aws

Guide de l’utilisateur

AWS Resource Access Manager

AWS Resource Access Manager: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS Resource Access Manager ?

AWS Resource Access Manager(AWS RAM) vous permet de partager vos ressources en toute sécurité au sein de votre organisation ou de vos unités organisationnelles (UO), ainsi qu'avec des rôles et des utilisateursAWS Identity and Access Management (IAM) pour les types de ressources pris en charge.Comptes AWS Si vous en avez plusieursComptes AWS, vous pouvez créer une ressource une seule fois et l'utiliserAWS RAM pour la rendre utilisable par ces autres comptes. Si votre compte est géré parAWS Organizations, vous pouvez partager des ressources avec tous les autres comptes de l'organisation ou uniquement avec les comptes appartenant à une ou plusieurs unités organisationnelles (UO) spécifiées. Vous pouvez également partager avec un identifiant de compte spécifiqueComptes AWS, que le compte fasse partie ou non d'une organisation. Certains types de ressources pris en charge vous permettent également de les partager avec des rôles et des utilisateurs IAM spécifiés.

Table des matières

Aperçus vidéo

La vidéo suivante fournit une brève introduction à un partage de ressourcesAWS RAM et décrit comment créer un partage de ressources. Pour plus d'informations, veuillez consulter ???.

La vidéo suivante montre comment appliquer des autorisationsAWS gérées à vosAWS ressources. Pour plus d'informations, veuillez consulter ???.

Cette vidéo montre comment créer et associer des autorisations gérées par le client selon la bonne pratique que l'on appelle principe du moindre privilège. Pour plus d'informations, consultez ???.

Avantages d'AWS RAM

Pourquoi utiliser AWS RAM ? Cette méthode offre les avantages suivants :

- Réduit vos frais opérationnels : créez une ressource une seule fois, puis utilisez-laAWS RAM pour partager cette ressource avec d'autres comptes. Vous n'aurez ainsi plus besoin d'allouer des ressources en double dans chaque compte, ce qui permet de réduire les frais d'exploitation. Dans le compte propriétaire de la ressource, celaAWS RAM simplifie l'octroi de l'accès à tous les rôles et utilisateurs de ce compte sans avoir à utiliser des politiques d'autorisation basées sur l'identité.
- Assure sécurité et cohérence — Simplifiez la gestion de la sécurité de vos ressources partagées en utilisant un ensemble unique de politiques et d'autorisations. Si vous deviez plutôt créer des ressources dupliquées dans tous vos comptes distincts, vous auriez pour tâche de mettre en œuvre des politiques et des autorisations identiques, puis de les maintenir identiques sur tous ces comptes. Au lieu de cela, tous les utilisateurs d'un partage deAWS RAM ressources sont gérés par un ensemble unique de politiques et d'autorisations. AWS RAMoffre une expérience cohérente pour partager différents types deAWS ressources.
- Offre visibilité et auditabilité : consultez les détails d'utilisation de vos ressources partagées grâce à l'intégration d'AWS RAMAmazon CloudWatch etAWS CloudTrail. AWS RAMfournit une visibilité complète sur les ressources et les comptes partagés.

Qu'en est-il de l'accès intercompte avec des politiques basées sur les ressources ?

Vous pouvez partager certains types deAWS ressources avec d'autres personnesComptes AWS en attachant une politique basée sur les ressources qui identifieAWS Identity and Access Management les principaux (rôles et utilisateurs IAM) extérieurs à vousCompte AWS. Toutefois, le partage d'une ressource en y joignant une politique neAWS RAM permet pas de tirer parti des avantages supplémentaires qui en découlent. En utilisant,AWS RAM vous obtenez les fonctions suivantes :

- Vous pouvez partager avec une organisation ou une unité d'organisation (UO) sans avoir à énumérer tous lesCompte AWS ID.
- Les utilisateurs peuvent voir les ressources partagées avec eux directement dans laService AWS console d'origine et les opérations de l'API, comme si ces ressources se trouvaient directement dans le compte de l'utilisateur. Par exemple, si vous avez l'AWS RAMhabitude de partager un

sous-réseau Amazon VPC avec un autre compte, les utilisateurs de ce compte peuvent voir le sous-réseau dans la console Amazon VPC et dans les résultats des opérations d'API Amazon VPC effectuées sur ce compte. Les ressources partagées en joignant une politique basée sur les ressources ne sont pas visibles de cette façon ; vous devez plutôt découvrir la ressource et y faire explicitement référence par son Amazon Resource Name (ARN).

- Les propriétaires d'une ressource peuvent voir quels responsables ont accès à chaque ressource individuelle qu'ils ont partagée.
- Si vous partagez des ressources avec un compte qui ne fait pas partie de votre organisation,AWS RAM lance un processus d'invitation. Le destinataire doit accepter l'invitation avant que ce mandataire puisse accéder aux ressources partagées. Une fois que vous avez activé la fonctionnalité de partage au sein de votre organisation, le partage avec les comptes de l'organisation ne nécessite pas d'invitations.

Si vous avez partagé des ressources à l'aide d'une politique d'autorisation basée sur les ressources, vous pouvez transformer ces ressources en ressources entièrementAWS RAM gérées en procédant de l'une des manières suivantes :

- Utilisez l'opération d'API PromoteResourceShareCreatedFromPolicy.
- Utilisez l'équivalent de l'opération d'API, à savoir la promote-resource-share-created-from-policycommandeAWS Command Line Interface (AWS CLI).

Fonctionnement du partage de ressources

Lorsque vous partagez une ressource du compte propriétaire avec une autre ressourceCompte AWS, le compte consommateur, vous accordez l'accès à la ressource partagée aux principaux du compte consommateur. Toutes les politiques et autorisations qui s'appliquent aux rôles et aux utilisateurs du compte utilisateur s'appliquent également à la ressource partagée. Les ressources du partage semblent être des ressources natives du partage avec lequelComptes AWS vous les avez partagées.

Vous pouvez partager des ressources mondiales et régionales. Pour plus d'informations, veuillez consulter Partage des ressources régionales par rapport aux ressources mondiales.

Partage de vos ressources

Avec AWS RAM, vous pouvez partager des ressources dont vous êtes propriétaire en créant un partage de ressources. Pour créer un partage de ressources, spécifiez les éléments suivants :

- LeRégion AWS partage de ressources. Dans la console, sélectionnez dans le menu déroulant Région dans le coin supérieur droit de la console. Dans leAWS CLI, vous utilisez le`--region` paramètre.
  - Un partage de ressources ne peut contenir que des ressources régionales qui sont dans leRégion AWS même partage de ressources.
  - Un partage de ressources ne peut contenir des ressources mondiales que s'il se trouve dans la région d'origine désignée pour les ressources mondiales, USA Est (Virginie du Nord),`us-east-1`.
- Nom du partage de ressources.
- Liste des ressources auxquelles vous souhaitez accorder l'accès dans le cadre de ce partage de ressources.
- Les mandataires auxquels vous accordez accès à la ressource. Les principaux peuvent être individuelsComptes AWS, les comptes d'une organisation ou d'une unité organisationnelle (OU) peuvent être des rôles ou des utilisateurs individuelsAWS Identity and Access Management (IAM).AWS Organizations

  > **Note**
  >
  > Les types de ressource ne peuvent pas tous être partagés avec les utilisateurs et les rôles IAM. Pour plus d'informations sur les ressources que vous pouvez partager avec ces responsables, consultezRessources partageables AWS.

- Une autorisation gérée à associer à chaque type de ressource que vous incluez dans un partage de ressources. L'autorisation gérée détermine ce que les responsables des autres comptes peuvent faire avec les ressources du partage de ressources.

  Le comportement de l'autorisation dépend du type de mandant :

  - Si le compte principal est différent de celui qui possède la ressource, les autorisations associées au partage de ressources sont les autorisations maximales pouvant être accordées aux rôles et aux utilisateurs de ces comptes. L'administrateur de ces comptes doit ensuite accorder aux rôles et aux utilisateurs individuels l'accès à la ressource partagée selon des politiques IAM basées sur l'identité. Les autorisations accordées dans ces politiques ne peuvent pas dépasser celles définies dans les autorisations associées au partage de ressources.

Le compte propriétaire des ressources conserve la pleine propriété des ressources qu'il partage.

Utilisation de ressources partagées

Lorsque le propriétaire d'une ressource la partage avec votre compte, vous pouvez accéder à la ressource partagée comme vous le feriez si votre compte en était propriétaire. Vous pouvez accéder à la ressource en utilisant la console, lesAWS CLI commandes et les opérations d'API du service concerné. Les opérations d'API que les principaux utilisateurs de votre compte sont autorisés à effectuer varient en fonction du type de ressource et sont spécifiées par l'AWS RAMautorisation associée au partage de ressources. Toutes les politiques IAM et politiques de contrôle des services configurées sur votre compte continuent également de s'appliquer, ce qui vous permet de tirer parti de vos investissements existants en matière de contrôles de sécurité et de gouvernance.

Lorsque vous accédez à une ressource partagée à l'aide du service de cette ressource, vous avez les mêmes capacités et limitesCompte AWS que le propriétaire de la ressource.

- Si la ressource est régionale, vous pouvez y accéder uniquement depuis le compteRégion AWS dans lequel elle se trouve sur le compte propriétaire.
- Si la ressource est globale, vous pouvez y accéder depuis n'importe quelRégion AWS outil et console de service compatibles avec la ressource. Vous pouvez consulter et gérer le partage de ressources et ses ressources globales dans laAWS RAM console et dans les outils uniquement dans la région d'origine désignée, à savoir USA Est (Virginie du Nord)`us-east-1`.

Accès à AWS RAM

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

Console AWS RAM

AWS RAM fournit une interface utilisateur basée sur le Web, la console AWS RAM. Si ce n'est déjà faitCompte AWS, accédez à la console en sélectionnant à la console en sélectionnant à laAWS RAM console en sélectionnant à un AWS Management Consoleet en sélectionnantAWS RAM depuis la page d'accueil de la console.

Vous pouvez également accéder directement à la AWS RAMconsole dans votre navigateur. Si ce n'est déjà fait, il est demandé à le faire avant que la console.

AWS CLIet outils pour Windows PowerShell

LesAWS CLI etAWS Tools for PowerShell fournissent un accès direct aux opérations de l'APIAWS RAM publique. AWSprend en charge ces outils surWindowsmacOS, etLinux. Pour plus

d'informations sur le démarrage, consultez le Guide deAWS Command Line Interface l'utilisateur ou le Guide deAWS Tools for Windows PowerShell l'utilisateur. Pour plus d'informations sur les commandes pourAWS RAM, consultez la Référence de AWS CLIcommande ou la Référence de l'AWS Tools for Windows PowerShellapplet de commande.

Kits de développement logiciel (SDK) AWS

AWSfournit des commandes d'API pour un large éventail de langages de programmation. Pour plus d'informations sur le démarrage, consultez le Guide de référenceAWS des SDK et des outils.

API de requête

Si vous n'utilisez aucun des langages de programmation pris en charge, l'API de requêteAWS RAM HTTPS vous donne un accès programmatique àAWS RAM etAWS. Avec l'AWS RAMAPI, vous pouvez envoyer des demandes HTTPS directement au service. Lorsque vous utilisez l'API AWS RAM, vous devez inclure un code pour signer numériquement les demandes à l'aide de vos informations d'identification. Pour plus d'informations, consultez la AWS RAM API Reference (Référence d'API).

Tarification de AWS RAM

Aucuns frais supplémentaires ne sont facturés pour l'utilisationAWS RAM ou la création de partages de ressources et le partage de vos ressources entre comptes. Les coûts d'utilisation des ressources varient en fonction du type de ressource. Pour plus d'informations sur leAWS mode de facturation des ressources partageables, consultez la documentation du service propriétaire de la ressource.

Conformité et normes internationales

PCI DSS

AWS RAMprend en charge le traitement, le stockage et la transmission des données de cartes bancaires par un commerçant ou un fournisseur de services et a été validé comme étant conforme à la norme PCI (Payment Card Industry) DSS (Data Security Standard).

Pour plus d'informations sur PCI DSS, et notamment sur la manière de demander une copie du package de conformité PCI AWS, veuillez consulter PCI DSS, niveau 1.

FedRAMP

AWS RAMest autorisé comme FedRAMP Moderate dans les régionsRégions AWS : USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio), USA Est (Ohio)

AWS RAMest autorisé en tant que FedRAMP High dans les régions suivantesRégions AWS :AWS GovCloud (États-Unis ouest) etAWS GovCloud (États-Unis est).

Le Federal Risk and Authorization Management Program (FedRAMP) est un programme gouvernemental qui fournit une approche standard de l'évaluation de la sécurité, de l'autorisation et de la surveillance continue pour les produits et services de cloud.

Pour plus d'informations sur la conformité à FedRAMP, consultez FedRAMP.

SOC et ISO

AWS RAMpeut être utilisé pour les charges de travail soumises à la conformité au contrôle de l'organisation des services (SOC) et aux normes ISO 9001, ISO 27001, ISO 27017, ISO 27018 et ISO 27701 de l'Organisation internationale de normalisation (ISO). Les clients des secteurs de la finance, de la santé et d'autres secteurs réglementés peuvent obtenir des informations sur les processus et les contrôles de sécurité qui protègent les données des clients, qui peuvent être consultés dans les rapports SOC et les certificatsAWS ISO et CSA STAR dans AWS Artifact.

Pour plus d'informations sur la conformité à la norme SOC, consultez SOC.

Pour plus d'informations sur la conformité à la norme ISO, consultez ISO 9001, ISO 27001, ISO 27017, ISO 27018 et ISO 27701.

Démarrer avec AWS RAM

AvecAWS Resource Access Manager, vous pouvez partager les ressources que vous possédez avec d'autres personnesComptes AWS. Si votre compte est géré parAWS Organizations, vous pouvez également partager des ressources avec les autres comptes de votre organisation. Vous pouvez également utiliser des ressources qui ont été partagées avec vous par d'autresComptes AWS.

Si vous n'activez pas le partage dansAWS Organizations, vous ne pouvez pas partager de ressources avec votre organisation ou avec les unités organisationnelles (UO) de votre organisation. Dans le cas contraire, vous pouvez toujours partager de ressources avec des particuliersComptes AWSdans votre organisation. Pourtypes de ressources pris en charge, vous pouvez également partager des ressources avec des particuliersAWS Identity and Access Managementrôles ou utilisateurs (IAM) au sein de votre organisation. Dans ce cas, ces principaux sont traités comme s'ils étaient des comptes externes, plutôt que comme faisant partie de votre organisation. Ils reçoivent une invitation à rejoindre le partage de ressources et bénéficient d'un accès à la partagée.

Table des matières

Termes et concepts pourAWS RAM

Les concepts suivants vous aident à comprendre comment utiliserAWS Resource Access Manager(AWS RAM) pour partager vos ressources.

Partage de ressources

Vous partagez des ressources en utilisantAWS RAMen créant unpartage de ressources. Un partage de ressources comporte les trois éléments suivants :

- Une liste d'un ou de plusieursAWSressources à partager.
- Une liste d'un ou de plusieursprincipesà qui l'accès aux ressources est accordé.
- UNautorisation géréepour chaque type de ressource que vous incluez dans le partage. Chaque autorisation gérée s'applique à toutes les ressources de ce type dans ce partage de ressources.

Après avoir utiliséAWS RAMpour créer un partage de ressources, les principaux spécifiés dans le partage de ressources peuvent avoir accès aux ressources du partage.

- Si vous activezAWS RAMpartage avecAWS Organizations, et les directeurs avec lesquels vous partagez font partie de la même organisation que le compte de partage, ces principaux peuvent y accéder dès que l'administrateur de leur compte leur accorde l'autorisation d'utiliser les ressources à l'aide d'unAWS Identity and Access Managementpolitique d'autorisation (IAM).
- Si vous ne l'activez pasAWS RAMen partageant avec des Organisations, vous pouvez toujours partager des ressources avec des individusComptes AWSqui font partie de votre organisation. L'administrateur du compte consommateur reçoit une invitation à rejoindre le partage de ressources, et il doit accepter l'invitation avant que les principaux spécifiés dans le partage de ressources puissent accéder aux ressources partagées.
- Vous pouvez également partager avec des comptes extérieurs à votre organisation, si le type de ressource le permet. L'administrateur du compte consommateur reçoit une invitation à rejoindre le partage de ressources, et il doit accepter l'invitation avant que les principaux spécifiés dans le partage de ressources puissent accéder aux ressources partagées. Pour plus d'informations sur les types de ressources compatibles avec ce type de partage, voirRessources partageables AWSet consultezPeut partager avec des comptes extérieurs à son organisationcolonne.

Partage de compte

Lecompte de partagecontient la ressource qui est partagée et dans laquelle leAWS RAMl'administrateur créeAWSpartage de ressources en utilisantAWS RAM.

UnAWS RAMl'administrateur est un administrateur principal IAM autorisé à créer et à configurer des partages de ressources dans leCompte AWS. Parce queAWS RAMfonctionne en associant une politique basée sur les ressources aux ressources d'un partage de ressources, leAWS RAMl'administrateur doit également être autorisé à appelerPutResourcePolicyopération dansService AWSpour chaque type de ressource inclus dans un partage de ressources.

Principaux consommateurs

Lecompte consommateurest leCompte AWSavec lequel une ressource est partagée. Le partage de ressources peut spécifier un compte entier comme principal ou, pour certains types de ressources, des rôles individuels ou des utilisateurs du compte. Pour plus d'informations sur les types de ressources compatibles avec ce type de partage, voirRessources partageables AWSet consultezPeut partager avec les rôles et les utilisateurs IAMcolonne.

AWS RAMsoutient également les fournisseurs de services en tant que consommateurs de parts de ressources. Pour plus d'informations sur les types de ressources compatibles avec ce type de partage, voirRessources partageables AWSet consultezPeut être partagé avec les responsables du servicecolonne.

Les principaux du compte consommateur ne peuvent effectuer que les actions autorisées partous les deuxdes autorisations suivantes :

- Les autorisations gérées associées au partage de ressources. Ils spécifient lemaximumautorisations qui peuvent être accordées aux principaux du compte consommateur.
- Les politiques basées sur l'identité IAM associées à des rôles ou utilisateurs individuels par l'administrateur IAM dans le compte consommateur. Ces politiques doivent accorder`Allow`accès aux actions spécifiées et auNom de ressource Amazon (ARN)d'une ressource dans le compte de partage.

AWS RAMprend en charge les principaux types d'IAM suivants en tant que consommateurs de partages de ressources :

- Un autreCompte AWS— Le partage des ressources met les ressources incluses dans le compte de partage à la disposition du compte consommateur.
- Rôles ou utilisateurs IAM individuels dans un autre compte— Certains types de ressources prennent en charge le partage direct avec des rôles ou utilisateurs IAM individuels. Spécifiez ce type principal à partir de son ARN.
  - Rôle IAM—`arn:aws:iam::123456789012:role/rolename`
  - Utilisateur IAM—`arn:aws:iam::123456789012:user/username`
- Service principal— Partagez une ressource avec unAWSservice pour accorder au service l'accès à un partage de ressources. Le partage du principal des services permetAWSservice permettant de prendre des mesures en votre nom afin d'alléger le fardeau opérationnel.

  Pour partager avec un directeur de service, choisissez d'autoriser le partage avec n'importe qui, puis, sousSélectionnez le type principal, choisissezService principalà partir de la liste déroulante. Spécifiez le nom du directeur du service au format suivant :

  - *`service-id`*`.amazonaws.com`

  Pour atténuer le risque de confusion entre les adjoints, la politique en matière de ressources indique le numéro de compte du propriétaire de la ressource dans le`aws:SourceAccount`clé de condition.

- Comptes dans une organisation— Si le compte de partage est géré parAWS Organizations, le partage de ressources peut alors spécifier l'identifiant de l'organisation à partager avec tous les comptes de l'organisation. Le partage de ressources peut également spécifier un ID d'unité organisationnelle (UO) à partager avec tous les comptes de cette UO. Un compte de partage ne peut être partagé qu'avec sa propre organisation ou ses identifiants d'unité organisationnelle au sein de sa propre organisation. Spécifiez les comptes d'une organisation en fonction de l'ARN de l'organisation ou de l'unité d'organisation.
  - Tous les comptes d'une organisation— Voici un exemple d'ARN d'une organisation dansAWS Organizations:

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>
    ```

  - Tous les comptes d'une unité organisationnelle— Voici un exemple d'ARN d'un ID d'unité d'organisation :

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
    ```

> **Important**
>
> Lorsque vous partagez avec une organisation ou une unité d'organisation, et que cette étendue inclut le compte propriétaire du partage de ressources, tous les principaux du compte de partage ont automatiquement accès aux ressources du partage. L'accès accordé est défini par les autorisations gérées associées au partage. Cela est dû au fait que la politique basée sur les ressources quiAWS RAMs'attache à chaque ressource utilisée dans le partage`"Principal": "*"`. Pour plus d'informations, veuillez consulter Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.
> Les directeurs des autres comptes consommateurs n'ont pas immédiatement accès aux ressources de l'action. Les administrateurs des autres comptes doivent d'abord associer des politiques d'autorisation basées sur l'identité aux principaux appropriés. Ces politiques doivent accorder`Allow`accès aux ARN des ressources individuelles dans le partage de ressources. Les autorisations définies dans ces politiques ne peuvent pas dépasser celles spécifiées dans l'autorisation gérée associée au partage de ressources.

Politique basée sur une ressource

Les politiques basées sur les ressources sont des documents texte JSON qui mettent en œuvre le langage de politiques IAM. Contrairement aux politiques basées sur l'identité que vous pouvez attacher au principal, tel qu'un rôle ou un utilisateur IAM, vous pouvez attacher des politiques basées sur les ressources à la ressource.AWS RAMrédige des politiques basées sur les ressources en votre nom sur la base des informations que vous fournissez pour votre partage de ressources. Vous devez spécifier`Principal`élément de politique qui détermine qui peut accéder à la ressource. Pour plus d'informations, veuillez consulter la rubriquePolitiques basées sur l'identité et Politiques basées sur une ressourcedans leIAM User Guide.

Les politiques basées sur les ressources générées parAWS RAMsont évalués en même temps que tous les autres types de politiques IAM. Cela inclut toutes les politiques basées sur l'identité IAM associées aux principaux qui tentent d'accéder à la ressource, ainsi que les politiques de contrôle des services (SCP) pourAWS Organizationsqui pourrait s'appliquer àCompte AWS. Politiques basées sur les ressources générées parAWS RAMparticipez à la même logique d'évaluation des politiques que toutes les autres politiques IAM. Pour plus de détails sur l'évaluation des politiques et sur la manière de déterminer les autorisations qui en résultent, voirLogique d'évaluation de stratégiesdans leIAM User Guide.

AWS RAMfournit une expérience de partage de ressources simple et sécurisée en fournissant easy-to-use politiques basées sur les ressources.

Pour les types de ressources qui prennent en charge les politiques basées sur les ressources,AWS RAMconstruit et gère automatiquement les politiques basées sur les ressources pour vous. Pour une ressource donnée,AWS RAMconstruit la politique basée sur les ressources en combinant les informations provenant de tous les partages de ressources qui incluent cette ressource. Par exemple, considérez un Amazon SageMaker pipeline que vous partagez en utilisantAWS RAMet incluez-les dans deux partages de ressources différents. Vous pouvez utiliser un partage de ressources pour fournir un accès en lecture seule à l'ensemble de votre organisation. Vous pouvez ensuite utiliser l'autre partage de ressources pour octroyer uniquement SageMaker autorisations d'exécution pour un seul compte.AWS RAMcombine automatiquement ces deux ensembles d'autorisations différents en une seule politique de ressources comportant plusieurs instructions. Il attache ensuite la politique basée sur les ressources combinées à la ressource du pipeline. Vous pouvez consulter cette politique de ressources sous-jacente en appelant leGetResourcePolicyopération.Services AWSutilisez ensuite cette politique basée sur les ressources pour autoriser tout principal qui tente d'effectuer une action sur la ressource partagée.

Bien que vous puissiez créer manuellement les politiques basées sur les ressources et les associer à vos ressources en appelant`PutResourcePolicy`, nous vous recommandons d'utiliserAWS RAMcar il offre les avantages suivants :

- Découvrabilité pour les consommateurs d'actions— Si vous partagez des ressources en utilisantAWS RAM, les utilisateurs peuvent voir toutes les ressources partagées avec eux directement dans la console du service propriétaire des ressources et les opérations d'API comme si ces ressources se trouvaient directement dans le compte de l'utilisateur. Par exemple, si vous partagez unAWS CodeBuildprojet avec un autre compte, les utilisateurs du compte consommateur peuvent voir le projet dans le CodeBuild console et dans les résultats de CodeBuild Opérations API effectuées. Les ressources partagées en joignant directement une politique basée sur les ressources ne sont pas visibles de cette façon. Au lieu de cela, vous devez découvrir et faire référence explicitement à la ressource par son ARN.
- Facilité de gestion pour les actionnaires— Si vous partagez des ressources en utilisantAWS RAM, les propriétaires des ressources du compte de partage peuvent voir de manière centralisée quels autres comptes ont accès à leurs ressources. Si vous partagez une ressource à l'aide d'une politique basée sur les ressources, vous ne pouvez voir les comptes consommateurs qu'en examinant la politique relative aux ressources individuelles dans la console de service ou l'API correspondante.
- Efficacité— Si vous partagez des ressources en utilisantAWS RAM, vous pouvez partager plusieurs ressources et les gérer en tant qu'unité. Les ressources partagées en utilisant uniquement des politiques basées sur les ressources nécessitent des politiques individuelles associées à chaque ressource que vous partagez.
- Simplicité— AvecAWS RAM, vous n'avez pas besoin de comprendre le langage de politiques IAM basé sur JSON.AWS RAMfournit ready-to-use AWSautorisations gérées que vous pouvez choisir d'associer à vos partages de ressources.

En utilisantAWS RAM, vous pouvez même partager certains types de ressources qui ne sont pas encore compatibles avec les politiques basées sur les ressources. Pour ces types de ressources,AWS RAMgénère automatiquement une politique basée sur les ressources en tant que représentation des autorisations réelles. Les utilisateurs peuvent consulter cette représentation en appelantGetResourcePolicy. Cela inclut les types de ressources suivants :

- Amazon Aurora — Clusters de base de données
- Amazon EC2 : réservations de capacité et hôtes dédiés
- AWS License Manager— Configurations de licence

- AWS Outposts— Tables de routage, avant-postes et sites des passerelles locales
- Amazon Route 53 — Règles de transfert
- Amazon Virtual Private Cloud : adresses IPv4, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit et domaines de multidiffusion de passerelles de transit appartenant au client

Exemples deAWS RAMpolitiques basées sur les ressources

Si vous partagez une ressource d'image EC2 Image Builder avec une personnecompte,AWS RAMgénère une politique semblable à l'exemple suivant et l'attache à toutes les ressources d'image incluses dans le partage de ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

Si vous partagez une ressource EC2 Image BuilderRôle ou utilisateur IAMdans un autreCompte AWS,AWS RAMgénère une politique semblable à l'exemple suivant et l'attache à toutes les ressources d'image incluses dans le partage de ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
```

```
      "Action": [
          "imagebuilder:GetImage",
          "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
  ]
}
```

Si vous partagez une ressource d'image EC2 Image Builder avec tous les comptes d'une organisation ou avec les comptes d'une unité d'organisation,AWS RAMgénère une politique semblable à l'exemple suivant et l'attache à toutes les ressources d'image incluses dans le partage de ressources.

> **Note**
>
> Cette politique utilise`"Principal": "*"`puis utilise le`"Condition"`élément pour restreindre les autorisations aux identités qui correspondent à la valeur spécifiée`PrincipalOrgID`. Pour plus d'informations, veuillez consulter Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
```

```
    ]
}
```

Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources

Lorsque vous incluez`"Principal": "*"`dans une politique basée sur les ressources, la politique accorde l'accès à tous les principaux IAM du compte contenant la ressource, sous réserve des restrictions imposées par un`Condition`élément, s'il existe. Explicite`Deny`les instructions de toute politique qui s'applique au principal appelant remplacent les autorisations accordées par cette politique. Cependant, unimplicite `Deny`(c'est-à-dire l'absence d'unexplicite `Allow`) dans toutes les politiques d'identité, politiques de limites d'autorisations ou politiques de session applicablespasaboutissent à`Deny`aux principaux autorisés à accéder à une action en vertu d'une telle politique basée sur les ressources.

Si ce comportement n'est pas souhaitable pour votre scénario, vous pouvez le limiter en ajoutant unexplicite `Deny`déclaration relative à une politique d'identité, à une limite d'autorisations ou à une politique de session qui affecte les rôles et les utilisateurs concernés.

Autorisations gérées

Les autorisations gérées définissent les actions que les principaux peuvent effectuer et dans quelles conditions sur les types de ressources pris en charge dans un partage de ressources. Lorsque vous pouvez créer un partage de ressources, vous pouvez spécifier l'autorisations gérées à utiliser pour chaque type de ressource inclus dans le partage de ressources. Une autorisation gérée répertorie l'ensemble de`actions`et`conditions`que les directeurs peuvent exécuter avec la ressource partagée à l'aide deAWS RAM.

Vous ne pouvez associer qu'une seule autorisation gérée pour chaque type de ressource dans un partage de ressources. Vous ne pouvez pas créer un partage de ressources dans lequel certaines ressources d'un certain type utilisent une autorisation gérée et d'autres ressources du même type utilisent une autorisation gérée différente. Pour ce faire, vous devez créer deux partages de ressources différents et répartir les ressources entre eux, en accordant à chaque ensemble une autorisation de gestion différente. Il existe deux types d'autorisations gérées :

AWSautorisations gérées

AWSles autorisations gérées sont créées et gérées parAWSet accordez des autorisations pour les scénarios clients courants.AWS RAMdéfinit au moins unAWSautorisation gérée pour chaque type de ressource pris en charge. Certains types de ressources en prennent en charge

plusieursAWSautorisation gérée, avec une autorisation gérée désignée commeAWSpar défaut. LedéfautAWSautorisation géréeest associé à moins que vous ne spécifiez le contraire.

Autorisations gérées par le client

Les autorisations gérées par le client sont des autorisations gérées que vous créez et gérez en spécifiant précisément quelles actions peuvent être effectuées, dans quelles conditions, les ressources étant partagées à l'aide deAWS RAM. Par exemple, vous souhaitez limiter l'accès en lecture à vos pools Amazon VPC IP Address Manager (IPAM), qui vous aident à gérer vos adresses IP à grande échelle. Vous pouvez créer des autorisations gérées par le client pour que vos développeurs puissent attribuer des adresses IP, mais vous ne pouvez pas consulter la plage d'adresses IP attribuées par d'autres comptes de développeurs. Vous pouvez suivre la meilleure pratique du moindre privilège, en n'accordant que les autorisations nécessaires pour effectuer des tâches sur des ressources partagées.

Vous définissez votre propre autorisation pour un type de ressource dans un partage de ressources avec la possibilité d'ajouter des conditions telles queClés contextuelles globalesetclés spécifiques au servicepour spécifier les conditions dans lesquelles les principaux ont accès à la ressource. Ces autorisations peuvent être utilisées dans un ou plusieursAWS RAMpartage. Les autorisations gérées par le client sont spécifiques à la région.

AWS RAMutilise les autorisations gérées comme entrée pour créer lepolitiques basées sur les ressourcespour les ressources que vous partagez.

Version d'autorisation gérée

Toute modification apportée à une autorisation gérée est représentée comme une nouvelle version de cette autorisation gérée. La nouvelle version est la version par défaut pour tous les nouveaux partages de ressources. Chaque autorisation gérée possède toujours une version désignée comme version par défaut. Lorsque vous ouAWScrée une nouvelle version d'autorisation gérée, vous devez explicitement mettre à jour l'autorisation gérée pour chaque partage de ressources existant. Vous pouvez évaluer les modifications avant de les appliquer à votre partage de ressources au cours de cette étape. Tous les nouveaux partages de ressources utiliseront automatiquement la nouvelle version de l'autorisation gérée pour le type de ressource correspondant.

AWSversions d'autorisations gérées

AWSgère toutes les modifications apportées àAWSautorisations gérées. Ces modifications répondent à de nouvelles fonctionnalités ou suppriment les défauts découverts. Vous ne pouvez appliquer la version d'autorisation gérée par défaut qu'à vos partages de ressources.

Versions d'autorisations gérées par le client

Vous gérez toutes les modifications apportées aux autorisations gérées par les clients. Vous pouvez créer une nouvelle version par défaut, définir une ancienne version comme version par défaut ou supprimer des versions qui ne sont plus associées à des partages de ressources. Chaque autorisations gérées par le client peut avoir jusqu'à cinq versions.

Lorsque vous créez ou mettez à jour un partage de ressources, vous ne pouvez joindre que la version par défaut de l'autorisation gérée spécifiée. Pour plus d'informations, veuillez consulter Mise àAWS niveau des autorisations gérées vers une version plus récente.

Partage de vos AWS ressources

Pour partager une ressource dont vous êtes propriétaire en utilisantAWS RAM, procédez comme suit :

- Activez le partage des ressources au sein de AWS Organizations (facultatif)
- Création d'un partage de ressources

Remarques

- Le partage d'une ressource avec des personnes extérieures au Compte AWS propriétaire de la ressource ne modifie pas les autorisations ou les quotas qui s'appliquent à la ressource dans le compte qui l'a créée.
- AWS RAMest un service régional. Les principaux partenaires avec lesquels vous partagez peuvent accéder aux partages de ressources uniquement dans le pays Régions AWS dans lequel ils ont été créés.
- Certaines ressources comportent des considérations particulières et des conditions préalables au partage. Pour en savoir plus, consultez Ressources partageables AWS.

Activez le partage des ressources au sein de AWS Organizations

Lorsque votre compte est géré parAWS Organizations, vous pouvez en profiter pour partager des ressources plus facilement. Avec ou sans Organizations, un utilisateur peut partager avec des comptes individuels. Toutefois, si votre compte appartient à une organisation, vous pouvez le partager avec des comptes individuels, ou avec tous les comptes de l'organisation ou d'une unité d'organisation sans avoir à énumérer chaque compte.

Pour partager des ressources au sein d'une organisation, vous devez d'abord utiliser la AWS RAM console ou AWS Command Line Interface (AWS CLI) pour activer le partage avecAWS Organizations. Lorsque vous partagez des ressources au sein de votre organisation, AWS RAM il n'envoie pas d'invitations aux principaux. Les responsables de votre organisation ont accès aux ressources partagées sans avoir à échanger d'invitations.

Lorsque vous activez le partage des ressources au sein de votre organisation, AWS RAM crée un rôle lié à un service appelé. **`AWSServiceRoleForResourceAccessManager`** Ce rôle ne peut être assumé que par le AWS RAM service et accorde AWS RAM l'autorisation de récupérer des informations sur l'organisation dont il est membre, à l'aide de la politique AWS géréeAWSResourceAccessManagerServiceRolePolicy.

Si vous n'avez plus besoin de partager des ressources avec l'ensemble de votre organisation ou de vos unités d'organisation, vous pouvez désactiver le partage des ressources. Pour en savoir plus, consultez Désactiver le partage de ressources avec AWS Organizations.

Autorisations minimales

Pour exécuter les procédures ci-dessous, vous devez vous connecter en tant que principal au compte de gestion de l'organisation disposant des autorisations suivantes :

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

Prérequis

- Vous ne pouvez effectuer ces étapes que lorsque vous êtes connecté en tant que principal dans le compte de gestion de l'organisation.

- Toutes les fonctionnalités de l'organisation doivent être activées. Pour plus d'informations, consultez la section Activation de toutes les fonctionnalités de votre organisation dans le Guide de AWS Organizations l'utilisateur.

> **Important**
>
> Vous devez activer le partage avec à AWS Organizations l'aide de la AWS RAM console ou de la AWS CLI commande enable-sharing-with-aws-organization. Cela garantit que le`AWSServiceRoleForResourceAccessManager` rôle lié à un service est créé. Si vous activez l'accès sécurisé à l'aide AWS Organizations de la AWS Organizations console ou de la enable-aws-service-accessAWS CLIcommande, le rôle `AWSServiceRoleForResourceAccessManager` lié au service n'est pas créé et vous ne pouvez pas partager de ressources au sein de votre organisation.

Console

Pour activer le partage des ressources au sein de votre organisation

1. Ouvrez la page Paramètres dans la AWS RAM console.
2. Sélectionnez Activer le partage avec AWS Organizations, puis Enregistrer les paramètres.

AWS CLI

Pour activer le partage des ressources au sein de votre organisation

Utilisez la commande enable-sharing-with-aws-organization.

Cette commande peut être utilisée dans n'importe quelle régionRégion AWS, et elle permet le partage avec AWS Organizations toutes les régions prises en charge. AWS RAM

```
$ aws ram enable-sharing-with-aws-organization
{
    "returnValue": true
}
```

Création d'un partage de ressources

Pour partager des ressources dont vous êtes propriétaire, créez un partage de ressources. Voici la procédure générale :

1. Ajoutez les ressources que vous souhaitez partager.
2. Pour chaque type de ressource que vous incluez dans le partage, spécifiez l'autorisation gérée à utiliser pour ce type de ressource.
   - Vous pouvez choisir entre l'une des autorisations AWS gérées disponibles, une autorisation gérée par le client existante ou créer une nouvelle autorisation gérée par le client.
   - AWSles autorisations gérées sont créées par AWS pour couvrir les cas d'utilisation standard.
   - Les autorisations gérées par le client vous permettent de personnaliser vos propres autorisations gérées pour répondre à vos besoins commerciaux et de sécurité.

   > **Note**
   >
   > Si l'autorisation gérée sélectionnée comporte plusieurs versions, elle associe AWS RAM automatiquement la version par défaut. Vous ne pouvez joindre que la version désignée par défaut.

3. Spécifiez les principaux auxquels vous souhaitez avoir accès aux ressources.

Considérations

- Si vous devez ultérieurement supprimer une AWS ressource que vous avez incluse dans un partage, nous vous recommandons de supprimer d'abord la ressource de tout partage de ressources qui l'inclut ou de supprimer le partage de ressources.
- Les types de ressources que vous pouvez inclure dans un partage de ressources sont répertoriés surRessources partageables AWS.
- Vous ne pouvez partager une ressource que si elle vous appartient. Vous ne pouvez pas partager une ressource partagée avec vous.
- AWS RAMest un service régional. Lorsque vous partagez une ressource avec des principaux d'autres entitésComptes AWS, ces derniers doivent accéder à chaque ressource depuis la même source Région AWS que celle dans laquelle elle a été créée. Pour les ressources globales prises en charge, vous pouvez accéder à ces ressources à partir de toutes Région AWS les ressources prises en charge par la console de service et les outils de cette ressource. Vous pouvez consulter

ces partages de ressources et leurs ressources globales dans la AWS RAM console et les outils uniquement dans la région d'origine désignée, à savoir l'est des États-Unis (Virginie du Nord)`us-east-1`. Pour plus d'informations AWS RAM et pour obtenir des ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.

- Si le compte à partir duquel vous partagez fait partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, tous les directeurs de l'organisation avec lesquels vous partagez des ressources sont automatiquement autorisés à accéder aux partages de ressources sans avoir à recourir à des invitations. Le responsable d'un compte avec lequel vous partagez des ressources en dehors du contexte d'une organisation reçoit une invitation à rejoindre le partage des ressources et n'a accès aux ressources partagées qu'après avoir accepté l'invitation.
- Si vous partagez avec un directeur de service, vous ne pouvez associer aucun autre principal au partage de ressources.
- Si le partage s'effectue entre des comptes ou des principaux membres d'une organisation, toute modification apportée à l'adhésion à l'organisation affecte de manière dynamique l'accès au partage des ressources.
  - Si vous ajoutez Compte AWS à l'organisation ou à une unité d'organisation ayant accès à un partage de ressources, ce nouveau compte de membre accède automatiquement au partage de ressources. L'administrateur du compte avec lequel vous avez partagé peut ensuite autoriser les principaux de ce compte à accéder aux ressources de ce partage.
  - Si vous supprimez un compte de l'organisation ou une unité d'organisation ayant accès à un partage de ressources, tous les principaux de ce compte perdent automatiquement l'accès aux ressources accessibles via ce partage de ressources.
  - Si vous avez partagé directement avec un compte membre ou avec des rôles ou utilisateurs IAM dans le compte membre, puis que vous supprimez ce compte de l'organisation, tous les principaux de ce compte perdent l'accès aux ressources accessibles via ce partage de ressources.

> **Important**
>
> Lorsque vous partagez avec une organisation ou une unité d'organisation, et que cette étendue inclut le compte propriétaire du partage de ressources, tous les principaux du compte de partage ont automatiquement accès aux ressources du partage. L'accès accordé est défini par les autorisations gérées associées au partage. Cela est dû au fait que la politique basée sur les ressources qui AWS RAM s'attache à chaque ressource

du partage utilise. `"Principal": "*"` Pour en savoir plus, consultez Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.
Les directeurs des autres comptes consommateurs n'ont pas immédiatement accès aux ressources de l'action. Les administrateurs des autres comptes doivent d'abord associer des politiques d'autorisation basées sur l'identité aux principaux appropriés. Ces politiques doivent accorder `Allow` l'accès aux ARN des ressources individuelles du partage de ressources. Les autorisations définies dans ces politiques ne peuvent pas dépasser celles spécifiées dans l'autorisation gérée associée au partage de ressources.

- Vous ne pouvez ajouter que l'organisation dont votre compte est membre et les unités d'organisation de cette organisation à vos partages de ressources. Vous ne pouvez pas ajouter des unités d'organisation ou des organisations extérieures à votre propre organisation à un partage de ressources en tant que principaux. Toutefois, vous pouvez ajouter des rôles IAM individuels Comptes AWS ou, pour les services pris en charge, des rôles IAM et des utilisateurs extérieurs à votre organisation en tant que principaux d'un partage de ressources.

  Note

  Les types de ressource ne peuvent pas tous être partagés avec les utilisateurs et les rôles IAM. Pour plus d'informations sur les ressources que vous pouvez partager avec ces responsables, consultezRessources partageables AWS.

- Pour les types de ressources suivants, vous avez sept jours pour accepter l'invitation à rejoindre le partage pour les types de ressources suivants. Si vous n'acceptez pas l'invitation avant son expiration, elle est automatiquement refusée.

  Important

  Pour les types de ressources partagées ne figurant pas dans la liste suivante, vous avez 12 heures pour accepter l'invitation à rejoindre le partage de ressources. Au bout de 12 heures, l'invitation expire et l'utilisateur final principal du partage de ressources est dissocié. L'invitation ne peut plus être acceptée par les utilisateurs finaux.

  - Amazon Aurora — Clusters de bases de données
  - Amazon EC2 : réservations de capacité et hôtes dédiés
  - AWS License Manager— Configurations de licence

- AWS Outposts— Tables de routage, avant-postes et sites des passerelles locales
- Amazon Route 53 — Règles de transfert
- Amazon VPC : adresses IPv4, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit, domaines de multidiffusion des passerelles de transit

Console

Pour créer un partage de ressources

1. Ouvrez la console AWS RAM.
2. Étant donné que les partages de AWS RAM ressources existent de manière spécifiqueRégions AWS, choisissez le partage approprié Région AWS dans la liste déroulante située dans le coin supérieur droit de la console. Pour voir les partages de ressources contenant des ressources globales, vous devez Région AWS définir la valeur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales. Si vous souhaitez inclure des ressources mondiales dans le partage des ressources, vous devez choisir la région d'origine désignée, USA Est (Virginie du Nord)`us-east-1`.
3. Si vous êtes nouveau dans ce AWS RAM domaine, choisissez Créer un partage de ressources sur la page d'accueil. Sinon, choisissez Créer un partage de ressources sur la page Partagé par moi : partages de ressources.
4. À l'étape 1 : Spécifier les détails du partage des ressources, procédez comme suit :

   a. Dans Nom, entrez un nom descriptif pour le partage de ressources.

   b. Sous Ressources, choisissez les ressources à ajouter au partage de ressources comme suit :

      - Pour Sélectionner le type de ressource, choisissez le type de ressource à partager. Cela filtre la liste des ressources partageables uniquement pour les ressources du type sélectionné.
      - Dans la liste des ressources qui s'affiche, cochez les cases à côté des ressources individuelles que vous souhaitez partager. Les ressources sélectionnées sont déplacées sous Ressources sélectionnées.

Si vous partagez des ressources associées à une zone de disponibilité spécifique, l'utilisation de l'ID de zone de disponibilité (AZ ID) vous permet de déterminer l'emplacement relatif de ces ressources sur tous les comptes. Pour en savoir plus, consultez Identifiants de zone de disponibilité pour vosAWS ressources.

c. (Facultatif) Pour associer des balises au partage de ressources, sous Balises, entrez une clé et une valeur de balise. Ajoutez-en d'autres en choisissant Ajouter un nouveau tag. Répétez cette étape si nécessaire. Ces balises s'appliquent uniquement au partage de ressources lui-même, et non aux ressources du partage de ressources.

5. Choisissez Suivant.

6. À l'étape 2 : associer une autorisation gérée à chaque type de ressource, vous pouvez choisir d'associer une autorisation gérée créée par AWS au type de ressource, choisir une autorisation gérée par le client existante ou créer votre propre autorisation gérée par le client pour les types de ressources pris en charge. Pour en savoir plus, consultez Types d'autorisations gérées.

   Choisissez Créer une autorisation gérée par le client pour créer une autorisation gérée par le client qui répond aux exigences de votre cas d'utilisation du partage. Pour de plus amples informations, veuillez consulter Créer une autorisation gérée par le client. Une fois le processus terminé, choisissez,

   puis vous pouvez sélectionner l'autorisation gérée par votre nouveau client dans la liste déroulante Autorisations gérées.

   > **Note**
   >
   > Si l'autorisation gérée sélectionnée comporte plusieurs versions, elle associe AWS RAM automatiquement la version par défaut. Vous ne pouvez joindre que la version désignée par défaut.

   Pour afficher les actions autorisées par l'autorisation gérée, développez Afficher le modèle de politique pour cette autorisation gérée.

7. Choisissez Suivant.

8. À l'étape 3 : Accorder l'accès aux principaux, procédez comme suit :

a. Par défaut, l'option Autoriser le partage avec n'importe qui est sélectionnée, ce qui signifie que, pour les types de ressources compatibles, vous pouvez partager des ressources extérieures à votre organisation. Comptes AWS Cela n'affecte pas les types de ressources qui ne peuvent être partagés qu'au sein d'une organisation, tels que les sous-réseaux Amazon VPC. Vous pouvez également partager certains types de ressources pris en charge avec des rôles et des utilisateurs IAM.

   Pour limiter le partage des ressources aux seuls comptes et aux principaux de votre organisation, choisissez Autoriser le partage uniquement au sein de votre organisation.

b. Pour les directeurs, procédez comme suit :

   - Pour ajouter l'organisation, une unité organisationnelle (UO) ou une unité Compte AWS faisant partie d'une organisation, activez Afficher la structure organisationnelle. Cela affiche une vue arborescente de votre organisation. Cochez ensuite la case à côté de chaque principal que vous souhaitez ajouter.

     > **Important**
     >
     > Lorsque vous partagez avec une organisation ou une unité d'organisation, et que cette étendue inclut le compte propriétaire du partage de ressources, tous les principaux du compte de partage ont automatiquement accès aux ressources du partage. L'accès accordé est défini par les autorisations gérées associées au partage. Cela est dû au fait que la politique basée sur les ressources qui AWS RAM s'attache à chaque ressource du partage utilise. `"Principal": "*"` Pour en savoir plus, consultez Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.
     > Les directeurs des autres comptes consommateurs n'ont pas immédiatement accès aux ressources de l'action. Les administrateurs des autres comptes doivent d'abord associer des politiques d'autorisation basées sur l'identité aux principaux appropriés. Ces politiques doivent accorder `Allow` l'accès aux ARN des ressources individuelles du partage de ressources. Les autorisations définies dans ces politiques ne peuvent pas dépasser celles spécifiées dans l'autorisation gérée associée au partage de ressources.

   - Si vous sélectionnez l'organisation (l'ID commence paro-), les Comptes AWS principaux membres de l'organisation peuvent accéder au partage des ressources.

- Si vous sélectionnez une unité d'organisation (l'ID commence parou-), les principaux de l'ensemble de cette unité d'Comptes AWSorganisation et de ses unités d'organisation secondaires peuvent accéder au partage de ressources.
- Si vous sélectionnez une personneCompte AWS, seuls les principaux de ce compte peuvent accéder au partage des ressources.

> **Note**
>
> Le bouton Afficher la structure organisationnelle apparaît uniquement si le partage avec AWS Organizations est activé et si vous êtes connecté au compte de gestion de l'organisation.
> Vous ne pouvez pas utiliser cette méthode pour spécifier un rôle ou un utilisateur Compte AWS externe à votre organisation, ni un rôle ou un utilisateur IAM. Vous devez plutôt désactiver Afficher la structure organisationnelle et utiliser la liste déroulante et la zone de texte pour saisir l'ID ou l'ARN.

- Pour spécifier un principal par ID ou ARN, y compris les principaux extérieurs à l'organisation, sélectionnez le type de principal pour chaque principal. Entrez ensuite l'ID (pour une organisation ou une Compte AWS unité d'organisation) ou l'ARN (pour un rôle ou un utilisateur IAM), puis choisissez Ajouter. Les principaux types et formats d'ID et d'ARN disponibles sont les suivants :
  - Compte AWS— Pour ajouter unCompte AWS, entrez l'identifiant de compte à 12 chiffres. Par exemple :

    ```
    123456789012
    ```

  - Organisation : pour ajouter tous les éléments Comptes AWS de votre organisation, entrez l'ID de l'organisation. Par exemple :

    ```
    o-abcd1234
    ```

  - Unité organisationnelle (UO) : pour ajouter une UO, entrez son ID. Par exemple :

    ```
    ou-abcd-1234efgh
    ```

  - Rôle IAM : pour ajouter un rôle IAM, entrez l'ARN du rôle. Utilisez la syntaxe suivante :

    ```
    arn:partition:iam::account:role/role-name
    ```

Par exemple :

```
arn:aws:iam::123456789012:role/MyS3AccessRole
```

> **Note**
>
> Pour obtenir l'ARN unique d'un rôle IAM, consultez la liste des rôles dans la console IAM, utilisez la AWS CLI commande get-role ou l'action API. GetRole

- Utilisateur IAM : pour ajouter un utilisateur IAM, entrez son ARN. Utilisez la syntaxe suivante :

  ```
  arn:partition:iam::account:user/user-name
  ```

  Par exemple :

  ```
  arn:aws:iam::123456789012:user/bob
  ```

  > **Note**
  >
  > Pour obtenir l'ARN unique d'un utilisateur IAM, consultez la liste des utilisateurs dans la console IAM, utilisez la get-userAWS CLIcommande ou l'action de l'GetUserAPI.

- Principal de service — Pour ajouter un principal de service, choisissez Service principal dans la boîte de dialogue Sélectionner le type de principal. Entrez le nom du directeur du AWS service. Utilisez la syntaxe suivante :
  - *service-id*.amazonaws.com

    Par exemple :

    ```
    pca-connector-ad.amazonaws.com
    ```

c. Pour les principes sélectionnés, vérifiez que les principaux que vous avez spécifiés apparaissent dans la liste.

9. Choisissez Suivant.

10. À l'étape 4 : Révision et création, passez en revue les détails de configuration de votre partage de ressources. Pour modifier la configuration d'une étape, choisissez le lien correspondant à l'étape à laquelle vous souhaitez revenir et apportez les modifications requises.
11. Après avoir passé en revue le partage de ressources, choisissez Créer un partage de ressources.

    L'association entre la ressource et le mandataire peut prendre quelques minutes. Laissez ce processus se terminer avant d'essayer d'utiliser le partage de ressources.
12. Vous pouvez ajouter et supprimer des ressources et des principes ou appliquer des balises personnalisées à votre partage de ressources à tout moment. Vous pouvez modifier l'autorisation gérée pour les types de ressources inclus dans votre partage de ressources, pour les types qui prennent en charge plus que l'autorisation gérée par défaut. Vous pouvez supprimer votre partage de ressources lorsque vous ne souhaitez plus partager les ressources. Pour en savoir plus, consultez PartagezAWS les ressources que vous possédez.

AWS CLI

Pour créer un partage de ressources

Utilisez la commande create-resource-share. La commande suivante crée un partage de ressources qui est partagé avec tous les membres Comptes AWS de l'organisation. Le partage contient une configuration de AWS License Manager licence et accorde les autorisations gérées par défaut pour ce type de ressource.

> **Note**
>
> Si vous souhaitez utiliser une autorisation gérée par le client avec un type de ressource dans ce partage de ressources, vous pouvez soit utiliser une autorisation gérée par le client existante, soit créer une nouvelle autorisation gérée par le client. Notez l'ARN de l'autorisation gérée par le client, puis créez le partage de ressources. Pour plus d'informations, consultez Créer une autorisation gérée par le client.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
```

```
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

Utilisation deAWS ressources partagées

Pour commencer à utiliser les ressources qui ont été partagées avec votre compte viaAWS Resource Access Manager, effectuez les tâches suivantes.

Tâches

- Répond à l'invitation de partage des ressources.
- Utilisez les ressources qui sont partagées avec vous

Répond à l'invitation de partage des ressources.

Si vous recevez une invitation à rejoindre un partage des ressources, vous devez l'accepter.

Les invitations ne sont pas utilisées dans les scénarios suivants :

- Si vous faites partie d'une organisation dansAWS Organizations et que le partage au sein de votre organisation est activé, les utilisateurs de l'organisation ont automatiquement accès aux ressources partagées.
- Si vous partagez avecCompte AWS le propriétaire de la ressource, les responsables de ce compte ont automatiquement accès aux ressources partagées sans invitation.

Console

Pour répondre aux invitations

1. Ouvrez la page Partagé avec moi : partages de ressources dans laAWS RAM console.

   > **Note**
   >
   > Un partage de ressources n'est visible queRégion AWS dans l'endroit où il a été créé. Si un partage de ressources attendu n'apparaît pas dans la console, vous devrez peut-être passer à un autre àRégion AWS l'aide de la commande déroulante située dans le coin supérieur droit.

2. Consultez la liste des partages de ressources auxquels vous avez accès.

   La colonne État indique votre statut de participation actuel pour le partage de ressources. LePending statut indique que vous avez été ajouté à un partage de ressources, mais que vous n'avez pas encore accepté ou rejeté l'invitation.

3. Pour répondre à l'invitation au partage de ressources, sélectionnez l'ID du partage de ressources et choisissez Accepter le partage de ressources pour accepter l'invitation, ou Rejeter le partage de ressources pour refuser l'invitation. Si vous rejetez l'invitation, vous n'aurez pas accès aux ressources. Si vous acceptez l'invitation, vous aurez accès aux ressources.

AWS CLI

Pour commencer, consultez la liste des invitations à partager des ressources qui vous sont proposées. L'exemple de commande suivant a été exécuté dans laus-west-2 région et indique qu'un partage de ressources est disponible dansPENDING cet État.

```
$ aws ram get-resource-share-invitations
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
            "resourceShareName": "MyNewResourceShare",
            "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
            "senderAccountId": "111122223333",
```

```
            "receiverAccountId": "444455556666",
            "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
            "status": "PENDING"
        }
    ]
}
```

Vous pouvez utiliser le nom de ressource Amazon (ARN) de l'invitation de la commande précédente comme paramètre dans la commande suivante pour accepter cette invitation.

```
$ aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
        "resourceShareName": "MyNewResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
        "senderAccountId": "111122223333",
        "receiverAccountId": "444455556666",
        "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
        "status": "ACCEPTED"
    }
}
```

La sortie indique que le`status` a été remplacé par`ACCEPTED`. Les ressources incluses dans ce partage de ressources sont désormais mises à la disposition des mandants sur le compte d'acceptation.

Utilisez les ressources qui sont partagées avec vous

Une fois que vous avez accepté l'invitation à rejoindre un partage de ressources, vous pouvez effectuer des actions spécifiques sur les ressources partagées. Ces actions varient selon le type de ressource. Pour plus d'informations, veuillez consulter Ressources partageables AWS. Les ressources sont disponibles directement dans la console de service et les opérations API/CLI de chaque ressource. Si la ressource est régionale, vous devez utiliser la bonneRégion AWS dans la console de service ou dans la commande API/CLI. Si la ressource est globale, vous devez utiliser la région d'origine désignée, USA Est (Virginie du Nord).`us-east-1` Pour afficher la ressource

dansAWS RAM, vous devez ouvrir laAWS RAM console dansRégion AWS laquelle le partage de ressources a été créé.

Utilisation deAWS ressources partagées

Vous pouvez utiliserAWS Resource Access Manager (AWS RAM) pour partagerAWS des ressources qui vous appartiennent et accéder àAWS des ressources partagées avec vous.

Table des matières

Partage des ressources régionales par rapport aux ressources mondiales

Cette rubrique décrit les différences entre la façon dont AWS Resource Access Manager (AWS RAM) fonctionne avec les ressources régionales et mondiales.

Les ressources sont régionales ou mondiales. Vous pouvez utiliser le quatrième champ de l'Amazon Resource Name (ARN) pour déterminer si une ressource est régionale ou globale. Les ressources régionales montrent leRégion AWS. S'il est vide, la ressource est globale.

Quelles sont les différences entre les ressources régionales et mondiales ?

Ressources régionales

La plupart des ressources que vous pouvez partager AWS RAM sont régionales. Vous les créez dans une région spécifiéeRégion AWS, puis ils existent dans cette région. Pour voir ou interagir avec ces ressources, vous devez diriger vos opérations vers cette région. Par exemple, pour créer une instance Amazon Elastic Compute Cloud (Amazon EC2) avec leAWS Management Console, vous choisissez Région AWS celui dans lequel vous souhaitez créer l'instance. Si vous utilisez le AWS Command Line Interface (AWS CLI) pour créer l'instance, vous incluez le `--region` paramètre. Les AWS SDK disposent chacun de leur propre mécanisme équivalent pour spécifier la région utilisée par l'opération.

Il existe plusieurs raisons d'utiliser les ressources régionales. L'une des bonnes raisons est de vous assurer que les ressources et les points de terminaison de service que vous utilisez pour y accéder sont aussi proches que possible du client. Cela améliore les performances en minimisant la latence. Une autre raison est de fournir une limite d'isolation. Cela vous permet de créer des copies indépendantes des ressources dans plusieurs régions afin de répartir la charge et d'améliorer l'évolutivité. Dans le même temps, il isole les ressources les unes des autres pour améliorer la disponibilité.

Si vous en spécifiez une autre Région AWS dans la console ou dans une AWS CLI commande, vous ne pouvez plus voir ni interagir avec les ressources que vous pouviez voir dans la région précédente.

Lorsque vous examinez le nom de ressource Amazon (ARN) d'une ressource régionale, la région qui contient la ressource est spécifiée comme quatrième champ de l'ARN. Par exemple, une instance Amazon EC2 est une ressource régionale. Ces ressources ont des ARN qui ressemblent à l'exemple suivant pour un VPC existant dans la `us-east-1` région.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Ressources mondiales

Certains AWS services prennent en charge des ressources auxquelles vous pouvez accéder dans le monde entier, ce qui signifie que vous pouvez utiliser ces ressources où que vous soyez.

Vous ne spécifiez pas de Région AWS dans la console d'un service global. Pour accéder à une ressource globale, vous ne spécifiez aucun `--region` paramètre lorsque vous utilisez les opérations du service AWS CLI et du AWS SDK.

Les ressources globales prennent en charge les cas où il est essentiel qu'une seule instance d'une ressource particulière puisse exister à la fois. Dans de tels scénarios, la réplication ou la synchronisation entre des copies de différentes régions ne sont pas adéquates. Le fait de devoir accéder à un point de terminaison global unique, avec l'augmentation possible de la latence, est considéré comme acceptable pour garantir que toute modification soit instantanément visible pour les utilisateurs de la ressource. Par exemple, lorsque vous créez un réseau central AWS Cloud WAN en tant que ressource globale, il est cohérent pour tous les utilisateurs. Il apparaît comme un réseau mondial unique et contigu couvrant toutes les régions.

Le nom de ressource Amazon (ARN) d'une ressource globale n'inclut pas de région. Le quatrième champ d'un tel ARN est vide, comme l'exemple d'ARN suivant pour un réseau central Cloud WAN.

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

Les partages de ressources et leurs régions

AWS RAMest un service régional et un partage de ressources est régional. Par conséquent, un partage de ressources peut contenir des ressources provenant de la même source Région AWS que le partage de ressources, ainsi que toutes les ressources globales prises en charge. La région dans laquelle vous créez le partage de ressources est la région d'origine du partage de ressources.

> **Important**
>
> Actuellement, vous pouvez créer des partages de ressources avec des ressources globales uniquement dans la région d'origine désignée, région USA Est (Virginie du Nord),`us-east-1`. Bien que vous ne puissiez créer le partage de ressources que dans cette région d'origine unique, toute ressource globale partagée apparaît comme une ressource globale standard lorsqu'elle est affichée dans la console ou dans les opérations CLI et SDK de ce service. La restriction à la région d'origine s'applique uniquement au partage de ressources, et non aux ressources qu'il contient.

Pour partager une ressource régionale que vous avez créée dans la `us-west-2` région, vous devez configurer la AWS RAM console pour utiliser `us-west-2` et créer le partage de ressources dans cette région. Vous ne pouvez pas créer un partage de ressources incluant des ressources régionales provenant de différentes sourcesRégions AWS. Cela signifie que pour partager des ressources provenant des deux `us-west-2` et`eu-north-1`, vous devez créer deux partages de ressources différents. Vous ne pouvez pas combiner des ressources provenant de deux régions différentes en un seul partage de ressources.

Pour partager une ressource globale dans la AWS RAM console, vous devez configurer la AWS RAM console pour qu'elle utilise la région d'origine désignée, USA Est (Virginie du Nord)`us-east-1`. Créez ensuite le partage de ressources dans la région d'origine désignée. Vous pouvez mélanger des ressources globales dans un partage de ressources uniquement avec des ressources de la `us-east-1` région.

Même si la ressource globale est visible dans un partage de AWS RAM ressources situé uniquement dans la région d'origine désignée, elle reste une ressource globale une fois que vous l'avez partagée. Vous pouvez y accéder dans le partagé Comptes AWS depuis n'importe quelle région à partir de laquelle vous pouviez y accéder dans l'originalCompte AWS.

Considérations

- Pour créer un partage de ressources dans la AWS RAM console, vous devez utiliser la région qui contient les ressources que vous souhaitez partager. Si vous souhaitez inclure une ressource globale, vous devez utiliser la région d'origine désignée pour créer le partage. Par exemple, pour partager un réseau principal AWS Cloud WAN, vous devez créer le partage de ressources dans la `us-east-1` région.
- Pour afficher ou modifier un partage de ressources dans la AWS RAM console, vous devez utiliser la région qui contient le partage de ressources. De même, les opérations du SDK AWS RAM AWS CLI et vous permettent d'interagir uniquement avec les partages de ressources situés dans la région que vous avez spécifiée dans votre opération. Pour afficher ou modifier les partages de ressources qui contiennent des ressources globales, vous devez utiliser la région d'origine désignée, USA Est (Virginie du Nord)`us-east-1`.
- Pour afficher une ressource régionale dans la AWS RAM console afin de l'inclure dans un partage de ressources, vous devez utiliser la région qui contient la ressource régionale.
- Pour afficher une ressource globale dans la AWS RAM console et l'inclure dans un partage de ressources, vous devez utiliser la région d'origine désignée, USA Est (Virginie du Nord)`us-east-1`.

- Vous pouvez créer un partage de ressources avec des ressources régionales et mondiales uniquement dans la région d'origine désignée, USA Est (Virginie du Nord)`us-east-1`.

PartagezAWS les ressources que vous possédez

Vous pouvez utiliserAWS Resource Access Manager (AWS RAM) pour partager les ressources que vous spécifiez avec les principes que vous spécifiez. Cette section explique comment créer de nouveaux partages de ressources, modifier des partages de ressources existants et supprimer des partages de ressources dont vous n'avez plus besoin.

Rubriques

Affichage des partages de ressources que vous avez créés dansAWS RAM

Vous pouvez afficher la liste des partages de ressources que vous avez créés. Vous pouvez voir les ressources que vous partagez et les personnes avec lesquelles elles sont partagées.

Console

Pour consulter vos partages de ressources

1. Ouvrez la page Partagée par moi : partages de ressources dans laAWS RAM console.
2. Comme les partages deAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la appropriée dans le coin supérieur droit de la console. Pour afficher les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur USA Est (Virginie du Nord), (`us-east-1`). Pour en savoir plus sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Si l'une des autorisations gérées utilisées par les partages de ressources dans les résultats comporte une nouvelle version de l'autorisation gérée désignée comme valeur par défaut, la

page affiche une bannière pour vous avertir. Vous pouvez choisir de mettre à jour toutes les versions d'autorisations gérées en une seule fois en choisissant Réviser et tout mettre à jour en haut de la page.

Sinon, pour les partages de ressources individuels avec une ou plusieurs nouvelles versions d'autorisations gérées, la colonne État affiche Mise à jour disponible. Le choix de ce lien lance le processus de révision des versions d'autorisations gérées mises à jour et vous permet de les attribuer en tant que versions pour les types de ressources pertinents dans ce partage de ressources unique.

4. (Facultatif) Appliquez un filtre pour rechercher des partages de ressources spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche. Vous pouvez saisir un mot clé, par exemple une partie du nom d'un partage de ressources, pour répertorier uniquement les partages de ressources qui incluent ce texte dans le nom. Choisissez la zone de texte pour afficher la liste déroulante des champs attributaires suggérés. Après en avoir sélectionné une, vous pouvez choisir parmi la liste des valeurs disponibles pour ce champ. Vous pouvez ajouter d'autres attributs ou mots clés jusqu'à ce que vous trouviez la ressource recherchée.
5. Choisissez le nom du partage de ressources à vérifier. La console affiche les informations suivantes concernant le partage de ressources :

   - Résumé : indique le nom du partage de ressources, son identifiant, son propriétaire, le nom de la ressource Amazon (ARN), la date de création, indique si le partage avec des comptes externes est autorisé et son état actuel.
   - Autorisations gérées : répertorie les autorisations gérées associées à ce partage de ressources. Il ne peut y avoir qu'une autorisation gérée par type de ressource inclus dans le partage de ressources. Chaque autorisation gérée affiche la version de cette autorisation gérée associée au partage de ressources. S'il ne s'agit pas de la version par défaut, la console affiche un lien Mettre à jour vers la version par défaut. Si vous choisissez ce lien, vous avez la possibilité de mettre à jour le partage de ressources pour utiliser la version par défaut.
   - Ressources partagées : répertorie les ressources individuelles incluses dans le partage de ressources. Choisissez l'ID d'une ressource pour ouvrir un nouvel onglet de navigateur afin d'afficher la ressource dans la console de son service natif.
   - Responsables partagés : répertorie les principaux responsables avec lesquels les ressources sont partagées.

- Balises : répertorie les paires clé-valeur associées au partage de ressources lui-même ; il ne s'agit pas des balises attachées aux ressources individuelles incluses dans le partage de ressources.

AWS CLI

Pour consulter vos partages de ressources

Vous pouvez utiliser la get-resource-sharescommande avec le paramètre`--resource-owner` défini pour`SELF` afficher les détails des partages de ressources créés dans votreCompte AWS.

L'exemple suivant montre les partages de ressources qui sont partagés dans le currentRégion AWS (`us-east-1`) pour l'appelCompte AWS. Pour obtenir les partages de ressources créés dans une autre région, utilisez le`--region` *<region-code>* paramètre. Pour inclure des partages de ressources contenant des ressources globales, vous devez spécifier la région USA Est (Virginie du Nord),`us-east-1`.

```
$  aws ram get-resource-shares \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "name": "MyLicenseConfigShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
```

```
            "featureSet": "STANDARD"
        }
    ]
}
```

Création d'un partage de ressources dans AWS RAM

Pour partager des ressources dont vous êtes propriétaire, créez un partage de ressources. Voici la procédure générale :

1. Ajoutez les ressources que vous souhaitez partager.
2. Pour chaque type de ressource que vous incluez dans le partage, spécifiez l'autorisation gérée à utiliser pour ce type de ressource.
   - Vous pouvez choisir entre l'une des autorisations AWS gérées disponibles, une autorisation gérée par le client existante ou créer une nouvelle autorisation gérée par le client.
   - AWSles autorisations gérées sont créées par AWS pour couvrir les cas d'utilisation standard.
   - Les autorisations gérées par le client vous permettent de personnaliser vos propres autorisations gérées pour répondre à vos besoins commerciaux et de sécurité.

   > **Note**
   >
   > Si l'autorisation gérée sélectionnée comporte plusieurs versions, elle associe AWS RAM automatiquement la version par défaut. Vous ne pouvez joindre que la version désignée par défaut.

3. Spécifiez les principaux auxquels vous souhaitez avoir accès aux ressources.

Considérations

- Si vous devez ultérieurement supprimer une AWS ressource que vous avez incluse dans un partage, nous vous recommandons de supprimer d'abord la ressource de tout partage de ressources qui l'inclut ou de supprimer le partage de ressources.
- Les types de ressources que vous pouvez inclure dans un partage de ressources sont répertoriés surRessources partageables AWS.
- Vous ne pouvez partager une ressource que si elle vous appartient. Vous ne pouvez pas partager une ressource partagée avec vous.

- AWS RAMest un service régional. Lorsque vous partagez une ressource avec des responsables d'autres entitésComptes AWS, ces derniers doivent accéder à chaque ressource depuis la même source Région AWS que celle dans laquelle elle a été créée. Pour les ressources globales prises en charge, vous pouvez accéder à ces ressources à partir de toutes Région AWS les ressources prises en charge par la console de service et les outils de cette ressource. Vous pouvez consulter ces partages de ressources et leurs ressources globales dans la AWS RAM console et les outils uniquement dans la région d'origine désignée, à savoir l'est des États-Unis (Virginie du Nord)`us-east-1`. Pour plus d'informations AWS RAM et pour obtenir des ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
- Si le compte à partir duquel vous partagez fait partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, tous les directeurs de l'organisation avec lesquels vous partagez des ressources sont automatiquement autorisés à accéder aux partages de ressources sans avoir à recourir à des invitations. Le responsable d'un compte avec lequel vous partagez des ressources en dehors du contexte d'une organisation reçoit une invitation à rejoindre le partage des ressources et n'a accès aux ressources partagées qu'après avoir accepté l'invitation.
- Si vous partagez avec un directeur de service, vous ne pouvez associer aucun autre principal au partage de ressources.
- Si le partage s'effectue entre des comptes ou des principaux membres d'une organisation, toute modification apportée à l'adhésion à l'organisation affecte de manière dynamique l'accès au partage des ressources.
  - Si vous ajoutez Compte AWS à l'organisation ou à une unité d'organisation ayant accès à un partage de ressources, ce nouveau compte de membre accède automatiquement au partage de ressources. L'administrateur du compte avec lequel vous avez partagé peut ensuite autoriser les principaux de ce compte à accéder aux ressources de ce partage.
  - Si vous supprimez un compte de l'organisation ou une unité d'organisation ayant accès à un partage de ressources, tous les principaux de ce compte perdent automatiquement l'accès aux ressources accessibles via ce partage de ressources.
  - Si vous avez partagé directement avec un compte membre ou avec des rôles ou utilisateurs IAM dans le compte membre, puis que vous supprimez ce compte de l'organisation, tous les principaux de ce compte perdent l'accès aux ressources accessibles via ce partage de ressources.

> **Important**
>
> Lorsque vous partagez avec une organisation ou une unité d'organisation, et que cette étendue inclut le compte propriétaire du partage de ressources, tous les principaux du compte de partage ont automatiquement accès aux ressources du partage. L'accès accordé est défini par les autorisations gérées associées au partage. Cela est dû au fait que la politique basée sur les ressources qui AWS RAM s'attache à chaque ressource du partage utilise. `"Principal": "*"` Pour en savoir plus, consultez Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.
> Les directeurs des autres comptes consommateurs n'ont pas immédiatement accès aux ressources de l'action. Les administrateurs des autres comptes doivent d'abord associer des politiques d'autorisation basées sur l'identité aux principaux appropriés. Ces politiques doivent accorder `Allow` l'accès aux ARN des ressources individuelles du partage de ressources. Les autorisations définies dans ces politiques ne peuvent pas dépasser celles spécifiées dans l'autorisation gérée associée au partage de ressources.

- Vous ne pouvez ajouter que l'organisation dont votre compte est membre et les unités d'organisation de cette organisation à vos partages de ressources. Vous ne pouvez pas ajouter des unités d'organisation ou des organisations extérieures à votre propre organisation à un partage de ressources en tant que principaux. Toutefois, vous pouvez ajouter des rôles IAM individuels Comptes AWS ou, pour les services pris en charge, des rôles IAM et des utilisateurs extérieurs à votre organisation en tant que principaux d'un partage de ressources.

> **Note**
>
> Les types de ressource ne peuvent pas tous être partagés avec les utilisateurs et les rôles IAM. Pour plus d'informations sur les ressources que vous pouvez partager avec ces responsables, consultezRessources partageables AWS.

- Pour les types de ressources suivants, vous avez sept jours pour accepter l'invitation à rejoindre le partage pour les types de ressources suivants. Si vous n'acceptez pas l'invitation avant son expiration, elle est automatiquement refusée.

> **Important**
>
> Pour les types de ressources partagées ne figurant pas dans la liste suivante, vous avez 12 heures pour accepter l'invitation à rejoindre le partage de ressources. Au bout de

12 heures, l'invitation expire et l'utilisateur final principal du partage de ressources est dissocié. L'invitation ne peut plus être acceptée par les utilisateurs finaux.

- Amazon Aurora — Clusters de bases de données
- Amazon EC2 : réservations de capacité et hôtes dédiés
- AWS License Manager— Configurations de licence
- AWS Outposts— Tables de routage, avant-postes et sites des passerelles locales
- Amazon Route 53 — Règles de transfert
- Amazon VPC : adresses IPv4, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit, domaines de multidiffusion des passerelles de transit

Console

Pour créer un partage de ressources

1. Ouvrez la console AWS RAM.
2. Étant donné que les partages de AWS RAM ressources existent de manière spécifiqueRégions AWS, choisissez le partage approprié Région AWS dans la liste déroulante située dans le coin supérieur droit de la console. Pour voir les partages de ressources contenant des ressources globales, vous devez Région AWS définir la valeur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales. Si vous souhaitez inclure des ressources mondiales dans le partage des ressources, vous devez choisir la région d'origine désignée, USA Est (Virginie du Nord)`us-east-1`.
3. Si vous êtes nouveau dans ce AWS RAM domaine, choisissez Créer un partage de ressources sur la page d'accueil. Sinon, choisissez Créer un partage de ressources sur la page Partagé par moi : partages de ressources.
4. À l'étape 1 : Spécifier les détails du partage des ressources, procédez comme suit :
   a. Dans Nom, entrez un nom descriptif pour le partage de ressources.
   b. Sous Ressources, choisissez les ressources à ajouter au partage de ressources comme suit :

- Pour Sélectionner le type de ressource, choisissez le type de ressource à partager. Cela filtre la liste des ressources partageables uniquement pour les ressources du type sélectionné.
- Dans la liste des ressources qui s'affiche, cochez les cases à côté des ressources individuelles que vous souhaitez partager. Les ressources sélectionnées sont déplacées sous Ressources sélectionnées.

  Si vous partagez des ressources associées à une zone de disponibilité spécifique, l'utilisation de l'ID de zone de disponibilité (AZ ID) vous permet de déterminer l'emplacement relatif de ces ressources sur tous les comptes. Pour en savoir plus, consultez Identifiants de zone de disponibilité pour vosAWS ressources.

c. (Facultatif) Pour associer des balises au partage de ressources, sous Balises, entrez une clé et une valeur de balise. Ajoutez-en d'autres en choisissant Ajouter un nouveau tag. Répétez cette étape si nécessaire. Ces balises s'appliquent uniquement au partage de ressources lui-même, et non aux ressources du partage de ressources.

5. Choisissez Suivant.
6. À l'étape 2 : associer une autorisation gérée à chaque type de ressource, vous pouvez choisir d'associer une autorisation gérée créée par AWS au type de ressource, choisir une autorisation gérée par le client existante ou créer votre propre autorisation gérée par le client pour les types de ressources pris en charge. Pour en savoir plus, consultez Types d'autorisations gérées.

   Choisissez Créer une autorisation gérée par le client pour créer une autorisation gérée par le client qui répond aux exigences de votre cas d'utilisation du partage. Pour de plus amples informations, veuillez consulter Créer une autorisation gérée par le client. Une fois le processus terminé, choisissez,

   puis vous pouvez sélectionner l'autorisation gérée par votre nouveau client dans la liste déroulante Autorisations gérées.

> **Note**
>
> Si l'autorisation gérée sélectionnée comporte plusieurs versions, elle associe AWS RAM automatiquement la version par défaut. Vous ne pouvez joindre que la version désignée par défaut.

Pour afficher les actions autorisées par l'autorisation gérée, développez Afficher le modèle de politique pour cette autorisation gérée.

7. Choisissez Suivant.
8. À l'étape 3 : Accorder l'accès aux principaux, procédez comme suit :

   a. Par défaut, l'option Autoriser le partage avec n'importe qui est sélectionnée, ce qui signifie que, pour les types de ressources compatibles, vous pouvez partager des ressources extérieures à votre organisation. Comptes AWS Cela n'affecte pas les types de ressources qui ne peuvent être partagés qu'au sein d'une organisation, tels que les sous-réseaux Amazon VPC. Vous pouvez également partager certains types de ressources pris en charge avec des rôles et des utilisateurs IAM.

   Pour limiter le partage des ressources aux seuls comptes et aux principaux de votre organisation, choisissez Autoriser le partage uniquement au sein de votre organisation.

   b. Pour les directeurs, procédez comme suit :

   - Pour ajouter l'organisation, une unité organisationnelle (UO) ou une unité Compte AWS faisant partie d'une organisation, activez Afficher la structure organisationnelle. Cela affiche une vue arborescente de votre organisation. Cochez ensuite la case à côté de chaque principal que vous souhaitez ajouter.

     > **Important**
     >
     > Lorsque vous partagez avec une organisation ou une unité d'organisation, et que cette étendue inclut le compte propriétaire du partage de ressources, tous les principaux du compte de partage ont automatiquement accès aux ressources du partage. L'accès accordé est défini par les autorisations gérées associées au partage. Cela est dû au fait que la politique basée sur les ressources qui AWS RAM s'attache à chaque ressource du partage

utilise. `"Principal": "*"` Pour en savoir plus, consultez Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.
Les directeurs des autres comptes consommateurs n'ont pas immédiatement accès aux ressources de l'action. Les administrateurs des autres comptes doivent d'abord associer des politiques d'autorisation basées sur l'identité aux principaux appropriés. Ces politiques doivent accorder `Allow` l'accès aux ARN des ressources individuelles du partage de ressources. Les autorisations définies dans ces politiques ne peuvent pas dépasser celles spécifiées dans l'autorisation gérée associée au partage de ressources.

- Si vous sélectionnez l'organisation (l'ID commence paro-), les Comptes AWS principaux membres de l'organisation peuvent accéder au partage des ressources.
- Si vous sélectionnez une unité d'organisation (l'ID commence parou-), les principaux de l'ensemble de cette unité d'Comptes AWSorganisation et de ses unités d'organisation secondaires peuvent accéder au partage de ressources.
- Si vous sélectionnez une personneCompte AWS, seuls les principaux de ce compte peuvent accéder au partage des ressources.

> **Note**
>
> Le bouton Afficher la structure organisationnelle apparaît uniquement si le partage avec AWS Organizations est activé et si vous êtes connecté au compte de gestion de l'organisation.
> Vous ne pouvez pas utiliser cette méthode pour spécifier un rôle ou un utilisateur Compte AWS externe à votre organisation. Vous devez plutôt désactiver Afficher la structure organisationnelle et utiliser la liste déroulante et la zone de texte pour saisir l'ID ou l'ARN.

- Pour spécifier un principal par ID ou ARN, y compris les principaux extérieurs à l'organisation, sélectionnez le type de principal pour chaque principal. Entrez ensuite l'ID (pour une organisation ou une Compte AWS unité d'organisation) ou l'ARN (pour un rôle ou un utilisateur IAM), puis choisissez Ajouter. Les principaux types et formats d'ID et d'ARN disponibles sont les suivants :
  - Compte AWS— Pour ajouter unCompte AWS, entrez l'identifiant de compte à 12 chiffres. Par exemple :

```
123456789012
```

- Organisation : pour ajouter tous les éléments Comptes AWS de votre organisation, entrez l'ID de l'organisation. Par exemple :

  ```
  o-abcd1234
  ```

- Unité organisationnelle (UO) : pour ajouter une UO, entrez l'ID de l'UO. Par exemple :

  ```
  ou-abcd-1234efgh
  ```

- Rôle IAM : pour ajouter un rôle IAM, entrez l'ARN du rôle. Utilisez la syntaxe suivante :

  ```
  arn:partition:iam::account:role/role-name
  ```

  Par exemple :

  ```
  arn:aws:iam::123456789012:role/MyS3AccessRole
  ```

  > **Note**
  >
  > Pour obtenir l'ARN unique d'un rôle IAM, consultez la liste des rôles dans la console IAM, utilisez la AWS CLI commande get-role ou l'action API. GetRole

- Utilisateur IAM : pour ajouter un utilisateur IAM, entrez son ARN. Utilisez la syntaxe suivante :

  ```
  arn:partition:iam::account:user/user-name
  ```

  Par exemple :

  ```
  arn:aws:iam::123456789012:user/bob
  ```

  > **Note**
  >
  > Pour obtenir l'ARN unique d'un utilisateur IAM, consultez la liste des utilisateurs dans la console IAM, utilisez la get-userAWS CLIcommande ou l'action de l'GetUserAPI.

- Principal de service — Pour ajouter un principal de service, choisissez Service principal dans la boîte de dialogue Sélectionner le type de principal. Entrez le nom du directeur du AWS service. Utilisez la syntaxe suivante :
  - *service-id*.amazonaws.com

    Par exemple :

    pca-connector-ad.amazonaws.com

c. Pour les principes sélectionnés, vérifiez que les principaux que vous avez spécifiés apparaissent dans la liste.

9. Choisissez Suivant.
10. À l'étape 4 : révision et création, passez en revue les détails de configuration de votre partage de ressources. Pour modifier la configuration d'une étape, choisissez le lien correspondant à l'étape à laquelle vous souhaitez revenir et apportez les modifications requises.
11. Après avoir passé en revue le partage de ressources, choisissez Créer un partage de ressources.

    L'association entre la ressource et le mandataire peut prendre quelques minutes. Laissez ce processus se terminer avant d'essayer d'utiliser le partage de ressources.
12. Vous pouvez ajouter et supprimer des ressources et des principes ou appliquer des balises personnalisées à votre partage de ressources à tout moment. Vous pouvez modifier l'autorisation gérée pour les types de ressources inclus dans votre partage de ressources, pour les types qui prennent en charge plus que l'autorisation gérée par défaut. Vous pouvez supprimer votre partage de ressources lorsque vous ne souhaitez plus partager les ressources. Pour en savoir plus, consultez PartagezAWS les ressources que vous possédez.

AWS CLI

Pour créer un partage de ressources

Utilisez la commande create-resource-share. La commande suivante crée un partage de ressources qui est partagé avec tous les membres Comptes AWS de l'organisation. Le partage contient une configuration de AWS License Manager licence et accorde les autorisations gérées par défaut pour ce type de ressource.

> **Note**
>
> Si vous souhaitez utiliser une autorisation gérée par le client avec un type de ressource dans ce partage de ressources, vous pouvez soit utiliser une autorisation gérée par le client existante, soit créer une nouvelle autorisation gérée par le client. Notez l'ARN de l'autorisation gérée par le client, puis créez le partage de ressources. Pour plus d'informations, consultez Créer une autorisation gérée par le client.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

Mettre à jour un partage de ressources dansAWS RAM

Vous pouvez mettre à jour un partage de ressourcesAWS RAM à tout moment des manières suivantes :

- Vous pouvez ajouter des principes, des ressources ou des balises à un partage de ressources que vous avez créé.
- Pour les types de ressources qui prennent en charge plus que l'autorisationAWS gérée par défaut, vous pouvez choisir l'autorisation gérée qui s'applique aux ressources de chaque type.

- Lorsqu'une autorisation gérée associée au partage de ressources possède une nouvelle version par défaut, vous pouvez mettre à jour l'autorisation gérée pour utiliser la nouvelle version.
- Vous pouvez révoquer l'accès à des ressources partagées en supprimant les principaux ou les ressources d'un partage de ressources. Si vous révoquez l'accès, les responsables n'ont plus accès aux ressources partagées.

> **Note**
>
> Les responsables avec lesquels vous partagez des ressources peuvent quitter votre partage de ressources si celui-ci est vide ou s'il ne contient que des types de ressources permettant de quitter un partage de ressources. Si le partage de ressources contient des types de ressources qui ne prennent pas en charge le départ, un message s'affiche pour informer les responsables qu'ils doivent contacter le propriétaire du partage. Dans ce cas, en tant que propriétaire du partage de ressources, vous devez supprimer les principaux de votre partage de ressources. Pour afficher la liste des types de ressources ne prenant pas en charge cette action, consultezConditions préalables pour quitter un partage de ressources.

Console

Pour mettre à jour un partage des ressources.

1. Accédez à la page Partagée par moi : partages de ressources dans laAWS RAM console.
2. Étant donné que les partages desAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la clé appropriée dans la liste déroulante en haut à droite de la console. Pour afficher les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur le partage des ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Sélectionnez le partage de ressources, puis choisissez Modifier.
4. À l'étape 1 : Spécifiez les détails du partage de ressources, passez en revue les détails du partage de ressources et, si nécessaire, mettez à jour l'un des éléments suivants :

    a. (Facultatif) Pour modifier le nom du partage des ressources, modifiez le nom.

    b. (Facultatif) Pour ajouter une ressource au partage de ressources, sous Ressources, choisissez le type de ressource, puis cochez la case à côté de la ressource pour l'ajouter

au partage de ressources. Les ressources globales n'apparaissent que si vous définissez la région sur USA Est (Virginie du Nord), (`us-east-1`) dans leAWS Management Console.

c. (Facultatif) Pour supprimer une ressource du partage de ressources, localisez la ressource sous Ressources sélectionnées, puis choisissez le X à côté de l'identifiant de la ressource.

d. (Facultatif) Pour ajouter une identification au partage de ressources, sous balise, saisissez une clé et une valeur de ressources. Pour ajouter plusieurs paires clé/valeur de balise, choisissez Ajouter une nouvelle balise. Vous pouvez ajouter jusqu'à 50 balises.

e. Pour supprimer une étiquette du partage de ressources, sous Balises, localisez la balise et choisissez Supprimer à côté de celle-ci.

5. Choisissez Suivant.

6. (Facultatif) À l'étape 2 : associer une autorisation gérée à chaque type de ressource, vous pouvez choisir d'associer une autorisation gérée créée parAWS le type de ressource, choisir une autorisation gérée par le client existante ou créer votre propre autorisation gérée par le client. Pour plus d'informations, veuillez consulter Types d'autorisations gérées.

   Vous pouvez également choisir Créer une autorisation gérée par le client pour créer une autorisation gérée par le client qui répond aux exigences de votre cas d'utilisation en matière de partage. Pour plus d'informations, veuillez consulter Créer une autorisation gérée par le client. Une fois le processus terminé,

   choisissez 
   puis sélectionnez votre nouvelle autorisation gérée par le client dans la liste déroulante des autorisations gérées.

   Pour afficher les actions autorisées par l'autorisation gérée, cliquez sur Afficher le modèle de politique pour cette autorisation gérée.

7. Si la version de l'autorisation gérée actuellement attribuée au partage de ressources n'est pas la version par défaut actuelle, vous pouvez effectuer la mise à jour vers la version par défaut en choisissant Mettre à jour vers la version par défaut.

> **Note**
>
> Tant que vous n'avez pas enregistré les modifications apportées au partage de ressources après la dernière étape, vous pouvez annuler la mise à jour de version

en choisissant Revenir à la version précédente. Toutefois, pour les autorisationsAWS gérées, une fois que vous avez enregistré le partage de ressources, la modification est définitive et vous ne pouvez plus revenir à la version précédente.

8. Choisissez Suivant.
9. À l'étape 3 : choisissez les principaux auxquels l'accès est autorisé, passez en revue les principaux sélectionnés et, si nécessaire, mettez à jour l'un des éléments suivants :

   a. (Facultatif) Pour modifier si le partage est activé avec des responsables au sein ou en dehors de votre organisation, choisissez l'une des options suivantes :

      - Pour partager des ressources avec des rôlesComptes AWS ou des utilisateurs IAM individuels qui ne font pas partie de votre organisation, choisissez Autoriser le partage avec des responsables externes.
      - Pour restreindre le partage des ressources aux seuls responsables de votre organisationAWS Organizations, choisissez Autoriser le partage uniquement avec les responsables de votre organisation.

   b. Pour Principals, procédez comme suit :

      - (Facultatif) Pour ajouter une organisation, une unité organisationnelle (UO) ou un membre auCompte AWS sein de votre organisation, activez l'option Afficher la structure organisationnelle pour afficher une arborescence de votre organisation. Sélectionnez ensuite la case à cocher en regard de chaque principal que vous souhaitez ajouter.

        Important

        Lorsque vous partagez avec une organisation ou une unité d'organisation, et que cette étendue inclut le compte propriétaire du partage de ressources, tous les responsables du compte de partage ont automatiquement accès aux ressources du partage. L'accès accordé est défini par les autorisations gérées associées au partage. Cela est dû au fait que la politique basée sur les ressources quiAWS RAM s'attache à chaque ressource du partage utilise`"Principal": "*"`. Pour plus d'informations, veuillez consulter Implications de l'utilisation"Principal": "*"dans une politique basée sur les ressources.

Les propriétaires des autres comptes consommateurs n'ont pas immédiatement accès aux ressources de l'action. Les administrateurs des autres comptes doivent d'abord associer des politiques d'autorisation basées sur l'identité aux principaux responsables appropriés. Ces politiques doivent accorder l'`Allow`accès aux ARN des ressources individuelles incluses dans le partage de ressources. Les autorisations définies dans ces politiques ne peuvent pas dépasser celles spécifiées dans l'autorisation gérée associée au partage de ressources.

> **Note**
>
> Le bouton Afficher la structure organisationnelle apparaît uniquement si le partage avecAWS Organizations est activé et que vous êtes connecté en tant que principal au compte de gestion de l'organisation.
> Vous ne pouvez pas utiliser cette méthode pour spécifier un utilisateur ou un rôle IAMCompte AWS externe à votre organisation. Vous devez plutôt ajouter ces principaux en saisissant leurs identifiants, qui sont affichés dans la zone de texte située sous le bouton Afficher la structure organisationnelle. Consultez le bullet suivant.

- (Facultatif) Pour ajouter un principal par son identifiant, choisissez le type de principal dans la liste déroulante, puis entrez l'ID ou l'ARN du principal. Enfin, choisissez Ajouter.

  Si vous sélectionnez une personneCompte AWS, seul ce compte peut accéder au partage de ressources. Vous pouvez choisir l'une des options suivantes :

  - AutreCompte AWS (autre que le propriétaire de la ressource) : met la ressource à la disposition de l'autre compte. L'administrateur de ce compte doit terminer le processus en accordant l'accès à la ressource partagée à l'aide de politiques d'autorisation basées sur l'identité à des rôles et à des utilisateurs individuels. Ces autorisations ne peuvent pas dépasser celles définies dans les autorisations gérées associées au partage de ressources.
  - CeciCompte AWS (propriétaire de la ressource) : tous les rôles et utilisateurs du compte propriétaire de la ressource reçoivent automatiquement l'accès défini par les autorisations gérées associées au partage de ressources.

- L'ajout apparaît immédiatement dans la liste des principaux sélectionnés.

  Vous pouvez ensuite ajouter des comptes, des unités d'organisation ou votre organisation supplémentaires en répétant cette étape.

- (Facultatif) Pour supprimer un principal, localisez-le sous Principes principaux sélectionnés, cochez sa case, puis choisissez Désélectionner.

10. Choisissez Suivant.
11. À l'étape 4 : révision et mise à jour, passez en revue les détails de configuration de votre partage de ressources.
12. Pour modifier la configuration d'une étape, choisissez le lien correspondant à l'étape à laquelle vous souhaitez revenir, puis apportez les modifications requises.

    Si des autorisations gérées utilisent toujours des versions autres que la version par défaut, vous pouvez également y remédier en choisissant Mettre à jour vers la version par défaut.
13. Choisissez Mettre à jour le partage des ressources lorsque les modifications seront terminées.

AWS CLI

Pour mettre à jour un partage des ressources.

Vous pouvez utiliser lesAWS CLI commandes suivantes pour modifier un partage des ressources :

- Pour renommer un partage de ressources ou pour modifier si les principaux externes sont autorisés, utilisez la commande update-resource-share. L'exemple suivant renomme le partage de ressources spécifié et le définit pour n'autoriser que les principaux membres de son organisation. Vous devez utiliser le point de terminaison du serviceRégion AWS qui contient le partage de ressources.

```
$ aws ram update-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --name "my-renamed-resource-share" \
    --no-allow-external-principals
{
    "resourceShare": {
```

```
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-renamed-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- Pour ajouter une ressource à un partage de ressources, utilisez la commande associate-resource-share. L'exemple suivant ajoute un sous-réseau au partage de ressources spécifié.

```
$ aws ram associate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "ASSOCIATING",
        "external": false
    ]
}
```

- Pour ajouter ou remplacer une autorisation gérée pour un type de ressource dans un partage de ressources, utilisez les commandes list-permissionset associate-resource-share-permission. Vous ne pouvez attribuer qu'une seule autorisation gérée par type de ressource dans un partage de ressources. Si vous essayez d'ajouter une autorisation gérée à un type de ressource qui possède déjà une autorisation gérée, vous devez inclure l'`--replace`option, sinon la commande échoue et génère une erreur.

  L'exemple de commande suivant répertorie les ARN pour les autorisations gérées disponibles pour un sous-réseau Amazon Elastic Compute Cloud (Amazon EC2), puis utilise l'un de ces

ARN pour remplacer l'autorisationAWS gérée actuellement attribuée pour ce type de ressource dans le partage de ressources spécifié.

```
$ aws ram list-permissions \
    --resource-type ec2:Subnet
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionSubnet",
            "resourceType": "ec2:Subnet",
            "creationTime": "2020-02-27T11:38:26.727000-08:00",
            "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
        }
    ]
}
$ aws ram associate-resource-share-permission \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
    "returnValue": true
}
```

- Pour supprimer une ressource d'un partage de ressources, utilisez la commande disassociate-resource-share. L'exemple suivant supprime le sous-réseau Amazon EC2 avec l'ARN spécifié du partage de ressources spécifié.

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
```

```
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
    ]
}
```

- Pour modifier les balises associées à un partage de ressources, utilisez les commandes tag-resourceet untag-resource. L'exemple suivant ajoute la baliseproject=lima au partage des ressources spécifié.

```
$ aws ram tag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tags key=project,value=lima
```

L'exemple suivant supprime la balise avec une clé deproject du partage de ressources spécifié.

```
$ aws ram untag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tag-keys=project
```

Les commandes de balise ne produisent aucune sortie lorsqu'elles réussissent.

Affichage de vos ressources partagées dansAWS RAM

Vous pouvez rechercher la liste des ressources individuelles que vous avez partagées sur tous les partages de ressources. La liste vous permet de déterminer les ressources que vous partagez actuellement, le nombre de partages de ressources dans lesquels elles sont incluses et le nombre de personnes principales qui y ont accès.

Console

Pour consulter les ressources que vous partagez actuellement

1. Ouvrez la page Partagée par moi : Ressources partagées dans laAWS RAM console.

2. Comme les partages deAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la liste déroulante qui se trouve dans le coin supérieur droit de la console. Pour rechercher les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur USA Est (Virginie du Nord), (`us-east-1`). Pour en savoir plus sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Pour chaque ressource partagée, les informations suivantes sont disponibles :

   - ID de ressource : ID de la ressource. Choisissez l'ID d'une ressource pour ouvrir un nouvel onglet de navigateur afin d'afficher la ressource dans sa console de service native.
   - Le type de ressource : le type de ressource.
   - Date du dernier partage : date à laquelle la ressource a été partagée pour la dernière fois.
   - Partage de ressources : nombre de partages de ressources qui incluent la ressource. Pour voir la liste des partages de ressources, choisissez le numéro.
   - Responsables : nombre de responsables pouvant accéder à la ressource. Choisissez la valeur pour afficher les principaux.

AWS CLI

Pour consulter les ressources que vous partagez actuellement

Vous pouvez utiliser la commande list-resources avec le paramètre`--resource-owner` défini sur`SELF` pour afficher les détails des ressources que vous partagez actuellement.

L'exemple suivant montre les ressources incluses dans les partages de ressources dans leRégion AWS (`us-east-1`) pour l'appelCompte AWS. Pour obtenir les ressources que vous partagez dans une autre région, utilisez le`--region` *`<region-code>`* paramètre.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner SELF
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
```

```
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
        },
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-07-22T11:48:11.104000-07:00",
            "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
        }
    ]
}
```

Affichage des principaux acteurs avec lesquels vous partagez des ressources dansAWS RAM

Vous pouvez rechercher les mandataires avec qui vous partagez vos ressources sur tous les partages de ressources. La consultation de cette liste de mandataires vous permet de déterminer qui a accès à vos ressources partagées.

Console

Pour consulter les principaux acteurs avec lesquels vous partagez des ressources

1. Accédez à la page Partagé par moi : Principes principaux de laAWS RAM console.
2. Comme les partages deAWS RAM ressources sont spécifiquesRégions AWS, choisissezRégion AWS la dans la liste déroulante dans le coin supérieur droit de la console. Pour rechercher les partages de ressources qui contiennent des ressources globales, vous devez définir la sur sur sur sur sur sur sur sur sur sur laRégion AWS sur sur sur sur sur sur sur vous devez définir la sur sur sur sur sur sur sur sur sur surus-east-1 Pour en savoir plus sur le partage de ressources mondiales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Appliquez un filtre pour trouver des principes spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche. Choisissez la zone de texte pour afficher la liste déroulante des champs attributaires suggérés. Après en avoir sélectionné une, vous pouvez

choisir parmi la liste des valeurs disponibles pour ce champ. Vous pouvez ajouter d'autres attributs ou mots clés jusqu'à ce que vous trouviez la ressource recherchée.

4. Pour chaque principal de la liste, la console affiche les informations suivantes :

   - ID principal — L'identifiant du mandant. Choisissez l'ID pour ouvrir un nouvel onglet de navigateur afin d'afficher le principal dans sa console native.
   - Partage de ressources : nombre de partages de ressources que vous avez partagés avec le principal spécifié. Sélectionnez le numéro pour afficher la liste des partages de ressources.
   - Ressources : nombre de ressources que vous avez partagées avec le principal. Sélectionnez le numéro pour afficher la liste des ressources partagées.

AWS CLI

Pour consulter les principaux acteurs avec lesquels vous partagez des ressources

Vous pouvez utiliser la commande list-principals pour obtenir la liste des principaux auxquels vous faites référence dans les partages de ressources que vous avez créés dans le compte actuelRégion AWS pour le compte appelant.

L'exemple suivant répertorie les principaux ayant accès aux partages créés dans la région par défaut pour le compte appelant. Dans cet exemple, les principales sont l'organisation du compte appelant et une organisation distincteCompte AWS, dans le cadre de deux partages de ressources différents. Vous devez utiliser le point de terminaison du serviceRégion AWS qui contient le partage de ressources.

```
$ aws ram list-principals \
    --region us-east-1 \
    --resource-owner SELF
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-09-14T20:40:58.532000-07:00",
            "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
            "external": false
        },
```

```
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
            "creationTime": "2021-09-15T15:00:31.601000-07:00",
            "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
            "external": true
        }
    ]
}
```

Supprimer un partage de ressources dansAWS RAM

Vous pouvez supprimer un partage de ressources à tout moment. Lorsque vous supprimez un partage de ressources, tous les principaux associés au partage de ressources perdent l'accès aux ressources partagées. La suppression d'un partage de ressources ne supprime pas les ressources partagées.

> **Pour supprimer uneAWS ressource**
>
> Si vous devez supprimer uneAWS ressource que vous avez incluse dans un partage de ressources, vousAWS recommande de commencer par supprimer la ressource de tout partage de ressources qui l'inclut ou de supprimer le partage de ressources.

Le partage de ressources supprimé reste visible dans laAWS RAM console pendant une courte période après sa suppression, mais son statut passe à`Deleted`.

Console

Pour supprimer un partage de ressources

1. Ouvrez la page Partagée par moi : partages de ressources dans laAWS RAM console.
2. Comme les partages deAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la dans la liste déroulante dans le coin supérieur droit de la console. Pour voir les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur comment partager des ressources à l'échelle mondiale, consultezPartage des ressources régionales par rapport aux ressources mondiales.

3. Sélectionnez le partage de ressources que vous souhaitez supprimer.

> **Warning**
>
> Veillez à sélectionner le partage de ressources approprié. Vous ne pouvez pas récupérer un partage de ressources après l'avoir supprimé.

4. Choisissez Supprimer, puis dans le message de confirmation, choisissez Supprimer.
5. Le partage de ressources supprimé disparaît au bout de deux heures. En attendant, il reste visible dans la console avec un statut supprimé.

AWS CLI

Pour supprimer un partage de ressources

Vous pouvez utiliser la delete-resource-sharecommande pour supprimer un partage de ressources dont vous n'avez plus besoin.

Il utilise d'abord la get-resource-sharescommande pour obtenir l'Amazon Resource Name (ARN) du partage de ressources que vous souhaitez supprimer. Ensuite, il delete-resource-sharel'utilise pour supprimer le partage de ressources spécifié.

```
$  aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
$ aws ram delete-resource-share \
```

```
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
    "returnValue": true
}
```

Accédez aux AWS ressources partagées avec vous

Avec AWS Resource Access Manager (AWS RAM), vous pouvez afficher les partages de ressources auxquels vous avez été ajouté, les ressources partagées auxquelles vous pouvez accéder et celles Comptes AWS qui ont partagé des ressources avec vous. Vous pouvez également quitter un partage de ressources lorsque vous n'avez plus besoin d'accéder à ses ressources partagées.

Table des matières

Accepter et rejeter les invitations à partager des ressources

Pour accéder aux ressources partagées, le propriétaire du partage de ressources doit vous ajouter en tant que principal. Le propriétaire peut ajouter l'un des éléments suivants en tant que principal au partage de ressources.

- L'organisation dont votre compte est membre
- Une unité organisationnelle (UO) qui contient votre compte
- Votre compte individuel
- Pour les types de ressources pris en charge, votre rôle ou utilisateur IAM spécifique

Si vous êtes ajouté au partage de ressources par le biais d'un membre d'une organisation et Compte AWS que le partage au sein de l'organisation est activé, vous avez automatiquement accès aux ressources partagées sans avoir à accepter d'invitation. AWS Organizations Les responsables

du service ont également un accès automatique aux ressources partagées sans accepter d'invitation. Si le compte par le biais duquel vous avez accès est ultérieurement supprimé de l'organisation, tous les principaux de ce compte perdent automatiquement l'accès aux ressources accessibles via ce partage de ressources.

Si vous êtes ajouté à un partage de ressources par l'un des moyens suivants, vous recevez une invitation à rejoindre le partage de ressources :

- Un compte externe à votre organisation dans AWS Organizations
- Un compte au sein de votre organisation lorsque le partage avec n' AWS Organizations est pas activé

Si vous recevez une invitation à rejoindre un partage de ressources, vous devez l'accepter pour accéder à ses ressources partagées. Si vous refusez l'invitation, vous ne pourrez pas accéder aux ressources partagées.

Pour les types de ressources suivants, vous avez sept jours pour accepter l'invitation à rejoindre le partage pour les types de ressources suivants. Si vous n'acceptez pas l'invitation avant son expiration, elle est automatiquement refusée.

> **Important**
>
> Pour les types de ressources partagées ne figurant pas dans la liste suivante, vous avez 12 heures pour accepter l'invitation à rejoindre le partage de ressources. Au bout de 12 heures, l'invitation expire et l'utilisateur final principal du partage de ressources est dissocié. L'invitation ne peut plus être acceptée par les utilisateurs finaux.

- Amazon Aurora — Clusters de bases de données
- Amazon EC2 : réservations de capacité et hôtes dédiés
- AWS License Manager — Configurations de licence
- AWS Outposts — Tables de routage, avant-postes et sites des passerelles locales
- Amazon Route 53 — Règles de transfert
- Amazon VPC : adresses IPv4, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit, domaines de multidiffusion de passerelles de transit appartenant au client

Console

Pour répondre à une invitation à partager une ressource

1. Accédez à la page Partagé avec moi : partage de ressources dans la AWS RAM console.
2. Étant donné que les partages de AWS RAM ressources existent de manière spécifique Régions AWS, choisissez le partage approprié Région AWS dans la liste déroulante située dans le coin supérieur droit de la console. Pour voir les partages de ressources contenant des ressources globales, vous devez Région AWS définir la valeur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Consultez la liste des partages de ressources auxquels vous avez été ajouté.

   La colonne État indique votre statut de participation actuel pour le partage des ressources. Le `Pending` statut indique que vous avez été ajouté à un partage de ressources, mais que vous n'avez pas encore accepté ou rejeté l'invitation.
4. Pour répondre à l'invitation de partage de ressources, sélectionnez l'ID de partage de ressources et choisissez Accepter le partage de ressources pour accepter l'invitation, ou Rejeter le partage de ressources pour refuser l'invitation. Si vous rejetez l'invitation, vous n'aurez pas accès aux ressources. Si vous acceptez l'invitation, vous avez accès aux ressources.

AWS CLI

Pour répondre à une invitation à partager une ressource

Vous pouvez utiliser les commandes suivantes pour accepter ou rejeter les invitations à un partage de ressources :

- get-resource-share-invitations
- accept-resource-share-invitation
- reject-resource-share-invitation

1. L'exemple suivant commence par utiliser la get-resource-share-invitationscommande pour récupérer une liste de toutes les invitations disponibles pour l'utilisateur Compte AWS. Le AWS CLI `query` paramètre vous permet de limiter la sortie aux seules invitations dont le paramètre `status` est défini sur`PENDING`. Cet exemple montre qu'une invitation du compte

111111111111 concerne actuellement PENDING le compte courant indiqué. 123456789012 Région AWS

```
$ aws ram get-resource-share-invitations \
    --region us-east-1 \
    --query 'resourceShareInvitations[?status==`PENDING`]'
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
            "resourceShareName": "Test TrngAcct Resource Share",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
            "senderAccountId": "111111111111",
            "receiverAccountId": "123456789012",
            "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
            "status": "PENDING"
        }
    ]
}
```

2. Une fois que vous avez trouvé l'invitation que vous souhaitez accepter, notez ce qui se trouve resourceShareInvitationArn dans la sortie à utiliser dans la commande suivante pour accepter l'invitation.

```
$ aws ram accept-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "ACCEPTED"
```

```
    }
}
```

En cas de succès, notez que la réponse indique que le `status` est passé de `PENDING` à`ACCEPTED`.

Si vous souhaitez plutôt rejeter l'invitation, exécutez la reject-resource-share-invitationcommande avec les mêmes paramètres.

```
$ aws ram reject-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "REJECTED"
    }
}
```

Affichage des partages de ressources partagés avec vous

Vous pouvez consulter les partages de ressources auxquels vous avez accès. Vous pouvez voir quels responsables partagent des ressources avec vous et quelles ressources ils partagent.

Console

Pour consulter les partages de ressources

1. Accédez à la page Partagé avec moi : partages de ressources dans laAWS RAM console.
2. Comme les partages deAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la appropriée dans la liste déroulante située dans

le coin supérieur droit de la console. Pour rechercher les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur Est des États-Unis (Virginie du Nord), (`us-east-1`). Pour en savoir plus sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.

3. (Facultatif) Appliquez un filtre pour rechercher des partages de ressources spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche. Vous pouvez saisir un mot clé, par exemple une partie du nom d'un partage de ressources, pour répertorier uniquement les partages de ressources qui incluent ce texte dans le nom. Choisissez la zone de texte pour afficher la liste déroulante des champs attributaires suggérés. Après en avoir sélectionné une, vous pouvez choisir parmi la liste des valeurs disponibles pour ce champ. Vous pouvez ajouter d'autres attributs ou mots clés jusqu'à ce que vous trouviez la ressource souhaitée.
4. LaAWS RAM console affiche les informations suivantes :

   - Nom : nom du partage de ressources.
   - ID — L'ID du partage de ressources. Choisissez l'ID pour afficher la page de détails du partage de ressources.
   - Propriétaire : ID de la personneCompte AWS qui a créé le partage de ressources.
   - Statut : statut actuel du partage de ressources. Les valeurs possibles incluent :
     - `Active`— Le partage de ressources est actif et peut être utilisé.
     - `Deleted`— Le partage de ressources est supprimé et ne peut plus être utilisé.
     - `Pending`— Une invitation à accepter le partage de ressources est en attente de réponse.

AWS CLI

Pour consulter les partages de ressources

Utilisez la get-resource-sharescommande avec le`--resource-owner` paramètre défini sur`OTHER-ACCOUNTS`.

L'exemple suivant montre la liste des partages de ressources partagés dans le compte spécifiéRégion AWS avec le compte appelant par d'autresComptes AWS.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
```

```
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Env Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
            "name": "Prod Env Shared Subnets",
            "owningAccountId": "222222222222",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:56:24.737000-07:00",
            "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```


Affichage des ressources partagées avec vous

Vous pouvez afficher les ressources partagées auxquelles vous avez accès. Vous pouvez voir quels responsables ont partagé les ressources avec vous et quels partages de ressources incluent les ressources.

Console

Pour consulter les ressources partagées avec vous

1. Accédez à la page Partagé avec moi : Ressources partagées dans laAWS RAM console.
2. Comme les partages deAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la appropriée dans la liste déroulante située dans le coin supérieur droit de la console. Pour rechercher les partages de ressources qui contiennent des ressources globales, vous devez définir le sur USA Est (Virginie du Nord), fauteRégion AWS

de quoi les définir sur USA Est (Virginie du Nord)), faute de quoi les`us-east-1` données sont partagées. Pour en savoir plus sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.

3. Appliquez un filtre pour rechercher des ressources partagées spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche.
4. Les informations suivantes sont disponibles :

   - ID de ressource : ID de la ressource. Choisissez l'ID de la ressource pour l'afficher dans sa console de service.
   - Le type de ressource : le type de ressource.
   - Date du dernier partage : date à laquelle la ressource a été partagée avec vous.
   - Partage de ressources : nombre de partages de ressources dans lesquels la ressource est incluse. Choisissez la valeur pour afficher les partages de ressources.
   - ID du propriétaire : identifiant du principal propriétaire de la ressource.

AWS CLI

Pour consulter les ressources partagées avec vous

Vous pouvez utiliser la commande list-resources pour afficher les ressources qui sont partagées avec vous.

L'exemple de commande suivant affiche les détails de la ressource accessible via un partage de ressources dans la zone spécifiéeRégion AWS depuis une autre ressourceCompte AWS.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:111111111111:license-
configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "status": "AVAILABLE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
```

```
        }
    ]
}
```

Afficher les principaux utilisateurs qui partagent avec vous

Vous pouvez rechercher une liste de tous les mandataires qui partagent des ressources avec vous. Vous pouvez rechercher les ressources et les partages de ressources qu'ils partagent avec vous.

Console

Pour rechercher les mandataires qui partagent des ressources avec vous

1. Ouvrez la console AWS RAM à l'adresse https://console.aws.amazon.com/ram.
2. Comme les partages deAWS RAM ressources sont spécifiquesRégions AWS, choisissez la dans la listeRégion AWS déroulante qui se trouve dans le coin supérieur droit de la console, choisissez la dans la liste déroulante. Pour rechercher les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur la région Est (Virginie du Nord), (`us-east-1`). Pour en savoir plus sur le partage de ressources mondiales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Dans le volet de navigation, choisissez Shared with me (Partagé avec moi), Principals (Mandataires).
4. (Facultatif) Vous pouvez appliquer un filtre pour rechercher des mandataires spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche.
5. La console affiche les informations suivantes :
   - Identifiant principal : identifiant du mandant qui partage avec vous.
   - Partage de ressources : nombre de partages de ressources auxquels le mandant vous a ajouté. Choisissez le numéro pour rechercher la liste des partages de ressources.
   - Ressources : le nombre de ressources que le directeur partage avec vous. Choisissez la valeur pour afficher la liste des ressources.

AWS CLI

Pour rechercher les mandataires qui partagent des ressources avec vous

Vous pouvez utiliser la commande list-principals pour récupérer la liste des principaux qui partagent des ressources avec votreCompte AWS.

L'exemple de commande suivant affiche des informations sur laCompte AWS personne qui a partagé un partage de ressources avec le compte utilisé pour appeler l'opération dans la zone spécifiéeRégion AWS.

```
$  aws ram list-principals \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "principals": [
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
            "external": true
        }
    ]
}
```

Quitter un partage de ressources

Si vous n'avez plus besoin d'accéder aux ressources partagées avec vous, vous pouvez quitter un partage de ressources à tout moment. Lorsque vous quittez un partage de ressources, vous perdez l'accès aux ressources partagées.

Conditions préalables pour quitter un partage de ressources

- Vous ne pouvez quitter un partage de ressources que s'il a été partagé avec vous en tant qu'individu Compte AWS et non dans le contexte d'une organisation. Vous ne pouvez pas quitter un partage de ressources si vous y avez été ajouté par un membre Compte AWS de votre organisation et si le partage avec AWS Organizations est activé. L'accès aux partages de ressources au sein d'une organisation est automatique.
- Pour quitter un partage de ressources, vérifiez que le partage de ressources est vide ou qu'il contient uniquement des types de ressources permettant de quitter un partage.

Les seuls types de ressources qui permettent de quitter un partage de ressources sont les suivants.

Service	Type de ressource
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

AWS Outposts	`ec2:LocalGatewayRouteTable`
	`outposts:Outpost`
	`outposts:Site`

Amazon Route 53	`route53resolver:ResolverRule`

Amazon VPC	`ec2:CoipPool`
	`ec2:PrefixList`
	`ec2:Subnet`
	`ec2:TrafficMirrorTarget`
	`ec2:TransitGateway`
	`ec2:TransitGatewayMulticastDomain`

Comment quitter un partage de ressources

Console

Pour quitter un partage de ressources

1. Accédez à la page Partagé avec moi : partages de ressources dans la AWS RAM console.
2. Étant donné que les partages de AWS RAM ressources existent de manière spécifiqueRégions AWS, choisissez le partage approprié Région AWS dans la liste déroulante située dans le coin supérieur droit de la console. Pour voir les partages de ressources contenant des ressources globales, vous devez Région AWS définir la valeur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur le partage de ressources globales, consultezPartage des ressources régionales par rapport aux ressources mondiales.
3. Sélectionnez le partage de ressources que vous souhaitez quitter.
4. Choisissez Quitter le partage des ressources, puis dans la boîte de dialogue de confirmation, choisissez Quitter.

AWS CLI

Pour quitter un partage de ressources

Vous pouvez utiliser la disassociate-resource-sharecommande pour quitter un partage de ressources.

Les exemples de commandes suivants font perdre à la commande Compte AWS qui appelle l'accès aux ressources partagées par le partage de ressources spécifié par l'ARN. Vous devez diriger la demande vers le point de terminaison du service Région AWS qui contient le partage de ressources que vous souhaitez quitter.

1. Tout d'abord, récupérez la liste des partages de ressources pour récupérer l'ARN du partage de ressources que vous souhaitez quitter.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
```

```
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Environment Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

2. Ensuite, vous pouvez exécuter la commande pour quitter ce partage de ressources. Notez que vous devez également spécifier votre identifiant de compte123456789012, en tant que principal à dissocier du partage de ressources spécifié, qui est partagé par compte111111111111.

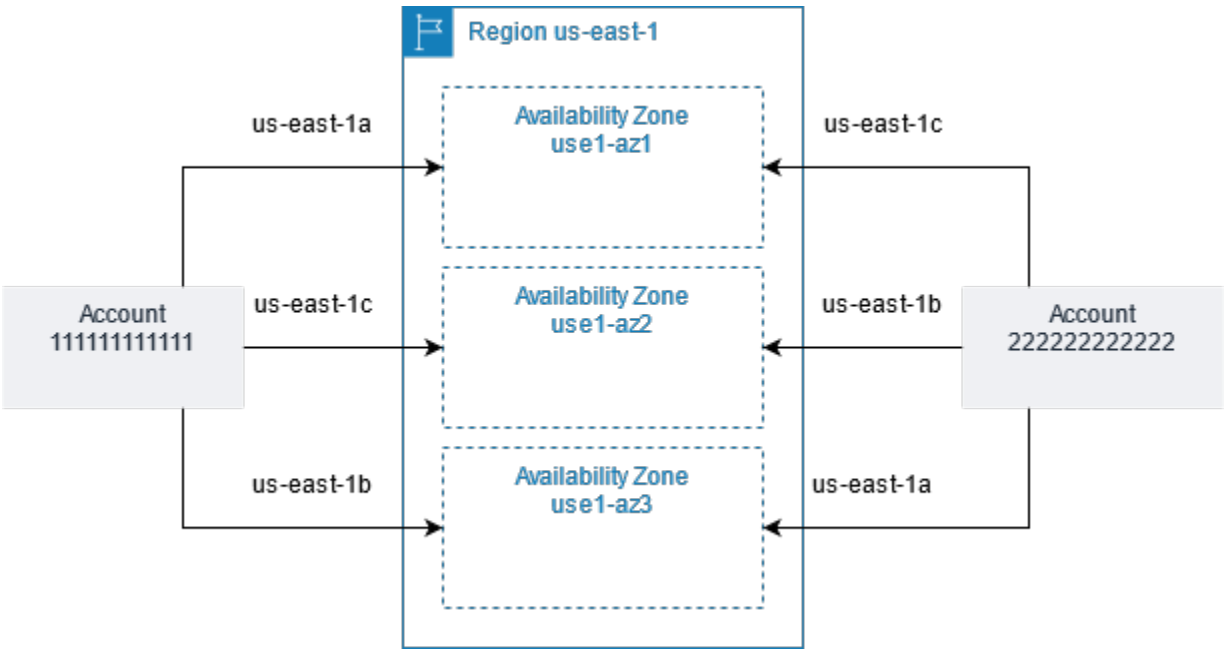
```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
            "external": false
        }
    ]
}
```

Identifiants de zone de disponibilité pour vosAWS ressources

AWSmappe les zones de disponibilité physiques de manière aléatoire aux noms des zones de disponibilité de chacune d'ellesCompte AWS. Cette approche permet de répartir les ressources entre les zones de disponibilité d'une régionRégion AWS, au lieu que les ressources soient probablement

concentrées dans la zone de disponibilité « a » pour chaque région. Par conséquent, la zone de disponibilité`us-east-1a` de votreAWS compte peut ne pas représenter la même localisation physique que celle`us-east-1a` d'un autreAWS compte. Pour de plus amples informations, veuillez consulter Régions et zones de disponibilité dans le Amazon EC2 Guide de l'utilisateur.

L'illustration suivante montre comment les ID AZ sont identiques pour tous les comptes, même si les noms des zones de disponibilité peuvent être mappés différemment pour chaque compte.



Pour certaines ressources, vous devez identifier non seulement la zone de disponibilitéRégion AWS, mais également la zone de disponibilité. Par exemple, un sous-réseau Amazon VPC. Au sein d'un seul compte, le mappage d'une zone de disponibilité à un nom spécifique n'est pas important. Mais, lorsque vous avez l'AWS RAMhabitude de partager une telle ressource avec d'autresComptes AWS personnes, la cartographie est importante. Ce mappage aléatoire complique la capacité du compte accédant à la ressource partagée à savoir à quelle zone de disponibilité référencer. À cette fin, ces ressources vous permettent également d'identifier l'emplacement réel de vos ressources par rapport à vos comptes à l'aide de l'identifiant AZ. Un ID de zone de disponibilité est un identifiant unique et cohérent pour une zone de disponibilité dans toutes les zones de disponibilitéComptes AWS. Par exemple,`use1-az1` il s'agit d'un ID de zone de`us-east-1` disponibilité pour une zone de disponibilité dans chaqueAWS compte.

Vous pouvez utiliser les ID de zone de disponibilité pour déterminer l'emplacement des ressources dans un compte par rapport aux ressources d'un autre compte. Par exemple, si vous partagez avec un autre compte un sous-réseau dans la zone de disponibilité portant l'ID `use1-az2`, ce sous-réseau est accessible par cet autre compte dans la zone de disponibilité portant également l'ID `use1-az2`.

L'ID de zone de disponibilité de chaque sous-réseau s'affiche dans la console Amazon VPC et peut être interrogé à l'aide duAWS CLI.

Console

Pour afficher les ID de zone de disponibilité pour votre compte

1. Accédez à la page de la AWS RAMconsole dans laAWS RAM console.
2. Vous pouvez consulter les ID AZ actuelsRégion AWS sous Votre identifiant AZ.

AWS CLI

Pour afficher les ID de zone de disponibilité pour votre compte

L'exemple de commande suivant montre les ID AZ des zones de disponibilité de la région us-west-2 et la manière dont ils sont mappés pour l'appelCompte AWS.

```
$ aws ec2 describe-availability-zones \
    --region us-west-2
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az2",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
```

```
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        }
    ]
}
```

Ressources partageables AWS

Avec AWS Resource Access Manager (AWS RAM), vous pouvez partager des ressources créées et gérées par d'autres Services AWS. Vous pouvez partager des ressources avec des individus Comptes AWS. Vous pouvez également partager des ressources avec les comptes d'une organisation ou des unités organisationnelles (UO) dans AWS Organizations. Certains types de ressources pris en charge vous permettent également de partager des ressources avec des rôles et des utilisateurs individuels AWS Identity and Access Management (IAM).

Les sections suivantes répertorient les types de ressources, regroupés par Service AWS, que vous pouvez partager à l'aide de AWS RAM. Les colonnes des tableaux indiquent les fonctionnalités prises en charge par chaque type de ressource :

Peut être partagé avec les utilisateurs et les rôles IAM	 Oui, vous pouvez partager des ressources de ce type avec des rôles et des utilisateurs individuels AWS Identity and Access Management (IAM), en plus des comptes.  Non, vous ne pouvez partager des ressources de ce type qu'avec des comptes.
Peut partager avec des comptes extérieurs à son organisation	 Oui, vous ne pouvez partager des ressources de ce type qu'avec des comptes individuels, au sein ou en dehors de son organisation. Voir Considérations pour plus d'informations.

	 Non, vous ne pouvez partager des ressources de ce type qu'avec des comptes membres de la même organisation.
Peut utiliser les autorisations gérées par le client	Tous les types de ressources sont pris en AWS RAM charge par les autorisations AWS gérées par le support, mais un Oui dans cette colonne signifie que les autorisations gérées par le client sont également prises en charge pour ce type de ressource.  Oui, les ressources de ce type prennent en charge l'utilisation des autorisations gérées par le client.  Non, les ressources de ce type ne prennent pas en charge l'utilisation des autorisations gérées par le client.
Peut être partagé avec les responsables du service	 Oui, vous pouvez partager des ressources de ce type avec Services AWS.  Non, vous ne pouvez pas partager de ressources de ce type avec Services AWS.

AWS App Mesh

Vous pouvez partager les AWS App Mesh ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Maillage `appmesh:Mesh`	Créez et gérez un maillage de manière centralisée, et partagez-le avec d'autres personnes Comptes AWS ou avec votre organisation. Un maillage partagé permet aux ressources créées par différents Comptes AWS utilisateurs de communiquer entre elles dans le même maillage. Pour plus d'informations, consultez la section Utilisation des maillages partagés dans le Guide de l'AWS App Mesh utilisateur.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

AWS AppSync API GraphQL

Vous pouvez partager les ressources d'API AWS AppSync GraphQL suivantes en utilisant. AWS RAM

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
API GraphyQL `appsync:Apis`	Gérez les API AWS AppSync GraphQL de manière centralisée et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes de partager des AWS AppSync API dans le cadre de la création d'une API AWS AppSync fusionnée unifiée qui peut accéder aux données de plusieurs API de sous-schéma sur différents comptes d'une même région. Pour plus d'informations, consultez la section API fusionnées	O	O Peut partager avec n'importe qui Compte AW	O	Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	dans le guide du AWS AppSync développeur.				

Amazon Aurora

Vous pouvez partager les ressources Amazon Aurora suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Clusters de bases de données `rds:Cluster`	Créez et gérez un cluster de base de données de manière centralisée, et partagez-le avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet à plusieurs de Comptes AWS cloner un cluster de base	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	de données partagé et géré de manière centralisée. Pour plus d'informations, consultez la section Clonage entre comptes avec Amazon Aurora AWS RAM et Amazon Aurora dans le guide de l'utilisateur Amazon Aurora.				

AWS Private Certificate Authority

Vous pouvez partager les Autorité de certification privée AWS ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Autorité de certification privée (CA) `acm-pca:CertificateAuthority`	Créez et gérez des autorités de certification privées (CA) pour l'infrastructure à clé publique (PKI) interne de votre organisation, et partagez ces autorités de certification avec d'autres autorités Comptes AWS ou avec votre organisation. Cela permet AWS Certificate Manager aux utilisateurs d'autres comptes d'émettre des certificats X.509 signés par votre autorité de certification partagée. Pour plus d'informations, consultez la section Contrôle de l'accès à une autorité de certification privée dans le Guide de AWS Private Certificate Authority l'utilisateur.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Oui

Amazon DataZone

Vous pouvez partager les DataZone ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
DataZone Domaine `datazone:Domain`	Créez et gérez des domaines de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes de créer des DataZone domaines Amazon. Pour plus d'informations, consultez la section Qu'est-ce qu'Amazon DataZone dans le guide de DataZone l'utilisateur Amazon.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

AWS CodeBuild

Vous pouvez partager les AWS CodeBuild ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Projet `codebuild:Project`	Créez un projet et utilisez-le pour exécuter des builds. Partagez le projet avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs utilisateurs Comptes AWS de consulter les informations relatives à un projet et d'analyser ses versions. Pour plus d'informations, consultez la section Utilisation de projets partagés dans le Guide de AWS CodeBuild l'utilisateur.	 Oui	 Oui Peut partager avec n'importe qui Compte AWS	 Oui	 Non
Groupe de rapports `codebuild:ReportGroup`	Créez un groupe de rapports et utilisez-le pour créer des rapports lorsque vous créez un projet. Partagez le groupe	 Oui	 Oui Peut partager avec	 Oui	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	de rapports avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs Comptes AWS utilisateurs de consulter le groupe de rapports et ses rapports, ainsi que les résultats des scénarios de test pour chaque rapport. Un rapport peut être consulté pendant 30 jours après sa création, puis il expire et n'est plus consultable. Pour plus d'informations, consultez la section Utilisation de projets partagés dans le Guide de AWS CodeBuild l'utilisateur.		n'importe qui Compte AW		

Amazon EC2

Vous pouvez partager les ressources Amazon EC2 suivantes en utilisant. AWS RAM

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Réserves de capacité `ec2:CapacityReservation`	Créez et gérez les réservations de capacité de manière centralisée, et partagez la capacité réservée avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs de Comptes AWS lancer leurs instances Amazon EC2 dans une capacité réservée gérée de manière centralisée. Pour plus d'informations, consultez la section Travailler avec des réservations de capacité partagée dans le guide de l'utilisateur Amazon EC2. **Important** Si vous ne remplissez pas toutes	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	les conditions requises pour partager une réservation de capacité, l'opération de partage peut échouer. Si cela se produit et qu'un utilisateur tente de lancer une instance Amazon EC2 dans le cadre de cette réservation de capacité, celle-ci est lancée en tant qu'instance à la demande, ce qui peut entraîner des coûts plus élevés. Nous vous recommandons de vérifier que vous pouvez				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	accéder à la réservation de capacité partagée en essayant de l'afficher dans la console Amazon EC2. Vous pouvez également surveiller les défaillances des partages de ressources afin de pouvoir prendre des mesures correctives avant que les utilisateurs ne lancent des instances, de manière à augmenter vos coûts. Pour plus d'informations, consultez Exemple :				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	alerte en cas d'échec du partage de ressources.				
Hôtes dédiés `ec2:DedicatedHost`	Allouez et gérez les hôtes dédiés Amazon EC2 de manière centralisée, et partagez la capacité d'instance de l'hôte avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs de Comptes AWS lancer leurs instances Amazon EC2 sur des hôtes dédiés gérés de manière centralisée. Pour plus d'informations, consultez la section Travailler avec des hôtes dédiés partagés dans le guide de l'utilisateur Amazon EC2.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Groupes de placement `ec2:PlacementGroup`	Partagez les groupes de placement que vous possédez au sein de votre Comptes AWS organisation et en dehors de celle-ci. Vous pouvez lancer des instances Amazon EC2 depuis n'importe quel compte avec lequel vous partagez un placement dans un groupe de placement partagé. Pour plus d'informations, consultez Partager un groupe de placement dans le guide de l'utilisateur Amazon EC2.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

EC2 Image Builder

Vous pouvez partager les ressources EC2 Image Builder suivantes en AWS RAM utilisant.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Composants `imagebuilder:Component`	Créez et gérez les composants de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Gérez les personnes autorisées à utiliser des composants de génération et de test prédéfinis dans leurs recettes d'images. Pour plus d'informations, consultez les ressources Share EC2 Image Builder dans le guide de l'utilisateur d'EC2 Image Builder.	 Oui	 Oui Peut partager avec n'importe qui Compte AWS	 Oui	 Non
Recettes de contenants `imagebuilder:ContainerRecipe`	Créez et gérez vos recettes de contenants de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation.	 Oui	 Oui Peut partager avec n'importe	 Oui	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	Cela vous permet de gérer les personnes autorisées à utiliser des documents prédéfinis pour dupliquer les versions d'images de conteneurs. Pour plus d'informations, consultez les ressources Share EC2 Image Builder dans le guide de l'utilisateur d'EC2 Image Builder.		qui Compte AW		

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Images `imagebuilder:Image`	Créez et gérez vos images dorées de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Gérez les personnes autorisées à utiliser les images créées avec EC2 Image Builder au sein de votre organisation. Pour plus d'informations, consultez les ressources Share EC2 Image Builder dans le guide de l'utilisateur d'EC2 Image Builder.	 Oui	 Oui Peut partager avec n'importe qui Compte AWS	 Oui	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Recettes d'images `imagebuilder:ImageRecipe`	Créez et gérez vos recettes d'images de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela vous permet de gérer les personnes autorisées à utiliser des documents prédéfinis pour dupliquer les builds d'AMI. Pour plus d'informations, consultez les ressources Share EC2 Image Builder dans le guide de l'utilisateur d'EC2 Image Builder.	 Oui	 Oui Peut partager avec n'importe qui Compte AW	 Oui	 Non

Amazon FSx pour OpenZFS

Vous pouvez partager les ressources Amazon FSx pour OpenZFS suivantes en utilisant. AWS RAM

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Volume FSx `fsx:Volume`	Créez et gérez les volumes FSx pour OpenZFS de manière centralisée, et partagez-les avec d'autres personnes ou Comptes AWS avec votre organisation. Cela permet à plusieurs comptes d'effectuer une réplication de données à l'aide de OpenZfs snapshots sous des volumes partagés via des API FSx ou`CreateVolume` . `CopySnapshotAndUpdateVolume` Pour plus d'informations, consultez la section Réplication de données à la demande dans le guide de l'utilisateur d'Amazon FSx pour OpenZFS.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

AWS Glue

Vous pouvez partager les AWS Glue ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Catalogues de données `glue:Catalog`	Gérez un catalogue de données central et partagez les métadonnées relatives aux bases de données et aux tables avec Comptes AWS votre organisation. Cela permet aux utilisateurs d'exécuter des requêtes sur les données de plusieurs comptes. Pour plus d'informations, consultez la section Partage de tables de catalogues de données et de bases de données entre AWS comptes dans le guide du AWS Lake Formation développeur.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Bases de données `glue:Database`	Créez et gérez des bases de données de catalogues de données de manière centralisée, et partagez-les avec Comptes AWS votre organisation. Les bases de données sont des ensembles de tables de catalogues de données. Cela permet aux utilisateurs d'exécuter des requêtes et d'extraire, de transformer et de charger des tâches (ETL) qui peuvent joindre et interroger des données sur plusieurs comptes. Pour plus d'informations, consultez la section Partage de tables de catalogues de données et de bases de données entre AWS comptes dans le	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	guide du AWS Lake Formation développeur.				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Tables `glue:Table`	Créez et gérez les tables de catalogue de données de manière centralisée, et partagez-les avec Comptes AWS votre organisation. Les tables du catalogue de données contiennent des métadonnées relatives aux tables de données d'Amazon S3, des sources de données JDBC, d'Amazon Redshift, des sources de streaming et d'autres magasins de données. Cela permet aux utilisateurs d'exécuter des requêtes et des tâches ETL qui peuvent joindre et interroger des données sur plusieurs comptes. Pour plus d'informations, consultez la section Partage de	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	tables de catalogues de données et de bases de données entre AWS comptes dans le guide du AWS Lake Formation développeur.				

AWS License Manager

Vous pouvez partager les AWS License Manager ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Configurations de licence `license-manager:LicenseConfiguration`	Créez et gérez les configurations de licence de manière centralisée, et partagez-les avec d'autres Comptes AWS personnes ou avec	 N	 O Peut partager avec	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	votre organisation. Cela vous permet d'appliquer des règles de licence gérées de manière centralisée qui sont basées sur les termes de vos contrats d'entreprise sur plusieurs d'entre eux Comptes AWS. Pour plus d'informations, consultez la section Configurations de licence dans le License Manager dans le Guide de l'utilisateur du License Manager.		n'importe qui Compte AW		

AWS Marketplace

Vous pouvez partager les AWS Marketplace ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Entité Marketplace Catalog `aws-marketplace:Entity`	Créez, gérez et partagez des entités au sein Comptes AWS ou au sein de votre organisation dans AWS Marketplace. Pour plus d'informations, voir Partage de ressources AWS RAM dans la AWS Marketplace Catalog API référence.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

AWS Migration Hub Refactor Spaces

Vous pouvez partager les AWS Migration Hub Refactor Spaces ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Refactoriser l'environnement des espaces `refactor-spaces:Environment`	Créez un environnement Refactor Spaces et utilisez-le pour contenir vos applications Refactor Spaces. Partagez l'environnement avec d'autres comptes Comptes AWS ou avec tous les comptes de votre organisation. Cela permet à plusieurs utilisateurs Comptes AWS de consulter des informations sur l'environnement et les applications qu'il contient. Pour plus d'informations, consultez la section Sharing Refactor Spaces dans les environnements utilisés AWS RAM dans le guide de AWS Migration Hub Refactor Spaces l'utilisateur.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

AWS Network Firewall

Vous pouvez partager les AWS Network Firewall ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Politiques de pare-feu `network-firewall:FirewallPolicy`	Créez et gérez des politiques de pare-feu de manière centralisée, et partagez-les avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet à plusieurs comptes d'une organisation de partager un ensemble commun de comportements de surveillance, de protection et de filtrage du réseau. Pour plus d'informations, consultez la section Partage de politiques de pare-feu et de groupes de règles dans le Guide du AWS Network Firewall développeur.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service

Groupes de règles
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Créez et gérez des groupes de règles apatrides et dynamiques de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes d'une organisation AWS Organizations de partager un ensemble de critères d'inspection et de gestion du trafic réseau. Pour plus d'informations, consultez la section [Partage de politiques de pare-feu et de groupes de règles] dans le Guide du AWS Network Firewall développeur.	 O	 O
			
			Peut partager avec n'importe qui Compte AW
				 N	 Non

AWS Outposts

Vous pouvez partager les AWS Outposts ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Outposts `outposts:Outpost`	Créez et gérez des Outposts de manière centralisée, et partagez-les avec d'autres membres de votre Comptes AWS organisation. Cela permet à plusieurs comptes de créer des sous-réseaux et des volumes EBS sur vos Outposts partagés et gérés de manière centralisée. Pour plus d'informations, consultez la section Utilisation des ressources AWS Outposts partagées dans le Guide de l'AWS Outposts utilisateur.	 N	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Table de routage de passerelle locale `ec2:LocalGatewayRouteTable`	Créez et gérez des associations VPC avec une passerelle locale de manière centralisée, et partagez-les avec d'autres membres de votre Comptes AWS organisation. Cela permet à plusieurs comptes de créer des associations VPC avec une passerelle locale et d'afficher la configuration de la table de routage et de l'interface virtuelle. Pour plus d'informations, consultez les ressources Shareable Outpost dans le guide de l'AWS Outposts utilisateur.	 N	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Sites `outposts:Site`	Créez et gérez des sites Outpost et partagez-les avec d'autres membres Comptes AWS de votre organisation. Cela permet à plusieurs comptes de créer et de gérer des Outposts sur le site partagé et permet de partager le contrôle entre les ressources Outpost et le site. Pour plus d'informations, consultez la section Utilisation des ressources AWS Outposts partagées dans le Guide de l'AWS Outposts utilisateur.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Amazon S3 on Outposts

Vous pouvez partager la ressource Amazon S3 on Outposts suivante en utilisant. AWS RAM

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
S3 sur Outpost `s3-outposts:Outpost`	Créez et gérez des compartiments, des points d'accès et des points de terminaison Amazon S3 sur l'Outpost. Cela permet à plusieurs comptes de créer et de gérer des Outposts sur le site partagé et permet de partager le contrôle entre les ressources Outpost et le site. Pour plus d'informations, consultez la section Utilisation des ressources AWS Outposts partagées dans le Guide de l'AWS Outposts utilisateur.	 N	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 O	 Non

Explorateur de ressources AWS

Vous pouvez partager les Explorateur de ressources AWS ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Vues `resource-explorer-2:View`	Créez et configurez les vues Resource Explorer de manière centralisée, et partagez-les avec d'autres Comptes AWS membres de votre organisation. Cela permet aux rôles et aux utilisateurs multiples Comptes AWS de rechercher et de découvrir les ressources accessibles via la vue. Pour plus d'informations, consultez la section Partage des vues de l'explorateur de ressources dans le guide de Explorateur de ressources AWS l'utilisateur.	 N	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 N	 Non

AWS Resource Groups

Vous pouvez partager les AWS Resource Groups ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Groupes de ressources `resource-groups:Group`	Créez et gérez un groupe de ressources hôte de manière centralisée, et partagez-le avec d'autres Comptes AWS membres de votre organisation. Cela permet à plusieurs de Comptes AWS partager un groupe d'hôtes dédiés Amazon EC2 créés à l'aide de. AWS License Manager Pour plus d'informations, consultez la section [Groupes de ressources hôtes AWS License Manager dans](#) le Guide de AWS License Manager l'utilisateur.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Amazon Route 53

Vous pouvez partager les ressources Amazon Route 53 suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Groupes de règles du pare-feu DNS Route 53 Resolver `route53resolver:FirewallRuleGroup`	Créez et gérez les groupes de règles du pare-feu DNS Route 53 Resolver de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes de partager un ensemble de critères pour inspecter et gérer les requêtes DNS sortantes qui passent par Route 53 Resolver. Pour plus d'informations, consultez la section [Partage des groupes de règles du pare-feu DNS Route 53 Resolver entre Comptes AWS] eux dans le manuel du développeur Amazon Route 53.	O	O Peut partager avec n'importe qui Compte AW	N	Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Route 53 Profiles `route53profiles:Profile`	Créez et gérez Route 53 de Profiles manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes d'appliquer les configurations DNS spécifiées dans la Route 53 Profiles à plusieurs VPC. Pour plus d'informations, consultez Amazon Route 53 Profiles dans le manuel du développeur Amazon Route 53.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Règles du résolveur `route53resolver:ResolverRule`	Créez et gérez les règles Resolver de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes de transférer les requêtes DNS de leurs clouds privés virtuels (VPC) vers les adresses IP cibles définies dans les règles du résolveur partagées et gérées de manière centralisée. Pour plus d'informations, consultez les sections Partage des règles du résolveur avec d'autres utilisateurs Comptes AWS et utilisation de règles partagées dans le manuel du développeur Amazon Route 53.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Journaux de requêtes `route53resolver:ResolverQueryLogConfig`	Créez et gérez les journaux de requêtes de manière centralisée, et partagez-les avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet Comptes AWS à plusieurs d'entre eux de consigner les requêtes DNS provenant de leurs VPC dans un journal des requêtes géré de manière centralisée. Pour plus d'informations, consultez la section [Partager les configurations de journalisation des requêtes du résolveur avec d'autres Comptes AWS](#) personnes dans le guide du développeur Amazon Route 53.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Application Recovery Controller Amazon Route 53

Vous pouvez partager les ressources Amazon Route 53 Application Recovery Controller suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Cluster ARC Route 53 `route53-recovery-control:Cluster`	Créez et gérez les clusters ARC Route 53 de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes de créer des panneaux de contrôle et des contrôles de routage dans un seul cluster partagé, ce qui réduit la complexité et le nombre total de clusters dont une organisation a besoin. Pour plus d'informations, consultez la section Partage de clusters entre comptes dans le guide du développe	O	O Peut partager avec n'importe qui Compte AW	O	Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	ur d'Amazon Route 53 Application Recovery Controller.				

Amazon Simple Storage Service

Vous pouvez partager les Amazon Simple Storage Service ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Subventions d'accès `s3:AccessGrants`	Créez et gérez l'instance S3 Access Grants de manière centralisée, et partagez-la avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes de consulter	 Oui	 Oui Peut partager avec n'importe	 Oui	 Oui

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	et de supprimer des ressources partagées. Pour plus d'informations, consultez S3 Access octroie un accès entre comptes dans le guide de l' Amazon Simple Storage Service utilisateur.		qui Compte AW		

Amazon SageMaker

Vous pouvez partager les SageMaker ressources Amazon suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
SageMaker Catalogue	Pour la découvrabilité : permet aux propriétaires de comptes	 N	 O	 Oui	

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
`sagemaker:SagemakerCatalog`	d'accorder des autorisations de découvrabilité à d'autres comptes, pour toutes les ressources de groupes d'entités du SageMaker catalogue. Une fois l'accès accordé, les utilisateurs de ces comptes peuvent consulter les groupes de fonctionnalités qui ont été partagés avec eux dans le catalogue. Pour plus d'informations, consultez la section Découverte et accès aux groupes de fonctionnalités entre comptes dans le manuel Amazon SageMaker Developer Guide. **Note** La découvrabilité et l'accès		Peut partager avec n'importe qui Compte AW		

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	sont des autorisations distinctes dans. SageMaker				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
SageMaker Groupe de fonctionnalités `sagemaker:FeatureGroup`	Pour l'accès : permet aux propriétaires de comptes d'accorder des autorisations d'accès à d'autres comptes, pour certaines ressources de groupes de fonctionnalités. Une fois l'accès accordé, les utilisateurs de ces comptes peuvent utiliser les groupes de fonctionnalités qui ont été partagés avec eux. Pour plus d'informations, consultez la section Découverte et accès aux groupes de fonctionnalités entre comptes dans le manuel Amazon SageMaker Developer Guide. **Note** La découvrabilité et l'accès	 O	 O Peut partager avec n'importe qui Compte AW	 Oui	

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	sont des autorisations distinctes dans. SageMaker				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Groupe de lignées `sagemaker:LineageGroup`	Amazon vous SageMaker permet de créer des groupes de lignage à partir des métadonnées de votre pipeline afin de mieux comprendre son historique et ses relations. Partagez le groupe de lignage avec d'autres comptes Comptes AWS ou avec les comptes de votre organisation. Cela permet à plusieurs utilisateurs Comptes AWS de consulter les informations sur le groupe de lignage et d'interroger les entités de suivi qu'il contient. Pour plus d'informations, consultez la section Suivi du lignage entre comptes dans le manuel Amazon	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	SageMaker Developer Guide.				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
SageMaker Cartes modèles `sagemaker:ModelCard`	Amazon SageMaker crée des fiches modèles pour documenter les détails essentiels de vos modèles d'apprentissage automatique (ML) en un seul endroit afin de rationaliser la gouvernance et les rapports. Partagez vos cartes modèles avec d'autres comptes Comptes AWS ou avec les comptes de votre organisation afin de mettre en place une stratégie multi-comptes pour vos opérations d'apprentissage automatique. Cela permet Comptes AWS de partager l'accès aux cartes modèles pour leurs activités de machine learning avec d'autres comptes. Pour	 Oui	 Oui Peut partager avec n'importe qui Compte AWS	 Non	

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	plus d'informations, consultez la section Amazon SageMaker Model Cards dans le manuel Amazon SageMaker Developer Guide.				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
SageMaker oléoduc `sagemaker:Pipeline`	Avec Amazon SageMaker Model Building Pipelines, vous pouvez créer, automatiser et gérer des flux de travail de end-to-end machine learning à grande échelle. Partagez vos pipelines avec d'autres comptes Comptes AWS ou avec les comptes de votre organisation afin de mettre en place une stratégie multi-comptes pour vos opérations d'apprentissage automatique. Cela permet à plusieurs Comptes AWS utilisateurs de consulter des informations sur un pipeline et ses exécutions avec un accès facultatif pour démarrer, arrêter et réessayer des	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	pipelines à partir d'autres comptes. Pour plus d'informations, consultez la section Support entre comptes pour les SageMaker pipelines dans le manuel Amazon SageMaker Developer Guide.				

AWS Service Catalog AppRegistry

Vous pouvez partager les AWS Service Catalog AppRegistry ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Application `servicecatalog:Application`	Créez une application et utilisez-la pour suivre les ressources appartenant à cette application dans l'ensemble de votre AWS environnement. Partagez l'application avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs Comptes AWS utilisateurs de consulter des informations sur l'application et les ressources associées localement. Pour plus d'informations, consultez la section Création d'applications dans le Guide de l'utilisateur du Service Catalog.	 N	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Groupe d'attributs `servicecatalog:AttributeGroup`	Créez un groupe d'attributs et utilisez-le pour stocker les métadonnées relatives à vos applications. Partagez les groupes d'attributs avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs utilisateurs Comptes AWS de consulter les informations relatives aux groupes d'attributs. Pour plus d'informations, consultez la section Création de groupes d'attributs dans le Guide de l'utilisateur du Service Catalog.	N	N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	O	Non

AWS Systems Manager Incident Manager

Vous pouvez partager les AWS Systems Manager Incident Manager ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Contacts `ssm-contacts:Contact`	Créez et gérez les contacts et les plans d'escalade de manière centralisée, et partagez les coordonnées avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à de nombreuses personnes de Comptes AWS visualiser les engagements survenant lors d'un incident. Pour plus d'informations, consultez la section Utilisation de contacts partagés et de plans de réponse dans le guide de l'utilisateur de AWS Systems Manager Incident Manager.	 Oui	 Oui Peut partager avec n'importe qui Compte AW	 Oui	 Non
Plans de réponse	Créez et gérez des plans d'intervention de manière centralisée, et partagez-les avec	 Oui	 Oui	 Oui	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
`ssm-incidents:ResponsePlan`	d'autres Comptes AWS personnes ou avec votre organisation. Cela leur permet de Comptes AWS relier les CloudWatch alarmes Amazon et les règles relatives aux EventBridge événements Amazon aux plans de réponse, créant ainsi automatiquement un incident lorsqu'il est détecté. L'incident a également accès aux métriques de ces autres Comptes AWS. Pour plus d'informations, consultez la section Utilisation de contacts partagés et de plans de réponse dans le guide de l'utilisateur de AWS Systems Manager Incident Manager.		Peut partager avec n'importe qui Compte AW		

AWS Systems Manager Magasin de paramètres

Vous pouvez partager les ressources AWS Systems Manager Parameter Store suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Paramètre `ssm:Parameter`	Créez un paramètre et utilisez-le pour stocker des données de configuration auxquelles vous pouvez faire référence dans vos scripts, commandes, documents SSM et flux de travail de configuration et d'automatisation. Partagez le paramètre avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs Comptes AWS utilisateurs de consulter les informations relatives à la chaîne et d'améliorer la sécurité en séparant vos données de votre code. Pour	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	plus d'informations, consultez la section Utilisation de paramètres partagés dans le Guide de AWS Systems Manager l'utilisateur.				

Amazon VPC

Vous pouvez partager les ressources Amazon Virtual Private Cloud (Amazon VPC) suivantes en utilisant. AWS RAM

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Adresses IPv4 appartenant au client `ec2:CoipPool`	Au cours du processus AWS Outposts d'installation, AWS crée un pool d'adresses, appelé pool d'adresse	N	N	N	Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	s IP appartenant au client, sur la base des informations que vous fournissez concernant votre réseau local. Les adresses IP appartenant aux clients fournissent une connectivité locale ou externe aux ressources de vos sous-réseaux Outposts via votre réseau local. Vous pouvez attribuer ces adresses aux ressources de votre Outpost, telles que les instances EC2, en utilisant des adresses IP élastiques ou en utilisant le paramètre de sous-réseau qui attribue automatiquement les adresses IP appartenant aux clients. Pour plus d'informations, voir Adresses IP appartena		Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.		

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	nt au client dans le Guide de l'utilisateur AWS Outposts .				
Pools de gestionnaires d'adresses IP (IPAM) `ec2:IpamPool`	Partagez des pools IPAM Amazon VPC de manière centralisée avec d'autres rôles ou utilisateurs IAM Comptes AWS, ou avec l'ensemble d'une organisation ou d'une unité organisationnelle (UO). AWS Organizations Cela permet à ces principaux d'allouer des CIDR du pool à AWS des ressources, telles que des VPC, dans leurs comptes respectifs. Pour plus d'informations, consultez Partager un pool IPAM à l'aide du guide AWS RAM de l'utilisateur du gestionnaire d'adresses IP Amazon VPC.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Découvertes de ressources du gestionnaire d'adresses IP (IPAM) `ec2:IpamResourceDiscovery`	Partagez les découvertes de ressources avec d'autres Comptes AWS. Une découverte de ressources est un composant IPAM Amazon VPC qui permet à IPAM de gérer et de surveiller les ressources appartenant au compte propriétaire. Pour plus d'informations, consultez la section Travailler avec les découvertes de ressources dans le guide de l'utilisateur Amazon VPC IPAM.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Listes de préfixes `ec2:PrefixList`	Créez et gérez des listes de préfixes de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet d'inclure plusieurs listes de préfixes de Comptes AWS référence dans leurs ressources, telles que les groupes de sécurité VPC et les tables de routage de sous-réseaux. Pour plus d'informations, consultez la section Utilisation de listes de préfixes partagées dans le guide de l'utilisateur Amazon VPC.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Sous-réseaux `ec2:Subnet`	Créez et gérez des sous-réseaux de manière centralisée, et partagez-les au Comptes AWS sein de votre organisation. Cela permet à plusieurs de Comptes AWS lancer leurs ressources applicatives dans des VPC gérés de manière centralisée. Ces ressources incluent les instances Amazon EC2, les bases de données Amazon Relational Database Service (RDS), les clusters Amazon Redshift et les fonctions . AWS Lambda Pour plus d'informations, consultez la section Utilisation du partage VPC dans le guide de l'utilisateur Amazon VPC.	 N	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	Note Pour inclure un sous-réseau lorsque vous créez un partage de ressources, vous devez disposer des autorisations `ec2:DescribeVpcs` `ec2:DescribeSubnets` et, en plus `deram:CreateResourceShare`. Les sous-réseaux par défaut ne sont pas partageables. Vous ne pouvez partager que les sous-réseaux que vous				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	avez créés vous-même.				
Cibles reflétant le trafic `ec2:TrafficMirrorTarget`	Créez et gérez des cibles reflétant le trafic de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs utilisateurs d' Comptes AWS envoyer du trafic réseau en miroir depuis des sources de trafic miroir de leurs comptes vers une cible miroir de trafic partagée et gérée de manière centralisée. Pour plus d'informations, consultez la section Cibles de mise en miroir du trafic entre comptes dans le Guide de mise en miroir du trafic.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Passerelles de transit `ec2:TransitGateway`	Créez et gérez les passerelles de transport en commun de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs Comptes AWS itinéraires de trafic entre leurs VPC et les réseaux sur site via une passerelle de transit partagée et gérée de manière centralisée. Pour plus d'informations, consultez Partage d'une passerelle de transit dans les passerelles de transit Amazon VPC. **Note** Pour inclure une passerelle de transit lorsque vous	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
	créez un partage de ressources, vous devez disposer de l'`ec2:DescribeTransitGateway` autorisation en plus de `ram:CreateResourceShare` .				

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Domaines de multidiffusion Transit Gateway `ec2:TransitGatewayMulticastDomain`	Créez et gérez les domaines de multidiffusion des passerelles de transit de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs d' Comptes AWS enregistrer et de désenregistrer des membres du groupe ou des sources de groupe dans le domaine de multidiffusion. Pour plus d'informations, consultez la section Utilisation de domaines de multidiffusion partagés dans le Guide des passerelles de transit.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Accès vérifié par AWS groupe `ec2:VerifiedAccessGroup`	Créez et gérez Accès vérifié par AWS des groupes de manière centralisée, puis partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet aux applications de plusieurs comptes d'utiliser un ensemble unique et partagé de Accès vérifié par AWS points de terminaison. Pour plus d'informations, consultez la section Partager votre Accès vérifié par AWS groupe AWS Resource Access Manager dans le guide de Accès vérifié par AWS l'utilisateur.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Amazon VPC Lattice

Vous pouvez partager les ressources Amazon VPC Lattice suivantes en utilisant. AWS RAM

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Service Amazon VPC Lattice `vpc-lattice:Service`	Créez et gérez les services Amazon VPC Lattice de manière centralisée, et partagez-les avec des particuliers Comptes AWS ou avec votre organisation. Cela permet aux propriétaires de services de se connecter, de sécuriser et d'observer les service-to-service communications dans un environnement multi-comptes. Pour plus d'informations, consultez la section Utilisation de ressources partagées dans le guide de l'utilisateur de VPC Lattice.	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Non
Réseau de services Amazon VPC Lattice	Créez et gérez les réseaux de services Amazon VPC Lattice de manière centralis	 N	 O	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
`vpc-lattice:ServiceNetwork`	ée, et partagez-les avec des particuliers Comptes AWS ou avec votre organisation. Cela permet aux propriétaires de réseaux de services de se connecter, de sécuriser et d'observer les service-to-service communications dans un environnement multi-comptes. Pour plus d'informations, consultez la section Travailler avec des ressources partagées dans le guide de l'utilisateur Amazon VPC Lattice.		Peut partager avec n'importe qui Compte AW		

AWS Réseau WAN dans le cloud

Vous pouvez partager les ressources AWS Cloud WAN suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut être partagé avec les utilisateurs et les rôles IAM	Peut partager avec des comptes extérieurs à son organisation	Peut utiliser les autorisations gérées par le client	Peut être partagé avec les responsables du service
Réseau central Cloud WAN `networkmanager:CoreNetwork`	Créez et gérez un réseau central Cloud WAN de manière centralisée, et partagez-le avec d'autres Comptes AWS. Cela permet Comptes AWS à plusieurs hôtes d'accéder et de provisionner des hôtes sur un seul réseau central Cloud WAN. Pour plus d'informations, consultez la section Partager un réseau central dans le Guide de l'utilisateur du AWS Cloud WAN.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Gestion des autorisations dansAWS RAM

DansAWS RAM, il existe deux types d'autorisations gérées, les autorisationsAWS gérées et les autorisations gérées par le client.

Les autorisations gérées définissent la manière dont un consommateur peut agir sur les ressources d'un partage de ressources. Lorsque vous créez un partage de ressources, vous devez spécifier l'autorisation gérée à utiliser pour chaque type de ressource inclus dans le partage de ressources. Le modèle de stratégie inclus dans l'autorisation gérée contient tous les éléments nécessaires à une stratégie basée sur les ressources, à l'exception du principal et de la ressource. L'Amazon Resource Name (ARN) de la ressource et l'ARN des ressources. AWS RAMcrée ensuite la politique basée sur les ressources qu'il associe à toutes les ressources de ce partage de ressources.

Chaque autorisation gérée peut avoir une ou plusieurs versions. Une version est désignée comme version par défaut pour cette autorisation gérée. De temps en temps,AWS met à jour une autorisationAWS gérée pour un type de ressource en créant une nouvelle version et en désignant cette nouvelle version comme version par défaut. Vous pouvez également mettre à jour les autorisations gérées par vos clients en créant de nouvelles versions. Les autorisations gérées qui sont déjà associées à un partage de ressources ne sont pas automatiquement mises à jour. LaAWS RAM console indique quand une nouvelle version par défaut est disponible et vous pouvez consulter les modifications apportées à la nouvelle version par défaut par rapport à la précédente.

> **Note**
>
> Nous vous recommandons de passer à la nouvelle version des autorisationsAWS gérées. Ces mises à jour ajoutent généralement la prise en charge des nouvelles ou des mises à jourServices AWS qui peuvent partager des types de ressources supplémentaires à l'aide deAWS RAM. Une nouvelle version par défaut peut également corriger les failles de sécurité.

> **Important**
>
> Vous pouvez uniquement associer la version par défaut de l'autorisation gérée à un nouveau partage de ressources.

Vous pouvez récupérer la liste des autorisations gérées disponibles. Pour plus d'informations, veuillez consulter Affichage des autorisations gérées.

Rubriques

Affichage des autorisations gérées

Vous pouvez consulter les détails des autorisations gérées que vous pouvez attribuer aux types de ressources dans vos partages de ressources. Vous pouvez identifier les autorisations gérées qui sont attribuées aux partages de ressources. Pour consulter ces informations, utilisez la bibliothèque d'autorisations gérées de laAWS RAM console.

Console

Pour afficher des informations détaillées sur les autorisations gérées disponibles dansAWS RAM

1. Accédez à la page de la bibliothèque d'autorisations gérées dans laAWS RAM console.
2. Comme les partages deAWS RAM ressources existentRégion AWS de manière spécifiqueRégions AWS, choisissez la plus appropriée dans la liste déroulante dans le coin supérieur droit de la console. Pour afficher les partages de ressources qui contiennent des ressources globales, vous devezRégion AWS définir le sur USA Est (Virginie du Nord), (`us-east-1`). Pour plus d'informations sur le partage de ressources mondiales, consultezPartage des ressources régionales par rapport aux ressources mondiales. Bien que toutes les régions partagent les mêmes autorisationsAWS gérées disponibles, cela affecte le nombre de partages de ressources associés affichés pour chaque autorisation gérée dansStep 5. Les autorisations gérées par le client ne sont disponibles que dans la région dans laquelle elles ont été créées.
3. Dans la liste des autorisations gérées, choisissez la permission gérée pour laquelle vous souhaitez afficher les détails. Vous pouvez utiliser la zone de recherche pour filtrer la liste

des autorisations gérées en saisissant une partie d'un nom ou un type de ressource, ou en choisissant un type d'autorisations gérées dans la liste déroulante.

4. (Facultatif) Pour modifier les préférences d'affichage, cliquez sur l'icône d'engrenage dans le coin supérieur droit du panneau des autorisations gérées. Vous pouvez modifier les préférences suivantes :

   - Taille de page : nombre de ressources affichées sur chaque page.
   - Lignes d'enroulement : indique si les lignes doivent être enroulées dans les lignes du tableau.
   - Colonnes : indique s'il faut afficher ou masquer les informations relatives au type de ressource et aux partages associés.

   Une fois que vous avez fini de définir les préférences d'affichage, choisissez Confirmer.

5. Pour chaque autorisation gérée, la liste affiche les informations suivantes :

   - Nom de l'autorisation gérée : nom de l'autorisation gérée.
   - Type de ressource : type de ressource associé à l'autorisation gérée.
   - Type d'autorisation gérée : indique si l'autorisation gérée est une autorisationAWS gérée ou une autorisation gérée par le client.
   - Partages associés : nombre de partages de ressources associés à l'autorisation gérée. Si un nombre apparaît, vous pouvez le choisir pour afficher un tableau des partages de ressources contenant les informations suivantes :
     - Nom du partage de ressources : nom du partage de ressources associé à l'autorisation gérée.
     - Version des autorisations gérées : version de l'autorisation gérée associée à ce partage de ressources.
     - Propriétaire :Compte AWS numéro du propriétaire du partage de ressources.
     - Autoriser les responsables externes : indique si ce partage de ressources autorise le partage avec des responsables extérieurs à l'organisation dansAWS Organizations.
     - Statut : statut actuel de l'association entre le partage de ressources et l'autorisation gérée.
   - État : indique si l'autorisation gérée est :
     - Joignable : vous pouvez associer l'autorisation gérée à vos partages de ressources.

- Injoignable : vous ne pouvez pas associer l'autorisation gérée à vos partages de ressources.
- Suppression : l'autorisation gérée n'est plus active et sera bientôt supprimée.
- Supprimé : l'autorisation gérée a été supprimée. Il reste visible pendant deux heures avant de disparaître de la bibliothèque d'autorisations gérées.

Vous pouvez choisir le nom de l'autorisation gérée pour afficher plus d'informations sur cette autorisation gérée. La page de détails sur une autorisation gérée affiche les informations suivantes :

- Type de ressource : type deAWS ressource auquel s'applique cette autorisation gérée.
- Nombre de versions : vous pouvez avoir jusqu'à cinq versions d'une autorisation gérée par le client.
- Version par défaut — Spécifie quelle version est la version par défaut et donc attribuée automatiquement à tous les nouveaux partages de ressources qui utilisent cette autorisation gérée. Tout partage de ressources existant qui utilise des versions différentes affiche une invite vous demandant de mettre à jour le partage de ressources vers la version par défaut.
- ARN : nom de ressource Amazon (ARN) de l'autorisation gérée. Les ARN pour les autorisationsAWS gérées utilisent le format suivant :

  `arn:aws:ram::aws:permission/AWSRAM[DefaultPermission]ShareableResourceType`

  La sous-chaîne*[DefaultPermission]* (sans les crochets dans un ARN réel) est présente dans le nom de la seule autorisation gérée pour ce type de ressource qui est désigné par défaut.
- Versions avec autorisations gérées : vous pouvez choisir les informations relatives à la version à afficher dans les onglets situés sous cette liste déroulante.
  - Onglet Détails :
    - Heure de création : date et heure de création de cette version de l'autorisation gérée.
    - Heure de la dernière mise à jour : date et heure de la dernière mise à jour de cette version de l'autorisation gérée.

- Onglet modèle de politique : liste des actions de service et des conditions, le cas échéant, que cette version de l'autorisation gérée autorise les principaux à exécuter sur le type de ressource associé.
- Partages de ressources associés : liste des partages de ressources qui utilisent cette version de l'autorisation gérée.

AWS CLI

Pour afficher des informations détaillées sur les autorisations gérées disponibles dansAWS RAM

Vous pouvez utiliser la list-permissionscommande pour obtenir la liste des autorisations gérées pouvant être utilisées sur les partages de ressources en coursRégion AWS pour le compte appelant.

```
$ aws ram list-permissions
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:31.732000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-11-18T07:05:46.976000-08:00",
```

```
            "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },

        ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
 PERMISSIONS ...

        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "resourceType": "networkmanager:CoreNetwork",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:46.557000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
            "version": "1",
            "defaultVersion": true,
            "name": "My-Test-CMP",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2023-03-08T06:54:10.038000-08:00",
            "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "CUSTOMER_MANAGED"
        }
    ]
}
```

Vous pouvez également trouver l'ARN d'une autorisation gérée spécifique par son nom dans le`--query` paramètre de la`list-permissions`AWS CLI commande. L'exemple suivant filtre la sortie pour n'inclure dans les résultats du`permissions` tableau que les éléments correspondant au nom spécifié. Nous précisons également que nous voulons voir uniquement le champ ARN dans les résultats, et au format texte brut au lieu du JSON par défaut.

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
```

```
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

Une fois que vous avez trouvé l'ARN de l'autorisation gérée spécifique qui vous intéresse, vous pouvez récupérer ses détails, y compris le texte de sa politique JSON, en exécutant la commande get-permission.

```
$ aws ram get-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
        "version": "1",
        "defaultVersion": true,
        "name": "My-Test-CMP",
        "resourceType": "ec2:IpamPool",
        "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```

Création et utilisation d'autorisations gérées par le client dansAWS RAM

AWS Resource Access Manager(AWS RAM) fournit au moins une autorisationAWS gérée pour chaque type de ressource que vous pouvez partager. Toutefois, il se peut que ces autorisations gérées ne fournissent pas l'accès avec le moindre privilège pour votre cas d'utilisation en matière de partage. Lorsque l'une des autorisationsAWS gérées fournies ne fonctionne pas, vous pouvez créer votre propre autorisation gérée par le client.

Les autorisations gérées par le client sont des autorisations gérées que vous créez et gérez en spécifiant précisément quelles actions peuvent être effectuées et dans quelles conditions avec les ressources partagéesAWS RAM. Par exemple, vous souhaitez limiter l'accès en lecture à vos pools Amazon VPC IP Address Manager (IPAM), qui vous aident à gérer vos adresses IP à grande échelle. Vous pouvez créer des autorisations gérées par le client pour que vos développeurs puissent attribuer des adresses IP, mais vous ne pouvez pas consulter la plage d'adresses IP attribuées par d'autres comptes de développeurs. Vous pouvez suivre la bonne pratique du privilège, principe du privilège, principe du privilège, principe qui ne faut accorder que les autorisations requises pour des tâches sur des ressources partagées.

En outre, vous pouvez mettre à jour ou supprimer les autorisations gérées par le client selon vos besoins.

Rubriques

Créer une autorisation gérée par le client

Les autorisations gérées par le client sont spécifiques à unRégion AWS. Assurez-vous de créer cette autorisation gérée par le client dans la région appropriée.

Console

Pour créer une autorisation gérée par le client

1. Effectuez l'une des actions suivantes :
   - Accédez à la bibliothèque d'autorisations gérées et choisissez Créer une autorisation gérée par le client.
   - Accédez directement à la page Créer une autorisation gérée par le client dans la console.
2. Pour les détails des autorisations gérées par le client, entrez un nom d'autorisation gérée par le client.
3. Choisissez le type de ressource auquel cette autorisation gérée s'applique.

4. Pour le modèle de politique, vous définissez les opérations autorisées à être effectuées sur ce type de ressource.

   - Vous pouvez choisir Importer une autorisation gérée pour utiliser les actions d'une autorisation gérée existante.
   - Sélectionnez ou désélectionnez les informations de niveau d'accès pour répondre à vos besoins dans l'éditeur visuel.
   - Ajoutez ou modifiez des conditions à l'aide de l'éditeur JSON.

5. (Facultatif) Pour associer des balises à l'autorisation gérée, dans Tags, entrez une clé et une valeur de balise. Ajoutez des balises supplémentaires en choisissant Ajouter une nouvelle étiquette. Répétez cette étape si nécessaire.
6. Lorsque vous avez terminé, choisissez Create Customer Managed Permission.

AWS CLI

Pour créer une autorisation gérée par le client

- Exécutez la commande create-permission et spécifiez un nom, le type de ressource auquel s'applique l'autorisation gérée par le client et le corps du texte du modèle de politique.

  L'exemple de commande suivant crée une autorisation gérée pour le type de`imagebuilder:Component` ressource.

```
$ aws ram create-permission \
    --name TestCMP \
    --resource-type imagebuilder:Component \
    --policy-template "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}"
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "1",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "resourceType": "imagebuilder:Component",
        "status": "ATTACHABLE",
        "creationTime": 1680033769.401,
        "lastUpdatedTime": 1680033769.401
```

```
    }
}
```

Créer une nouvelle version d'une autorisation gérée par le client

Si le cas d'utilisation de votre autorisation gérée par le client change, vous pouvez créer une nouvelle version de l'autorisation gérée. Cela n'affecte pas vos partages de ressources existants, mais uniquement les nouveaux partages de ressources à venir qui utilisent cette autorisation gérée par le client.

Chaque autorisation gérée peut avoir jusqu'à cinq versions, mais vous ne pouvez associer que la version par défaut.

Console

Pour créer une nouvelle version d'une autorisation gérée par le client

1. Accédez à la bibliothèque des autorisations gérées.
2. Filtrez la liste des autorisations gérées par le client ou recherchez le nom de l'autorisation gérée par le client que vous souhaitez modifier.
3. Sur la page de détails des autorisations gérées, dans la section Versions des autorisations gérées, choisissez Créer une version.
4. Pour le modèle de politique, vous pouvez ajouter ou supprimer des actions et des conditions à l'aide de l'éditeur visuel ou de l'éditeur JSON.

   Vous avez également la possibilité de choisir Importer une autorisation gérée pour utiliser un modèle de politique existant.
5. Lorsque vous avez terminé, choisissez Create version en bas de la page.

AWS CLI

Pour créer une nouvelle version d'une autorisation gérée par le client

1. Recherchez l'Amazon Resource Name (ARN) de l'autorisation gérée pour laquelle vous souhaitez créer une nouvelle version. Pour ce faire, appelez list-permissions avec le `--permission-type CUSTOMER_MANAGED` paramètre pour inclure uniquement les autorisations gérées par le client.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. Une fois que vous avez obtenu l'ARN, vous pouvez appeler l'create-permission-versionopération et fournir le modèle de politique mis à jour.

```
$ aws ram create-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "2",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "status": "ATTACHABLE",
        "resourceType": "imagebuilder:Component",
        "permission": "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}",
        "creationTime": 1680038973.79,
        "lastUpdatedTime": 1680038973.79
    }
}
```

La sortie inclut le numéro de version de la nouvelle version.

Choisissez une autre version comme version par défaut pour une autorisation gérée par le client

Vous pouvez définir une autre version d'autorisation gérée par le client comme nouvelle version par défaut.

Console

Pour définir une nouvelle version par défaut pour une autorisation gérée par le client

1. Accédez à la bibliothèque des autorisations gérées.
2. Filtrez la liste des autorisations gérées par le client ou recherchez le nom de l'autorisation gérée par le client que vous souhaitez modifier.
3. Sur la page de détails des autorisations gérées par le client, dans la section Versions des autorisations gérées, utilisez la liste déroulante pour choisir la version que vous souhaitez définir comme nouvelle version par défaut.
4. Choisissez Définir comme version par défaut.
5. Lorsque la boîte de dialogue apparaît, confirmez que vous souhaitez que cette version soit la version par défaut pour tous les nouveaux partages de ressources qui utilisent cette autorisation gérée par le client. Si vous êtes d'accord, choisissez Définir comme version par défaut.

AWS CLI

Pour définir une nouvelle version par défaut pour une autorisation gérée par le client

1. Trouvez le numéro de version que vous souhaitez définir comme version par défaut en appelant list-permission-versions.

   L'exemple de commande suivant récupère les versions actuelles pour l'autorisation gérée spécifiée.

```
$ aws ram list-permission-versions \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "permissions": [
        {
```

```
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "1",
            "defaultVersion": false,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "UNATTACHABLE",
            "creationTime": 1680033769.401,
            "lastUpdatedTime": 1680035597.345
        },
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. Une fois que vous avez défini le numéro de version par défaut, vous pouvez lancer l'set-default-permission-versionopération.

```
$ aws ram-cmp set-default-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 2
```

Cette commande ne renvoie aucun résultat en cas de succès. Vous pouvez exécuter list-permission-versionsà nouveau et vérifier que le`defaultVersion` champ de la version choisie est désormais défini sur`true`.

Supprimer une version d'autorisation gérée par le client

Vous pouvez avoir jusqu'à cinq versions pour chaque autorisation gérée par le client. Lorsqu'une version n'est plus nécessaire et n'est plus utilisée, vous pouvez la supprimer. Vous ne pouvez pas supprimer la version par défaut d'une autorisation gérée par le client. Les versions supprimées restent visibles dans la console pendant deux heures au maximum avec un statut de suppression avant d'être complètement supprimées.

Console

Pour supprimer une version d'autorisation gérée par le client

1. Accédez à la bibliothèque des autorisations gérées.
2. Filtrez la liste des autorisations gérées par le client ou recherchez le nom de l'autorisation gérée par le client avec la version que vous souhaitez supprimer.
3. Assurez-vous que la version que vous souhaitez supprimer n'est pas actuellement la version par défaut.
4. Dans la section Versions de la page, choisissez l'onglet Partages de ressources associés pour voir si des partages utilisent cette version.

   Si des partages sont associés, vous devez modifier la version des autorisations gérées par le client avant de pouvoir supprimer cette version.
5. Choisissez Supprimer la version sur le côté droit de la section Version.
6. Dans la boîte de dialogue de confirmation, choisissez Supprimer pour confirmer la suppression de cette version de votre autorisation gérée par le client.

   Choisissez Annuler si vous ne souhaitez pas supprimer cette version de votre autorisation gérée par le client.

AWS CLI

Pour supprimer une version d'une autorisation gérée par le client

1. Appelez l'list-permission-versionsopération pour récupérer les numéros de version disponibles.
2. Une fois que vous avez le numéro de version, fournissez-le en tant que paramètre à delete-permission-version.

```
$ aws ram-cmp delete-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 1
```

Cette commande ne renvoie aucun résultat en cas de succès. Vous pouvez exécuter list-permission-versionsà nouveau et vérifier que la version n'est plus incluse dans la sortie.

Supprimer une autorisation gérée par le client

Si une autorisation gérée par le client n'est plus nécessaire et n'est plus utilisée, vous pouvez la supprimer. Vous ne pouvez pas supprimer une autorisation gérée par le client associée à un partage de ressources. L'autorisation gérée par le client supprimée disparaît au bout de deux heures. D'ici là, il reste visible dans la bibliothèque d'autorisations gérées avec un statut supprimé.

Console

Pour supprimer une autorisation gérée par le client

1. Accédez à la bibliothèque des autorisations gérées.
2. Filtrez la liste des autorisations gérées par le client ou recherchez le nom de l'autorisation gérée par le client que vous souhaitez supprimer.
3. Vérifiez qu'aucun partage n'est associé dans la liste des autorisations gérées avant de sélectionner l'autorisation gérée par le client.

   S'il existe toujours des partages de ressources associés à l'autorisation gérée, vous devez attribuer une autre autorisation gérée à tous les partages de ressources avant de pouvoir continuer.
4. Dans le coin supérieur droit de la page de détails des autorisations gérées par le client, choisissez Supprimer l'autorisation gérée.
5. Lorsque la boîte de dialogue de confirmation apparaît, choisissez Supprimer pour supprimer l'autorisation gérée.

AWS CLI

Pour supprimer une autorisation gérée par le client

1. Trouvez l'ARN de l'autorisation gérée que vous souhaitez supprimer en appelant list-permissions avec le`--permission-type CUSTOMER_MANAGED` paramètre pour inclure uniquement les autorisations gérées par le client.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. Une fois que vous avez obtenu l'ARN de l'autorisation gérée de suppression, fournissez-le en tant que paramètre pour delete-permission.

```
$ aws ram delete-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "returnValue": true,
    "permissionStatus": "DELETING"
}
```

Mise àAWS niveau des autorisations gérées vers une version plus récente

AWSMet parfois à jour les autorisationsAWS gérées pouvant être associées à un partage de ressources pour un type de ressource spécifique. Lorsque cela estAWS fait, une nouvelle version de l'autorisationAWS gérée est créée. Les partages de ressources qui incluent le type de ressource spécifié ne sont pas automatiquement mis à jour pour utiliser la dernière version de l'autorisation gérée. Vous devez mettre à jour explicitement l'autorisation gérée pour chaque partage de ressources. Cette étape supplémentaire est requise pour que vous puissiez évaluer les modifications avant de les appliquer à vos partages de ressources.

Console

Chaque fois que la console affiche une page répertoriant les autorisations associées à un partage de ressources et qu'une ou plusieurs de ces autorisations utilisent une version autre que la version par défaut pour l'autorisation, la console affiche une bannière en haut de la page de console. La bannière indique que votre partage de ressources utilise une version autre que la version par défaut.

En outre, les autorisations individuelles peuvent afficher un bouton Mettre à jour la version par défaut à côté du numéro de version actuel lorsque cette version n'est pas la version par défaut.

Cliquez sur ce bouton pour démarrer l'assistant de mise à jour du partage de ressources. À l'étape 2 de l'assistant, vous pouvez mettre à jour la version de toutes les autorisations autres que celles par défaut afin d'utiliser leurs versions par défaut.

Les modifications ne sont pas enregistrées tant que vous n'avez pas terminé l'assistant en choisissant Soumettre sur la dernière page de l'assistant.

> **Note**
>
> Vous ne pouvez joindre que la version par défaut et vous ne pouvez pas revenir à une autre version.
> Pour les autorisations gérées par le client, après avoir mis à jour les autorisations vers la version par défaut, vous ne pouvez pas appliquer une autre version à un partage de ressources, sauf si vous avez d'abord défini cette autre version comme version par défaut. Par exemple, si vous avez mis à jour une autorisation vers la version par défaut, puis que vous avez détecté une erreur que vous souhaitez annuler, vous pouvez désigner la version précédente comme version par défaut. Vous pouvez également créer une

nouvelle version différente, puis la désigner comme version par défaut. Après avoir exécuté l'une de ces options, vous devez mettre à jour vos partages de ressources pour utiliser ce qui est désormais la version par défaut.

AWS CLI

Pour mettre à jour la version d'une autorisationAWS gérée

1. Exécutez la commande get-resource-sharesavec le`--permission-arn` paramètre pour spécifier le nom de ressource Amazon (ARN) de l'autorisation gérée que vous souhaitez mettre à jour. La commande renvoie donc uniquement les partages de ressources qui utilisent cette autorisation gérée.

   Par exemple, l'exemple de commande suivant renvoie les détails de chaque partage de ressources qui utilise l'autorisationAWS gérée par défaut pour les réservations de capacité Amazon EC2.

   ```
   $ aws ram get-resource-shares \
       --resource-owner SELF \
       --permission-arn arn:aws:ram::aws:permission/
   AWSRAMDefaultPermissionCapacityReservation
   ```

   La sortie inclut l'ARN de chaque partage de ressources avec au moins une ressource dont l'accès est contrôlé par cette autorisation gérée.
2. Pour chaque partage de ressources spécifié dans la commande précédente, exécutez la commande associate-resource-share-permission. Incluez le`--resource-share-arn` pour spécifier le partage de ressources à mettre`--permission-arn` à jour, le pour spécifier l'autorisationAWS gérée que vous mettez à jour et le`--replace` paramètre pour spécifier que vous souhaitez mettre à jour le partage afin d'utiliser la dernière version de cette autorisation gérée. Il n'est pas nécessaire de spécifier le numéro de version ; la version par défaut est automatiquement utilisée.

   ```
   $ aws ram associate-resource-share-permission \
       --resource-share-arn < ARN of one of the shares from the output of the
    previous command > \
       --permission-arn arn:aws:ram::aws:permission/
   AWSRAMDefaultPermissionCapacityReservation \
       --replace
   ```

3. Répétez la commande de l'étape précédente pour chaque commande`ResourceShareArn` que vous avez reçue dans les résultats de la commande de l'étape 1.

Considérations relatives à l'utilisation des autorisations gérées par le client dansAWS RAM

Les autorisations gérées par le client ne sont disponiblesRégion AWS que dans la version dans laquelle vous les créez. Les types de ressources ne prennent pas tous en charge les autorisations gérées par le client. Pour obtenir la liste des types de ressources pris en charge dansAWS Resource Access Manager, consultezRessources partageables AWS.

Les autorisations gérées par le client avec plusieurs instructions ne sont pas prises en charge. Vous ne pouvez utiliser qu'un seul opérateur non négatif dans les autorisations gérées par le client.

Les conditions suivantes ne sont pas prises en charge dans les autorisations gérées par le client :

- Le directeur de l'organisation était chargé de :
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Principal d'un service spécifique lié à :
  - `aws:SourceArn`
  - `aws:SourceAccount`
- Tags du système :
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

Comment fonctionnent les autorisations gérées

Pour une présentation rapide, regardez la vidéo suivante qui montre comment les autorisations gérées vous permettent d'appliquer la meilleure pratique du moindre privilège d'accès à vosAWS ressources.

Cette vidéo montre comment créer et associer des autorisations gérées par les clients en suivant la bonne pratique que l'on appelle principe du moindre privilège. Pour plus d'informations, consultez ???.

Lorsque vous créez un partage de ressources, vous associez une autorisationAWS gérée à chaque type de ressource que vous souhaitez partager. Si l'autorisation gérée comporte plusieurs versions, le nouveau partage de ressources utilise toujours la version désignée par défaut.

Après avoir créé le partage de ressources,AWS RAM utilise l'autorisation gérée pour générer une politique basée sur les ressources qui est attachée à chaque ressource partagée.

Le modèle de politique d'une autorisation gérée spécifie les éléments suivants :

Effet

Indique s'il est`Allow` possible d'effectuer une opération sur une ressource partagée ou`Deny` s'il s'agit de l'autorisation principale requise. Pour une autorisation gérée, l'effet est toujours le même`Allow`. Pour de plus amples informations, veuillez consulter Effets dans l'Guide de l'utilisateur IAM.

Action

La liste des opérations que le principal est autorisé à effectuer. Il peut s'agir d'une action dans leAWS Management Console ou d'une opération dans leAWS Command Line Interface (AWS CLI) ouAWS l'API. Les actions sont définies par l'AWSautorisation. Pour plus d'informations, consultez la section Action du guide de l'utilisateur IAM.

Condition

Quand et comment un mandant peut interagir avec une ressource dans le cadre d'un partage de ressources. Les conditions ajoutent un niveau de sécurité supplémentaire à vos ressources partagées. Utilisez-les pour limiter l'accès à vos ressources partagées pour des actions sensibles. Par exemple, vous pouvez inclure des conditions exigeant que les actions proviennent d'une plage d'adresses IP d'entreprise spécifique, ou que les actions doivent être effectuées par des utilisateurs authentifiés à l'aide d'une authentification multifactorielle. Pour de plus amples informations sur les conditions, veuillez consulter la rubrique Clés de contexte des conditionsAWS globales dans le Guide de l'utilisateur IAM. Pour plus d'informations sur les conditions spécifiques des services, consultez la rubrique Actions, ressources et clés de condition pour lesAWS services.

> **Note**
>
> Des conditions sont disponibles pour les autorisations gérées par le client et les types de ressources pris en charge pour les autorisationsAWS gérées.
> Pour plus d'informations sur les conditions qui ne peuvent pas être utilisées avec des autorisations gérées par le client, consultezConsidérations relatives à l'utilisation des autorisations gérées par le client dansAWS RAM.

Types d'autorisations gérées

Lorsque vous créez un partage de ressources, vous choisissez une autorisation gérée à associer à chaque type de ressource que vous incluez dans le partage de ressources. AWSles autorisations gérées sont définies par le serviceAWS propriétaire des ressources et gérées parAWS RAM. Vous créez et gérez vos propres autorisations gérées par le client.

- AWSautorisation gérée : une autorisation gérée par défaut est disponible pour chaque type de ressource pris enAWS RAM charge. L'autorisation gérée par défaut est celle utilisée pour un type de ressource, sauf si vous choisissez explicitement l'une des autorisations gérées supplémentaires. L'autorisation gérée par défaut est destinée à prendre en charge les scénarios clients les plus courants pour le partage de ressources du type spécifié. L'autorisation gérée par défaut permet aux responsables d'effectuer des actions spécifiques définies par le service pour le type de ressource. Par exemple, pour le type de`ec2:Subnet` ressource Amazon VPC, l'autorisation gérée par défaut permet aux responsables d'effectuer les actions suivantes :
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  Les noms des autorisationsAWS gérées par défaut utilisent le format suivant :`AWSRAMDefaultPermission`*`ShareableResourceType`*. Par exemple, pour le type de`ec2:Subnet` ressource, le nom de l'autorisationAWS gérée par défaut est`AWSRAMDefaultPermissionSubnet`.

> **Note**
>
> L'autorisation gérée par défaut est distincte de la version par défaut d'une autorisation gérée. Toutes les autorisations gérées, qu'il s'agisse des autorisations par défaut ou de

l'une des autorisations gérées supplémentaires prises en charge par certains types de ressources, sont des autorisations distinctes et complètes ayant des effets et des actions différents qui prennent en charge différents scénarios de partage, tels que l'accès en lecture-écriture ou en lecture seule. Toute autorisation gérée, qu'elle soit gérée par le clientAWS ou qu'elle soit gérée par le client, peut avoir plusieurs versions, dont l'une est la version par défaut pour cette autorisation.

Par exemple, lorsque vous partagez un type de ressource qui prend en charge à la fois un accès total (`ReadetWrite`) une autorisation gérée en lecture seule, vous pouvez créer un partage de ressources pour l'administrateur doté de l'autorisation gérée d'accès complet. Vous pouvez ensuite créer un partage de ressources distinct pour d'autres développeurs à l'aide de l'autorisation gérée en lecture seule afin de respecter la pratique consistant à accorder le moindre privilège.

> **Note**
>
> Tous lesAWS services qui fonctionnent avecAWS RAM prennent en charge au moins une autorisation gérée par défaut. Vous pouvez consulter les autorisations disponibles pour chacuneService AWS sur la page de la bibliothèque des autorisations gérées. Cette page fournit des informations détaillées sur chaque autorisation gérée disponible, y compris les partages de ressources actuellement associés à l'autorisation et indique si le partage avec des responsables externes est autorisé, le cas échéant. Pour plus d'informations, veuillez consulter Affichage des autorisations gérées.
>
> Pour les services qui ne prennent pas en charge les autorisations gérées supplémentaires, lorsque vous créez un partage de ressources, appliqueAWS RAM automatiquement l'autorisation par défaut définie pour le type de ressource que vous choisissez. Si cette option est prise en charge, vous aurez également la possibilité de choisir Créer une autorisation gérée par le client sur la page Associer des autorisations gérées.

- Autorisation gérée par le client : les autorisations gérées par le client sont des autorisations gérées que vous créez et gérez en spécifiant précisément quelles actions peuvent être effectuées et dans quelles conditions avec les ressources partagéesAWS RAM. Par exemple, vous souhaitez limiter l'accès en lecture à vos pools Amazon VPC IP Address Manager (IPAM), qui vous aident à gérer vos adresses IP à grande échelle. Vous pouvez créer des autorisations gérées par le client pour que vos développeurs puissent attribuer des adresses IP, mais vous ne pouvez pas consulter la plage d'adresses IP attribuées par d'autres comptes de développeurs. Vous pouvez suivre

la bonne pratique que l'on appelle principe du moindre privilège, en accordant uniquement les autorisations requises pour effectuer des tâches sur des ressources partagées.

Sécurité dans AWS RAM

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Resource Access Manager (AWS RAM), consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS RAM. Les rubriques suivantes expliquent comment configurer AWS RAM pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour surveiller et sécuriser vos ressources AWS RAM.

Rubriques

Protection des données dans AWS RAM

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Resource Access Manager. Comme décrit dans ce modèle, AWS est responsable de la protection

de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour les Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 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).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela est également valable lorsque vous utilisez AWS RAM ou d'autres Services AWS à l'aide de la console, de l'API, d'AWS CLI ou des kits SDK AWS. Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez

une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Gestion des identités et des accès pour AWS RAM

AWS Identity and Access Management (IAM) est un AWS service qui aide un administrateur à contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs d'IAM contrôlent qui peut être authentifié (connecté) et autorisé (disposant d'autorisations) à utiliser AWS les ressources. À l'aide d'IAM, vous créez des principes principaux, tels que des rôles, des utilisateurs et des groupes dans votre. Compte AWS Vous contrôlez les autorisations dont disposent ces directeurs pour effectuer des tâches à l'aide de AWS ressources. Vous pouvez utiliser IAM sans frais supplémentaires. Pour plus d'informations sur la gestion et la création de politiques IAM personnalisées, consultez la section Gestion des politiques IAM dans le Guide de l'utilisateur IAM.

Rubriques

Fonctionnement de AWS RAM avec IAM

Par défaut, les responsables IAM ne sont pas autorisés à créer ou modifier lesAWS RAM ressources. Pour autoriser les responsables IAM à créer ou à modifier des ressources et à exécuter des tâches, vous exécutez l'une des étapes suivantes. Ces actions autorisent les utilisateurs à utiliser des actions d'API et des ressources spécifiques.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center.

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

AWS RAMfournit plusieurs politiquesAWS gérées que vous pouvez utiliser pour répondre aux besoins de nombreux utilisateurs. Pour de plus amples informations, veuillez consulter Politiques AWS gérées pour AWS RAM.

Si vous souhaitez contrôler plus précisément les autorisations que vous accordez à vos utilisateurs, vous pouvez créer vos propres politiques dans la console IAM. Pour plus d'informations sur la création de politiques et leur association à vos rôles et utilisateurs IAM, consultez la section Politiques et autorisations dans IAM du Guide de l'AWS Identity and Access Managementutilisateur.

Les sections suivantes fournissent des informationsAWS RAM spécifiques sur la création d'une politique d'autorisation IAM.

Table des matières

Structure d'une politique

Une politique d'autorisation IAM est un document JSON qui inclut les déclarations suivantes : Effet, Action, Ressource et Condition. Une stratégie IAM prend généralement la forme suivante.

```
{
```

```
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
        "Condition":{
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

Effet

L'instruction Effect indique si la politique autorise ou refuse l'autorisation principale d'effectuer une action. Les valeurs possibles incluent :`Allow` et`Deny`.

Action

L'instruction Action spécifie les actions d'AWS RAMAPI pour lesquelles la politique autorise ou refuse l'autorisation. Pour obtenir la liste complète des actions autorisées, consultez la section Actions définies parAWS Resource Access Manager dans le guide de l'utilisateur IAM.

Ressource

La déclaration des ressources spécifie lesAWS RAM ressources qui sont affectées par la politique. Pour spécifier une ressource dans la déclaration, vous devez utiliser son unique ARN. Pour obtenir la liste complète des ressources autorisées, consultez la section Ressources définies parAWS Resource Access Manager dans le guide de l'utilisateur IAM.

Condition

Les déclarations de condition sont facultatives. Ils peuvent être utilisés pour affiner les conditions d'application de la stratégie. AWS RAMprend également en charge les clés de condition suivantes :

- `aws:RequestTag/${TagKey}`— Teste si la demande de service inclut une balise avec la clé de balise spécifiée, existe et possède la valeur spécifiée.
- `aws:ResourceTag/${TagKey}`— Vérifie si la ressource faisant l'objet de la demande de service est associée à une balise associée à une clé de balise que vous spécifiez dans la politique.

  L'exemple de condition suivant vérifie que la ressource référencée dans la demande de service possède une balise attachée avec le nom de clé « Owner » et la valeur « Dev Team ».

```
"Condition" : {
    "StringEquals" : {
        "aws:ResourceTag/Owner" : "Dev Team"
    }
}
```

- `aws:TagKeys`— Spécifie les clés de balise qui doivent être utilisées pour créer ou baliser un partage de ressources.
- `ram:AllowsExternalPrincipals`— Teste si le partage de ressources dans la demande de service autorise le partage avec des responsables externes. Un mandant externe est uneCompte AWS personne extérieure à votre organisation dansAWS Organizations. Si cela correspond à`False`, vous ne pouvez partager ce partage de ressources qu'avec des comptes appartenant à la même organisation.
- `ram:PermissionArn`— Vérifie si l'ARN d'autorisation spécifié dans la demande de service correspond à une chaîne ARN que vous spécifiez dans la politique.
- `ram:PermissionResourceType`— Teste si l'autorisation spécifiée dans la demande de service est valide pour le type de ressource que vous spécifiez dans la politique. Spécifiez les types de ressources à l'aide du format indiqué dans la liste des types de ressources partageables.
- `ram:Principal`— Vérifie si l'ARN du principal spécifié dans la demande de service correspond à une chaîne ARN que vous spécifiez dans la politique.
- `ram:RequestedAllowsExternalPrincipals`— Vérifie si la demande de service inclut le`allowExternalPrincipals` paramètre et si son argument correspond à la valeur spécifiée dans la politique.
- `ram:RequestedResourceType`— Teste si le type de ressource de la ressource sur laquelle on agit correspond à une chaîne de type de ressource que vous spécifiez dans la politique. Spécifiez les types de ressources à l'aide du format indiqué dans la liste des types de ressources partageables.
- `ram:ResourceArn`— Vérifie si l'ARN de la ressource faisant l'objet de la demande de service correspond à un ARN que vous spécifiez dans la politique.
- `ram:ResourceShareName`— Vérifie si le nom du partage de ressources faisant l'objet de la demande de service correspond à une chaîne que vous spécifiez dans la politique.
- `ram:ShareOwnerAccountId`— Teste que le numéro d'identification du compte du partage de ressources faisant l'objet de la demande de service correspond à une chaîne que vous spécifiez dans la politique.

Politiques AWS gérées pour AWS RAM

AWS Resource Access Managerfournit actuellement plusieursAWS RAMles politiques gérées, qui sont décrites dans cette rubrique.

Politiques gérées par AWS

- AWS Politique gérée par: AWSResourceAccessManagerReadOnlyAccess
- AWS Politique gérée par: AWSResourceAccessManagerFullAccess
- AWS Politique gérée par: AWSResourceAccessManagerResourceShareParticipantAccess
- AWS Politique gérée par: AWSResourceAccessManagerServiceRolePolicy
- Mises à jour AWS RAM vers des politiques gérées par AWS

Dans la liste précédente, vous pouvez associer les trois premières politiques à vos rôles, groupes et utilisateurs IAM pour accorder des autorisations. La dernière politique de la liste est réservée auAWS RAMle rôle lié au service du service.

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la rubrique Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS Politique gérée par: AWSResourceAccessManagerReadOnlyAccess

Vous pouvez attacher la politique `AWSResourceAccessManagerReadOnlyAccess` à vos identités IAM.

Cette politique fournit des autorisations en lecture seule pour les partages de ressources détenus par votreCompte AWS.

Pour ce faire, il autorise l'exécution de l'un des`Get*`ou`List*`opérations. Il ne permet pas de modifier un partage de ressources.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ram`— Permet aux administrateurs de consulter les détails des partages de ressources détenus par le compte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS Politique gérée par: AWSResourceAccessManagerFullAccess

Vous pouvez attacher la politique `AWSResourceAccessManagerFullAccess` à vos identités IAM.

Cette politique fournit un accès administratif complet pour afficher ou modifier les partages de ressources détenus par votreCompte AWS.

Pour ce faire, il autorise l'exécution de n'importe quel`ram`opérations.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ram`— Permet aux directeurs d'afficher ou de modifier toute information concernant les partages de ressources détenus parCompte AWS.

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

AWS Politique gérée par: AWSResourceAccessManagerResourceShareParticipantAccess

Vous pouvez attacher la politique `AWSResourceAccessManagerResourceShareParticipantAccess` à vos identités IAM.

Cette politique permet aux directeurs d'accepter ou de rejeter les partages de ressources qui sont partagés avec ceCompte AWS, et pour consulter les détails de ces partages de ressources. Il ne permet pas de modifier ces partages de ressources.

Il le fait en accordant l'autorisation d'exécuter certains`ram`opérations.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ram`— Permet aux administrateurs d'accepter ou de rejeter les invitations au partage de ressources et de consulter les détails des partages de ressources partagés avec le compte.

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

```
        {
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourcePolicies",
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShares",
                "ram:ListPendingInvitationResources",
                "ram:ListPrincipals",
                "ram:ListResources",
                "ram:RejectResourceShareInvitation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS Politique gérée par: AWSResourceAccessManagerServiceRolePolicy

LeAWSpolitique géréeAWSResourceAccessManagerServiceRolePolicyne peut être utilisé qu'avec le rôle lié au service pourAWS RAM. Vous ne pouvez pas joindre, détacher, modifier ou supprimer cette politique.

Cette politique fournitAWS RAMavec un accès en lecture seule à la structure de votre organisation. Lorsque vous activez l'intégration entreAWS RAMetAWS Organizations,AWS RAMcrée automatiquement un rôle lié à un service nomméAWSServiceRoleForResourceAccessManagerque le service suppose lorsqu'il a besoin de rechercher des informations concernant votre organisation et ses comptes, par exemple lorsque vous consultez la structure de l'organisation dansAWS RAMconsole.

Pour ce faire, il accorde l'autorisation en lecture seule d'exécuterorganizations:Describeetorganizations:Listopérations qui fournissent des détails sur la structure et les comptes de l'organisation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `organizations`— Permet aux directeurs de consulter des informations sur la structure de l'organisation, y compris les unités organisationnelles etComptes AWSils contiennent.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
            ]
        }
    ]
}
```

Mises à jour AWS RAM vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour AWS RAM 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 d'historique du document AWS RAM.

Modification	Description	Date
AWS Resource Access Manager a démarré le suivi des modifications	AWS RAMa documenté ses politiques gérées existantes et a commencé à suivre les modifications.	16 septembre 2021

Utilisation des rôles liés à un service pour AWS RAM

AWS Resource Access Manager utilise des rôles AWS Identity and Access Management (IAM) liés à des services. Un rôle lié à un service est un type unique de rôle IAM directement lié au service. AWS RAM Les rôles liés aux services sont prédéfinis par AWS et incluent toutes les autorisations AWS RAM nécessaires pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service AWS RAM facilite la configuration car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. AWS RAMdéfinit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, ne AWS RAM peut assumer que ses rôles liés aux services. Les autorisations définies incluent à la fois une politique de confiance et une politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS qui fonctionnent avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS RAM

AWS RAMutilise le rôle lié au service nommé `AWSServiceRoleForResourceAccessManager` lorsque vous activez le partage avec. AWS Organizations Ce rôle autorise le AWS RAM service à consulter les détails de l'organisation, tels que la liste des comptes des membres et les unités organisationnelles auxquelles appartient chaque compte.

Ce rôle lié à un service fait confiance au service suivant pour assumer le rôle :

- `ram.amazonaws.com`

La politique d'autorisation de rôle nommée AWSResourceAccessManagerServiceRolePolicy est attachée à ce rôle lié au service et permet d'AWS RAMeffectuer les actions suivantes sur les ressources spécifiées :

- Actions : actions en lecture seule qui permettent de récupérer des informations sur la structure de votre organisation. Pour obtenir la liste complète des actions, vous pouvez consulter la politique dans la console IAM : AWSResourceAccessManagerServiceRolePolicy.

Pour qu'un directeur active le AWS RAM partage au sein de votre organisation, ce principal (une entité IAM telle qu'un utilisateur, un groupe ou un rôle) doit être autorisé à créer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Gguide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS RAM

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez le AWS RAM partage au sein de votre organisation dans le AWS Management Console ou que vous l'exécutez EnableSharingWithAwsOrganizationdans votre compte à l'AWS CLIaide d'une AWS API, vous AWS RAM créez le rôle lié au service pour vous.

Appelez `enable-sharing-with-aws-organizations` pour créer le rôle lié au service dans votre compte.

Si vous supprimez ce rôle lié à un service, vous AWS RAM n'êtes plus autorisé à consulter les détails de la structure de votre organisation.

Modification d'un rôle lié à un service pour AWS RAM

AWS RAMne vous permet pas de modifier le rôle AWSResourceAccessManagerServiceRolePolicy lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS RAM

Vous pouvez également utiliser la console IAM, l'AWS CLI ou l'API AWS pour supprimer manuellement le rôle lié à un service.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service `AWSResourceAccessManagerServiceRolePolicy`. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS RAM

AWS RAM prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour de plus amples informations, veuillez consulter Régions et points de terminaison AWS dans le Référence générale d'Amazon Web Services.

Exemples de stratégies IAM pour AWS RAM

Cette rubrique inclut des exemples de politiques IAM AWS RAM qui illustrent le partage de ressources et de types de ressources spécifiques et la restriction du partage.

Exemples de politiques IAM

- Exemple 1 : Autoriser le partage de ressources spécifiques
- Exemple 2 : Autoriser le partage de types de ressources spécifiques
- Exemple 3 : Restreindre le partage avec des utilisateurs externes Comptes AWS

Exemple 1 : Autoriser le partage de ressources spécifiques

Vous pouvez utiliser une politique d'autorisation IAM pour restreindre les administrateurs à associer uniquement des ressources spécifiques à des partages de ressources.

Par exemple, la politique suivante limite les responsables à partager uniquement la règle de résolution avec le nom de ressource Amazon (ARN) spécifié. L'opérateur `StringEqualsIfExists` autorise une demande si la demande n'inclut pas de `ResourceArn` paramètre ou si elle inclut ce paramètre, si sa valeur correspond exactement à l'ARN spécifié.

Pour plus d'informations sur quand et pourquoi utiliser des `...IfExists` opérateurs, consultez... IfExistsconditionnez les opérateurs dans le guide de l'utilisateur IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
```

```
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

Exemple 2 : Autoriser le partage de types de ressources spécifiques

Vous pouvez utiliser une politique IAM pour limiter les mandants à associer uniquement des types de ressources spécifiques à des partages de ressources.

Par exemple, la politique suivante limite les mandants à partager uniquement les règles du résolveur.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

Exemple 3 : Restreindre le partage avec des utilisateurs externes Comptes AWS

Vous pouvez utiliser une politique IAM pour empêcher les directeurs de partager des ressources avec Comptes AWS des personnes extérieures à l'organisation. AWS

Par exemple, la politique IAM suivante empêche les administrateurs d'ajouter des éléments externes Comptes AWS aux partages de ressources.

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

```
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

Exemples de politiques de contrôle des services pour AWS Organizations et AWS RAM

AWS RAM prend en charge les politiques de contrôle des services (SCP). Les SCP sont des politiques que vous attachez aux éléments d'une organisation pour gérer les autorisations au sein de cette organisation. Un SCP s'applique à tout ce qui se Comptes AWS trouve sous l'élément auquel vous attachez le SCP. Les politiques de contrôle des services (SCP) offrent un contrôle central sur les autorisations maximales disponibles pour tous les comptes de votre organisation. Ils peuvent vous aider à garantir le respect Comptes AWS des directives de contrôle d'accès de votre organisation. Pour plus d'informations, consultez la section Politiques de contrôle de service du Guide de l'utilisateur AWS Organizations.

Prérequis

Procédez comme suit pour utiliser les SCP :

- Activez toutes les fonctions de votre organisation. Pour plus d'informations, consultez la section Activation de toutes les fonctionnalités de votre organisation dans le guide de AWS Organizations l'utilisateur
- Activez les SCP au sein de votre organisation. Pour plus d'informations, voir Activation et désactivation des types de politiques dans le guide de l'AWS Organizationsutilisateur
- Créez les SCP dont vous avez besoin. Pour plus d'informations sur la création de SCP, voir Création et mise à jour de SCP dans le guide de l'AWS Organizationsutilisateur.

Exemples de politiques de contrôle des services

Table des matières

Les exemples suivants montrent comment contrôler les différents aspects liés au partage des ressources dans une organisation.

Exemple 1 : empêcher le partage externe

Le SCP suivant empêche les utilisateurs de créer des partages de ressources qui autorisent le partage avec des responsables extérieurs à l'organisation de l'utilisateur qui partage les ressources.

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

Exemple 2 : Empêcher les utilisateurs d'accepter des invitations à partager des ressources provenant de comptes externes à votre organisation

Le SCP suivant empêche tout principal d'un compte concerné d'accepter une invitation à utiliser un partage de ressources. Les partages de ressources partagés avec d'autres comptes de la même

organisation que le compte de partage ne génèrent pas d'invitations et ne sont donc pas affectés par ce SCP.

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

Exemple 3 : Autoriser des comptes spécifiques à partager des types de ressources spécifiques

Le SCP suivant autorise uniquement les comptes 111111111111 et permet de 222222222222 créer de nouveaux partages de ressources qui partagent des listes de préfixes Amazon EC2 ou d'associer des listes de préfixes à des partages de ressources existants.

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

```
    ]
}
```

Exemple 4 : empêcher le partage avec l'ensemble de l'organisation ou avec des unités organisationnelles

Le SCP suivant empêche les utilisateurs de créer des partages de ressources qui partagent des ressources avec l'ensemble d'une organisation ou avec des unités organisationnelles. Les utilisateurs peuvent partager avec un membre Comptes AWS de l'organisation, ou avec des rôles ou des utilisateurs IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Exemple 5 : autoriser le partage uniquement avec des principaux spécifiques

L'exemple de SCP suivant permet aux utilisateurs de partager des ressources uniquement avec l'unité `o-12345abcdef`, organisationnelle de l'organisation`ou-98765fedcba`, et Compte AWS`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"
                    ]
                }
            }
        }
    ]
}
```

Désactiver le partage de ressources avec AWS Organizations

Si vous avez précédemment activé le partage avec AWS Organizations et que vous n'avez plus besoin de partager les ressources avec l'ensemble de votre organisation ou de vos unités organisationnelles (UO), vous pouvez désactiver le partage. Lorsque vous désactivez le partage avecAWS Organizations, toutes les organisations ou unités d'organisation sont supprimées des partages de ressources que vous avez créés et elles perdent l'accès aux ressources partagées. Les comptes externes (comptes ajoutés au partage de ressources sur invitation) ne seront pas affectés et continueront d'être associés au partage de ressources.

Pour désactiver le partage avec AWS Organizations

1. Désactivez l'accès sécurisé à AWS Organizations l'aide de la AWS Organizations disable-aws-service-accessAWS CLIcommande.

   ```
   $  aws organizations disable-aws-service-access --service-principal
    ram.amazonaws.com
   ```

> **Important**
>
> Lorsque vous désactivez l'accès sécurisé àAWS Organizations, les principaux de vos organisations sont retirés de tous les partages de ressources et perdent l'accès à ces ressources partagées.

2. Utilisez la console IAMAWS CLI, ou les opérations de l'API IAM pour supprimer le rôle lié au AWSServiceRoleForResourceAccessManagerservice. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Journalisation et surveillance dans AWS RAM

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances d'AWS RAM et de vos solutions AWS. Vous devez recueillir les données de surveillance de toutes les parties de votre solution AWS de telle sorte que vous puissiez déboguer plus facilement une éventuelle défaillance à plusieurs points. AWS fournit plusieurs outils pour surveiller vos ressources AWS RAM et répondre aux incidents potentiels :

CloudWatch Événements Amazon

fournit un near-real-time flux d'événements système qui décrivent les modifications apportées auxAWS ressources. CloudWatch Events permet d'effectuer des calculs automatisés pilotés par des événements, car vous pouvez écrire des règles pour surveiller certains événements et déclencher des actions automatisées dans d'autresAWS services lorsque ces événements se produisent. Pour plus d'informations, veuillez consulter Surveillance àAWS RAM l'aide d' CloudWatch événements.

AWS CloudTrail

Capture les appels d'API et les événements associés créés par ou au nom de vousCompte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour plus d'informations, veuillez consulter Journalisation des appels d'API AWS RAM avec AWS CloudTrail.

Surveillance àAWS RAM l'aide d' CloudWatch événements

À l'aide d'Amazon CloudWatch Events, vous pouvez configurer des notifications automatiques pour des événements spécifiques dansAWS RAM. Les événements deAWS RAM sont fournis à CloudWatch Events presque en temps réel. Vous pouvez configurer les CloudWatch événements pour surveiller les événements et invoquer des cibles en réponse à des événements indiquant des modifications apportées à vos partages de ressources. Les modifications apportées à un partage de ressources déclenchent des événements à la fois pour le propriétaire du partage de ressources et pour les principaux utilisateurs autorisés à accéder au partage de ressources.

Lorsque vous créez un modèle d'événement, la source est `aws.ram`.

> **Note**
>
> Prenez soin d'écrire du code qui dépend de ces événements. Ces événements ne sont pas garantis, mais sont générés sur la base du meilleur effort. Si une erreur se produit lors de laAWS RAM tentative d'émission d'un événement, le service essaie plusieurs fois. Cependant, le délai peut expirer et entraîner la perte de cet événement spécifique.

Pour de plus amples informations, consultez le Guide de l'utilisateur Amazon CloudWatch Events.

Exemple : alerte en cas d'échec du partage de ressources

Imaginez le scénario dans lequel vous souhaitez partager des réservations de capacité Amazon EC2 avec d'autres comptes de votre organisation. C'est un bon moyen de réduire vos coûts.

Toutefois, si vous ne remplissez pas toutes les conditions requises pour partager une réservation de capacité, l'exécution des tâches asynchrones liées au partage des ressources peut échouer silencieusement. Si l'opération de partage échoue et que vos utilisateurs d'autres comptes tentent de lancer des instances avec l'une de ces réservations de capacité, Amazon EC2 agit comme si la réservation de capacité était complète et lance l'instance en tant qu'instance à la demande. Cela peut entraîner des coûts plus élevés que prévu.

Pour surveiller les échecs de partage de ressources, configurez une règle Amazon CloudWatch Events qui vous avertira en cas d'échec d'un partage deAWS RAM ressources. Le didacticiel suivant utilise une rubrique Amazon Simple Notification Service (SNS), qui enverra une notification à tous les abonnés de la rubrique lorsqu'une EventBridge panne de partage de ressources sera découverte.

Pour plus d'informations sur Amazon SNS, consultez le Guide du développeur d'Amazon Simple Notification Service.

Pour créer une règle qui vous avertit en cas d'échec du partage de ressources

1. Ouvrez la EventBridge console Amazon.
2. Dans le volet de navigation, choisissez Règles, puis dans la liste Règles, choisissez Créer une règle.
3. Entrez un nom et une description facultative pour votre règle, puis choisissez Suivant.
4. Faites défiler la page jusqu'à la zone Modèle d'événement et choisissez Modèles personnalisés (éditeur JSON).
5. Copiez-collez le modèle d'événement suivant :

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. Choisissez Suivant.
7. Pour Cible 1, sous Type de cible, choisissez Service AWS.
8. Sous Sélectionner une cible, choisissez la rubrique SNS.
9. Dans Rubrique, sélectionnez la rubrique SNS dans laquelle vous voulez publier la notification. Ce sujet doit déjà exister.
10. Choisissez Suivant, puis choisissez à nouveau Suivant pour voir et vérifier votre configuration.
11. Lorsque vous êtes satisfait de vos options, sélectionnez Créer une règle.
12. De retour sur la page des règles, assurez-vous que votre nouvelle règle est marquée comme activée. Si nécessaire, cliquez sur le bouton radio à côté du nom de votre règle, puis choisissez Activer.

Tant que cette règle est activée, tout partage deAWS RAM ressources qui échoue génère une alerte SNS destinée aux destinataires de la rubrique sur laquelle vous avez publié.

Vous pouvez également vérifier que les réservations de capacité partagée sont accessibles aux comptes avec lesquels vous les avez partagées en essayant de les consulter sur la console Amazon EC2 à partir de ces comptes.

Journalisation des appels d'API AWS RAM avec AWS CloudTrail

AWS RAMest intégré àAWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWS service dans leAWS RAM. CloudTrail capture les appels d'API deAWS RAM en tant qu'événements. Les appels capturés incluent des appels de la console AWS RAM et les appels de code vers les opérations d'API AWS RAM. Si vous créez un journal d'activité, vous pouvez activer la livraison continue des CloudTrail événements dans un compartiment Amazon S3 que vous spécifiez, y compris les évènements pourAWS RAM. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Historique des événements. Utilisez les informations collectées par CloudTrail pour déterminer la demande qui a été envoyée à AWS RAM, l'adresse IP à l'origine de la demande, l'auteur de la demande, la date de la demande, ainsi que d'autres informations.

Pour plus d'informations CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

AWS RAMinformations dans CloudTrail

CloudTrail est activé dans votreCompte AWS lors de la création de ce dernier. Lorsqu'une activité a lieu dans Historique des événementsAWS RAM, celle-ci est enregistrée dans un CloudTrail événement avec d'autres événementsAWS de services dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS RAM, créez un journal d'activité. Un journal CloudTrail de suivi permet de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autresAWS services pour analyser plus en profondeur les données d'événement collectées dans les CloudTrail journaux et agir sur celles-ci. Pour plus d'informations, consultez les ressources suivantes :

- Création d'un journal d'activité pour votre Compte AWS

- Service AWSintégrations avec des CloudTrail journaux
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et Réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes lesAWS RAM actions sont enregistrées CloudTrail et documentées dans la référence deAWS RAM l'API. Par exemple, les appels adressés aux actions `CreateResourceShare` `AssociateResourceShare`, `EnableSharingWithAwsOrganization` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initiée la demande.

- Compte AWSinformations d'identification root
- Informations d'identification de sécurité temporaires correspondant à un rôle ou un utilisateur fédéré AWS Identity and Access Management (IAM).
- Informations d'identification de sécurité à long terme d'un utilisateur IAM.
- Autre service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des AWS RAM entrées des fichiers journaux

Un journal de suivi est une configuration qui permet la remise d'événements sous forme de fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une série ordonnée des appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de CloudTrail journal pour l'`CreateResourceShare`action.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Résilience dans AWS RAM

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 RAM

En tant que service géré, AWS Resource Access Manager il est protégé par la sécurité AWS globale du réseau. 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 AWS pour accéder à AWS RAM 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.

Résolution des problèmes liés à AWS RAM

Utilisez les informations de cette section du guide pour vous aider à diagnostiquer et à résoudre les problèmes courants lorsque vous travaillez avec AWS Resource Access Manager (AWS RAM).

Rubriques

Erreur : « Votre identifiant de compte n'existe pas dans une AWS organisation »

Scénario

Le message d'erreur « Votre identifiant de compte n'existe pas dans une AWS organisation » s'affiche lorsque vous tentez de partager une ressource avec des comptes ou des unités organisationnelles (UO) de votre organisation.

Cause

Cette erreur peut se produire si le rôle lié au service AWSServiceRoleForResourceAccessManagern'est pas correctement créé lorsque vous activez l'intégration entre etAWS Resource Access Manager. AWS Organizations

Solution

Pour recréer le rôle lié au service requis, effectuez les étapes suivantes pour désactiver l'intégration, puis la réactiver.

1. Connectez-vous au compte de gestion de votre organisation à l'aide d'un rôle IAM ou d'un utilisateur disposant d'autorisations administratives.
2. Accédez à la page Services de la AWS Organizations console.
3. Choisissez RAM.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Accédez à la page Paramètres de la AWS RAM console.
6. Cochez la case Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

> **Important**
>
> Lorsque vous désactivez l'accès sécurisé àAWS Organizations, les principaux de votre organisation sont retirés de tous les partages de ressources et n'ont plus accès à ces ressources partagées.

Vous devriez désormais être en mesure de AWS RAM partager vos ressources avec les comptes et les unités d'organisation de l'organisation.

Erreur : « AccessDeniedException »

Scénario

Vous obtenez une exception d'accès refusé lorsque vous essayez de partager une ressource ou d'afficher un partage de ressources.

Cause

Vous pouvez recevoir cette erreur si vous tentez de créer un partage de ressources alors que vous ne disposez pas des autorisations requises. Cela peut être dû à des autorisations insuffisantes dans les politiques associées à votre principal AWS Identity and Access Management (IAM). Cela peut également se produire en raison des restrictions mises en place par une politique de contrôle des AWS Organizations services (SCP) qui vous Compte AWS concerne.

Solution

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center.

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Pour résoudre l'erreur, vous devez vous assurer que les autorisations sont accordées par `Allow` des instructions figurant dans la politique d'autorisation utilisée par le principal auteur de la demande. De plus, les autorisations ne doivent pas être bloquées par les SCP de votre organisation.

Pour créer un partage de ressources, vous devez disposer des deux autorisations suivantes :

- `ram:CreateResourceShare`

- `ram:AssociateResourceShare`

Pour consulter un partage de ressources, vous devez disposer des autorisations suivantes :

- `ram:GetResourceShares`

Pour associer des autorisations à un partage de ressources, vous devez disposer des autorisations suivantes :

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  Il s'agit d'un espace réservé. Vous devez la remplacer par l'autorisation PutPolicy « » (ou équivalent) pour le service propriétaire de la ressource que vous souhaitez partager.
  Par exemple, si vous partagez une règle de résolution Route 53, l'autorisation requise

serait :`route53resolver:PutResolverRulePolicy`. Si vous souhaitez autoriser la création d'un partage de ressources contenant plusieurs types de ressources, vous devez inclure l'autorisation appropriée pour chaque type de ressource que vous souhaitez autoriser.

L'exemple suivant montre à quoi peut ressembler une telle politique d'autorisation IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare",
                "ram:GetResourceShares",
                "resourceOwningService:PutPolicyAction"
            ],
            "Resource": "*"
        }
    ]
}
```

Erreur : « UnknownResourceException »

Scénario

L'une des erreurs suivantes s'affiche :

- « CannotCreateResourceShare: UnknownResourceException : OrganizationalUnit ou- *xxxx* n'a pas pu être trouvé »
- « CannotUpdateResourceShare: UnknownResourceException : OrganizationalUnit ou- *xxxx* n'a pas pu être trouvé ».

Cause

Ces erreurs peuvent se produire si vous activez l'intégration entre AWS RAM et en AWS Organizations utilisant la console Organizations ou l'AWSServiceAccess API Organizations Enable au lieu d'utiliser la AWS RAM console. Lorsque vous activez l'intégration à l'aide de la console ou

de l'API Organizations, le service ne crée pas le `AWSServiceRoleForResourceAccessManager` rôle dans votre compte. Ce rôle est nécessaire pour accéder aux informations concernant votre organisation. Le rôle n'ayant pas été créé, AWS RAM vous ne pouvez pas accéder aux informations relatives aux comptes ou aux unités organisationnelles (UO) de votre organisation.

Solution

Pour résoudre le problème, désactivez l'intégration entre AWS RAM etAWS Organizations. Réactivez-le ensuite en appelant l'opération AWS RAM EnableSharingWithAwsOrganizationAPI ou en utilisant le AWS Management Console pour effectuer les étapes suivantes.

1. Connectez-vous au compte de gestion de votre organisation à l'aide d'un rôle IAM ou d'un utilisateur disposant d'autorisations administratives.
2. Accédez à la page Services de la AWS Organizations console.
3. Choisissez RAM.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Accédez à la page Paramètres de la AWS RAM console.
6. Cochez la case Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

> **Important**
>
> Lorsque vous désactivez l'accès sécurisé àAWS Organizations, les principaux de votre organisation sont retirés de tous les partages de ressources et n'ont plus accès à ces ressources partagées.

Vous devriez désormais être en mesure de AWS RAM partager vos ressources avec les comptes et les unités d'organisation de l'organisation.

Erreurs lors de la tentative de partage avec des comptes extérieurs à mon organisation

Scénario

L'une des erreurs suivantes s'affiche lorsque vous essayez de partager des ressources avec des comptes extérieurs à votre organisation :

- « Vous ne pouvez pas partager la ressource en dehors de votre organisation. «
- « La ressource que vous essayez de partager ne peut être partagée qu'au sein de votre AWS organisation. «
- « InvalidParameterException: L'identifiant du compte principal ne figure pas dans votre AWS organisation. Vous n'êtes pas autorisé à ajouter des éléments externes Comptes AWS à un partage de ressources. «
- « OperationNotPermittedException: La ressource que vous essayez de partager ne peut être partagée qu'au sein de votre AWS organisation. «

Causes possibles et solutions

Certains types de ressources ne peuvent être partagés qu'avec les comptes d'une même organisation

Certains types de ressources ne peuvent pas être partagés avec un compte qui n'est pas membre de cette organisation. Les connexions privées virtuelles (VPC) qui font partie d'Amazon Elastic Compute Cloud (Amazon EC2) sont un exemple de type de ressource soumis à cette restriction.

Pour vérifier si vous pouvez partager un type de ressource particulier avec des comptes et des responsables extérieurs à votre organisation, consultez la section Ressources partageables AWS.

Le rôle lié au service n'a pas été créé correctement

Ce problème peut se produire si le rôle lié au service `AWSServiceRoleForResourceAccessManager` n'a pas été créé correctement lorsque vous avez activé l'intégration entre etAWS RAM. AWS Organizations

Si vous recevez l'une de ces erreurs lorsque vous tentez de partager une ressource avec un compte appartenant à votre organisation, effectuez les étapes suivantes pour supprimer et recréer le rôle lié au service.

1. Connectez-vous au compte de gestion de votre organisation à l'aide d'un rôle IAM ou d'un utilisateur disposant d'autorisations administratives.
2. Accédez à la page Services de la AWS Organizations console.
3. Choisissez RAM.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Accédez à la page Paramètres de la AWS RAM console.
6. Cochez la case Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

> **Important**
>
> Lorsque vous désactivez l'accès sécurisé àAWS Organizations, les principaux de votre organisation sont retirés de tous les partages de ressources et n'ont plus accès à ces ressources partagées.

Impossible de voir les ressources partagées dans le compte de destination

Scénario

Les utilisateurs ne peuvent pas voir les ressources qui, selon eux, sont partagées avec eux par d'autres utilisateursComptes AWS.

Causes possibles et solutions

Le partage avec AWS Organizations a été activé en utilisant Organizations au lieu de AWS RAM

S'il AWS Organizations a été activé en utilisant Organizations au lieu deAWS RAM, le partage au sein de l'organisation échoue. Pour vérifier si cela est à l'origine du problème, accédez à la

page Paramètres de la AWS RAM console et vérifiez que la case Activer le partage avec est AWS Organizations cochée.

- Si la case est cochée, cela n'en est pas la cause.
- Si la case n'est pas cochée, cela peut en être la cause. Ne cochez pas encore la case. Procédez comme suit pour corriger la situation.

1. Connectez-vous au compte de gestion de votre organisation à l'aide d'un rôle IAM ou d'un utilisateur disposant d'autorisations administratives.
2. Accédez à la page Services de la AWS Organizations console.
3. Choisissez RAM.
4. Choisissez Disable trusted access (Désactiver l'accès approuvé).
5. Accédez à la page Paramètres de la AWS RAM console.
6. Cochez la case Activer le partage avec AWS Organizations, puis sélectionnez Enregistrer les paramètres.

> **Important**
>
> Lorsque vous désactivez l'accès sécurisé àAWS Organizations, les principaux de votre organisation sont retirés de tous les partages de ressources et n'ont plus accès à ces ressources partagées.

Vous devrez peut-être mettre à jour le partage et spécifier les comptes ou les unités organisationnelles de l'organisation avec lesquels le partager.

Le partage de ressources ne spécifie pas ce compte en tant que compte principal

Dans le fichier Compte AWS qui a créé le partage de ressources, affichez le partage de ressources dans la AWS RAMconsole. Vérifiez que le compte qui ne peut pas accéder aux ressources est répertorié en tant que compte principal. Si ce n'est pas le cas, mettez à jour le partage pour ajouter le compte en tant que principal.

Le rôle ou l'utilisateur du compte ne dispose pas des autorisations minimales requises

Lorsque vous partagez une ressource du compte A avec un autre compte B, les rôles et les utilisateurs du compte B n'ont pas automatiquement accès aux ressources du partage.

L'administrateur du compte B doit d'abord autoriser les rôles IAM et les utilisateurs du compte B qui ont besoin d'accéder à la ressource. À titre d'exemple, la politique suivante indique comment vous pouvez accorder un accès en lecture seule aux rôles et aux utilisateurs du compte B pour une ressource du compte A. La politique spécifie la ressource par son Amazon Resource Name (ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
        }
    ]
}
```

Le paramètre de la ressource est différent Région AWS de celui de la console actuelle

AWS RAMest un service régional. Les ressources existent dans une région spécifiqueRégion AWS, et pour les voir, elles AWS Management Console doivent être configurées pour afficher les ressources de cette région.

Le Région AWS code auquel la console est actuellement en train d'accéder est affiché dans le coin supérieur droit de la console. Pour le modifier, choisissez le nom de la région actuelle et, dans le menu déroulant, choisissez la région dont vous souhaitez consulter les ressources.

Erreur : limite dépassée

Scénario

Vous recevez le message « Vous avez atteint la limite du nombre de ressources que vous pouvez partager » ou « ResourceShareLimitExceededException» lorsque vous essayez de partager des ressources.

Cause

Ces erreurs se produisent lorsque vous atteignez le nombre maximum de ressources que vous pouvez partager à l'aide du AWS RAM service ou de Service AWS celui qui a créé la ressource que vous essayez de partager. Ce quota (anciennement appelé limite) peut affecter à la fois le compte de partage ou le compte avec lequel vous partagez la ressource.

Solution

1. Pour consulter vos quotas, Compte AWS là où l'erreur s'affiche, accédez à l'une des pages suivantes, en fonction du type de quota que vous atteignez :
   - La AWS RAMpage de la console Service Quotas
   - La page des personnes Service AWS dont les ressources sont affectées par le quota
2. Faites défiler la page vers le bas et choisissez le quota approprié.
3. S'il est disponible pour ce quota, sélectionnez Demander une augmentation du quota.
4. Entrez une nouvelle valeur pour le quota, puis choisissez Request.
5. La demande apparaît sur la page d'historique des demandes de quotas, où vous pouvez vérifier le statut de la demande jusqu'à ce qu'elle soit finalisée.

L'autre compte de mon organisation ne reçoit jamais d'invitation

Scénario

Lorsque vous partagez des ressources avec un autre compte géré par la même organisationAWS Organizations, celui-ci ne reçoit aucune invitation.

Cause

Ce comportement est normal si le partage au sein de l'AWSorganisation est activé sur votre compte.

Lorsque cette option est activée et que vous partagez avec un autre compte de votre organisation, aucune invitation n'est envoyée et aucune acceptation n'est requise. Tous les comptes d'organisation auxquels vous faites référence en tant que principaux dans le partage de ressources peuvent immédiatement commencer à accéder aux ressources du partage.

Si votre compte n'a pas activé le partage au sein de l'AWSorganisation, lorsque vous partagez avec d'autres comptes, même s'ils appartiennent à la même AWS organisation, ils sont traités comme

des comptes autonomes. Des invitations sont envoyées et doivent être acceptées avant que les utilisateurs puissent accéder aux ressources des partages.

Vous ne pouvez pas partager un sous-réseau VPC

Scénario

Lorsque vous essayez de AWS RAM partager un sous-réseau VPC avec un autre compte, l'opération de partage réussit. Toutefois, le compte consommateur s'affiche `LIMIT EXCEEDED` pour cette ressource dans la AWS RAM console.

Cause

Certains types de ressources individuels sont soumis à des restrictions spécifiques au service, distinctes de celles appliquées par. AWS RAM Certaines de ces restrictions peuvent effectivement empêcher le partage même si vous n'avez pas atteint l'une des restrictions dansAWS RAM. Les limites sont un exemple de ces restrictions. Amazon Virtual Private Cloud (Amazon VPC) limite le nombre de sous-réseaux que vous pouvez partager avec un autre compte individuel. Si vous essayez de partager un sous-réseau avec un compte consommateur qui contient déjà le nombre maximal de sous-réseaux, ce compte consommateur s'affiche `LIMIT EXCEEDED` dans la console pour cette ressource. Pour plus d'informations sur cette limite, consultez Amazon VPC Quotas — Partage VPC dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Pour résoudre ce problème, vérifiez d'abord s'il existe d'autres partages de ressources susceptibles de partager la ressource spécifiée avec le compte concerné, puis supprimez les partages dont vous n'avez peut-être plus besoin. Vous pouvez également demander l'augmentation d'une limite qui prend en charge l'ajustement. Utilisez la console Service Quotas pour demander une augmentation de limite.

> **Note**
>
> AWS RAMne détecte pas automatiquement les modifications d'augmentation des limites. Vous devez réassocier la ressource ou le principal au partage de ressources pour que la RAM détecte le changement.

Quotas de service pour AWS RAM

Vous Compte AWS avez les limites suivantes relatives à AWS Resource Access Manager (AWS RAM). Vous pouvez demander une augmentation de certaines de ces limites. Pour demander une augmentation de limite, contactez AWS Support.

Note

Les définitions suivantes s'appliquent à la description figurant dans les quotas ci-dessous :

- Ressource : élément Service AWS créé individuellement que vous souhaitez partager, tel qu'un compartiment Amazon S3 ou une instance Amazon EC2. Chaque ressource référencée dans un partage de ressources compte pour une ressource par rapport à ce quota. Si vous partagez la même ressource dans trois partages de ressources différents, cela augmente de trois le nombre de vos partages pour ce quota.
- Partage de ressources : conteneur AWS RAM créé que vous pouvez utiliser pour partager des ressources. Chaque partage de ressources, quel que soit le nombre de ressources qu'il contient, compte pour un par rapport à votre quota.
- Principal partagé : identifiant que vous avez associé à un partage de ressources. Il peut s'agir d'un rôle ou d'un utilisateur AWS Identity and Access Management (IAM), d'un Compte AWS identifiant, d'une unité organisationnelle ou d'une organisation entière. Chaque principal partagé auquel vous faites référence dans un partage de ressources en ajoute un à votre quota d'utilisation. Si vous partagez avec l'ensemble d'une organisation en faisant référence à son identifiant, cela ne compte que pour une seule organisation par rapport à ce quota.
- Autorisation gérée par le client : autorisations gérées que vous créez pour répondre à des cas d'utilisation spécifiques en utilisant l'accès minimal pour gérer la façon dont vos ressources partagées sont utilisées.

Ressource	Limite par défaut
Nombre maximum de partages de ressources par Région AWS	25 000

Ressource	Limite par défaut
Nombre maximum d'associations de ressources par partage de ressources	5 000
Nombre maximum d'associations principales par partage de ressources	5 000
Nombre maximum d'autorisations gérées par le client	1 500
Nombre maximum d'autorisations gérées par le client par type de ressource	10
Nombre maximum de versions par autorisation gérée par le client	5
Nombre maximal d'associations de ressources sur l'ensemble des partages de ressources d'un Région AWS **Note** Chaque ressource incluse dans un partage de ressources est prise en compte dans cette limite. Si une ressource est incluse dans 10 partages de ressources différents, cela en compte 10 par rapport à la limite.	25 000

Ressource	Limite par défaut
Nombre maximal d'associations principales pour tous les partages de ressources d'un Région AWS **Note** Chaque principal inclus dans un partage de ressources est pris en compte dans cette limite. Si un principal est inclus dans 10 parts de ressources différentes, cela en compte 10 dans la limite.	25 000
Nombre maximum d'invitations en attente par compte de partage • Ce quota s'applique uniquement à l'envoi de comptes partagés avec des comptes qui ne font pas partie du même compteAWS Organizations. • Il n'existe aucun quota pour limiter le nombre d'invitations en attente qu'un compte récepteur peut avoir. • Les invitations ne sont pas utilisées lors du partage entre des comptes faisant partie d'un même compte AWS Organizations et vous avez activé le partage de ressources au sein duAWS Organizations.	250

Utilisation de AWS RAM avec un kit SDK AWS.

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

Documentation des kits SDK	Exemples de code
AWS SDK for C++	Exemples de code AWS SDK for C++
AWS SDK for Go	Exemples de code AWS SDK for Go
AWS SDK for Java	Exemples de code AWS SDK for Java
AWS SDK for JavaScript	Exemples de code AWS SDK for JavaScript
AWS SDK for .NET	Exemples de code AWS SDK for .NET
AWS SDK for PHP	Exemples de code AWS SDK for PHP
AWS SDK for Python (Boto3)	Exemples de code AWS SDK for Python (Boto3)
AWS SDK for Ruby	Exemples de code AWS SDK for Ruby

Exemple de disponibilité

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code via le lien de retour.

Historique du document pour le guide de AWS RAM l'utilisateur

Le tableau suivant décrit les ajouts importants à la AWS Resource Access Manager documentation. Nous mettons également à jour la documentation pour répondre aux commentaires que vous nous envoyez.

Pour être informé de ces mises à jour, vous pouvez vous abonner au AWS RAM flux RSS.

Modification	Description	Date
Support supplémentaire pour le partage Amazon Route 53 ResolverProfiles	Vous pouvez désormais l'utiliser AWS RAM pour partager Amazon Route 53 Resolver Profiles avec d'autres Comptes AWS membres de votre organisation.	22 avril 2024
Ajout de la prise en charge du partage des ressources du AWS Systems Manager Parameter Store.	Vous pouvez désormais partager des paramètres avancés de manière sécurisée et efficace au sein de votre organisation Comptes AWS ou au sein de celle-ci.	21 février 2024
Ajout de la prise en charge du partage des instantanés Amazon FSx pour OpenZFS.	Vous pouvez désormais partager des instantanés Amazon FSx pour OpenZFS avec d'autres membres de votre organisation. Comptes AWS	19 décembre 2023
Ajout d'un support pour partager Amazon Simple Storage Service les ressources.	Vous pouvez désormais partager Amazon Simple Storage Service l'instance Access Grants avec d'autres Comptes AWS personnes ou	27 novembre 2023

	avec votre organisation AWS RAM.	
Ajout du support pour partager des Explorateur de ressources AWS points de vue.	Vous pouvez désormais partager des Explorateur de ressources AWS points de vue avec d'autres Comptes AWS membres de votre organisation.	14 novembre 2023
Ajout de la prise en charge du partage des ressources d'Amazon Route 53 Application Recovery Controller.	Vous pouvez désormais partager des clusters Amazon Route 53 Application Recovery Controller avec d'autres Comptes AWS personnes ou avec votre organisation AWS RAM.	18 octobre 2023
Ajout d'un support pour partager les DataZone ressources Amazon.	Vous pouvez désormais partager les DataZone ressources Amazon avec d'autres personnes Comptes AWS ou avec votre organisation.	4 octobre 2023
Ajout du support pour le partage des principaux services.	Vous pouvez désormais associer des principaux de service à des partages de ressources. Cela permet à des services spécifiques de gérer les actions nécessaires pour les ressources clients en votre nom.	29 août 2023

Ajout de la prise en charge SageMaker du partage des ressources de la Model Card.	Vous pouvez désormais partager les ressources de la SageMaker Model Card avec d'autres Comptes AWS personnes ou avec votre organisation.	18 août 2023
Ajout de la prise en charge des groupes de SageMaker fonctionnalités Amazon Feature Store et du SageMaker catalogue en tant que ressources partageables.	Vous pouvez désormais partager les groupes de SageMaker fonctionnalités Amazon Feature Store et les ressources du SageMaker catalogue avec d'autres Comptes AWS personnes ou avec votre organisation.	20 juillet 2023
Augmentation du quota de service pour les invitations en attente.	Le nombre maximum d'invitations en attente par compte de partage est passé de 20 à 250.	8 juin 2023
Ajout du support pour les API AWS AppSync GraphQL en tant que ressources partageables.	Vous pouvez désormais partager des API AWS AppSync GraphQL avec d'autres Comptes AWS utilisateurs. AWS RAM	24 mai 2023
Ajout du support pour les Accès vérifié par AWS groupes en tant que ressources partageables.	Vous pouvez désormais créer et gérer Accès vérifié par AWS des groupes de manière centralisée, puis les partager avec d'autres personnes Comptes AWS ou avec votre organisation.	27 avril 2023

Ajout de la prise en charge des autorisations gérées par le client dans la AWS RAM console.	Vous pouvez désormais créer et gérer en toute sécurité des contrôles d'accès aux ressources précis pour les types de ressources pris en charge.	19 avril 2023
Ajout de la prise en charge du service Amazon VPC Lattice et des ressources partageables du réseau de services.	Vous pouvez désormais partager le service Amazon VPC Lattice et les ressources du réseau de services avec d'autres utilisateurs. Comptes AWS	31 mars 2023
Ajout de la prise en charge des entités du AWS Marketplace catalogue en tant que ressources partageables.	Vous pouvez désormais partager vos entités avec d'autres personnes sur Comptes AWS le Marketplace.	27 mars 2023
Ajout de la prise en charge de la gestion des versions d'autorisation dans la AWS RAM console.	Vous pouvez désormais utiliser la AWS RAM console pour afficher les détails des versions et mettre à jour les autorisations pour la version désignée par défaut.	16 janvier 2023
Mise à jour des meilleures pratiques IAM.	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	3 janvier 2023

Ajout de la prise en charge des groupes de placement Amazon EC2 en tant que ressources partageables.	Vous pouvez désormais partager des groupes de placement Amazon EC2 avec d'autres utilisateurs Comptes AWS pour y lancer leurs instances.	8 novembre 2022
Ajout de liens vers deux vidéos d'introduction sur AWS RAM.	Ajout de vidéos de présentation qui décrivent AWS RAM et expliquent comment partager une ressource avec d'autres personnes. Comptes AWS	29 août 2022
Ajout de la prise en charge des SageMaker pipelines Amazon.	Vous pouvez désormais partager des SageMaker pipelines avec d'autres personnes Comptes AWS.	2 août 2022
Ajout de la prise en charge des AWS Service Catalog AppRegistry applications et des groupes d'attributs en tant que types de ressources partageables.	Vous pouvez désormais partager AppRegistry des applications et des groupes d'attributs avec d'autres utilisateurs Comptes AWS.	17 juin 2022
AWS Resource Access Manager reçoit les certifications SOC et ISO.	AWS RAM a été validé comme étant conforme aux normes SOC (Service Organization Control) et ISO 9001, ISO 27001, ISO 27017, ISO 27018 et ISO 27701 de l'Organisation internationale de normalisation (ISO).	31 mai 2022

AWS Resource Access Manager reçoit la certification FedRAMP.	AWS RAM a été validé comme étant conforme au programme fédéral de gestion des risques et des autorisations (FedRAMP).	8 avril 2022
AWS Resource Access Manager reçoit la certification PCI DSS.	AWS RAM a été validé comme étant conforme à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI).	27 février 2022
Ajout de la prise en charge des découvertes de ressources IPAM Amazon VPC en tant que ressources partageables. En outre, vous pouvez désormais partager des pools IPAM avec des comptes extérieurs à une organisation.	Vous pouvez désormais partager les découvertes de ressources IPAM avec d'autres Comptes AWS personnes.	25 janvier 2022
Support supplémentaire pour le partage de ressources mondiales	Vous pouvez désormais partager des ressources globales avec d'autres Comptes AWS.	2 décembre 2021
Ajout de la prise en charge des réseaux principaux AWS Cloud WAN en tant que ressources mondiales partageables.	Vous pouvez désormais partager les réseaux principaux du Cloud WAN avec d'autres Comptes AWS.	2 décembre 2021

Support pour le partage de pools Amazon VPC IP Address Manager (IPAM)	Vous pouvez l'utiliser AWS RAM pour partager des pools IPAM Amazon VPC. Pour plus d'informations, consultez la section AWS Ressources partageables dans le Guide de l'AWS RAM utilisateur.	1er décembre 2021
Support pour le partage des SageMaker ressources Amazon	Vous pouvez l'utiliser AWS RAM pour partager des groupes de SageMaker lignées. Pour plus d'informations, consultez la section AWS Ressources partageables dans le Guide de l'AWS RAM utilisateur.	30 novembre 2021
Support pour le partage des AWS Migration Hub ressources Refactor Spaces	Vous pouvez l'utiliser AWS RAM pour partager des environnements Migration Hub. Pour plus d'informations, consultez la section AWS Ressources partageables dans le Guide de l'AWS RAM utilisateur.	29 novembre 2021
Ajout d'informations sur les politiques d'autorisation IAM AWS RAMAWS gérées par - managed.	Informations publiées sur les politiques d'autorisation AWS gérées disponibles auxquelles vous pouvez accéder dans la console IAM et associer aux principes IAM de votre. Compte AWS	16 septembre 2021

Ajout du support pour le partage des ressources S3 sur Outposts	Vous pouvez désormais l'utiliser AWS RAM pour partager S3 sur Outposts avec d'autres. Comptes AWS	5 août 2021
Ajout de la prise en charge des autorisations gérées supplémentaires et du partage de ressources avec les principaux IAM	Pour les types de ressources pris en charge, vous pouvez choisir parmi des autorisat ions AWS RAM gérées supplémentaires et partager des ressources avec des rôles et des utilisateurs IAM individuels.	10 juin 2021
Ajout de la prise en charge du partage AWS des ressources de Systems Manager Incident Manager	Vous pouvez désormais l'utiliser AWS RAM pour partager les contacts et les plans de réponse de AWS Systems Manager Incident Manager avec d'autres personnes Comptes AWS.	10 mai 2021
Ajout de la prise en charge du partage des ressources Amazon Route 53	Vous pouvez désormais les utiliser AWS RAM pour partager les groupes de règles du pare-feu DNS Amazon Route 53 Resolver avec d'autres Comptes AWS personnes.	31 mars 2021
Support supplémentaire pour le partage de AWS Transit Gateway ressources	Vous pouvez désormais les utiliser AWS RAM pour partager des domaines de multidiffusion de passerell e de transit avec d'autres Comptes AWS.	10 décembre 2020

Support supplémentaire pour le partage de AWS Network Firewall ressources	Vous pouvez désormais les utiliser AWS RAM pour partager des politiques de AWS Network Firewall pare-feu et des groupes de règles avec d'autres Comptes AWS.	17 novembre 2020
Ajout de la prise en charge du partage pour les Outposts et les tables de routage des passerelles locales	Vous pouvez désormais les utiliser AWS RAM pour partager les Outposts et les tables de routage des passerelles locales avec d'autres utilisateurs. Comptes AWS	15 octobre 2020
Ajout du support pour le partage des journaux de requêtes Route 53	Vous pouvez désormais AWS RAM partager les journaux de requêtes Route 53 avec d'autres utilisateurs Comptes AWS.	7 septembre 2020
Ajout du support pour le partage de AWS Private Certificate Authority ressources.	Vous pouvez désormais utiliser AWS RAM pour partager des autorités de certification Autorité de certification privée AWS privées (CA) avec d'autres Comptes AWS.	17 août 2020
Ajout de la prise en charge du partage des catalogues de données, des bases de données et des tables AWS Glue.	Vous pouvez désormais les utiliser AWS RAM pour partager des catalogues de données, des bases de données et des tables AWS Glue avec d'autres Comptes AWS utilisateurs.	7 juillet 2020

Ajout de la prise en charge du partage des listes de préfixes Amazon VPC.	Vous pouvez désormais les utiliser AWS RAM pour partager des listes de préfixes.	29 juin 2020
Ajout de la prise en charge du partage des AWS Outposts adresses IPv4 appartenant aux clients.	Vous pouvez désormais les utiliser AWS RAM pour partager des adresses IPv4 AWS Outposts appartenant à des clients avec d'autres personnes. Comptes AWS	22 avril 2020
Ajout du support pour le partage de AWS App Mesh maillages	Vous pouvez désormais l'utiliser AWS RAM pour partager des maillages avec d'autres Comptes AWS personnes.	17 janvier 2020
Ajout du support pour le partage de AWS CodeBuild projets et de groupes de rapports	Vous pouvez désormais l'utiliser AWS RAM pour partager AWS CodeBuild des projets et des groupes de rapports avec d'autres Comptes AWS.	13 décembre 2019
Support supplémentaire pour le partage de ressources supplémentaires	Vous pouvez désormais les utiliser AWS RAM pour partager des hôtes dédiés Amazon EC2, AWS Resource Groups des groupes de ressources, des composant s, des images et des recettes d'images Amazon EC2 Image Builder avec d'autres utilisate urs. Comptes AWS	2 décembre 2019

Ajout du support pour le partage des réservations de capacité à la demande	Vous pouvez désormais l'utiliser AWS RAM pour partager des réservations de capacité à la demande avec d'autres personnes Comptes AWS.	29 juillet 2019
Ajout de la prise en charge du partage de clusters de base de données Aurora	Vous pouvez désormais les utiliser AWS RAM pour partager des clusters de base de données Aurora avec d'autres Comptes AWS.	2 juillet 2019
Ajout de la prise en charge du partage des cibles de mise en miroir du trafic	Vous pouvez désormais les utiliser AWS RAM pour partager des cibles de mise en miroir du trafic avec d'autres Comptes AWS.	25 juin 2019
Ajout de la prise en charge du partage des configurations de licence	Vous pouvez désormais les utiliser AWS RAM pour partager les configurations AWS de licence de License Manager avec d'autres utilisateurs Comptes AWS.	5 décembre 2018
Ajout du support pour le partage de sous-réseaux	Vous pouvez désormais les utiliser AWS RAM pour partager des sous-réseaux Amazon VPC avec d'autres. Comptes AWS	27 novembre 2018
Support supplémentaire pour le partage des passerelles de transport en commun	Vous pouvez désormais les utiliser AWS RAM pour partager les passerelles de transit Amazon VPC avec d'autres. Comptes AWS	26 novembre 2018

Ajout du support pour le partage des règles du résolveur	Vous pouvez désormais les utiliser AWS RAM pour partager les règles de Route 53 Resolver avec d'autres Comptes AWS.	20 novembre 2018

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.