multi-comptes et multi-régions dans AWS Config vous permet de regrouper les données AWS Config de plusieurs comptes et Régions AWS dans 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 dans AWS Config qui collecte les données AWS Config de plusieurs comptes et régions source. Créez un agrégateur dans la région où vous souhaitez afficher les données AWS Config agrégées. Lors de la création d'un agrégateur, vous pouvez choisir d'ajouter des ID de compte individuels ou d'ajouter votre organisation. Pour plus d'informations sur AWS Config, consultez le Manuel du développeur AWS Config.

Vous pouvez également utiliser des API AWS Config pour gérer les règles AWS Config de tous les Comptes AWS de votre organisation. Pour plus d'informations, consultez Activation des règles AWS Config pour tous les comptes de votre organisation dans le Guide du développeur AWS Config.

Utilisez les informations suivantes pour vous aider à intégrer AWS Config 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 créé dans les comptes de votre organisation lorsque vous activez l'accès approuvé. Ce rôle permet à AWS Config d'effectuer les opérations prises en charge dans les comptes de votre organisation.

- `AWSServiceRoleForConfig`

Ce rôle est créé lorsque vous activez AWS Config dans votre organisation en créant un agrégateur multi-compte. AWS Config vous demande de sélectionner ou de créer un rôle et d'en fournir le nom. Il n'y a pas de nom généré automatiquement.

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.

Activation de l'accès approuvé 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 approuvé à l'aide de la console AWS Config ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Config pour activer l'intégration à Organizations. Cela permet à AWS Config 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 AWS Config. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Config, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console AWS Config

Pour activer l'accès approuvé à AWS Organizations à l'aide de AWS Config, créez un agrégateur multi-compte et ajoutez l'organisation. Pour obtenir des informations sur la façon de configurer un agrégateur multi-compte, consultez Configuration d'un agrégateur à l'aide de la console dans le Guide du développeur AWS Config.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Config, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Config qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Config en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

Désactivation de l'accès approuvé 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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Config en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal config.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

Hub d'optimisation des coûts et AWS Organizations

Hub d'optimisation des coûts 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 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 SDK.

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 la page Services, recherchez la ligne correspondant à Hub d'optimisation des coûts, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur de AWS Organizations Only, indiquez-lui Hub d'optimisation des coûts 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 l'activer Hub d'optimisation des coûts 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 AWSServiceAccess

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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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 Hub d'optimisation des coûts 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 AWSServiceAccess

AWS Control Tower et AWS Organizations

AWS Control Tower offre un moyen simple de configurer et de gérer un environnement AWS multi-comptes, suivant les meilleures pratiques normatives. L'orchestration AWS Control Tower étend les capacités de AWS Organizations. AWS Control Tower applique des contrôles préventifs et de détection (barrière de protection) pour empêcher vos organisations et vos comptes de s'écarter des meilleures pratiques (dérive).

L'orchestration AWS Control Tower étend les capacités de AWS Organizations.

Pour plus d'informations, consultez le Guide de l'utilisateur AWS Control Tower.

Utilisez les informations suivantes pour vous aider à intégrer AWS Control Tower à AWS Organizations.

Rôles nécessaires à l'intégration

Le rôle `AWSControlTowerExecution` doit être présent dans tous les comptes inscrits. Le rôle permet à AWS Control Tower de gérer vos comptes individuels et d'indiquer les informations les concernant à vos comptes d'audit et de journalisation.

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 Utilisation des stratégies basées sur l'identité (politique IAM) pour AWS Control Tower.

Principaux de service utilisés par AWS Control Tower

AWS Control Tower utilise le principal service `controltower.amazonaws.com`.

Activation de l'accès approuvé avec AWS Control Tower.

AWS Control Tower utilise un accès de confiance pour détecter les dérives à des fins de contrôles préventifs et pour suivre les modifications de compte et d'unité d'organisation qui provoquent des dérives.

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 en utilisant uniquement les outils d'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 approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès approuvé aux services :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Control Tower en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

Désactivation de l'accès approuvé 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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

> **Important**
>
> La désactivation de l'accès sécurisé à AWS Control Tower entraîne une dérive au niveau de votre zone de destination AWS Control Tower. 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 approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Control Tower en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

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 d'AWS Organizations permet de vous assurer que votre graphique de comportement Detective offre 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'un accès approuvé à AWS Organizations avant que vous ne puissiez désigner un compte membre comme administrateur délégué de ce service pour votre organisation.

Vous pouvez activer l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations.

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 la page Services, recherchez la ligne correspondant à Amazon Detective, choisissez le nom du service, puis choisissez Enable trusted access (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 uniquement d'AWS Organizations, indiquez à l'administrateur d'Amazon Detective d'activer maintenant ce service à l'aide de sa console afin qu'il fonctionne avec AWS Organizations.

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 gestion AWS Organizations peut désactiver l'accès approuvé avec Amazon Detective.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations.

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. Sur la page Services, recherchez la ligne correspondant à Amazon Detective, puis choisissez le nom du service.
3. Choisissez Disable trusted access (Désactiver l'accès approuvé).
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'Amazon Detective de désactiver maintenant ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

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 administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le principal du service de compte `account.amazonaws.com` en tant que 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 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 risque ou un problème opérationnel.

L'utilisation de DevOps Guru permet une prise en charge de plusieurs comptes avec AWS Organizations afin que vous puissiez 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 Contrôler les comptes 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 dans les comptes de votre organisation.

Vous pouvez supprimer ou modifier ce rôle uniquement si vous désactivez l'accès approuvé 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 à un service utilisés par DevOps Guru accordent l'accès aux principaux de service suivants :

- `devops-guru.amazonaws.com`

Pour plus d'informations, consultez Utilisation de rôles liés au service pour DevOps Guru dans le Guide de l'utilisateur Amazon DevOps Guru.

Pour activer l'accès approuvé 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, il active automatiquement l'accès approuvé pour DevOps Guru pour votre organisation. DevOps Guru a besoin d'un accès approuvé à AWS Organizations afin 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 d'Amazon DevOps Guru pour activer l'intégration à Organizations. Cela permet à Amazon DevOps Guru 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 DevOps Guru. Pour plus d'informations, consultez cette note.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations 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. Dans la page Services, recherchez la ligne correspondant à Amazon DevOps Guru, choisissez le nom du service, puis choisissez Enable trusted access (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 uniquement d'AWS Organizations, indiquez à l'administrateur d'Amazon DevOps Guru d'activer maintenant ce service à l'aide de sa console afin qu'il fonctionne avec AWS Organizations.

DevOps Guru console

Pour activer l'accès approuvé aux services à l'aide de la console DevOps Guru

1. Connectez-vous en tant qu'administrateur dans le compte de gestion et ouvrez la console DevOps Guru : Amazon DevOps Guru
2. Choisissez Enable trusted access (Activer l'accès approuvé).

Pour désactiver l'accès approuvé 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 de gestion AWS Organizations peut désactiver l'accès approuvé avec Amazon DevOps Guru.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations.

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. Sur la page Services, recherchez la ligne correspondant à Amazon DevOps Guru, puis choisissez le nom du service.
3. Choisissez Disable trusted access (Désactiver l'accès approuvé).
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Disable trusted access (Désactiver l'accès approuvé).

5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'Amazon DevOps Guru de désactiver maintenant ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

Activation d'un compte administrateur délégué pour DevOps Guru

Le compte administrateur délégué de DevOps Guru peut voir les données d'informations de tous les comptes membres intégrés à DevOps Guru à partir de l'organisation. Pour plus d'informations sur la manière dont un administrateur délégué gère les comptes d'organisation, consultez Contrôler les comptes de votre organisationdans 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 à partir de la console DevOps Guru ou à l'aide de la CLI Organizations `RegisterDelegatedAdministrator` ou de 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 DevOps Guru dans l'organisation.

DevOps Guru console

Pour configurer un administrateur délégué dans la console DevOps Guru

1. Connectez-vous en tant qu'administrateur dans le compte de gestion et ouvrez la console DevOps Guru : 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 administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le principal du service de compte `account.amazonaws.com` en tant que paramètres.

Désactivation d'un administrateur délégué pour DevOps Guru

Vous pouvez supprimer l'administrateur délégué à l'aide de la console DevOps Guru 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 la console DevOps Guru, consultez Contrôler les comptes 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) vous permet d'exécuter Microsoft Active Directory (AD) en tant que service géré. AWS Directory Service facilite la configuration et l'exécution des annuaires dans le cloud AWS ou la connexion de vos ressources AWS avec un Microsoft Active Directory local existant. AWS Managed Microsoft AD s'intègre également parfaitement à AWS Organizations pour autoriser le partage des annuaires en toute transparence entre plusieurs Comptes AWS et n'importe quel VPC dans une région. Pour plus d'informations, consultez le Guide d'administration AWS Directory Service.

Utilisez les informations suivantes pour vous aider à intégrer AWS Directory Service à AWS Organizations.

Activation de l'accès approuvé avec AWS 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 approuvé à l'aide de la console AWS Directory Service ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Directory Service pour activer l'intégration à Organizations. Cela permet à AWS Directory Service 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 AWS Directory Service. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Directory Service, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console AWS Directory Service

Pour partager un annuaire, ce qui active automatiquement l'accès approuvé, consultez Partager votre annuaire dans le Guide d'administration AWS Directory Service. Pour obtenir des instructions détaillées, consultez Didacticiel : Partage de votre annuaire Microsoft AD géré AWS.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations.

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 la page Services, recherchez la ligne correspondant à AWS Directory Service, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Directory Service qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec AWS Organizations.

Désactivation de l'accès approuvé avec AWS 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 approuvé avec AWS Organizations pendant que vous utilisez AWS Directory Service, tous les annuaires partagés précédemment continuent à 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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations.

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. Sur la page Services, recherchez la ligne correspondant à AWS Directory Service, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Directory Service qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS Firewall Manager et AWS Organizations

AWS Firewall Manager est un service managé de sécurité que vous utilisez pour configurer et gérer de façon centralisée les règles de pare-feu et autres protections dans l'ensemble des Comptes AWS et des applications de votre organisation. Avec Firewall Manager, vous pouvez déployer des règles AWS WAF, créer des protections AWS Shield Advanced, configurer et auditer des groupes de sécurité Amazon Virtual Private Cloud (Amazon VPC), et déployer des AWS Network Firewall. 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 sur AWS Firewall Manager, consultez le Guide du développeur AWS Firewall Manager.

Utilisez les informations suivantes pour vous aider à intégrer AWS Firewall 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 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 approuvé à l'aide de la console AWS Firewall Manager ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Firewall Manager pour activer l'intégration à Organizations. Cela permet à AWS Firewall Manager 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 AWS Firewall Manager. Pour plus d'informations, consultez cette note.
Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Firewall Manager, vous n'avez pas besoin de suivre ces étapes.

Vous devez vous connecter avec votre compte de gestion AWS Organizations et configurer un compte de l'organisation en tant que compte d'administrateur AWS Firewall Manager. 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 approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Firewall Manager, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Firewall Manager qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

Vous pouvez exécuter la commande suivante pour activer AWS Firewall Manager en tant que service approuvé pour Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal fms.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

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 approuvé à l'aide de AWS Firewall Manager ou d'outils AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Firewall Manager pour désactiver l'intégration à Organizations. Cela permet à AWS Firewall Manager d'effectuer le nettoyage nécessaire, par exemple en supprimant les ressources ou les rôles d'accès dont il 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 approuvé à l'aide de la console ou des outils de AWS Firewall Manager, 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 administrateur AWS Firewall Manager en suivant les instructions décrites dans Désignation d'un autre compte en tant que compte administrateur AWS Firewall Manager dans le Guide du développeur AWS Firewall Manager.

Si vous révoquez le compte administrateur, vous devez vous connecter au compte de gestion AWS Organizations et définir un nouveau compte administrateur pour AWS Firewall Manager.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS Firewall Manager, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Firewall Manager qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Firewall Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 obtenir des instructions sur la façon de désigner un compte membre en tant qu'administrateur Firewall Manager pour l'organisation, consultez Définir le compte administrateur AWS Firewall Manager dans le Guide du développeur AWS Firewall Manager.

Amazon GuardDuty et AWS Organizations

Amazon GuardDuty est un service de surveillance de sécurité continue qui analyse et traite une variété de sources de données, en utilisant des flux d'intelligence de menaces et le machine learning pour identifier les activités inattendues potentiellement non autorisées et malveillantes dans votre environnement AWS. Cela peut inclure des problèmes comme les escalades de privilèges, l'utilisation d'informations d'identification exposées, la communication avec des adresses IP, des URL ou des domaines malveillants ou la présence de logiciels malveillants sur vos instances Amazon Elastic Compute Cloud et vos charges de travail de conteneurs.

Vous pouvez aider à simplifier la gestion de GuardDuty en utilisant les Organizations pour gérer GuardDuty sur tous les comptes de votre organisation.

Pour de plus amples informations, consultez Gestion des comptes GuardDuty avec AWS Organizationsdans le Guide de l'utilisateur Amazon GuardDuty

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

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 GuardDuty d'effectuer dans votre organisation les opérations prises en charge dans les comptes de celle-ci. Vous pouvez supprimer ou modifier un rôle uniquement si vous désactivez l'accès approuvé entre GuardDuty et Organizations, ou si vous supprimez le compte membre de l'organisation.

- Le rôle lié à un service `AWSServiceRoleForAmazonGuardDuty` est automatiquement créé dans les comptes qui ont intégré GuardDuty aux Organizations. Pour de plus amples informations, consultez Gestion des comptes GuardDuty dans les organisations dans le Guide de l'utilisateur Amazon GuardDuty
- Le rôle lié à un service `AmazonGuardDutyMalwareProtectionServiceRolePolicy` est automatiquement créé dans les comptes qui ont activé la protection contre les logiciels malveillants GuardDuty. Pour de plus amples informations, consultez Autorisations des rôles liés à des services pour GuardDuty Malware Protection dans le Guide de l'utilisateur d'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`.

Activation de l'accès approuvé avec GuardDuty

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 uniquement en utilisant Amazon GuardDuty.

Amazon GuardDuty exige un accès approuvé à AWS Organizations avant que vous puissiez désigner un compte membre comme administrateur GuardDuty pour votre organisation. Si vous configurez un administrateur délégué à l'aide de sa console, GuardDuty active automatiquement l'accès approuvé pour vous.

Toutefois, si vous souhaitez configurer un compte administrateur délégué à l'aide de la AWS CLI ou de l'un des SDK AWS, vous devez appeler explicitement l'opération

EnableAWSServiceAccess et fournir en paramètre le mandataire du service. Ensuite, vous pouvez appeler EnableOrganizationAdminAccount pour déléguer le compte administrateur GuardDuty.

Désactivation de l'accès approuvé avec GuardDuty

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 en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver Amazon GuardDuty en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

Activation d'un compte 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 Autorisations requises pour désigner un administrateur délégué dans le Guide de l'utilisateur Amazon GuardDuty

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 AWS services et 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`

Activation de l'accès approuvé 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 SDK.

AWS CLI, AWS API

Pour activer 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 activer un accès sécurisé aux services :

- AWS CLI: enable-aws-service-access

  Vous pouvez exécuter 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 AWSServiceAccess

Désactivation de l'accès approuvé 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 AWS Organizations outils AWS Health ou.

> **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 SDK.

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 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 AWSServiceAccess

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 comme 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

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 via AWS Organizations en déléguant simplement un compte administrateur 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 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 accès approuvé à AWS Organizations avant que vous puissiez désigner un compte membre comme 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 administrateur délégué à l'aide de la CLI AWS ou de l'un des SDK AWS, vous devez appeler explicitement l'opération `EnableAWSServiceAccess` et fournir en paramètre le principal de service. Vous pouvez ensuite appeler `EnableDelegatedAdminAccount` pour déléguer le compte administrateur Inspector.

Vous pouvez activer l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès approuvé aux services :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer Amazon Inspector en tant que service approuvé avec Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

> **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 de gestion AWS Organizations peut désactiver l'accès approuvé avec Amazon Inspector.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver Amazon Inspector en tant que service approuvé avec Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

Activation d'un compte administrateur délégué pour Amazon Inspector

Grâce à Amazon Inspector, vous pouvez gérer plusieurs comptes dans une organisation à l'aide d'un administrateur délégué avec le service AWS Organizations.

Le compte de gestion AWS Organizations désigne un compte de l'organisation comme compte administrateur délégué d'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 administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le principal du service de compte `account.amazonaws.com` en tant que paramètres.

Désactivation d'un administrateur délégué pour Amazon Inspector

Seul un administrateur du compte de gestion AWS Organizations peut supprimer un compte 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 simplifie le processus d'apport de licences de fournisseurs de logiciels dans le cloud. Lorsque vous construisez une infrastructure cloud sur AWS, vous pouvez économiser en profitant d'opportunités BYOL (Réutilisez vos licences), c'est-à-dire en modifiant le rôle de votre inventaire de licence pour une utilisation avec des ressources 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 liant 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 à intégrer AWS License 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 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 pouvez activer l'accès approuvé uniquement avec 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 gestion AWS Organizations et l'associer à votre compte License Manager. Pour plus d'informations, consultez 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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande AWS CLI d'Organizations ou en appelant une opération d'API d'Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS License Manager en tant que service approuvé pour 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
  ```

- API AWS : DisableAWSServiceAccess

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.

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 exige un accès approuvé à AWS Organizations avant que vous puissiez désigner un compte membre comme administrateur Macie pour 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 approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès approuvé aux services :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer Amazon Macie en tant que service approuvé auprès d'Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

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 exige un accès approuvé à AWS Organizations avant que vous puissiez désigner un compte membre comme administrateur Macie pour 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 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.

AWS Marketplace crée et gère les licences à l'aide de 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 à intégrer AWS Marketplace 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 AWS Marketplace 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 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 mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par AWS Marketplace accordent l'accès aux mandataires de service suivants :

- `license-management.marketplace.amazonaws.com`

Activation de l'accès approuvé 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 approuvé à l'aide de la console AWS Marketplace ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Marketplace pour activer l'intégration à Organizations. Cela permet à AWS Marketplace 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 AWS Marketplace. Pour plus d'informations, consultez cette note.

Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Marketplace, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console AWS Marketplace

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 approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Marketplace, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Marketplace qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Marketplace en tant que service approuvé pour Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

Désactivation de l'accès approuvé 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 approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Marketplace en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

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, à une ou plusieurs unités d'organisation ou à un ou plusieurs comptes de votre organisation, chacun disposant de 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 Marketplacedans le Guide deAWS 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 deAWS Marketplace l'acheteur.

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 SDK.

AWS Management Console

Pour activer l'accès approuvé aux services à l'aide de la console Organizations

1. Connectez-vous à la consoleAWS 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 AWS Marketplace Private Marketplace, 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 de AWS Marketplace Private Marketplace 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 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 AWSServiceAccess

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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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 désactiver AWS Marketplace Private Marketplace en tant que service de confiance auprès des 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 AWSServiceAccess

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 deAWS 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 deAWS Marketplace l'acheteur

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 recommandons fortement d'utiliser la console Network Manager pour gérer les paramètres multi-comptes (activer/désactiver l'accès sécurisé et enregistrer/annuler l'enregistrement des administrateurs 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 AWS 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 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 AWS CloudFormation console, les rôles IAM déployés AWS 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 (Amazon Q) et AWS Organizations

Amazon Q Developer est un assistant conversationnel basé sur l'intelligence artificielle générative (IA) qui peut vous aider à comprendre, créer, étendre et exploiter AWS des applications. La version d'abonnement payant d'Amazon Q nécessite l'intégration des 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 d'effectuer des opérations prises en charge dans les comptes de votre organisation au sein de votre organisation. Créez le rôle à l'aide de la console, de l'API ou de la CLI Amazon Q, 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 Amazon Q et Organizations, ou si vous supprimez le compte membre de l'organisation.

Principaux de service utilisés par Amazon Q

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 accordent l'accès aux principaux de service suivants :

- `q.amazonaws.com`

Permettre un accès fiable avec Amazon Q

Amazon Q utilise un accès sécurisé pour partager les paramètres définis au niveau de l'organisation avec les comptes des membres. Par exemple, l'administrateur au niveau des Organisations peut activer la fonctionnalité X, et la fonctionnalité X est alors disponible pour tous les comptes membres de la même organisation. Pour plus d'informations, consultez la section Configuration des organisations dans le guide de l'utilisateur Amazon Q Developer.

Vous pouvez activer l'accès sécurisé en utilisant uniquement Amazon Q Developer.

Pour activer l'accès sécurisé pour Amazon Q, dans la console Amazon Q, suivez les instructions de la section Abonnements du guide de l'utilisateur Amazon Q pour les développeurs. À l'étape 6, sélectionnez Partager le profil des paramètres avec les comptes des membres.

Désactiver l'accès sécurisé avec Amazon Q

Vous pouvez désactiver l'accès sécurisé en utilisant uniquement les outils Amazon Q Developer.

Pour désactiver l'accès sécurisé pour Amazon Q, dans la console Amazon Q, suivez les instructions de la section Abonnements du guide de l'utilisateur Amazon Q pour les développeurs. À l'étape 6, désélectionnez Partager le profil des paramètres avec les comptes des membres.

AWS Resource Access Manager et AWS Organizations

AWS Resource Access Manager (AWS RAM) vous permet de partager des ressources AWS spécifiées que vous possédez avec d'autres Comptes AWS. Il s'agit d'un service centralisé qui fournit une expérience cohérente pour partager différents types de ressources AWS entre plusieurs comptes.

Pour plus d'informations sur AWS RAM, consultez le Guide de l'utilisateur AWS RAM.

Utilisez les informations suivantes pour vous aider à intégrer AWS Resource Access 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 AWS RAM 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 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 mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par AWS RAM accordent l'accès aux mandataires de service suivants :

- `ram.amazonaws.com`

Activation de l'accès approuvé 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 approuvé à l'aide de la console AWS Resource Access Manager ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Resource Access Manager pour activer l'intégration à Organizations. Cela permet à AWS Resource Access Manager 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 AWS Resource Access Manager. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Resource Access Manager, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console AWS RAM ou de la CLI

Consultez Activer le partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Resource Access Manager, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Resource Access Manager qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Resource Access Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

Désactivation de l'accès approuvé 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 approuvé à l'aide d'AWS Resource Access Manager ou d'outils AWS Organizations.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Resource Access Manager pour désactiver l'intégration à Organizations. Cela permet à AWS Resource Access Manager d'effectuer le nettoyage nécessaire, par exemple en supprimant les ressources ou les rôles d'accès dont il 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 approuvé à l'aide de la console ou des outils de AWS Resource Access Manager, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès approuvé à l'aide de la console AWS Resource Access Manager ou la CLI

Consultez Activer le partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS Resource Access Manager, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Resource Access Manager qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Resource Access Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 les identifiants. Resource Explorer fonctionne dans toutes les régions AWS 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 Comptes AWS de votre organisation dans le cadre de vos évaluations.

Utilisez les informations suivantes pour vous aider à intégrer Explorateur de ressources AWS 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 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 activer l'accès approuvé auprès 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 exige un accès approuvé à AWS Organizations avant que vous puissiez désigner un compte membre comme administrateur délégué pour 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 à Explorateur de ressources AWS d'effectuer toute configuration nécessaire, par exemple 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 console Explorateur de ressources AWS, Explorateur de ressources AWS active automatiquement l'accès approuvé pour vous.

Vous pouvez activer l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

AWS CLI, AWS API

Pour activer l'accès approuvé aux services à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès approuvé aux services :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer Explorateur de ressources AWS en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

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 de gestion AWS Organizations peut désactiver l'accès approuvé avec Explorateur de ressources AWS.

Vous pouvez désactiver l'accès approuvé à l'aide de Explorateur de ressources AWS ou d'outils AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'Explorateur de ressources AWS pour désactiver l'intégration à Organizations. Cela permet à Explorateur de ressources AWS d'effectuer le nettoyage nécessaire, par exemple en supprimant les ressources ou les rôles d'accès dont il 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 approuvé à l'aide de la console ou des outils de Explorateur de ressources AWS, vous n'avez pas besoin de suivre ces étapes.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver Explorateur de ressources AWS en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 via AWS Resource Access Manager en 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 console Explorateur de ressources AWS, Resource Explorer active automatiquement l'accès approuvé pour vous.

AWS CLI, AWS API

Si vous souhaitez configurer un compte administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le service de compte `resource-explorer-2.amazonaws.com` en tant que 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 et AWS Organizations

AWS Security Hub 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 collecte des données de sécurité provenant de l'ensemble de vos produits Comptes AWS, des AWS services que vous utilisez et des produits partenaires tiers pris en charge. Il vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité prioritaires.

Lorsque vous utilisez Security Hub et AWS Organizations conjointement, vous pouvez activer automatiquement Security Hub pour tous vos comptes, y compris les nouveaux comptes au fur et à mesure de leur ajout. Cela augmente la couverture des vérifications et conclusions de Security Hub, ce qui fournit une image plus complète et plus précise de votre posture de sécurité globale.

Pour plus d'informations sur Security Hub, consultez le Guide de l'utilisateurAWS Security Hub.

Utilisez les informations suivantes pour vous aider AWS Security Hub 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 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 Security Hub et Organizations, ou si vous supprimez le compte membre de l'organisation.

- `AWSServiceRoleForSecurityHub`

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 Security Hub autorisent l'accès aux mandataires de service suivants :

- `securityhub.amazonaws.com`

Activation de l'accès approuvé avec Security Hub

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, ce service active automatiquement l'accès approuvé pour Security Hub dans votre organisation.

Activation d'un compte administrateur délégué pour Security Hub

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 Security Hub 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 Security Hub.

Pour plus d'informations, consultez Désignation d'un compte administrateur Security Hub dans le Guide de l'utilisateurAWS Security Hub .

Pour désigner un compte membre comme administrateur délégué pour Security Hub

1. Connectez-vous au compte de gestion Organizations.
2. Effectuez l'une des actions suivantes :
   - Si Security Hub n'est pas activé sur votre compte de gestion, choisissez Accédez à Security Hub dans la console Security Hub.
   - Si Security Hub est activé sur votre compte de gestion, sur la console Security Hub, sous Général, choisissez Paramètres.
3. Sous Administrateur délégué, saisissez l'ID du compte.

Amazon S3 Storage Lens 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 SDK.

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 la page Services, recherchez la ligne correspondant à Amazon S3 Storage Lens, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. 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 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 Amazon S3 Storage Lens en tant que service approuvé auprès d'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 AWSServiceAccess

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 pouvez désactiver l'accès approuvé à l'aide uniquement 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 SDK.

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 SDK. 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 annuler l'enregistrement d'un administrateur délégué à l'aide de la console Amazon S3, du AWS CLI ou de l'un des SDK. AWS 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.

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 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 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`

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 pouvez activer l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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 la page Services, recherchez la ligne correspondant à Amazon Security Lake, 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 d'Amazon Security Lake 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 Amazon Security Lake en tant que service approuvé avec Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Activer AWSServiceAccess

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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'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 SDK.

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. Sur la page Services, recherchez la ligne correspondant à Amazon Security Lake, puis choisissez le nom du service.
3. Choisissez Disable trusted access (Désactiver l'accès approuvé).
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Disable trusted access (Désactiver l'accès approuvé).
5. 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 l'aide de sa console ou des outils qu'il n'utilise pas AWS Organizations.

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 désactiver Amazon Security Lake en tant que service approuvé avec Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- AWS API : Désactiver AWSServiceAccess

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'action `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'un AWS des SDK, 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 en utilisant l'action d'`DeleteDatalakeDelegatedAdmin`API Amazon Security Lake, la commande `delete-datalake-delegated-admin` 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 du Service Catalog à AWS Organizations simplifie le partage de portefeuilles et la copie de produits dans une organisation. Les administrateurs du Service Catalog peuvent faire référence à une organisation existante dans AWS Organizations lors du partage d'un portefeuille et ils peuvent partager le portefeuille avec n'importe quelle unité organisationnelle (UO) approuvée dans la structure d'arborescence de l'organisation. Cela élimine le besoin de partager les ID des portefeuilles et cela permet au compte de réception de référencer manuellement l'ID d'un portefeuille lors de son importation. 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 à intégrer AWS Service Catalog à 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 de l'accès approuvé.

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 approuvé à l'aide de la console AWS Service Catalog ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Service Catalog pour activer l'intégration à Organizations. Cela permet à AWS Service Catalog 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 AWS Service Catalog. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Service Catalog, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de l'interface de ligne de commande Service Catalog ou AWS SDK

Appelez l'une des commandes ou opérations suivantes :

- AWS CLI : aws servicecatalog enable-aws-organizations-access
- SDK AWS : AWSServiceCatalog::EnableAWSOrganizationsAccess

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Service Catalog, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Service Catalog qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Service Catalog en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

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 approuvé avec AWS Organizations tout en utilisant Service Catalog, cela ne supprime pas vos partages actuels, mais vous empêche de créer d'autres partages dans votre organisation. Les partages actuels ne seront pas synchronisés avec la structure de votre organisation si elle change après l'appel de cette action.

Vous pouvez désactiver l'accès approuvé à l'aide d'AWS Service Catalog ou d'outils AWS Organizations.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Service Catalog pour désactiver l'intégration à Organizations. Cela permet à AWS Service Catalog d'effectuer le nettoyage nécessaire, par exemple en supprimant les ressources ou les rôles d'accès dont il n'a plus besoin. Procédez comme suit uniquement si vous ne pouvez pas désactiver l'intégration à l'aide des outils fournis par AWS Service Catalog.
> Si vous désactivez l'accès approuvé à l'aide de la console ou des outils de AWS Service Catalog, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès approuvé à l'aide de l'interface de ligne de commande Service Catalog ou d'AWS SDK

Appelez l'une des commandes ou opérations suivantes :

- AWS CLI : aws servicecatalog disable-aws-organizations-access
- SDK AWS : DisableAWSOrganizationsAccess

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS Service Catalog, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Service Catalog qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Service Catalog en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

Service Quotas et AWS Organizations

Service Quotas est un service AWS qui vous permet d'afficher 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 lorsque les comptes sont créés.

Pour plus d'informations sur Service Quotas, consultez le Guide de l'utilisateur Service Quotas.

Utilisez les informations suivantes pour vous aider à intégrer Service Quotas 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 pouvez activer l'accès approuvé uniquement avec Service Quotas.

Vous pouvez activer l'accès approuvé à l'aide de la console Service Quotas, de la AWS CLI ou du kit SDK :

- Pour activer l'accès approuvé à l'aide de la console Service Quotas

  Connectez-vous à votre compte de gestion AWS Organizations, 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 l'accès approuvé à l'aide de la AWS CLI Service Quotas ou de SDK

  Appelez la commande ou l'opération suivante :
  - AWS CLI : aws service-quotas associate-service-quota-template
  - SDK AWS : AssociateServiceQuotaTemplate

AWS IAM Identity Center et AWS Organizations

AWS IAM Identity Center fournit des services d'authentification unique pour l'ensemble de vos Comptes AWS et de vos applications cloud. Il se connecte à Microsoft Active Directory via AWS Directory Service pour permettre aux utilisateurs de cet annuaire de se connecter à un portail d'accès AWS personnalisé à l'aide de leur noms d'utilisateur et mots de passe Active Directory existants. À partir du portail d'accès AWS, les utilisateurs ont accès à toutes les Comptes AWS et les applications cloud pour lesquelles ils disposent d'autorisations.

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 à intégrer AWS IAM Identity Center 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 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 approuvé à l'aide de la console AWS IAM Identity Center ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS IAM Identity Center pour activer l'intégration à Organizations. Cela permet à AWS IAM Identity Center 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 AWS IAM Identity Center. Pour plus d'informations, consultez cette note.
>
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS IAM Identity Center, vous n'avez pas besoin de suivre ces étapes.

IAM Identity Center exige un accès de confiance avec AWS Organizations pour fonctionner. 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 approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS IAM Identity Center, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS IAM Identity Center qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS IAM Identity Center en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

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.

IAM Identity Center exige un accès de confiance avec AWS Organizations pour fonctionner. Si vous désactivez l'accès de confiance en utilisant AWS Organizations pendant que vous utilisez IAM Identity Center, il 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 pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS IAM Identity Center, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS IAM Identity Center qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS IAM Identity Center en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 de visualiser et de contrôler vos ressources AWS. 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 opérationnel personnalisable qui fournit des informations sur vos ressources AWS. Vous pouvez synchroniser les données opérationnelles entre tous les Comptes AWS de votre organisation en utilisant Organizations et 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 centralisé où les ingénieurs d'exploitation et les professionnels de la TI peuvent consulter, étudier et résoudre des éléments de travail opérationnels (OpsItems) liés aux ressources AWS. Lorsque vous utilisez OpsCenter avec Organizations, cela permet de travailler avec des OpsItems à partir d'un compte de gestion (compte de gestion Organizations ou compte administrateur délégué Systems Manager) et d'un autre compte au cours d'une seule session. Une fois la configuration terminée, les utilisateurs peuvent effectuer les types d'actions suivants :
  - Créer, visualiser et mettre à jour des OpsItems sur un autre compte.
  - Afficher des informations détaillées sur les ressources AWS spécifiées dans les OpsItems sur un autre compte.
  - Démarrer les runbooks Systems Manager Automation pour résoudre les problèmes liés aux ressources AWS d'un autre compte.

  Pour plus d'informations, consultez AWS Systems ManagerOpsCenter dans le Guide de l'utilisateur AWS Systems Manager.

Utilisez les informations suivantes pour vous aider à intégrer AWS Systems 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 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 pouvez activer l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Systems Manager, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Systems Manager qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Systems Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : EnableAWSServiceAccess

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 exige un accès approuvé avec AWS Organizations pour synchroniser les données opérationnelles entre les Comptes AWS de votre organisation. Si vous désactivez l'accès approuvé, Systems Manager ne parvient pas à synchroniser les données opérationnelles et signale une erreur.

Vous pouvez désactiver l'accès approuvé en utilisant uniquement les outils d'Organizations.

Vous pouvez désactiver l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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. Sur la page Services, recherchez la ligne correspondant à AWS Systems Manager, puis choisissez le nom du service.
3. Choisissez Désactiver l'accès approuvé.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`** dans la zone, puis choisissez Désactiver l'accès approuvé.
5. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Systems Manager qu'il peut maintenant désactiver ce service à l'aide de sa console ou d'outils pour qu'il ne fonctionne plus avec AWS Organizations.

AWS CLI, AWS API

Pour désactiver l'accès approuvé à l'aide de la CLI ou du SDK Organizations

Vous pouvez utiliser les commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Systems Manager en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

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 AWS qui a été désigné comme compte pour la gestion des modèles

de modification, des demandes de modification, des runbooks de modification et des workflows 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'utilisateurAWS Systems Manager :

- Pour Explorer et OpsCenter, consultez Configuration d'un administrateur délégué.
- Pour Change Manager, consultez Configuration d'une organisation et d'un compte délégué pour Change Manager.

Politiques de balises et AWS Organizations

Les politiques de balises sont un type de politique dans 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.

Mandataires 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 approuvé soit en activant les politiques de balises dans l'organisation, soit en utilisant la console AWS Organizations.

> **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 plus d'informations, consultez Désactivation d'un type de politique.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant aux politiques de balises, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur des politiques de balises qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer les politiques de balises en tant que service approuvé avec Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal tagpolicies.tag.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

Désactivation de l'accès approuvé avec les politiques de balises

Vous pouvez désactiver l'accès approuvé pour les politiques de balises en désactivant le type de politique de balises dans la console AWS Organizations. Pour plus d'informations, consultez Désactivation d'un type de politique.

AWS Trusted Advisor et AWS Organizations

AWS Trusted Advisor examine votre environnement AWS et effectue des recommandations lorsqu'il est possible de faire des économies, d'améliorer la disponibilité et les performances du système, ou de remédier à des failles de sécurité. Lorsqu'il est intégré à Organizations, vous pouvez recevoir les résultats de vérification Trusted Advisor pour tous les comptes de votre organisation et télécharger des rapports pour afficher les résumés de vos vérifications et les ressources éventuelles affectées.

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 à intégrer AWS Trusted Advisor 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 Trusted Advisor 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 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 mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par Trusted Advisor accordent l'accès aux mandataires de service suivants :

- `reporting.trustedadvisor.amazonaws.com`

Activation de l'accès approuvé 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 pouvez activer l'accès approuvé uniquement avec AWS Trusted Advisor.

Pour activer l'accès approuvé à l'aide de la console Trusted Advisor

Consultez Activer la vue organisationnelle dans le Guide de l'utilisateur AWS Support.

Désactivation de l'accès approuvé avec Trusted Advisor

Pour en savoir plus sur les autorisations requises pour désactiver l'accès approuvé, consultez Autorisations requises pour désactiver l'accès approuvé.

Lorsque vous désactivez cette fonction, Trusted Advisor cesse d'enregistrer les informations de vérification pour tous les autres comptes de votre organisation. Vous ne pouvez pas afficher ou télécharger des rapports existants ou créer de nouveaux rapports.

Vous pouvez désactiver l'accès approuvé à l'aide d'AWS Trusted Advisor ou d'outils AWS Organizations.

> **Important**
>
> Dans la mesure du possible, nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Trusted Advisor pour désactiver l'intégration à Organizations. Cela permet à AWS Trusted Advisor d'effectuer le nettoyage nécessaire, par exemple en supprimant les ressources ou les rôles d'accès dont il 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 approuvé à l'aide de la console ou des outils de AWS Trusted Advisor, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès approuvé à l'aide de la console Trusted Advisor

Consultez Désactiver la vue organisationnelle dans le Guide de l'utilisateur AWS Support.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Trusted Advisor en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

Activation d'un compte 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**
>
> Seuls un utilisateur ou un rôle du compte de gestion d'Organizations peuvent configurer un compte membre en tant qu'administrateur délégué de Trusted Advisor dans l'organisation.

Pour obtenir des instructions sur l'activation d'un compte d'administrateur délégué pour Trusted Advisor, consultez Enregistrer les administrateurs délégués dans le AWS Support Guide de l'utilisateur.

AWS CLI, AWS API

Si vous souhaitez configurer un compte administrateur délégué à l'aide de la CLI d'AWS ou de l'un des SDK AWS, vous pouvez utiliser les commandes suivantes :

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- SDK AWS : appelez l'opération Organizations `RegisterDelegatedAdministrator` et le numéro d'identification du compte membre et identifiez le principal du service de compte `account.amazonaws.com` en tant que paramètres.

Désactiver un administrateur délégué pour Trusted Advisor

Vous pouvez supprimer l'administrateur délégué en utilisant soit la Trusted Advisor console, soit l'opération `DeregisterDelegatedAdministrator` CLI ou SDK des organisations. Pour plus d'informations sur le processus de désactivation du compte d'administrateur Trusted Advisor délégué à l'aide de la Trusted Advisor console, consultez Désenregistrer les administrateurs délégués dans le AWS SupportGuide de l'utilisateur.

AWS Well-Architected Tool et AWS Organizations

L'AWS Well-Architected Tool vous aide à documenter l'état de vos charges de travail et à les comparer aux dernières bonnes pratiques architecturales d'AWS.

L'utilisation de AWS Well-Architected Tool avec Organizations permet à la fois aux clients de AWS Well-Architected Tool et d'Organizations de simplifier le processus de partage des ressources AWS Well-Architected Tool avec les autres membres de leur organisation.

Pour plus d'informations, veuillez consulter la section Sharing your AWS Well-Architected Tool resources du Guide de l'utilisateur AWS Well-Architected Tool.

Utilisez les informations suivantes pour vous aider à intégrer AWS Well-Architected Tool 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 AWS WA Tool 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 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 mandataires de service autorisés par les relations d'approbation définies pour le rôle. Les rôles liés à un service utilisés par AWS WA Tool accordent l'accès aux mandataires de service suivants :

- `wellarchitected.amazonaws.com`

Activation de l'accès approuvé avec AWS WA Tool.

Permet la mise à jour d'AWS WA Tool pour refléter les changements hiérarchiques dans 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 approuvé à l'aide de la console AWS Well-Architected Tool ou de la console AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Well-Architected Tool pour activer l'intégration à Organizations. Cela permet à AWS Well-Architected Tool 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 AWS Well-Architected Tool. Pour plus d'informations, consultez cette note.
> Si vous activez l'accès approuvé à l'aide de la console ou des outils d'AWS Well-Architected Tool, vous n'avez pas besoin de suivre ces étapes.

Pour activer l'accès approuvé à l'aide de la console AWS WA Tool

Consultez la section Partage de vos ressources AWS Well-Architected Tool dans le AWS Well-Architected Tool Guide de l'utilisateur.

Vous pouvez activer l'accès approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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 la page Services, recherchez la ligne correspondant à AWS Well-Architected Tool, choisissez le nom du service, puis choisissez Activer l'accès approuvé.
3. Dans la boîte de dialogue de confirmation, activez Afficher l'option pour activer l'accès approuvé, saisissez **`enable`** dans la zone, puis choisissez Activer l'accès approuvé.
4. Si vous êtes l'administrateur uniquement d'AWS Organizations, indiquez à l'administrateur d'AWS Well-Architected Tool qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- AWS CLI : enable-aws-service-access

  Vous pouvez exécuter la commande suivante pour activer AWS Well-Architected Tool en tant que service approuvé pour Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : EnableAWSServiceAccess

Désactivation de l'accès approuvé 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 approuvé à l'aide de AWS Well-Architected Tool ou d'outils AWS Organizations.

> **Important**
>
> Nous vous recommandons vivement d'utiliser la console ou les outils d'AWS Well-Architected Tool pour désactiver l'intégration à Organizations. Cela permet à AWS Well-Architected Tool d'effectuer le nettoyage nécessaire, par exemple en supprimant les ressources ou les rôles d'accès dont il 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 approuvé à l'aide de la console ou des outils de AWS Well-Architected Tool, vous n'avez pas besoin de suivre ces étapes.

Pour désactiver l'accès approuvé à l'aide de la console AWS WA Tool

Consultez la section Partage de vos ressources AWS Well-Architected Tool dans le AWS Well-Architected Tool Guide de l'utilisateur.

Vous pouvez désactiver l'accès approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

  Vous pouvez exécuter la commande suivante pour désactiver AWS Well-Architected Tool en tant que service approuvé pour Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Cette commande ne produit aucune sortie lorsqu'elle réussit.
- API AWS : DisableAWSServiceAccess

Amazon VPC IP Address Manager (IPAM) et AWS Organizations

Amazon VPC IP Address Manager (IPAM) est une fonction VPC qui facilite la planification, le suivi et le contrôle des adresses IP pour vos charges de travail AWS.

AWS Organizations vous permet de contrôler l'utilisation des adresses IP à l'échelle de votre organisation et de partager 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.

Utilisez les informations suivantes pour vous aider à intégrer Amazon VPC IP Address Manager (IPAM) 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.
> IPAM a besoin d'un accès approuvé à AWS Organizations pour vous autoriser à désigner un compte membre comme 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 à partir de la console IPAM ou de l'API `EnableIpamOrganizationAdminAccount` d'IPAM, vous accordez automatiquement un accès

approuvé à IPAM. L'octroi d'un accès approuvé a pour effet de créer le rôle lié à un service `AWSServiceRoleForIPAM`dans le compte de gestion et dans tous les comptes membres de l'organisation. IPAM utilise le rôle lié à un service pour contrôler les CIDR associés aux ressources réseau EC2 de votre organisation et pour stocker les métriques liées à l'IPAM dans 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 approuvé avec IPAM à l'aide de la console AWS Organizations ou de l'API `EnableAWSServiceAccess`.

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 gestion AWS Organizations peut désactiver l'accès approuvé auprès d'IPAM à l'aide de l'API AWS Organizations d'`disable-aws-service-access`.

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 approuvé en exécutant une commande de AWS CLI Organizations ou en appelant une opération d'API Organizations dans l'un des SDK AWS.

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 commandes de AWS CLI ou les opérations d'API suivantes pour désactiver l'accès aux services approuvés :

- AWS CLI : disable-aws-service-access

Vous pouvez exécuter la commande suivante pour désactiver Amazon VPC IP Address Manager (IPAM) en tant que service approuvé auprès d'Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ipam.amazonaws.com
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- API AWS : DisableAWSServiceAccess

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 la Référence des commandes AWS AWS CLI.

> **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 d'AWS AWS CLI, consultez disable-ipam-organization-admin-account dans la Référence des commandes AWS AWS CLI.

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 d'accessibilité 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 (VPC).

L'utilisation de AWS Organizations avec Reachability Analyzer vous permet de suivre les chemins entre les comptes de vos organisations.

Pour plus d'informations, voir Analyses entre comptes pour 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 a besoin d'un accès approuvé à AWS Organizations pour vous autoriser à désigner un compte membre comme 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 approuvé à l'aide de la console AWS Organizations, en exécutant une commande AWS CLI ou en appelant une opération d'API dans l'un des SDK AWS.

AWS Management Console

Pour activer 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. 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 AWS Organizations uniquement, indiquez à l'administrateur de Reachability Analyzer qu'il peut maintenant activer ce service à l'aide de sa console pour le faire fonctionner avec 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 commandes de AWS CLI ou les opérations d'API suivantes pour activer l'accès aux services approuvés :

- 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.
- API AWS : EnableAWSServiceAccess

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, consultez RegisterDelegatedAdministrator dans la Référence des commandes Organizations.

> **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 les services AWS intégrés à Organizations

Nous vous recommandons de n'utiliser le compte de gestion AWS Organizations et ses utilisateurs et rôles que 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. En effet, les fonctionnalités de sécurité telles que les politiques de contrôle des services (SCP) de l'organisation ne restreignent 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.

De nombreux services AWS 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 AWS services 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 AWS services 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 AWS services 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 unités d'organisation, et les politiques organisationnelles
- Membres
- Tous les comptes et unités d'organisation.
- 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 chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Organizations, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris 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 AWS services 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 sur les VPC, 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 Elastic (ENI) auxquelles des adresses IP privées sont attribuées à partir de sous-réseaux VPC. Les demandes de votre VPC destinées à des points de terminaison AWS Organizations via une interface restent sur le réseau Amazon.

Pour 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 de AWS PrivateLink for AWS Organizations
- Création d'un point de terminaison d'un VPC
- Création d'une stratégie de point de terminaison d'un VPC pour AWS Organizations

Limites et restrictions de AWS PrivateLink for 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 d'un VPC

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 AWS 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 AWS CloudFormation, consultez la ressource AWS : :EC2 : :VPCEndpoint dans le guide de l'utilisateur.AWS CloudFormation

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 stratégie de point de terminaison d'un 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 la section Contrôler l'accès aux points de terminaison VPC à l'aide des politiques relatives aux points de terminaison dans le guide de l'utilisateur Amazon VPC.

Exemple : stratégie de point de terminaison d'un VPC pour les actions AWS Organizations

```
{
```

```
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management et AWS Organizations

L'accès à AWS Organizations requiert des informations d'identifications. Ces informations d'identification doivent être autorisées à accéder à des ressources AWS, comme un compartiment Amazon Simple Storage Service (Amazon S3), une instance Amazon Elastic Compute Cloud (Amazon EC2), ou une unité d'organisation (UO) AWS Organizations. Les sections suivantes fournissent des détails sur la façon dont vous pouvez utiliser AWS Identity and Access Management (IAM) pour sécuriser l'accès à votre organisation et contrôler qui peut administrer celle-ci.

Pour déterminer qui peut gérer quels éléments de votre organisation, AWS Organizations utilise le même modèle d'autorisations basées sur IAM que les autres services AWS. En tant qu'administrateur du compte de gestion d'une organisation, vous pouvez accorder des autorisations basées sur IAM permettant d'effectuer des tâches AWS Organizations en attachant des politiques à des utilisateurs, des groupes et des rôles dans le compte de gestion. Ces politiques spécifient les actions que ces mandataires peuvent exécuter. Vous pouvez attacher une politique d'autorisations IAM à un groupe dont l'utilisateur est membre ou directement à un utilisateur ou à un rôle. Comme bonne pratique, nous vous recommandons d'attacher des politiques à des groupes plutôt qu'à des utilisateurs. Vous avez également la possibilité d'accorder des autorisations d'administrateur complètes à d'autres personnes.

Pour la plupart des opérations d'administrateur pour AWS Organizations, vous devez attacher des autorisations à des utilisateurs ou à des groupes dans le compte de gestion. Si un utilisateur d'un compte membre a besoin d'effectuer des opérations d'administrateur pour votre organisation, vous devez accorder les autorisations AWS Organizations à un rôle IAM dans le compte de gestion et permettre à l'utilisateur du compte membre d'assumer ce rôle. Pour plus d'informations générales sur les politiques d'autorisations IAM, consultez Présentation des politiques IAM dans le Guide de l'utilisateur IAM.

Rubriques

Authentification

Vous pouvez utiliser les types d'identités suivants pour accéder à AWS :

- Utilisateur racine du Compte AWS – Lorsque vous vous inscrivez à AWS, vous fournissez une adresse de messagerie et un mot de passe qui sont associés à votre Compte AWS. Il s'agit de vos informations d'identification racine et elles fournissent un accès complet à l'ensemble de vos ressources AWS.

  > **Important**
  >
  > Lorsque vous souscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l'utilisateur root 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 administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

- Utilisateur IAM : un utilisateur IAM est simplement une identité au sein de votre Compte AWS qui dispose d'autorisations personnalisées spécifiques (par exemple, des autorisations pour créer un système de fichiers dans Amazon Elastic File System). Vous pouvez utiliser un nom d'utilisateur et un mot de passe IAM pour vous connecter aux pages web AWS sécurisées telles que la AWS Management Console, les forums de discussion AWS ou le Centre de support AWS.

  Outre un nom d'utilisateur et un mot de passe, vous pouvez générer des clés d'accès pour chaque utilisateur. Vous pouvez utiliser ces clés lorsque vous accédez aux services AWS par programmation, que ce soit par le biais d'un des divers kits SDK ou de la AWS Command Line Interface (AWS CLI). Les outils de l'AWS CLI et les kits SDK utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas les outils AWS, vous devez signer la demande vous-même. AWS Organizations prend en charge Signature Version 4, un

protocole permettant l'authentification des demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, voir Signing AWS API requests dans le guide de l'utilisateur IAM.

- Rôle IAM : un rôle IAM est une autre identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Il est similaire à un utilisateur IAM mais n'est pas associé à une personne en particulier. Un rôle IAM vous permet d'obtenir des clés d'accès temporaires qui permettent d'accéder aux ressources et services AWS. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :
  - Accès par des utilisateurs fédérés : au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités d'utilisateur préexistantes provenant d'AWS Directory Service, de votre annuaire d'utilisateurs d'entreprise ou d'un fournisseur d'identité web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour en savoir plus sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le Guide de l'utilisateur IAM.
  - Accès entre comptes : vous pouvez utiliser un rôle IAM de votre compte pour autoriser un autre Compte AWS à accéder aux ressources de votre compte. Par exemple, voir Tutoriel : Déléguer l'accès à l'Comptes AWSaide de rôles IAM dans le Guide de l'utilisateur IAM.
  - Accès au service AWS : vous pouvez utiliser un rôle IAM de votre compte pour autoriser un service AWS à accéder aux ressources de votre compte. Par exemple, vous pouvez créer un rôle qui autorise Amazon Redshift à accéder à un compartiment Amazon S3 en votre nom, puis à charger les données stockées dans le compartiment dans un cluster Amazon Redshift. 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.
  - Applications qui s'exécutent sur Amazon EC2 : au lieu de stocker des clés d'accès dans l'instance EC2 afin qu'elles soient utilisées par les applications s'exécutant sur l'instance et émettant des demandes d'API AWS, vous pouvez utiliser un rôle IAM afin de gérer des informations d'identification temporaires pour ces applications. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible pour toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais à moins d'avoir les autorisations requises, vous ne pouvez pas administrer de ressources AWS Organizations ni accéder à celles-ci. Par exemple, vous devez disposer d'autorisations pour créer une unité d'organisation ou attacher une stratégie de contrôle des services (SCP) à un compte.

Les sections suivantes décrivent comment gérer les autorisations pour AWS Organizations.

- Gestion des autorisations d'accès pour votre organisation AWS
- Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Organizations
- Contrôle d'accès basé sur les attributs avec des balises et AWS Organizations

Gestion des autorisations d'accès pour votre organisation AWS

Toutes les ressources AWS, y compris les racines, les unités d'organisation, les comptes et les politiques d'une organisation, sont détenues par un Compte AWS et les autorisations pour créer ou consulter 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 ressources AWS en attachant 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 rubrique Bonnes pratiques IAM du Guide de l'utilisateur IAM.

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.

Ressources et opérations AWS Organizations

Cette section explique comment les concepts AWS Organizations correspondent à leurs concepts IAM équivalents.

Ressources

Dans AWS Organizations, vous pouvez contrôler l'accès aux ressources suivantes :

- La racine et les unités d'organisation 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 utiliséesAWS Organizations, voir Types de ressources définis par AWS Organizations dans la référence d'autorisation de service.

Opérations

AWS fournit un ensemble d'opérations à utiliser avec les ressources dans 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 une liste des AWS Organizations opérations pouvant être utilisées comme autorisations dans une politique IAM, consultez la section Actions définies par les AWS Organizations dans le Service Authorization Reference.

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 pour fournir un contrôle plus précis sur 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 avec AWS Organizations :

- `aws:PrincipalOrgID` : simplifie la spécification de l'élément `Principal` dans une politique basée sur les ressources. Cette clé globale permet d'éviter de répertorier tous les ID de compte pour tous les 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 entité AWS Organizations. Pour plus d'informations sur les chemins, voir Comprendre le chemin de l'AWS Organizationsentité 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 pour les membres de l'une des deux unités d'organisation de la même organisation.

```
        "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 :

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_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.

```
{
    "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 AWSServiceAccess opérations d'activation AWSServiceAccess ou de désactivation 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 ou de la désactivation de l'accès approuvé avec AWS Organizations.

```
{
    "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

Le Compte AWS possède les ressources qui sont créées dans le compte, indépendamment de la personne qui les a créées. Plus précisément, le propriétaire des ressources est le Compte AWS de l'entité principal (à savoir, l'utilisateur root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande de création des ressources. Pour une organisation AWS, 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'unité d'organisation.)
- 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 d' 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 associées à une ressource sont appelées des politiques basées sur les ressources. AWS Organizations prend en charge uniquement les politiques basées sur l'identité (politiques IAM).

Rubriques

- Politiques d'autorisations basées sur l'identité (politiques IAM)
- Politiques basées sur les ressources

Politiques d'autorisations basées sur l'identité (politiques IAM)

Vous pouvez attacher des politiques aux identités IAM pour permettre à ces identités d'effectuer des opérations sur des ressources AWS. Par exemple, vous pouvez effectuer les opérations suivantes :

- Attacher une politique d'autorisations à un utilisateur ou à un groupe de votre compte : pour accorder à un utilisateur des autorisations lui permettant de créer une ressource AWS Organizations, comme une politique de contrôle des services (SCP) ou une unité d'organisation, vous pouvez attacher une politique d'autorisations à cet utilisateur ou à un groupe auquel il 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. Si vous souhaitez accorder des autorisations d'assumer le rôle à un service AWS, le mandataire de la politique d'approbation peut également être un principal du service AWS.

  Pour en savoir plus sur l'utilisation d'IAM pour déléguer des autorisations, consultez la rubrique 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.

```
{
   "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.

```
{
   "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.

```
{
   "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.

Politiques basées sur les ressources

Certains services, comme Amazon S3, prennent en charge les politiques d'autorisations basées sur les ressources. Par exemple, vous pouvez attacher une politique à un compartiment Amazon S3 pour gérer les autorisations d'accès à ce compartiment. Actuellement, AWS Organizations ne prend pas en charge les politiques basées sur les ressources.

Spécification des éléments d'une politique : actions, conditions, effets et ressources

Pour chaque ressource AWS Organizations, le service définit un ensemble d'opérations d'API ou 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 unité d'organisation, AWS Organizations définit des actions telles que :

- `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 la valeur `Effect` spécifiée, `organizations:CreateAccount` accorde ou refuse à l'utilisateur les autorisations d'effectuer l'opération AWS Organizations `CreateAccount`. 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, consultez la section 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 les 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 les ressources). AWS Organizations ne prend actuellement en charge que les politiques basées sur l'identité et pas celles basées sur les ressources.

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.

Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Organizations

En tant qu'administrateur du compte de gestion d'une organisation, vous pouvez contrôler l'accès aux ressources AWS en attachant des politiques d'autorisations à des identités AWS Identity and Access Management (IAM) (utilisateurs, groupes et rôles) au sein de l'organisation. 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. Si les autorisations sont accordées à un rôle, ce rôle peut être assumé par des utilisateurs dans d'autres comptes de l'organisation.

Par défaut, un utilisateur ne dispose d'aucune autorisation. Toutes les autorisations doivent être accordées explicitement par une politique. Si une autorisation n'est pas accordée explicitement, elle est implicitement refusée. Si une autorisation est refusée explicitement, ceci remplace toute autre politique qui aurait pu accorder cette autorisation. En d'autres termes, un utilisateur dispose uniquement des autorisations qui lui sont accordées explicitement et qui ne sont pas explicitement refusées.

Outre les techniques de base décrites dans cette rubrique, vous pouvez contrôler l'accès à votre organisation à l'aide des balises appliquées aux ressources de votre organisation : la racine de l'organisation, les unités organisationnelles (UO), les comptes et les politiques. Pour de plus amples informations, consultez Contrôle d'accès basé sur les attributs avec des balises et AWS Organizations.

Octroi des autorisations d'administration complètes à un utilisateur

Vous pouvez créer une politique IAM qui accorde des autorisations d'administrateur AWS Organizations 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 AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
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 politiques, 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 de plus amples 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"` et `"servicename:some*action"` sont tous les deux non valides dans des politiques de contrôle des services.

```
{
    "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'étend pas aux unités d'organisation enfants. Aucun accès de facturation n'est accordé. Notez que cela ne vous accorde pas un accès administratif aux Comptes AWS figurant dans l'unité d'organisation. Cela accorde uniquement les autorisations nécessaires pour effectuer des opérations AWS Organizations sur les comptes et les unités d'organisation enfants au sein de l'unité d'organisation spécifiée :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
```

```
    }
  ]
}
```

Vous obtenez les ID pour l'unité d'organisation et l'organisation à partir de la console AWS Organizations ou en appelant les API `List*`. 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 ARN des 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 autre mandataire de service que celui pour AWS IAM Identity Center, cette politique ne correspond pas et la demande est refusée :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur les ARN des différentes ressources, voir les types de ressources définis par AWS Organizations dans la référence d'autorisation de service.

Contrôle d'accès basé sur les attributs avec des balises et AWS Organizations

Le contrôle d'accès basé sur les attributs vous permet d'utiliser des attributs gérés par l'administrateur tels que des balises attachées aux ressources AWS et aux identités AWS 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.

Les ressources balisables AWS Organizations comprennent Comptes AWS, la racine, les unités d'organisation ou les politiques de l'organisation. 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, vous pouvez ajouter des éléments `Condition` à vos instructions de politique d'autorisations AWS Identity and Access Management(IAM) 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 effectivement « Autoriser l'utilisateur à gérer uniquement les unités d'organisation qui ont une balise avec une clé `X` et une valeur `Y` » ou « Autoriser l'utilisateur à gérer uniquement les unités d'organisation qui sont balisées avec une clé `Z` ayant la même valeur que la clé de balise `Z` attachée à l'utilisateur. »

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 effectuez une demande à l'aide de la AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'un des SDK AWS, 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`.

```
{
    "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, consultez 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.

```
{
    "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. Ainsi, l'exemple de politique suivant autorise une opération Organizations uniquement si les trois clés de balise spécifiées sont présentes dans la demande.

```
{
    "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.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
```

```
                    "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.

Ainsi, l'exemple de politique suivant refuse toute demande de l'utilisateur ou du rôle visant à créer un Compte AWS lorsque la demande n'a pas la balise `costcenter` ou fournit cette balise avec une valeur autre que 1, 2 ou 3.

```
{
    "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.

Journalisation et surveillance dans AWS Organizations

La bonne pratique consiste à surveiller votre organisation pour vous assurer que les modifications sont journalisées. Vous pouvez ainsi vous assurer que toutes les modifications inattendues peuvent être vérifiées et que les modifications non désirées peuvent être annulées. AWS Organizations prend actuellement en charge deux services AWS qui vous permettent de surveiller votre organisation et son activité.

Rubriques

- Journalisation des appels d'API AWS Organizations avec AWS CloudTrail
- Amazon EventBridge

Journalisation des appels d'API AWS Organizations avec AWS CloudTrail

AWS Organizations est intégré avec ,AWS CloudTrail un service qui fournit un registre des actions prises par un utilisateur, un rôle ou un service AWS dans AWS Organizations. CloudTrail capture tous les appels d'API pour AWS Organizations en tant qu'événements, y compris les appels émis par la console AWS Organizations et les appels de code transmis aux API AWS Organizations. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour AWS Organizations. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS Organizations, l'adresse IP à partir de laquelle elle a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, consultez le Guide de l'utilisateur AWS CloudTrail.

> **Important**
>
> Vous pouvez afficher toutes les informations CloudTrail pour AWS Organizations uniquement dans la région USA Est (Virginie du Nord). Si vous ne voyez pas votre activité AWS Organizations dans la console CloudTrail, définissez le paramètre de région de votre console sur USA Est (Virginie du Nord) à l'aide du menu dans le coin supérieur droit. Si vous interrogez CloudTrail avec la AWS CLI ou les outils SDK, adressez votre requête au point de terminaison USA Est (Virginie du Nord).

Informations AWS Organizations dans CloudTrail

CloudTrail est activé dans votre Compte AWS lors de la création de ce dernier. Quand une activité a lieu dans AWS Organizations, cette activité est enregistrée dans un événement CloudTrail avec d'autres événements de service AWS dans l'Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS Organizations, créez un journal d'activité. Un journal d'activité permet à CloudTrail de livrer des fichiers journaux dans un compartiment Amazon S3. Lorsque la journalisation CloudTrail est activée dans votre Compte AWS, les appels d'API passés aux actions AWS Organizations sont suivis dans des fichiers journaux CloudTrail, où ils sont consignés avec d'autres enregistrements de service AWS. Vous pouvez configurer d'autres services AWS afin d'analyser plus en profondeur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail

Toutes les actions AWS Organizations sont consignées par CloudTrail et documentées dans la Référence des API AWS Organizations. À titre d'exemple, les appels à `CreateAccount` (y compris l'événement `CreateAccountResult`), `ListHandshakesForAccount`, `CreatePolicy` et `InviteAccountToOrganization` génèrent des entrées dans les fichiers journaux CloudTrail.

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 requête a été effectuée par un autre service AWS

Pour de plus amples informations, consultez Élément userIdentity CloudTrail.

Présentation des AWS Organizations entrées des fichiers journaux

Un journal d'activité est une configuration qui permet d'envoyer les événements dans des fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

Exemple d'entrées de journal : CloseAccount

L'exemple suivant montre une entrée de journal CloudTrail pour un exemple d'appel `CloseAccount` qui est générée lorsque l'API est appelée et que le flux de travail pour clôturer le compte démarre le traitement 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 journal CloudTrail pour un appel `CloseAccountResult` après que le flux de travail de clôture de compte en arrière-plan se soit 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"
}
```

Exemple d'entrées de journal : CreateAccount

L'exemple suivant montre une entrée de journal CloudTrail pour un exemple d'appel `CreateAccount` qui est générée lorsque l'API est appelée et que le flux de travail pour créer le compte commence le traitement 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 journal CloudTrail pour un appel `CreateAccount` après que le flux de travail en arrière-plan pour créer le compte s'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 journal CloudTrail générée après qu'un flux de travail en arrière-plan `CreateAccount` pour créer le compte a échoué.

```
  {
  "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 journal CloudTrail pour un exemple d'appel `CreateOrganizationalUnit`.

```
{
    "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"
        }
    },
    "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 journal CloudTrail pour un exemple d'appel `InviteAccountToOrganization`.

```
{
    "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 journal CloudTrail pour un exemple d'appel `AttachPolicy`. 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"
```

```
}
```

Amazon EventBridge

AWS Organizations peut fonctionner avec Amazon EventBridge, anciennement Amazon CloudWatch Events, pour émettre 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 des règles EventBridge qui recherchent ces actions, puis envoient les événements générés aux 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.

Vous trouverez un didacticiel qui montre comment activer EventBridge pour contrôler les activités clés de votre organisation dans Didacticiel : Surveillance des modifications importantes apportées à votre organisation avec Amazon EventBridge.

Pour en savoir plus sur EventBridge, notamment sur sa configuration et son activation, consultez le Guide de l'utilisateur Amazon EventBridge.

Validation de la 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. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Organizations

L'infrastructure mondiale d'AWS est construite autour de zones de disponibilité et de Régions AWS. Les Régions AWSfournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone 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 Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Sécurité de l'infrastructure dans AWS Organizations

En tant que service géré, AWS Organizations est protégé par les procédures de sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez les appels d'API publiés par AWS pour accéder à Organizations via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous 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.

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

Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou

une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus 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).

AWS OrganizationsRéférence

Utilisez les rubriques de cette section pour trouver des informations de référence détaillées sur différents aspects concernant AWS Organizations.

Rubriques

Quotas pour AWS Organizations

Cette section spécifie les quotas qui s'appliquent à AWS Organizations.

Instructions d'attribution de noms

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

- Ils doivent être composés de caractères Unicode
- La longueur maximale de chaîne des noms varie selon l'objet. Pour voir la limite réelle pour chacun, consultez la Référence des API AWS Organizations et recherchez l'opération API qui crée l'objet. Regardez les détails du paramètre `Name` de cette opération. Par exemple : Nom du compte ou Nom de l'unité d'organisation.

Valeurs minimales et maximales

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

> **Note**
>
> Vous pouvez demander des augmentations de certaines de ces valeurs à l'aide de la console Service Quotas.
> Organizations est un service mondial hébergé physiquement dans la région USA Est (Virginie du Nord) (`us-east-1`). Par conséquent, vous devez utiliser `us-east-1` pour accéder aux quotas des Organizations lorsque vous utilisez la console Service Quotas AWS CLI, le ou un AWS SDK.

Nombre de personnes Comptes AWS dans une organisation	10 – La valeur maximale par défaut du nombre de comptes autorisés dans une organisation. Si vous devez en utiliser davantage, vous pouvez demander une augmentation à l'aide de la console Service Quotas. 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. Les comptes et organisations nouvellement créés peuvent avoir un quota inférieur à la valeur par défaut de 10 comptes.
Nombre de racines dans une organisation	1
Nombre d'unités d'organisation dans une organisation	1 000
Nombre de politiques dans une organisation	Politiques de désinscription des services d'IA : 1000 Politiques de sauvegarde : 1000 Politiques de contrôle des services : 2000 Politiques de tag : 1000
Taille maximale d'un document de politique	Politiques de désactivation des services IA : 2500 caractères Politiques de sauvegarde : 10 000 caractères Politiques de contrôle des services : 5 120 octets Politiques de balises : 10 000 caractères 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 d'unités d'organisation sous une racine.
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. 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 membres que vous pouvez clôturer au cours d'une période de 30 jours	10 % des comptes membres d'une organisation, avec un maximum de 1 000. • < 100 comptes – Vous pouvez clôturer jusqu'à 10 comptes membres • 100 à 10 000 comptes — Vous pouvez fermer jusqu'à 10 % des comptes de vos membres • > 10 000 comptes — Vous pouvez fermer jusqu'à 1 000 comptes de membres Par exemple, si vous avez 10 500 comptes membres, vous pouvez fermer jusqu'à 1 000 comptes (et non 1 050) sur une période de 30 jours. Une fois ce quota atteinte, vous pouvez clôturer des comptes supplémentaires dans la console AWS Billing ou attendre la réinitialisation de votre quota. Pour plus d'informations, consultez ce que vous devez savoir avant de fermer votre compte dans le Guide de gestion de AWS compte.
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

Délai d'expiration des handshakes

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

Invitation à rejoindre une organisation	15 jours
Demande d'activer toutes les fonctions dans une organisation	90 jours
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.

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 : au moins une politique de contrôle des services doit	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
	être attachée en permanence à chaque entité. Vous ne pouvez pas supprimer la dernière politique de contrôle des services d'une entité.			
Politique de désactivation des services IA	0	5	5	5
Politique de sauvegarde	0 USD	10	10	10
Politique de balises	0 USD	10	10	10

> **Note**
>
> Actuellement, vous ne pouvez avoir qu'une seule racine au sein d'une organisation.

Limites d'étranglement

Le tableau suivant répertorie les AWS Organizations API par catégorie de gestion et indique leurs taux d'accélération respectifs au niveau du compte et de l'organisation.

AWS Organizations API	Limite par compte (taux, rafale)	Limite par organisation (taux, rafale)
Gestion du compte		

AWS Organizations API	Limite par compte (taux, rafale)	Limite par organisation (taux, rafale)
CloseAccount	0,05, 1	
CreateAccount, CreateGovCloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10
Gestion des poignées de main		
AcceptHandshake, DescribeHandshake	1, 1	
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10
Gestion de l'organisation		
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	

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

AWS Organizations API	Limite par compte (taux, rafale)	Limite par organisation (taux, rafale)
Gestion des services		
ActiverAWSServiceAccess, désactiver AWSServiceAccess	1, 2	
ListeAWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

AWS Politiques gérées à utiliser avec AWS Organizations

Cette section identifie les politiques gérées par AWS qui vous sont proposées pour gérer votre administration. Vous ne pouvez pas modifier ni supprimer les politiques gérées AWS, mais vous pouvez les attacher aux entités de votre organisation ou les en détacher selon vos besoins.

Politiques gérées par AWS Organizations à utiliser avec AWS Identity and Access Management (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'avez pas besoin d'écrire la police vous-même et lorsque AWS met à jour la politique comme il convient pour prendre en charge les nouveaux services, vous obtenez automatiquement et immédiatement les avantages 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.

Nom de la politique	Description	ARN
AWSOrganizationsFullAccess	Fournit toutes les autorisations nécessaires à la création et à l'administration complète d'une organisation. Le contenu de cette déclaration de politique est repris dans l'extrait suivant :	arn:aws:iam : :aws:policy/AWSOrganizationsFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSOrganizationsFullAccess",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*"
        },
        {
            "Sid": "AWSOrganizationsFullAccessAccount",
            "Effect": "Allow",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:GetAlternateContact",
                "account:GetContactInformation",
                "account:PutContactInformation",
                "account:ListRegions",
                "account:EnableRegion",
```

Nom de la politique	Description	ARN

```
                "account:
DisableRegion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

Nom de la politique	Description	ARN
AWSOrganizationsReadOnlyAccess	Fournit un accès en lecture seule aux informations relatives à l'organisation. Elle ne permet pas à l'utilisateur d'apporter des modifications. Le contenu de cette déclaration de politique est repris dans l'extrait suivant :	arn:aws:iam : :aws:policy/AWSOrganizationsReadOnlyAccess

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSOrganizationsReadOnly",
         "Effect":"Allow",
         "Action":[
            "organizations:Describe*",
            "organizations:List*"
         ],
         "Resource": "*"
      },
      {
         "Sid": "AWSOrganizationsReadOnlyAccount",
         "Effect":"Allow",
         "Action":[
            "account:GetAlternateContact",
            "account:GetContactInformation",
            "account:ListRegions"
         ],
         "Resource": "*"
      }
   ]
```

Nom de la politique	Description	ARN
	`}`	

Mises à jour des politiques gérées par AWS dans Organizations

Le tableau suivant contient des détails sur les mises à jour des politiques gérées par AWS 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 AWS Organizations.

Modification	Description	Date
AWSOrganizationsFullAccess— mis à jour pour inclure `Sid` des éléments décrivant la déclaration de politique.	Organisations ont ajouté `Sid` des éléments `AWSOrganizationsFullAccess` à la politique gérée.	6 février 2024
AWSOrganizationsReadOnlyAccess— mis à jour pour inclure `Sid` des éléments décrivant la déclaration de politique.	Organisations ont ajouté `Sid` des éléments `AWSOrganizationsReadOnlyAccess` à la politique gérée.	6 février 2024
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.	Organizations a ajouté l'action `account:ListRegions`, `account:EnableRegion` et `account:DisableRegion` à la politique pour permettre l'accès en écriture afin d'activer ou de désactiver les régions d'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.	Organizations a ajouté l'action `account:ListRegions` à la politique pour permettre l'accès à l'affichage des régions d'un compte.	22 décembre 2022

Modification	Description	Date
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.	Organizations a ajouté les actions `account:GetContactInformation` et `account:PutContactInformation` à la politique pour permettre l'accès en écriture afin de modifier des contacts pour 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.	Organizations a ajouté l'action `account:GetContactInformation` à la politique pour permettre l'accès aux contacts pour un compte.	21 octobre 2022
AWSOrganizationsFullAccess— mis à jour pour permettre la création d'une organisation.	Organizations a ajouté l'autorisation `CreateServiceLinkedRole` à la politique pour permettre la création du rôle lié au service nécessaire 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.	Organizations a ajouté les actions `account:GetAlternateContact` ,`account:DeleteAlternateContact` ,`account:PutAlternateContact` à la politique pour permettre l'accès en écriture afin de modifier d'autres contacts pour un compte.	7 février 2022

Modification	Description	Date
AWSOrganizationsReadOnlyAccess— mis à jour pour autoriser les autorisations d'API du compte requises pour consulter les contacts alternatifs du compte via la console Organizations.	Organizations a ajouté l'action `account:GetAlternateContact` à la politique pour permettre l'accès à d'autres contacts pour un compte.	7 février 2022

Politiques de contrôle des services gérées par AWS Organizations

Les politiques de contrôle des services (SCP) sont similaires aux politiques d'autorisation IAM, mais sont une fonction d'AWS Organizations au lieu d'IAM. Vous utilisez des politiques de contrôle des services pour spécifier les autorisations maximales pour les entités concernées. Vous pouvez attacher des politiques SCP aux racines, aux unités d'organisation (UO) ou aux comptes de votre organisation. Vous pouvez créer vos propres politiques ou utiliser celles définies par IAM. Vous pouvez consulter la liste des politiques de votre organisation sur la page Politiques de la console Organizations.

> **Important**
>
> Au moins une politique SCP doit être attachée en permanence à chaque racine, unité d'organisation et compte.

Nom de la politique	Description	ARN
Complet AWSAccess	Accorde au compte de gestion AWS Organizations l'accès aux comptes membres.	arn:aws:organizations : :aws:policy/Service_Control_Policy/P-FullAWSAccess

Résolution des problèmes de AWS Organizations

Si vous rencontrez des problèmes lorsque vous utilisez AWS Organizations, consultez les rubriques de cette section.

Rubriques

Dépannage de problèmes généraux

Utilisez ces informations pour diagnostiquer et corriger les problèmes d'accès refusé ou autres que vous pouvez rencontrer lors de l'utilisation d'AWS Organizations.

Rubriques

Je reçois un message « Accès refusé » lorsque j'effectue 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 instructions de politique qui accordent ces autorisations incluent des conditions, comme des restrictions quant au moment de la journée ou à l'adresse IP, vous devez également répondre à 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 API manuellement (sans utiliser les kits SDK AWS), 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 en savoir plus, consultez la documentation de la boîte à outils du kit SDK de votre choix ou la rubrique Utilisation d'informations d'identification de sécurité temporaires pour demander l'accès aux ressources AWS 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. Quand vous créez un compte dans une organisation à l'aide de la console AWS Organizations, de l'API ou des commandes de l'AWS CLI, ces informations ne sont pas automatiquement collectées. Pour un compte que vous souhaitez rendre autonome, vous devez accepter le Contrat client AWS, choisir un plan de support, fournir et vérifier les coordonnées nécessaires, puis proposer un moyen de paiement. AWS utilise ce moyen de paiement pour débiter les frais de toutes les activités (à l'exception de celles entrant dans le cadre de l'offre gratuite AWS) AWS qui interviennent tant que le compte n'est pas attaché à une organisation. Pour de plus amples informations, veuillez consulter Quitter une organisation depuis votre compte membre.

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 Compte AWS, supprimez-le de votre organisation afin qu'il ne soit plus pris en compte dans le calcul de 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. Par exemple, il est impossible de supprimer immédiatement de nouveaux comptes créés. Réessayez l'action dans quelques jours. Si vous rencontrez des problèmes avec les quotas de comptes lors de l'ajout et de la suppression de comptes, consultez Valeurs minimales et maximales pour savoir comment demander une augmentation de quotas.

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. Les modifications que vous apportez à AWS Organizations nécessitent un certain temps avant de devenir visibles de tous les points de terminaison possibles. Une partie du retard s'explique par le temps requis 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 ralentir le processus. 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 ce retard, veuillez consulter 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.
- Ensuring Consistency When Using Amazon S3 and Amazon Elastic MapReduce for ETL Workflows dans le blog AWS sur le Big Data
- Cohérence éventuelle EC2 dans la Référence d'API Amazon EC2

Dépannage des politiques AWS Organizations

Utilisez ces informations pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de politiques AWS Organizations.

Politiques de contrôle des services

Les politiques de contrôle des services dans AWS Organizations sont similaires aux politiques IAM et partagent la même syntaxe. Cette syntaxe commence avec les règles de JavaScript Object Notation (JSON). JSON décrit un objet avec des paires nom-valeur qui constituent l'objet. La grammaire des politiques IAM exploite ce format en définissant ce à quoi correspondent les noms et les valeurs et elle peut être interprétée par les 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 plus de détails, veuillez consulter 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 (indiqués en *rouge*) :

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "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 :

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "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 :

```
{
  "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.

Appel de l'API à l'aide de demandes de requête HTTP

Cette section contient des informations générales sur l'utilisation de l'API de requête 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 de requête AWS Organizations, vous pouvez utiliser l'un des kits de développement logiciel AWS. Les kits SDK AWS se composent de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Ruby, .NET, iOS, Android, etc). Ils facilitent la création d'un accès par programmation à AWS Organizations et AWS. Par exemple, ils automatisent les tâches telles que la signature cryptographique des demandes, la gestion des erreurs et les nouvelles tentatives automatiques de demande. Pour en savoir plus sur les kits de développement logiciel AWS, y compris les procédures pour les télécharger et les installer, consultez Outils pour Amazon Web Services.

L'API de requête pour AWS Organizations vous permet d'appeler des actions de service. Les demandes d'API de requête sont des demandes HTTPS qui doivent contenir un paramètre `Action` qui indique l'opération à effectuer. AWS Organizations prend en charge les demandes 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 d'API AWS Organizations

Points de terminaison

AWS Organizations dispose d'un point de terminaison d'API mondial 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 d'API AWS Organizations

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 fortement de ne pas utiliser les informations d'identification de votre Utilisateur racine d'un compte AWS pour l'exécution des tâches quotidiennes 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 rubrique Signature des demandes d'API AWS du Guide de l'utilisateur IAM.

AWS Organizations ne prend pas en charge les versions précédentes, telles que Signature Version 2.

Pour plus d'informations, consultez les ressources suivantes :

- Informations d'identification de sécurité AWS : fournit des informations générales sur les types d'informations d'identification que vous pouvez utiliser pour accéder à AWS.
- Bonnes pratiques de sécurité en matière d'IAM : offre des suggestions concernant l'utilisation du service IAM pour sécuriser vos ressources AWS, y compris celles d'AWS Organizations.
- Informations d'identification de sécurité temporaires dans IAM : décrit comment créer et utiliser des informations d'identification de sécurité temporaires.

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

Modification	Description	Date
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.	1 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 AWSOrganizationsFullAccess et AWSOrganizationsReadOnlyAccess 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 AWSOrganizationsFullAccess 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

Fonctionnalité de clôture de compte Organizations à partir de la console AWS Organizations	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
Mise à jour de l'annonce pour mettre à jour d'autres contacts avec la console AWS Organizations	Organizations permet désormais de mettre à jour d'autres contacts pour les comptes de votre organisation à l'aide de la console AWS Organizations. 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 AWSOrganizationsFullAccess et AWSOrganizationsReadOnlyAccess 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 à AWS Organizations pour garantir que votre graphique de comportement Detective offre une visibilité sur l'activité de tous les comptes de votre organisation.	16 décembre 2021
L'intégration d'Organizations à AWS Config prend désormais en charge le regroupement de données multi-comptes et multi-régions.	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 ConfigGuide du développeur.	16 juin 2021

L'intégration d'Organizations à AWS Firewall Manager prend désormais en charge 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 fonction de sauvegarde continue de AWS Backup avec les politiques de sauvegarde de votre organisation.	10 mars 2021
L'intégration d'Organizations à AWS CloudFormation StackSets prend désormais en charge un administrateur délégué.	Vous pouvez désormais désigner un compte membre de votre organisation comme AWS 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 d'inviter des comptes pendant que vous activez toutes les fonctions	AWS a mis à jour le processus pour activer toutes les fonctions dans 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

Introduction de la version 2.0 de la console AWS Organizations	AWS a introduit une nouvelle version de la console AWS. 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 à AWS Marketplace	Vous pouvez désormais permettre à AWS Marketplace de partager plus facilement vos licences de logiciels 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 d'autres Comptes AWS dans l'organisation.	18 novembre 2020

Régions AWS en Chine prend désormais en charge AWS Resource Access Manager en tant que service de confiance par Organizations.	Vous pouvez désormais utiliser les fonctionnalités de AWS RAM qui s'intègrent à Organizations en tant que service approuvé lorsque vous utilisez Organizations et AWS RAM en Chine.	18 novembre 2020
Organizations prend désormais en charge l'intégration à AWS Security Hub	Vous pouvez activer Security Hub 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.	12 novembre 2020
Changement de nom du compte principal	AWS Organizations a changé le nom « 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 BackupManuel 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
Ajout de AWS Health comme service de confiance	Vous pouvez agréger des AWS Health événements entre des comptes de votre organisation.	4 août 2020
Politiques de désactivation des services d'intelligence artificielle (IA)	Vous pouvez utiliser des politiques de désactivation des services d'IA pour contrôler si les services d'IA de AWS peuvent stocker et utiliser du contenu client traité par ces services (contenu IA) pour le développement et l'amélioration continue des services et technologies d'IA de AWS.	8 juillet 2020
Ajout de politiques de sauvegarde et intégration à 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 à AWS 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 ressources des comptes de votre organisation.	26 novembre 2019
Intégration à Systems Manager	Vous pouvez synchroniser les données opérationnelles entre tous les Comptes AWS de votre organisation dans Systems Manager Explorer.	26 novembre 2019
lois : PrincipalOrgPaths	La nouvelle clé de condition globale vérifie le chemin d'accès à AWS Organizations pour l'utilisateur IAM, le rôle IAM ou l'utilisateur racine du Compte AWS qui effectue la demande.	20 novembre 2019

Intégration aux règles AWS Config	Vous pouvez utiliser les opérations d'API AWS Config pour gérer les règles AWS Config entre tous les Comptes AWS de votre organisation.	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 au Control Tower AWS	AWS Control Tower a été ajouté en tant que service pouvant fonctionner avec les comptes de votre organisation.	24 juin 2019
Intégration à AWS Identity and Access Management	IAM fournit les données relatives aux services consultés en dernier aux entités de votre organisat ion (racine de l'organisation, unités d'organisation et comptes). Vous pouvez utiliser ces données pour restreind re l'accès uniquement aux services AWS dont vous avez besoin.	20 juin 2019
Balisage des comptes	Vous pouvez ajouter et supprimer les balises de comptes de votre organisat ion et également afficher les balises d'un compte de votre organisation.	6 juin 2019

Ressources, conditions et l'élément `NotAction` dans les politiques de contrôle des services (SCP)	Vous pouvez désormais spécifier des ressources, des conditions et l'élément `NotAction` dans les politiques de contrôle des services pour refuser l'accès entre comptes dans votre organisation ou vos unités d'organisation (UO).	25 mars 2019
Nouveaux services pour un accès de confiance	AWS License Manager et Service Catalog ont été 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 ont été ajoutés en tant que services pouvant fonctionn er avec les comptes de votre organisation.	4 décembre 2018
Nouveau service pour un accès de confiance	AWS Directory Service a été 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 a été 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 ont été ajoutés en tant que services pouvant fonctionner avec les comptes de votre organisation.	18 avril 2018
Accès aux services de confiance	Vous pouvez désormais activer et désactiver l'accès pour que des services AWS sélectionnés fonctionnent 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	À présent, vous pouvez supprimer les comptes créés dans AWS Organizations sans contacter AWS Support.	19 décembre 2017
Prise en charge ajoutée pour le nouveau service AWS IAM Identity Center	AWS Organizations prend désormais en charge l'intégration à AWS IAM Identity Center (IAM Identity Center).	7 décembre 2017

AWS a ajouté un rôle lié au service à tous les comptes de l'organisation	Un rôle lié au service nommé `AWSServiceRoleForOrganizations` a été ajouté à tous les comptes d'une organisation pour permettre l'intégration entre AWS Organizations et les autres 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	Première version de la documentation AWS Organizations qui accompagnait le lancement du nouveau service.	17 février 2017

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.