Guide de l’utilisateur

AWS Resource Access Manager

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

AWS Resource Access Manager: Guide de l’utilisateur

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

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que c'est AWS RAM ? 1
Aperçus vidéo 1
Avantages de AWS RAM 2
Qu'en est-il de l'accès entre comptes avec des politiques basées sur les ressources ? 2
Comment fonctionne le partage des ressources 3
Partage de vos ressources 3
Utilisation de ressources partagées 5
Accès AWS RAM 5
Tarification pour AWS RAM 6
Conformité et normes internationales 6
PCI DSS 6
FedRAMP 7
SOC et ISO 7
Mise en route 8
Termes et concepts 8
Partage de ressources 8
Partage de compte 9
Principaux consommateurs 10
Stratégie basée sur une ressource 12
Autorisations gérées 17
Version d'autorisation gérée 18
Partage de vos ressources 19
Activez le partage des ressources au sein de AWS Organizations 19
Création d'un partage de ressources 21
Utilisation de ressources partagées 31
Répondre à l'invitation de partage de ressources 31
Utilisez les ressources partagées avec vous 33
Utilisation des ressources partagées 35
Ressources régionales et mondiales 35
Quelles sont les différences entre les ressources régionales et mondiales ? 36
Les partages de ressources et leurs régions 37
Ressources que vous détenez 39
Afficher les partages de ressources que vous avez créés 39
Création d'un partage de ressources 42

Mettre à jour un partage de ressources 52
Afficher vos ressources partagées 60
Afficher les principes avec lesquels vous partagez 61
Supprimer un partage de ressources 63
Ressources partagées avec vous 65
Acceptation et rejet des invitations 66
Afficher les partages de ressources partagés avec vous 70
Afficher les ressources partagées avec vous 72
Afficher les informations principales partagées avec vous 73
Quitter un partage de ressources 75
Zone de disponibilité IDs 78
Ressources partageables 81
AWS App Mesh 83
AWS AppSync API GraphQL 84
Amazon API Gateway 85
Contrôleur Amazon Application Recovery (ARC) 86
Amazon Aurora 88
AWS Backup 89
Amazon Bedrock 90
Billing and Cost Management 91
AWS Billing Afficher le service 93
AWS Cloud Map 95
AWS Réseau WAN dans le cloud 96
Amazon CloudFront 96
AWS CloudHSM 97
AWS CodeBuild 99
AWS CodeConnections 101
Amazon DataZone 102
Amazon EC2 102
EC2 Image Builder 108
Elastic Load Balancing 112
AWS End User Messaging SMS 114
Amazon FSx pour OpenZFS 118
AWS Glue 120
AWS License Manager 124
AWS Marketplace 125

AWS Migration Hub Refactor Spaces 126
Approbation multipartite 128
AWS Network Firewall 129
Oracle Database@AWS 132
AWS Outposts 135
Amazon S3 sur Outposts 137
AWS Autorité de certification privée 138
Explorateur de ressources AWS 140
Groupes de ressources AWS 141
Amazon Route 53 142
Amazon Simple Storage Service 146
Amazon SageMaker AI 147
AWS Service Catalog AppRegistry 158
AWS Systems Manager Incident Manager 160
AWS Systems Manager 164
Amazon VPC 167
Amazon VPC Lattice 179
Gestion des autorisations dans AWS RAM 184
Afficher les autorisations gérées 185
Création et utilisation d'autorisations gérées par le client 190
Création d'une autorisation gérée par le client 191
Création d'une nouvelle version d'une autorisation gérée par le client 193
Choisissez une version différente comme version par défaut pour une autorisation gérée par le client 195
Supprimer une version d'autorisation gérée par le client 197
Supprimer une autorisation gérée par le client 198
Mise à jour des versions d'autorisations gérées 200
Considérations relatives aux autorisations gérées par le client 202
Comment fonctionnent les autorisations gérées 203
Types d'autorisations gérées 204
Sécurité 207
Protection des données 208
Identity and Access Management 209
Comment AWS RAM fonctionne avec IAM 209
AWS politiques gérées 213
Utilisation des rôles liés à un service 218

Exemple de politiques IAM 220
Exemple SCPs 223
Désactiver le partage avec les Organisations 228
Journalisation et surveillance 229
Surveillance à l'aide EventBridge 230
Journalisation des appels d' AWS RAM API avec AWS CloudTrail 232
Résilience 234
Sécurité de l'infrastructure 235
AWS PrivateLink 235
Considérations 236
Création d'un point de terminaison d'interface 236
Création d'une politique de point de terminaison 236
Résolution de problème 238
Erreur : le numéro de compte n'existe pas 238
Scénario 238
Cause 238
Solution 238
Erreur : exception d'accès refusé 239
Scénario 239
Cause 239
Solution 239
Erreur : exception de ressource inconnue 241
Scénario 241
Cause 242
Solution 242
Erreur : le partage en dehors d'une organisation n'est pas autorisé 243
Scénario 243
Causes possibles et solutions 243
Erreur : Impossible de voir les ressources partagées 244
Scénario 244
Causes possibles et solutions 244
Erreur : limite dépassée, exception 247
Scénario 247
Cause 247
Solution 247
Aucune invitation reçue 247

Scénario 247
Cause 247
Impossible de partager un VPC 248
Scénario 248
Cause 248
Quotas de service 250
En utilisant le AWS SDKs 253
Historique de la documentation 254
..... cclxx

Qu'est-ce que c'est AWS Resource Access Manager ?

AWS Resource Access Manager (AWS RAM) vous permet de partager en toute sécurité vos ressources entre Comptes AWS, au sein de votre organisation ou de vos unités organisationnelles (OUs), ainsi qu'avec les rôles et utilisateurs AWS Identity and Access Management (IAM) pour les types de ressources pris en charge. Si vous en avez plusieurs Comptes AWS, vous pouvez créer une ressource une seule fois et l'utiliser AWS RAM pour la rendre utilisable par ces autres comptes. Si votre compte est géré par AWS Organizations, vous pouvez partager des ressources avec tous les autres comptes de l'organisation ou uniquement avec les comptes contenus dans une ou plusieurs unités organisationnelles spécifiées (OUs). Vous pouvez également partager avec un utilisateur spécifique Comptes AWS par identifiant de compte, 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 utilisateurs IAM spécifiques.

Table des matières

- Aperçus vidéo
- Avantages de AWS RAM
- Comment fonctionne le partage des ressources
- Accès AWS RAM
- Tarification pour AWS RAM
- Conformité et normes internationales

Aperçus vidéo

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

La vidéo suivante montre comment appliquer des autorisations AWS gérées à vos AWS ressources. Pour de plus amples informations, veuillez consulter ???.

Cette vidéo montre comment créer et associer des autorisations gérées par les clients conformément à la meilleure pratique du moindre privilège. Pour plus d'informations, voir,???.

Avantages de AWS RAM

Pourquoi utiliser AWS RAM ? Elle offre les avantages suivants :

- Réduit vos frais d'exploitation : créez une ressource une seule fois, puis AWS RAM utilisez-la pour la partager 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, AWS RAM simplifie l'octroi de l'accès à chaque rôle et utilisateur de ce compte sans avoir à utiliser de politiques d'autorisation basées sur l'identité.
- Assure la sécurité et la 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 la tâche de mettre en œuvre des politiques et des autorisations identiques, puis de les conserver identiques sur tous ces comptes. Au lieu de cela, tous les utilisateurs d'un partage de AWS RAM ressources sont gérés par un ensemble unique de politiques et d'autorisations. AWS RAM offre une expérience cohérente pour le partage de différents types de AWS ressources.
- Fournit de la visibilité et de l'auditabilité : consultez les détails d'utilisation de vos ressources partagées grâce à l'intégration AWS RAM avec Amazon CloudWatch et AWS CloudTrail. AWS RAM fournit une visibilité complète sur les ressources et les comptes partagés.

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

Vous pouvez partager certains types de AWS ressources avec d'autres Comptes AWS en attachant une politique basée sur les ressources qui identifie les principaux AWS Identity and Access Management (IAM) (rôles et utilisateurs IAM) extérieurs à la vôtre. Compte AWS Cependant, le partage d'une ressource en y associant une politique ne permet pas de tirer parti des avantages supplémentaires que cela AWS RAM apporte. En l'utilisant, AWS RAM vous bénéficiez des fonctionnalités suivantes :

- Vous pouvez partager avec une organisation ou une unité organisationnelle (UO) sans avoir à les Compte AWS IDs énumérer toutes.
- Les utilisateurs peuvent voir les ressources partagées avec eux directement dans la Service AWS console d'origine et dans les opérations de l'API, comme si ces ressources se trouvaient directement dans le compte de l'utilisateur. Par exemple, si vous partagez 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. AWS RAM Les ressources partagées en joignant une politique basée sur les ressources ne sont pas visibles de cette façon ; vous devez plutôt découvrir et faire explicitement référence à la ressource par son Amazon Resource Name (ARN).

- Les propriétaires d'une ressource peuvent voir quels principaux 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 lancez un processus d'invitation. Le destinataire doit accepter l'invitation avant que le principal 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 aucune invitation.

Si vous avez partagé des ressources à l'aide d'une politique d'autorisation basée sur les ressources, vous pouvez promouvoir ces ressources en ressources entièrement AWS RAM gérées en effectuant l'une des opérations suivantes :

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

Comment fonctionne le partage des ressources

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

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

Partage de vos ressources

Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Pour créer un partage de ressources, vous devez spécifier les éléments suivants :

- Le Région AWS dans lequel vous souhaitez créer le partage de ressources. Dans la console, vous pouvez choisir dans le menu déroulant Région situé dans le coin supérieur droit de la console. Dans le AWS CLI, vous utilisez le `--region` paramètre.
  - Un partage de ressources ne peut contenir que des ressources régionales identiques Région AWS au partage de ressources.
  - Un partage de ressources ne peut contenir des ressources mondiales que si le partage de ressources se trouve dans la région d'origine désignée pour les ressources mondiales, à savoir l'est des États-Unis (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 principaux auxquels vous accordez l'accès à la ressource partagent. Les principaux peuvent être des individus Comptes AWS, les comptes d'une organisation ou d'une unité organisationnelle (UO) AWS Organizations, des rôles ou des utilisateurs individuels AWS Identity and Access Management (IAM).

  > **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 principaux utilisateurs des autres comptes peuvent faire avec les ressources du partage de ressources.

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

  - Si le principal se trouve dans un compte 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 individuels et aux utilisateurs l'accès à la ressource partagée selon des politiques basées sur l'identité IAM. 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, les AWS CLI commandes et les opérations d'API du service concerné. Les opérations d'API que les principaux de votre compte sont autorisés à effectuer varient en fonction du type de ressource et sont spécifiées par l' AWS RAM autorisation attachée au partage de ressources. Toutes les politiques IAM et les politiques de contrôle des services configurées dans votre compte continuent également de s'appliquer, ce qui vous permet de tirer parti de vos investissements existants dans les contrôles de sécurité et de gouvernance.

Lorsque vous accédez à une ressource partagée en utilisant le service de cette ressource, vous avez les mêmes capacités et limites Compte AWS que le propriétaire de la ressource.

- Si la ressource est régionale, vous ne pouvez y accéder qu'à partir de Région AWS celle dans laquelle elle existe dans le compte propriétaire.
- Si la ressource est globale, vous pouvez y accéder depuis n'importe quel Région AWS outil pris en charge par la console de service et les outils de la ressource. Vous pouvez afficher et gérer le partage des ressources et ses 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`.

Accès AWS RAM

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

AWS RAM console

AWS RAM fournit une interface utilisateur basée sur le Web, la AWS RAM console. Si vous vous êtes inscrit à un Compte AWS, vous pouvez accéder à la AWS RAM console en vous connectant AWS Management Consoleet en choisissant sur la page AWS RAM d'accueil de la console.

Vous pouvez également accéder directement à la AWS RAM console dans votre navigateur. Si vous n'êtes pas encore connecté, vous êtes invité à le faire avant que la console n'apparaisse.

AWS CLI et outils pour Windows PowerShell

Les AWS CLI et Outils AWS pour PowerShell fournissent un accès direct aux opérations AWS RAM publiques de l'API. AWS prend en charge ces outils sur WindowsmacOS, etLinux.

Pour plus d'informations sur la mise en route, consultez le guide de AWS Command Line Interface l'utilisateur ou le guide de AWS Tools for Windows PowerShell l'utilisateur. Pour plus d'informations sur les commandes pour AWS RAM, consultez la référence des commandes ou la référence des AWS Tools for Windows PowerShell applets de AWS CLI commande.

AWS SDKs

AWS fournit des commandes d'API pour un large éventail de langages de programmation. Pour plus d'informations sur la mise en route, consultez le guide de référence AWS SDKs et Tools.

API de requête

Si vous n'utilisez pas l'un des langages de programmation pris en charge, l'API de requête AWS RAM HTTPS vous donne un accès programmatique à AWS RAM et AWS. Grâce à l' AWS RAM API, vous pouvez envoyer des requêtes HTTPS directement au service. Lorsque vous utilisez l' AWS RAM API, vous devez inclure du code pour signer numériquement les demandes à l'aide de vos informations d'identification. Pour plus d'informations, consultez la page Référence de l'API AWS RAM.

Tarification pour AWS RAM

Aucuns frais supplémentaires ne sont facturés pour l'utilisation AWS RAM ou la création de partages de ressources et pour 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 le mode AWS de facturation des ressources partageables, consultez la documentation relative au service propriétaire de la ressource.

Conformité et normes internationales

PCI DSS

AWS RAM prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et sa conformité à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) a été validée.

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

FedRAMP

AWS RAM est autorisé en tant que FedRAMP Moderate dans les pays Régions AWS suivants : USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Californie du Nord) et USA Ouest (Oregon).

AWS RAM est autorisé sous le nom de FedRAMP High dans les pays Régions AWS suivants AWS GovCloud : (US-West) et (US-East). AWS GovCloud

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 RAM peut 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 contrôles de sécurité qui protègent les données des clients. Ces informations figurent dans les rapports SOC, ainsi que dans AWS Artifactles certificats AWS ISO et CSA STAR.

Pour plus d'informations sur la conformité aux normes SOC, consultez la section SOC.

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

Commencer avec AWS RAM

Avec AWS Resource Access Manager, vous pouvez partager les ressources que vous possédez avec d'autres personnes Comptes AWS. Si votre compte est géré par AWS 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'autres personnes Comptes AWS.

Si vous n'activez pas le partage interne AWS Organizations, vous ne pouvez pas partager de ressources avec votre organisation ou avec les unités organisationnelles (UO) de votre organisation. Cependant, vous pouvez toujours partager des ressources avec des Comptes AWS membres de votre organisation. Pour les types de ressources pris en charge, vous pouvez également partager des ressources avec des rôles ou des utilisateurs individuels AWS Identity and Access Management (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 des ressources, et ils doivent accepter l'invitation pour accéder aux ressources partagées.

Table des matières

- Termes et concepts pour AWS RAM
- Partage de vos AWS ressources
- Utilisation de AWS ressources partagées

Termes et concepts pour AWS RAM

Les concepts suivants expliquent comment vous pouvez utiliser AWS Resource Access Manager (AWS RAM) pour partager vos ressources.

Partage de ressources

Vous partagez des ressources en AWS RAM créant un partage de ressources. Un partage de ressources comporte les trois éléments suivants :

- Liste d'une ou de plusieurs AWS ressources à partager.
- Liste d'un ou de plusieurs principaux auxquels l'accès aux ressources est accordé.

- Une autorisation gérée pour 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.

Une fois que AWS RAM vous avez créé un partage de ressources, les principaux spécifiés dans le partage de ressources peuvent avoir accès aux ressources du partage.

- Si vous activez le AWS RAM partage avec AWS Organizations et que les principaux 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 conformément à une politique d'autorisation AWS Identity and Access Management (IAM).
- Si vous n'activez pas le AWS RAM partage avec les Organisations, vous pouvez toujours partager des ressources avec Comptes AWS des membres 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, consultez Ressources partageables AWS la colonne Peut partager avec des comptes extérieurs à son organisation.

Partage de compte

Le compte de partage contient la ressource qui est partagée et dans laquelle l' AWS RAM administrateur crée le partage de AWS ressources en utilisant AWS RAM.

Un AWS RAM administrateur est un administrateur principal IAM autorisé à créer et à configurer des partages de ressources dans le Compte AWS. Comme AWS RAM cela fonctionne en associant une politique basée sur les ressources aux ressources d'un partage de ressources, l' AWS RAM administrateur doit également être autorisé à appeler l'`PutResourcePolicy`opération Service AWS pour chaque type de ressource inclus dans un partage de ressources.

Principaux consommateurs

Le compte consommateur est le compte Compte AWS sur 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, consultez Ressources partageables AWS et consultez la colonne Peut partager avec les rôles et utilisateurs IAM.

AWS RAM soutient également les principaux 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, consultez Ressources partageables AWS et consultez la colonne Peut être partagée avec les responsables du service.

Les principaux du compte consommateur ne peuvent effectuer que les actions autorisées par les deux autorisations suivantes :

- Les autorisations gérées associées au partage de ressources. Ils spécifient les autorisations maximales 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` l'accès à des actions spécifiées et à l'Amazon Resource Name (ARN) d'une ressource dans le compte de partage.

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

- Autre Compte AWS : le partage des ressources met les ressources incluses dans le compte de partage à la disposition du compte consommateur.
- Rôles IAM individuels ou utilisateurs d'un autre compte : certains types de ressources prennent en charge le partage direct avec des rôles ou utilisateurs IAM individuels. Spécifiez ce type principal par son ARN.
  - Rôle IAM — `arn:aws:iam::123456789012:role/rolename`
  - Utilisateur IAM — `arn:aws:iam::123456789012:user/username`
- Service principal : partagez une ressource avec un AWS service pour autoriser ce dernier à accéder à un partage de ressources. Le partage du capital de AWS service permet à un service de prendre des mesures en votre nom afin d'alléger la charge opérationnelle.

Pour partager avec un principal de service, choisissez d'autoriser le partage avec n'importe qui, puis, sous Sélectionner le type de principal, choisissez Service principal dans 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 l'ID de compte du propriétaire de la ressource dans la clé de `aws:SourceAccount` condition.

- Comptes d'une organisation : si le compte de partage est géré par AWS Organizations, le partage de ressources peut 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 partager qu'avec sa propre organisation ou une unité d'organisation IDs 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 dans AWS Organizations :

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

  - Tous les comptes d'une unité organisationnelle : voici un exemple d'ARN d'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 qui AWS RAM s'attache à chaque ressource du partage utilise. `"Principal": "*"` Pour de plus amples informations, veuillez consulter Implications de l'utilisation "Principal": "*" dans le cadre d'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 l'`Allow`accès aux ressources individuelles ARNs 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.

Stratégie basée sur une ressource

Les politiques basées sur les ressources sont des documents texte JSON qui implémentent le langage de politique IAM. Contrairement aux politiques basées sur l'identité que vous attachez au principal, telles qu'un rôle ou un utilisateur IAM, vous attachez des politiques basées sur les ressources à la ressource. AWS RAM rédige 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 un élément `Principal` de politique qui détermine qui peut accéder à la ressource. Pour plus d'informations, consultez les sections Politiques basées sur l'identité et politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Les politiques basées sur les ressources générées par AWS RAM sont évaluées en même temps que tous les autres types de politiques IAM. Cela inclut toutes les politiques basées sur l'identité IAM attachées aux principaux qui tentent d'accéder à la ressource, et les politiques de contrôle des services (SCPs) correspondantes peuvent AWS Organizations s'appliquer au. Compte AWS Les politiques basées sur les ressources générées par AWS RAM participent 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, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

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

Pour les types de ressources qui prennent en charge les politiques basées sur les ressources, construit et gère AWS RAM automatiquement les politiques basées sur les ressources pour vous. Pour une ressource donnée, AWS RAM élabore la politique basée sur les ressources en combinant les informations provenant de tous les partages de ressources qui incluent cette ressource. Prenons l'exemple d'un pipeline Amazon SageMaker AI que vous partagez en utilisant AWS RAM et en incluant 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 n'accorder que des autorisations d'exécution de l' SageMaker IA à un seul compte. AWS RAM combine automatiquement ces deux ensembles d'autorisations différents en une seule politique de ressources comportant plusieurs instructions. Il attache ensuite la politique combinée basée sur les ressources à la ressource du pipeline. Vous pouvez consulter cette politique de ressources sous-jacente en appelant l'GetResourcePolicyopération. Services AWS utilisez 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 de les utiliser AWS RAM car elles offrent les avantages suivants :

- Découvrabilité pour les consommateurs de partages : si vous partagez des ressources en utilisant AWS RAM, les utilisateurs peuvent voir toutes les ressources partagées avec eux directement dans la console du service propriétaire des ressources et dans les opérations d'API comme si ces ressources se trouvaient directement dans le compte de l'utilisateur. Par exemple, si vous partagez un AWS CodeBuild projet avec un autre compte, les utilisateurs du compte consommateur peuvent voir le projet dans la CodeBuild console et dans les résultats des opérations d' CodeBuild 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 propriétaires d'actions : si vous partagez des ressources en utilisant AWS 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 utilisant AWS 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 — Grâce à AWS RAM cela, vous n'avez pas besoin de comprendre le langage de politique IAM basé sur JSON. AWS RAM fournit des autorisations ready-to-use AWS gérées que vous pouvez choisir d'associer à vos partages de ressources.

En utilisant AWS 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, génère AWS RAM automatiquement une politique basée sur les ressources en tant que représentation des autorisations réelles. Les utilisateurs peuvent consulter cette représentation en appelant GetResourcePolicy. Cela inclut les types de ressources suivants :

- Amazon Aurora — Clusters de bases de données
- Amazon EC2 — réservations de capacité et hébergeurs 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 : IPv4 adresses, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit et domaines de multidiffusion de passerelles de transit appartenant au client

Exemples de politiques basées sur les ressources AWS RAM générées

Si vous partagez une EC2 ressource d'image Image Builder avec un compte individuel, AWS RAM génère une politique semblable à l'exemple suivant et l'associe à toutes les ressources d'image incluses dans le partage de ressources.

JSON

```
{
    "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 EC2 ressource d'image Image Builder avec un rôle ou un utilisateur IAM dans un autre Compte AWS, AWS RAM génère une politique semblable à l'exemple suivant et l'attache à toutes les ressources d'image incluses dans le partage de ressources.

JSON

```
{
    "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 EC2 ressource d'image Image Builder avec tous les comptes d'une organisation ou avec les comptes d'une unité d'organisation, AWS RAM génère une politique semblable à l'exemple suivant et l'associe à toutes les ressources d'image incluses dans le partage de ressources.

> **Note**
>
> Cette politique utilise `"Principal": "*"` puis utilise l'`"Condition"`élément pour restreindre les autorisations aux identités qui correspondent à celles spécifiées`PrincipalOrgID`. Pour de plus amples informations, veuillez consulter

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

JSON

```
{
    "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 le cadre d'une politique basée sur les ressources

Lorsque vous `"Principal": "*"` incluez une politique basée sur les ressources, celle-ci 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. `Deny`Les déclarations explicites contenues dans toute politique qui s'applique au principal appelant remplacent les autorisations accordées par cette politique. Cependant, un élément implicite `Deny` (c'est-à-dire l'absence d'explicite`Allow`) dans les politiques d'identité, les politiques de limites d'autorisations ou les politiques de session applicables n'autorise pas les principaux `Deny` à accéder à une action par le biais d'une telle politique basée sur les ressources.

Si ce comportement n'est pas souhaitable pour votre scénario, vous pouvez le limiter en ajoutant une `Deny` déclaration explicite 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 créez un partage de ressources, vous devez spécifier l'autorisation gérée à utiliser pour chaque type de ressource inclus dans le partage de ressources. Une autorisation gérée répertorie l'ensemble `actions` et les conditions que les principaux peuvent exécuter avec la ressource partagée à l'aide AWS RAM de celle-ci.

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 attribuant à chaque ensemble une autorisation de gestion différente. Il existe deux types d'autorisations gérées :

AWS autorisations gérées

> AWS les autorisations gérées sont créées et gérées par AWS et accordent des autorisations pour les scénarios clients courants. AWS RAM définit au moins une autorisation AWS gérée pour chaque type de ressource pris en charge. Certains types de ressources prennent en charge plusieurs autorisations AWS gérées, une autorisation gérée étant désignée AWS par défaut. L'autorisation AWS gérée par défaut est associée, sauf indication contraire de votre part.

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 avec des ressources partagées AWS 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 requises 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 que des clés contextuelles globales et des clés spécifiques au service afin de spécifier les conditions dans lesquelles les principaux ont accès à la ressource. Ces autorisations peuvent être utilisées dans un ou plusieurs AWS RAM partages. Les autorisations gérées par le client sont spécifiques à la région.

AWS RAM utilise les autorisations gérées comme entrée pour créer les politiques basées sur les ressources pour 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. Pour chaque autorisation gérée, une version est toujours désignée comme version par défaut. Lorsque vous créez ou AWS créez 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.

AWS versions d'autorisations gérées

AWS gère toutes les modifications apportées aux autorisations AWS 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 autorisation gérée 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 de plus amples informations, veuillez consulter Mise à jour des autorisations AWS gérées vers une version plus récente.

Partage de vos AWS ressources

Pour partager une ressource dont vous êtes propriétaire en utilisant AWS 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 RAM est un service régional. Les principaux partenaires avec lesquels vous partagez peuvent accéder aux partages de ressources uniquement dans le pays Régions AWS dans lequel les ressources ont été créées.
> - Certaines ressources comportent des considérations particulières et des conditions préalables au partage. Pour de plus amples informations, veuillez consulter Ressources partageables AWS.

Activez le partage des ressources au sein de AWS Organizations

Lorsque votre compte est géré par AWS 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 avec AWS 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.

> **Note**
>
> Lorsque le partage avec AWS Organizations est activé, tout partage de ressources au sein de l'organisation est limité aux utilisateurs de la même organisation. Cela signifie que si le consommateur quitte l'organisation, il perdra l'accès aux ressources du partage de ressources. Cela est vrai lorsque la ressource est partagée avec une unité d'organisation, l'ensemble de l'organisation ou un compte individuel au sein de l'organisation.

Si vous n'avez plus besoin de partager des ressources avec l'ensemble de votre organisation OUs, vous pouvez désactiver le partage des ressources. Pour de plus amples informations, veuillez consulter 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-access AWS CLI commande, 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. Choisissez Activer le partage avec AWS Organizations, puis sélectionnez 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 région Région 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.
   - AWS les 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 RAM est un service régional. Lorsque vous partagez une ressource avec des responsables d'autres entités Comptes 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 de plus amples informations, veuillez consulter Implications de l'utilisation "Principal": "*" dans le cadre d'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 l'`Allow`accès aux ressources individuelles ARNs 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 OUs depuis cette organisation à vos partages de ressources. Vous ne pouvez pas ajouter OUs d'organisations extérieures à votre propre organisation à un partage de ressources en tant que responsables. 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 hébergeurs 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 : IPv4 adresses appartenant au client, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit, domaines de multidiffusion de passerelles de transit

Console

Pour créer un partage de ressources

1. Ouvrez 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. 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 de plus amples informations, veuillez consulter Zone de disponibilité IDs pour vos AWS 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 de plus amples informations, veuillez consulter 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 Création d'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 de plus amples informations, veuillez consulter Implications de l'utilisation "Principal": "*" dans le cadre d'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 l'`Allow`accès aux ressources individuelles ARNs 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 Comptes AWS principaux membres de cette unité d'organisation et son enfant OUs peuvent accéder au partage des ressources.
- Si vous sélectionnez une personne Compte 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 un Compte 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-user AWS CLI commande 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 de plus amples informations, veuillez consulter Partagez AWS les ressources qui vous appartiennent.

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 de plus amples informations, veuillez consulter Création d'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 de AWS ressources partagées

Pour commencer à utiliser les ressources partagées avec votre compte AWS Resource Access Manager, effectuez les tâches suivantes.

Tâches

- Répondre à l'invitation de partage de ressources
- Utilisez les ressources partagées avec vous

Répondre à l'invitation de partage de ressources

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

Les invitations ne sont pas utilisées dans les scénarios suivants :

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

Console

Pour répondre aux invitations

1. Ouvrez la page Partagé avec moi : partage de ressources dans la AWS RAM console.

   > **Note**
   >
   > Un partage de ressources n'est visible que dans celui Région AWS dans lequel il a été créé. Si le partage de ressources attendu n'apparaît pas dans la console, vous devrez peut-être passer à un autre Région AWS en utilisant le menu déroulant situé dans le coin supérieur droit.

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

   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.

3. 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 commencer, obtenez une liste des invitations à partager des ressources qui sont à votre disposition. L'exemple de commande suivant a été exécuté dans la `us-west-2` région et montre qu'un partage de ressources est disponible dans l'`PENDING`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 l'Amazon Resource Name (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` est devenu`ACCEPTED`. Les ressources incluses dans ce partage de ressources sont désormais accessibles aux principaux du compte d'acceptation.

Utilisez les ressources partagées avec vous

Après avoir 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 de plus amples informations, veuillez consulter Ressources partageables AWS. Les ressources sont disponibles directement dans la console de service et les API/CLI opérations de chaque ressource. Si la ressource est régionale, vous devez utiliser la bonne option dans la console de service ou Région AWS 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 AWS

RAM, vous devez ouvrir la AWS RAM console dans Région AWS laquelle le partage de ressources a été créé.

Utilisation de AWS ressources partagées

Vous pouvez utiliser AWS Resource Access Manager (AWS RAM) pour partager AWS des ressources que vous possédez et accéder à AWS des ressources partagées avec vous.

Table des matières

- Partage des ressources régionales par rapport aux ressources mondiales
  - Quelles sont les différences entre les ressources régionales et mondiales ?
  - Les partages de ressources et leurs régions
- Partagez AWS les ressources qui vous appartiennent
  - Afficher les partages de ressources que vous avez créés dans AWS RAM
  - Création d'un partage de ressources dans AWS RAM
  - Mettre à jour un partage de ressources dans AWS RAM
  - Afficher vos ressources partagées dans AWS RAM
  - Afficher les principaux partenaires avec lesquels vous partagez des ressources dans AWS RAM
  - Supprimer un partage de ressources dans AWS RAM
- Accédez aux AWS ressources partagées avec vous
  - Accepter et rejeter les invitations à partager des ressources
  - Afficher les partages de ressources partagés avec vous
  - Afficher les ressources partagées avec vous
  - Afficher les informations principales partagées avec vous
  - Quitter un partage de ressources
    - Conditions préalables pour quitter un partage de ressources
    - Comment quitter un partage de ressources
- Zone de disponibilité IDs pour vos AWS ressources

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 mondiale. Les ressources régionales indiquent le Région AWS. Si ce champ 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 AWS spécifiée, afin qu'elles puissent être disponibles 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 AWS Management Console, vous devez choisir Région AWS celle dans laquelle vous souhaitez créer l'instance. Si vous utilisez le AWS Command Line Interface (AWS CLI) pour créer l'instance, vous incluez le `--region` paramètre. Ils ont AWS SDKs chacun leur propre mécanisme équivalent pour spécifier la région utilisée par l'opération.

Plusieurs raisons justifient l'utilisation des ressources régionales. L'une des bonnes raisons est de veiller à ce que les ressources et les points de terminaison de service que vous utilisez pour y accéder soient aussi proches que possible du client. Les performances sont ainsi améliorées grâce à la réduction de la latence. Une autre raison vise à fournir une limite d'isolement. Vous pouvez ainsi créer des copies indépendantes des ressources dans plusieurs régions afin de répartir la charge et d'améliorer la capacité de mise à l'échelle. Par ailleurs, les ressources sont isolées les unes des autres afin d'améliorer leur disponibilité.

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

Lorsque vous examinez l'Amazon Resource Name (ARN) d'une ressource régionale, la région qui contient la ressource est spécifiée dans le quatrième champ de l'ARN. Par exemple, une EC2 instance Amazon est une ressource régionale. Ces ressources ARNs 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 globales

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 devez pas spécifier de `--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 situées dans différentes régions ne sont pas adéquates. L'accès à un point de terminaison global unique, associé à une augmentation éventuelle de la latence, est considéré comme acceptable pour garantir que tout changement soit instantanément visible pour les consommateurs 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 dans toutes les régions.

L'Amazon Resource Name (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 RAM est un service régional et un partage de ressources est régional. Par conséquent, un partage de ressources peut contenir des ressources provenant du même type 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, la région USA Est (Virginie du Nord),`us-east-1`. Bien que vous ne puissiez créer le partage de ressources que dans cette seule région d'origine, toute ressource globale partagée apparaît comme une ressource globale standard lorsqu'elle est visualisée dans la console ou dans les opérations de la CLI et du SDK de ce service. La restriction à la région d'origine s'applique uniquement au partage des 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 qui inclut des ressources régionales provenant de différentes sources Régions AWS. Cela signifie que pour partager les ressources `us-west-2` des deux parties`eu-north-1`, vous devez créer deux partages de ressources différents. Vous ne pouvez pas combiner les ressources de deux régions différentes dans un seul partage de ressources.

Pour partager une ressource globale dans la AWS RAM console, vous devez configurer la AWS RAM console pour utiliser 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 combiner des ressources mondiales 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 uniquement dans la région d'origine désignée, elle reste une ressource mondiale une fois que vous l'avez partagée. Vous pouvez y accéder dans le partage Comptes AWS depuis n'importe quelle région à partir de laquelle vous pouviez y accéder dans l'original Compte 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 central 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 AWS RAM AWS CLI et le SDK vous permettent d'interagir uniquement avec les partages de ressources situés dans la région que vous spécifiez dans votre opération. Pour consulter ou modifier les partages de ressources contenant des ressources mondiales, 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 afin de 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`.

Partagez AWS les ressources qui vous appartiennent

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

Rubriques

- Afficher les partages de ressources que vous avez créés dans AWS RAM
- Création d'un partage de ressources dans AWS RAM
- Mettre à jour un partage de ressources dans AWS RAM
- Afficher vos ressources partagées dans AWS RAM
- Afficher les principaux partenaires avec lesquels vous partagez des ressources dans AWS RAM
- Supprimer un partage de ressources dans AWS RAM

Afficher les partages de ressources que vous avez créés dans AWS RAM

Vous pouvez consulter 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 Shared by me : 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. Si l'une des autorisations gérées utilisées par les partages de ressources dans les résultats comporte une nouvelle version de l'autorisation gérée désignée 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 Vérifier et mettre à jour tout en haut de la page.

Sinon, pour les partages de ressources individuels avec une ou plusieurs nouvelles versions d'autorisations gérées, la colonne État indique « 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.

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, tel qu'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 une liste déroulante des champs d'attributs suggérés. Après en avoir choisi un, vous pouvez le choisir dans 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.
5. Choisissez le nom du partage de ressources à examiner. La console affiche les informations suivantes concernant le partage de ressources :

   - Résumé : indique le nom du partage de ressources, son ID, son propriétaire, le nom de ressource Amazon (ARN), sa date de création, indique s'il autorise le partage avec des comptes externes et indique son statut actuel.
   - Autorisations gérées — Répertorie les autorisations gérées associées à ce partage de ressources. Il peut y avoir au plus 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 de mise 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.
   - Principaux partagés — Répertorie les principaux avec lesquels les ressources sont partagées.

- Balises : répertorie les paires clé-valeur de balises associées au partage de ressources lui-même ; il ne s'agit pas des balises associées 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 sur pour `SELF` afficher les détails des partages de ressources créés dans votre Compte AWS.

L'exemple suivant montre les partages de ressources partagés dans le fichier current Région AWS (`us-east-1`) pour l'appel Compte 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.
   - AWS les 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 RAM est un service régional. Lorsque vous partagez une ressource avec des responsables d'autres entités Comptes 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, USA Est (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 de plus amples informations, veuillez consulter Implications de l'utilisation "Principal": "*" dans le cadre d'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 l'`Allow`accès aux ressources individuelles ARNs 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 OUs depuis cette organisation à vos partages de ressources. Vous ne pouvez pas ajouter OUs d'organisations extérieures à votre propre organisation à un partage de ressources en tant que responsables. 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 hébergeurs 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 : IPv4 adresses appartenant au client, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit, domaines de multidiffusion de passerelles de transit

Console

Pour créer un partage de ressources

1. Ouvrez 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. 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 de plus amples informations, veuillez consulter Zone de disponibilité IDs pour vos AWS 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 autant de fois que 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 de plus amples informations, veuillez consulter 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 Création d'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 de plus amples informations, veuillez consulter

Implications de l'utilisation "Principal": "*" dans le cadre d'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 l'`Allow`accès aux ressources individuelles ARNs 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 Comptes AWS principaux membres de cette unité d'organisation et son enfant OUs peuvent accéder au partage des ressources.
- Si vous sélectionnez une personne Compte 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 un Compte 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-user AWS CLI commande 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 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 de plus amples informations, veuillez consulter Partagez AWS les ressources qui vous appartiennent.

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 de plus amples informations, veuillez consulter Création d'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 dans AWS RAM

Vous pouvez mettre à jour un partage de ressources AWS RAM à tout moment de la manière suivante :

- 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 d'autres autorisations que l'autorisation AWS gérée par défaut, vous pouvez choisir l'autorisation gérée qui s'applique aux ressources de chaque type.
- Lorsqu'une autorisation gérée attachée 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 aux ressources partagées en supprimant les principaux ou les ressources d'un partage de ressources. Si vous révoquez l'accès, les principaux n'ont plus accès aux ressources partagées.

> **Note**
>
> Les principaux avec lesquels vous partagez des ressources peuvent quitter votre partage de ressources si celui-ci est vide ou contient uniquement des types de ressources compatibles avec le fait de quitter un partage de ressources. Si le partage de ressources contient des types de ressources qui ne sont pas compatibles avec le départ, un message s'affiche pour informer les principaux 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 obtenir la liste des types de ressources qui ne prennent pas en charge cette action, consultezConditions préalables pour quitter un partage de ressources.

Console

Pour mettre à jour un partage de ressources

1. Accédez à la page Shared by me : 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. Sélectionnez le partage de ressources, puis choisissez Modifier.
4. À l'étape 1 : Spécifiez les détails du partage des ressources, passez en revue les détails du partage des ressources et, si nécessaire, mettez à jour l'un des éléments suivants :

   a. (Facultatif) Pour modifier le nom du partage de 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 apparaissent uniquement si vous définissez la région sur USA Est (Virginie du Nord), (`us-east-1`) dans le AWS Management Console.

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

   d. (Facultatif) Pour ajouter une balise au partage de ressources, sous Balises, entrez une clé et une valeur de balise dans les zones de texte vides. Pour ajouter plusieurs paires clé-valeur de balise, choisissez Ajouter une nouvelle balise. Vous pouvez ajouter jusqu'à 50 balises.

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

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 par AWS au type de ressource, choisir une autorisation gérée par le client existante ou créer votre propre autorisation gérée par le client. Pour de plus amples 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 du partage. Pour de plus amples informations, veuillez consulter Création d'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 des autorisations gérées.

Pour afficher les actions autorisées par l'autorisation gérée, développez 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 passer à la version par défaut en choisissant Mettre à jour vers la version par défaut.

> **Note**
>
> Jusqu'à ce que vous ayez enregistré les modifications apportées au partage des ressources après la dernière étape, vous pouvez annuler la mise à jour de version en choisissant Revenir à la version précédente. Toutefois, pour les autorisations AWS 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 autorisés à accéder, 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 les responsables internes ou externes à votre organisation, choisissez l'une des options suivantes :

      - Pour partager des ressources avec des rôles Comptes AWS ou des utilisateurs IAM individuels extérieurs à votre organisation, choisissez Autoriser le partage avec des responsables externes.
      - Pour limiter le partage des ressources aux seuls directeurs de votre organisation dans AWS Organizations, choisissez Autoriser le partage avec les principaux responsables de votre organisation uniquement.

   b. Pour les directeurs, procédez comme suit :

      - (Facultatif) Pour ajouter une organisation, une unité organisationnelle (UO) ou un membre au Compte AWS sein de votre organisation, activez Afficher la structure organisationnelle pour afficher 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 de plus amples informations, veuillez consulter Implications de l'utilisation "Principal": "*" dans le cadre d'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 l'`Allow`accès aux ressources individuelles ARNs 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.

> **Note**
>
> Le bouton Afficher la structure organisationnelle apparaît uniquement si le partage avec AWS Organizations est activé et si vous êtes connecté en tant que principal 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 ajouter ces principes en saisissant leurs identifiants, qui sont affichés dans la zone de texte située sous le commutateur Afficher la structure organisationnelle. Voir le point suivant de la bullet.

- (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 personne Compte AWS, seul ce compte peut accéder au partage des ressources. Vous pouvez choisir l'une des options suivantes.

- Autre Compte 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 aux rôles et aux utilisateurs individuels. Ces autorisations ne peuvent pas dépasser celles définies dans les autorisations gérées associées au partage de ressources.
- Ceci Compte 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 Principaux sélectionnés.

  Vous pouvez ensuite ajouter des comptes supplémentaires ou votre organisation en répétant cette étape. OUs

- (Facultatif) Pour supprimer un principal, localisez-le sous 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 avez une autre opportunité de résoudre ce problème en choisissant Mettre à jour vers la version par défaut.
13. Choisissez Mettre à jour le partage des ressources lorsque vous avez terminé d'apporter des modifications.

AWS CLI

Pour mettre à jour un partage de ressources

Vous pouvez utiliser les AWS CLI commandes suivantes pour modifier un partage de 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 service Région 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 avec une erreur.

  L'exemple de commande suivant répertorie les ARNs autorisations gérées disponibles pour un sous-réseau Amazon Elastic Compute Cloud (Amazon EC2), puis utilise l'une d'entre elles ARNs pour remplacer l'autorisation AWS 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 EC2 sous-réseau Amazon 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 balise `project=lima` au partage de 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 `project` de dans le 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 balisage ne produisent aucun résultat en cas de réussite.

Afficher vos ressources partagées dans AWS RAM

Vous pouvez consulter la liste des ressources individuelles que vous avez partagées, dans tous les partages de ressources. La liste vous aide à 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 Shared by me : Shared resources 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. 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.
   - Type de ressource : 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.
   - Principaux : nombre de directeurs autorisés à accéder à la ressource. Choisissez la valeur pour afficher les principes.

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 le Région AWS (`us-east-1`) pour l'appel Compte 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"
        }
    ]
}
```

Afficher les principaux partenaires avec lesquels vous partagez des ressources dans AWS RAM

Vous pouvez consulter les principaux partenaires avec lesquels vous partagez vos ressources, dans tous les partages de ressources. La consultation de cette liste de principes vous permet de déterminer qui a accès à vos ressources partagées.

Console

Pour consulter les principes avec lesquels vous partagez des ressources

1. Accédez à la page Shared by me : Principaux 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. Appliquez un filtre pour trouver des principes spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche. Choisissez la zone de texte pour afficher une liste déroulante des champs d'attributs suggérés. Après en avoir choisi un, vous pouvez le choisir dans 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. Pour chaque principal de la liste, la console affiche les informations suivantes :

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

AWS CLI

Pour consulter les principes avec lesquels vous partagez des ressources

Vous pouvez utiliser la commande list-principals pour obtenir une liste des principaux auxquels vous faites référence dans les partages de ressources que vous avez créés dans le compte Région AWS d'appel actuel.

L'exemple suivant répertorie les principaux qui ont accès aux partages créés dans la région par défaut pour le compte d'appel. Dans cet exemple, les principaux sont l'organisation du compte appelant et une organisation distincte Compte AWS, dans le cadre de deux partages de ressources différents. Vous devez utiliser le point de terminaison du service Région 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 dans AWS 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 une AWS ressource**
>
> Si vous devez supprimer une AWS ressource que vous avez incluse dans un partage de ressources, il est AWS recommandé de vous assurer au préalable de 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 la AWS 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 Shared by me : 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. Sélectionnez le partage de ressources que vous souhaitez supprimer.

   > **Warning**
   >
   > Assurez-vous de 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, sélectionnez 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 cette delete-resource-sharecommande pour supprimer un partage de ressources dont vous n'avez plus besoin.

L'exemple suivant utilise d'abord la get-resource-sharescommande pour obtenir le nom de ressource Amazon (ARN) du partage de ressources que vous souhaitez supprimer. Ensuite, il delete-resource-shareupprime 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
- Afficher les partages de ressources partagés avec vous
- Afficher les ressources partagées avec vous
- Afficher les informations principales partagées avec vous
- Quitter un partage de ressources

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 hébergeurs 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 : IPv4 adresses appartenant au client, listes de préfixes, sous-réseaux, cibles miroir du trafic, passerelles de transit, domaines de multidiffusion de passerelles de transit

Console

Pour répondre à une invitation à partager une ressource

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 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"
    }
}
```

Afficher les partages de ressources partagés avec vous

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

Console

Pour afficher les partages 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 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. (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, tel qu'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 une liste déroulante des champs d'attributs suggérés. Après en avoir choisi un, vous pouvez le choisir dans 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. La AWS 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 personne Compte 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 n'est plus utilisable.
  - `Pending`— Une invitation à accepter le partage de ressources attend une réponse.

AWS CLI

Pour afficher 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 Région AWS d'appel spécifié par d'autres utilisateurs Comptes 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"
        }
    ]
}
```

Afficher les ressources partagées avec vous

Vous pouvez afficher les ressources partagées auxquelles vous avez accès. Vous pouvez voir quels principaux 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 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. 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.
   - Type de ressource : 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 partagées avec vous.

L'exemple de commande suivant affiche des détails sur la ressource accessible via un partage de ressources dans le champ spécifié Région AWS depuis un autre Compte 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 informations principales partagées avec vous

Vous pouvez consulter la liste de tous les principaux responsables qui partagent des ressources avec vous. Vous pouvez voir les ressources et les partages de ressources qu'ils partagent avec vous.

Console

Pour voir les principaux responsables qui partagent des ressources avec vous

1. Ouvrez la AWS RAM console à la https://console.aws.amazon.com/ram/maison.
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. Dans le volet de navigation, choisissez Shared with me (Partagé avec moi), Principals (Mandataires).
4. (Facultatif) Vous pouvez appliquer un filtre pour rechercher des principes spécifiques. Vous pouvez appliquer plusieurs filtres pour affiner votre recherche.
5. La console affiche les informations suivantes :

   - ID principal — L'identifiant du principal qui partage avec vous.
   - Partages de ressources : nombre de partages de ressources auxquels le directeur vous a ajouté. Choisissez le numéro pour afficher la liste des partages de ressources.
   - Ressources — Le nombre de ressources que le principal partage avec vous. Choisissez la valeur pour afficher la liste des ressources.

AWS CLI

Pour voir les principaux responsables qui partagent des ressources avec vous

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

L'exemple de commande suivant affiche des détails sur Compte AWS le partage d'un partage de ressources avec le compte utilisé pour appeler l'opération dans le champ spécifié Région 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`

Service	Type de ressource

	`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 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. 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 compte`123456789012`, en tant que principal à dissocier du partage de ressources spécifié, qui est partagé par compte`111111111111`.

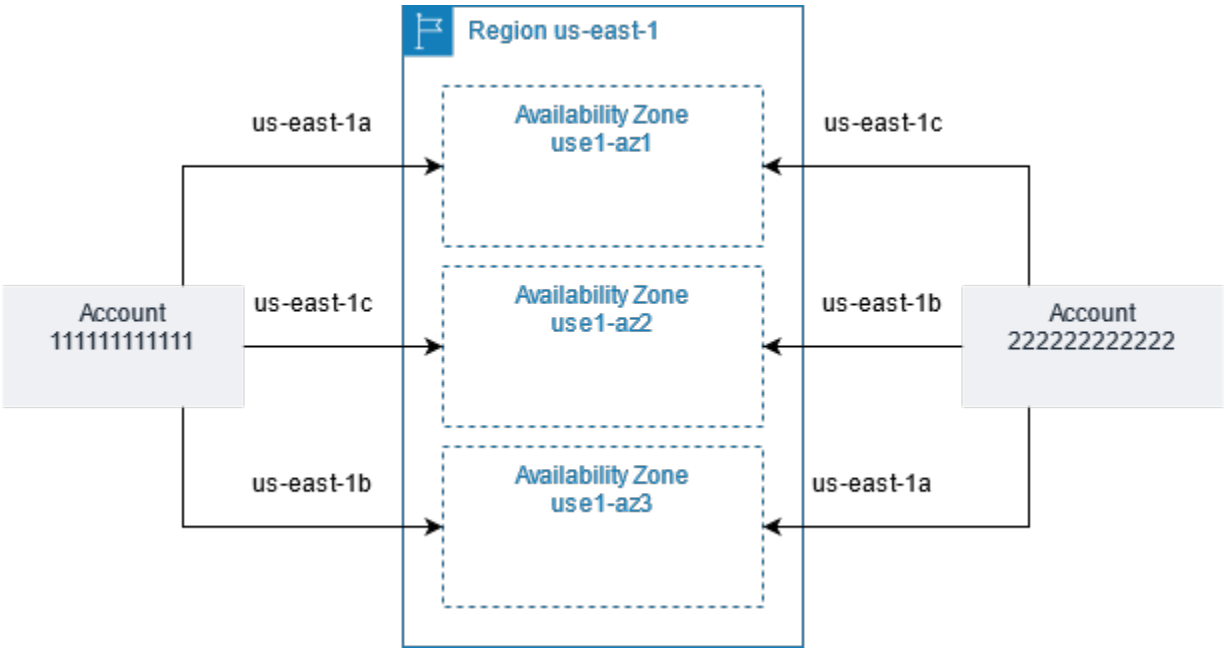
```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
```

```
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
            "external": false
        }
    ]
}
```

Zone de disponibilité IDs pour vos AWS ressources

AWS fait correspondre les zones de disponibilité physiques de manière aléatoire aux noms des zones de disponibilité de chacune d'entre elles Compte AWS. Cette approche permet de répartir les ressources entre les zones de disponibilité au sein d'une zone Région AWS, au lieu de les concentrer probablement dans la zone de disponibilité « a » pour chaque région. Par conséquent, la zone de disponibilité `us-east-1a` de votre AWS compte peut ne pas représenter le même emplacement physique que celle `us-east-1a` d'un autre AWS compte. Pour plus d'informations, consultez la section Régions et zones de disponibilité dans le guide de EC2 l'utilisateur Amazon.

L'illustration suivante montre comment les AZ IDs sont les mêmes 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 disponibilité Région AWS, mais également la zone de disponibilité. Par exemple, un sous-réseau Amazon VPC. Au sein d'un même compte, le mappage d'une zone de disponibilité à un nom spécifique n'est pas important. Mais,

lorsque vous partagez AWS RAM une telle ressource avec d'autres Comptes AWS, le mappage est important. Ce mappage aléatoire complique la capacité du compte accédant à la ressource partagée à savoir à quelle zone de disponibilité il doit faire référence. Pour vous aider, 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 AZ ID est un identifiant unique et cohérent pour une zone de disponibilité dans son ensemble Comptes AWS. Par exemple, `use1-az1` il s'agit d'un ID AZ pour une zone de disponibilité de la `us-east-1` région et il représente le même emplacement physique dans chaque AWS compte.

Vous pouvez utiliser AZ IDs pour déterminer l'emplacement des ressources d'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 AZ de chaque sous-réseau est affiché dans la console Amazon VPC et peut être demandé à l'aide du. AWS CLI

Console

Pour consulter l'AZ IDs des zones de disponibilité de votre compte

1. Accédez à la page de AWS RAM console dans la AWS RAM console.
2. Vous pouvez consulter l'AZ IDs du courant Région AWS sous Votre identifiant AZ.

AWS CLI

Pour consulter l'AZ IDs des zones de disponibilité de votre compte

L'exemple de commande suivant montre l'AZ IDs pour les zones de disponibilité de la région us-west-2 et la façon dont elles sont mappées pour l'appel. Compte 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 (OUs) 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 partager 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
Maillages `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 partager 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
AppSync GraphyQL APIs `appsync:Apis`	Gérez AWS AppSync GraphQL de APIs manière centralisée et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet de partager plusieurs comptes dans AWS AppSync APIs le cadre de la création d'une API AWS AppSync fusionnée unifiée qui peut accéder aux données de plusieurs sous-schémas APIs sur différents comptes d'une même région. Pour plus d'informations, voir Merged APIs	O	O Peut partager avec n'importe qui Compte AW	O	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 API Gateway

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 personnalisés privés API Gateway `apigateway:Domainnames`	Créez et gérez les noms de domaine de manière centralisée, et partagez-les avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet à plusieurs comptes d'invoquer vos noms de domaine qui sont mappés en	N	O Peut partager avec n'importe qui Compte AW	N	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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
	mode privé APIs. Pour plus d'informations, consultez la section Noms de domaine personnalisés pour le domaine privé APIs dans API Gateway dans le manuel Amazon API Gateway Developer Guide.				

Contrôleur Amazon Application Recovery (ARC)

Vous pouvez partager les ressources Amazon Application Recovery Controller (ARC) suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 ARC Route 53 `route53-recovery-control:Cluster`	Créez et gérez des clusters ARC 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 développeur Amazon Application Recovery Controller (ARC).	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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
Plans de changement de région ARC `arc-region-switch:Plan`	Créez et gérez des plans de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes d'utiliser les ressources d'un compte différent de celui qui héberge le plan. Pour plus d'informations, consultez la section Changement de région dans le guide du développeur Amazon Application Recovery Controller (ARC).	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Amazon Aurora

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 Aurora `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 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.	N	O Peut partager avec n'importe qui Compte AW	N	Non

AWS Backup

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
Coffres-forts de sauvegarde `backup:BackupVault`	Créez et gérez de manière centralisée des coffres-forts à espacement logique et partagez-les avec d'autres personnes ou Comptes AWS avec votre organisation. Cette option permet à plusieurs comptes d'accéder aux sauvegardes et de les restaurer à partir du ou des coffres-forts. Pour plus d'informations, consultez la section [Présentation des coffres-forts à espacement logique] dans le Guide du AWS Backup développeur.	 Oui	 Oui Peut partager avec n'importe qui Compte AW	 Oui	 Non

Amazon Bedrock

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
Modèle personnalisé Bedrock `bedrock:CustomModel`	Créez et gérez un modèle personnalisé de manière centralisée, et partagez-le avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs comptes d'utiliser le même modèle personnalisé pour les applications d'IA génératives. Pour plus d'informations, consultez la section Partager un modèle pour un autre compte dans le guide de l'utilisateur d'Amazon Bedrock.	 Oui	 Non Ne peut partager qu'avec Comptes AWS le personnel de sa propre organisation.	 Oui	 Non

Billing and Cost Management

Vous pouvez partager les ressources de Billing and Cost Management suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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
Tableaux de bord BCM `bcm-dashboards:dashboard`	Créez et gérez des tableaux de bord de Billing and Cost Management et partagez-les avec d'autres personnes Comptes AWS au sein ou en dehors de votre organisation. Lorsque vous partagez un tableau de bord, seules les configurations de tableau de bord sont partagées, et non les données sous-jacentes. Les destinataires ont accès à la mise en page du tableau de bord et aux configurations des widgets, et verront les données en fonction de leurs propres autorisations d'accès. Cette fonctionnalité de partage permet aux organisations d'établir des pratiques	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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
	communes de reporting des coûts et aide les différentes équipes à consulter les données de coûts de manière cohérente. Pour plus d'informations, consultez la section Partage des tableaux de bord dans le guide de l'utilisateur de Billing and Cost Management.				

AWS Billing Afficher le service

Vous pouvez partager les ressources AWS Billing View Service suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 de facturation `billing:billingview`	Créez et gérez des vues de facturation personnalisées de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet aux propriétaires d'applications et d'unités commerciales d'accéder aux AWS dépenses au niveau de l'unité commerciale à partir d'un compte membre. Pour plus d'informations, consultez la section Partage de vues de facturation personnalisées dans le guide de AWS Cost Management l'utilisateur.	N	N Ne peut partager qu'avec Comptes AWS le personnel de sa propre organisation.	O	Non

AWS Cloud Map

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
AWS Cloud Map Espaces de noms `servicediscovery:Namespace`	Créez et gérez des espaces de noms de manière centralisée, et partagez-les avec d'autres membres Comptes AWS de votre organisation. Cela permet à plusieurs services et instances de Comptes AWS découverte dans l'espace de noms partagé sans avoir besoin d'informations d'identification temporaires. Pour plus d'informations, consultez la section AWS Cloud Map Espaces de noms partagés dans le Guide du AWS Cloud Map développeur.	 O	 N Ne peut partager qu'avec Comptes AV le personnel de sa propre organisation.	 O	 Non

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 partager 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
Réseaux principaux `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

Amazon CloudFront

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
Amazon CloudFront VpcOrigin `cloudfront:VpcOrigin`	Créez et gérez les origines des CloudFront VPC de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs d' Comptes AWS utiliser les origines d'un VPC partagé pour les CloudFront distributions. Pour plus d'informations, consultez la section Travailler avec des ressources partagées CloudFront dans le manuel Amazon CloudFront Developer Guide.	N	O Peut partager avec n'importe qui Compte AW	N	Non

AWS CloudHSM

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
AWS CloudHSM Sauvegardes `cloudhsm:Backup`	Gérez les AWS CloudHSM sauvegardes de manière centralisée et partagez-les avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet à plusieurs utilisateurs Comptes AWS de consulter les informations relatives à la sauvegarde et de les utiliser pour restaurer un AWS CloudHSM cluster. Pour plus d'informations, consultez la section Gestion AWS CloudHSM des sauvegardes dans le Guide de AWS CloudHSM l'utilisateur.	 Oui	 Oui	 Oui	 Non

AWS CodeBuild

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
CodeBuild Projets `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 AW	Oui	Non
CodeBuild Groupes de rapports	Créez un groupe de rapports et utilisez-le pour créer des	Oui	Oui	Oui	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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
`codebuild:ReportGroup`	rapports lorsque vous créez un projet. Partagez le groupe 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.		Peut partager avec n'importe qui Compte AW		

AWS CodeConnections

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

Type et code de ressource	Cas d'utilisation	Peut partager 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
Connexions de code `codeconnections:Connection`	Gérez la réutilisation des connexions de code dans plusieurs comptes. En d'autres termes, le partage de connexions par code réduit la charge de travail de l'administrateur et réduit le besoin d'accès administrateur pour chaque compte nécessitant une connexion par code. Pour plus d'informations, consultez la section Partager des connexions avec Comptes AWS dans le guide de l'utilisateur de la console Developer Tools.	Non	Oui Peut partager avec n'importe qui Compte AW	Oui	Non

Amazon DataZone

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 Domaines `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

Amazon EC2

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 EC2 instances Amazon 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 EC2 l'utilisateur Amazon. **Important** Si vous ne remplissez	N	O Peut partager avec n'importe qui Compte AW	N	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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
	pas toutes 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 EC2 instance Amazon 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				

Type et code de ressource	Cas d'utilisation	Peut partager 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
	vous pouvez accéder à la réservation de capacité partagée en essayant de l'afficher dans la EC2 console Amazon. 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 de plus amples informati				

Type et code de ressource	Cas d'utilisation	Peut partager 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
	ons, veuillez consulter Exemple : alerte en cas de défaillance du partage des ressources.				

Type et code de ressource	Cas d'utilisation	Peut partager 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
Hôtes dédiés `ec2:DedicatedHost`	Allouez et gérez les hôtes EC2 dédiés Amazon de manière centralisée, et partagez la capacité d'instance de l'hôte avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet à plusieurs de Comptes AWS lancer leurs EC2 instances Amazon 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 EC2 l'utilisateur Amazon.	 N	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 EC2 instances Amazon depuis n'importe quel compte avec lequel vous partagez un placement dans un groupe de placement partagé. Pour plus d'informations, consultez la section Partager un groupe de placement dans le guide de EC2 l'utilisateur Amazon.	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 utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 d'Image Builder `imagebuilder:Component`	Créez et gérez les composants de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Gérez qui peut 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.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non
Recettes d'Image Builder Container `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. Cela vous permet de	 O	 O Peut partager avec n'importe	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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
	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 partager 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 du générateur d'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 partager 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
Image Builder : 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 AWS	 Oui	 Non

Elastic Load Balancing

Vous pouvez partager les ressources Elastic Load Balancing suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
Boutiques ELB Trust `elasticloadbalancing:TrustStore`	Créez et gérez les magasins de confiance Elastic Load Balancing de manière centralisée, et partagez-les avec d'autres Comptes AWS personnes ou avec votre organisation. Les administrateurs de sécurité peuvent gérer un seul ou un nombre réduit de magasins de confiance et activer les configurations TLS mutuelles entre les équilibreurs de charge d'application. Pour plus d'informations, consultez la section Partager votre magasin de confiance Elastic Load Balancing pour les équilibreurs de charge d'application dans le guide de l'utilisateur pour les équilibre	 O	 O	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	urs de charge d'application.				

AWS End User Messaging SMS

Vous pouvez partager la AWS End User Messaging SMS ressource suivante en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
AWS SMS Listes de désactivation vocale `sms-voice:OptOutList`	Créez une liste de désinscription et partagez-la avec les autres Comptes AWS membres de votre organisation. Vous pouvez partager la liste de désinscription afin que les autres applications puissent désactiver les numéros de	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	téléphone des utilisateurs parmi différents Comptes AWS ou qu'elles puissent vérifier l'état du numéro de téléphone de l'utilisateur. Pour plus d'informations, consultez la section Utilisation de ressources partagées dans le guide de AWS End User Messaging SMS l'utilisateur.				

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
AWS SMS Numéros de téléphone vocaux `sms-voice:PhoneNumber`	Créez et gérez des numéros de téléphone pour les partager avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs d' Comptes AWS envoyer des messages en utilisant le numéro de téléphone partagé. Pour plus d'informations, consultez la section Utilisation de ressources partagées dans le guide de AWS End User Messaging SMS l'utilisateur.	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Oui

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
AWS SMS Pool vocal `sms-voice:Pool`	Créez et gérez des pools pour les partager avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet à plusieurs d' Comptes AWS envoyer des messages en utilisant le pool partagé. Pour plus d'informations, consultez la section Utilisation de ressources partagées dans le guide de AWS End User Messaging SMS l'utilisateur.	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Oui

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
AWS SMS Expéditeur vocal IDs `sms-voice:SenderId`	Créez et gérez des expéditeurs IDs et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet d' Comptes AWS envoyer plusieurs messages en utilisant l'identifiant d'expéditeur partagé. Pour plus d'informations, consultez la section Utilisation de ressources partagées dans le guide de AWS End User Messaging SMS l'utilisateur.	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Oui

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 partager 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 partager avec les responsables du service
FSx Volumes `fsx:Volume`	Créez et gérez FSx des volumes OpenZFS de manière centralisée, et partagez-les avec d'autres personnes Comptes AWS ou 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 FSx APIs `CreateVolume` ou`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 partager 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 partager avec les responsables du service
AWS Glue Catalogue `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 partager 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 partager avec les responsables du service
AWS Glue 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 partager 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 partager avec les responsables du service
	guide du AWS Lake Formation développeur.				

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
AWS Glue 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 partager 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 partager 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 partager 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 partager 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 partager 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 partager 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 partager 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 partager avec les responsables du service
Entités du catalogue Marketplace `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 partager 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 partager 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

Approbation multipartite

Vous pouvez partager les ressources d'approbation multipartites suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
Équipe d'approbation multipartite `mpa:ApprovalTeam`	Créez et gérez des équipes d'approbation et partagez-les avec d'autres personnes Comptes AWS ou avec votre organisation. Cela permet Comptes AWS à d'autres utilisateurs de faire appel à une équipe d'approbation associée à une opération protégée. Une opération protégée est une liste prédéfinie d'opérations qui nécessitent l'approbation de l'équipe avant de pouvoir être exécutées. Pour plus d'informations, consultez la section Termes et concepts du Guide de l'utilisateur de	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	l'approbation multipartite.				

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 partager 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 partager avec les responsables du service
Pare-feu réseau `network-firewall:Firewall`	Créez et gérez des pare-feux de manière centralisée, et partagez-les avec d'autres utilisateurs Comptes AWS afin qu'ils puissent créer des points de terminaison de pare-feu. Cela permet à plusieurs comptes	O	O Peut partager avec n'importe qui Compte AW	N	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	d'utiliser les protections d'un seul pare-feu. Pour plus d'informations, consultez la section Partage de AWS Network Firewall ressources dans le guide du AWS Network Firewall développeur.				

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
Politiques de Network Firewall `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 entreprise 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 AWS Network Firewall ressources 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 partager 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 partager avec les responsables du service

Groupes de règles de Network Firewall
 	
`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 AWS Network Firewall ressources dans le guide du AWS Network Firewall développeur.	O	O
			
			Peut partager avec n'importe qui Compte AW
				N	Non

Oracle Database@AWS

Vous pouvez partager les Oracle Database@AWS ressources suivantes en utilisant AWS RAM.

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
Oracle Database@AWS Infrastructure Exadata `odb:CloudExadataInfrastructure`	Vous pouvez ainsi partager votre infrastructure Exadata et votre réseau ODB entre plusieurs Comptes AWS au sein d'une même AWS organisation. Oracle Database@AWS Cela vous permet de provisionner l'infrastructure une seule fois et de la réutiliser sur des comptes fiables, ce qui vous permet de réduire les coûts tout en séparant les responsabilités. Pour plus d'informations, voir Partage de ressources Oracle Database@AWS dans le guide de Oracle Database@AWS l'utilisateur.	N	N Ne peut partager qu'avec Comptes AW le personnel de sa propre organisation.	N	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
Oracle Database@AWS Réseau ODB `odb:OdbNetwork`	Avec Oracle Database@AWS, vous pouvez partager votre infrastructure Exadata et votre réseau ODB entre plusieurs Comptes AWS au sein d'une même AWS organisation. Cela vous permet de provisionner l'infrastructure une seule fois et de la réutiliser sur des comptes fiables, ce qui vous permet de réduire les coûts tout en séparant les responsabilités. Pour plus d'informations, voir Partage de ressources Oracle Database@AWS dans le guide de Oracle Database@AWS l'utilisateur.	N	N Ne peut partager qu'avec Comptes AWS le personnel de sa propre organisation.	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 partager 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 partager 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 partager 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 partager avec les responsables du service
Tables 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 partager 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 partager avec les responsables du service
Sites d'Outposts `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 sur Outposts

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager 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

AWS Autorité de certification privée

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
Autorité de certification privée (CAs) `acm-pca:CertificateAuthority`	Créez et gérez des autorités de certification privées (CAs) pour l'infrastructure à clé publique (PKI) interne de votre organisation, et partagez-les CAs avec d'autres personnes 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 Autorité de certification privée l'utilisateur.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Oui

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 partager 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 partager avec les responsables du service
Vues de l'explorateur de ressources `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

Groupes de ressources AWS

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager 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 EC2 dédiés Amazon créé 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 partager 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 partager avec les responsables du service
Groupes de règles Route 53 Resolver Firewall `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	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	développeur Amazon Route 53.				
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 VPCs. 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 partager 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 partager 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 (VPCs) 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 partager 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 partager avec les responsables du service
Configurations de journalisation des requêtes du résolveur `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'enregistrer les requêtes DNS qui en proviennent dans un journal VPCs de 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.	 Oui	 Oui Peut partager avec n'importe qui Compte AW	 Oui	 Non

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 partager 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 partager avec les responsables du service
Autorisations d'accès S3 `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 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.	 Oui	 Oui Peut partager avec n'importe qui Compte AW	 Oui	 Oui

Amazon SageMaker AI

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

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Catalogues de ressources sur l'IA `sagemaker:SagemakerCatalog`	Pour la découvrabilité : permet aux propriétaires de comptes d'accorder des autorisations de découvrabilité à d'autres comptes, pour toutes les ressources de groupes de fonctionnalités du catalogue SageMaker AI. 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	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	le manuel Amazon SageMaker AI Developer Guide. **Note** La découvrabilité et l'accès sont des autorisations distinctes dans l' SageMaker IA.				

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Groupes de fonctionnalités de l'IA `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 AI Developer Guide. **Note** La découvrabilité et l'accès	Oui	Oui Peut partager avec n'importe qui Compte AW	Oui	Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	sont des autorisations distinctes dans l' SageMaker IA.				

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Hubs d'IA `sagemaker:Hub`	Avec Amazon SageMaker AI JumpStart, vous pouvez les créer et les gérer de `sagemaker:Hub` manière centralisée, et les partager avec d'autres Comptes AWS membres de la même organisation. Pour plus d'informations, consultez la section Contrôlez l'accès aux modèles de base à l'aide de hubs privés sélectionnés dans Amazon SageMaker AI JumpStart dans le manuel Amazon SageMaker AI Developer Guide.	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Groupes AI Lineage `sagemaker:LineageGroup`	Amazon SageMaker AI vous 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	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	Amazon SageMaker AI Developer Guide.				

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Cartes modèles AI `sagemaker:ModelCard`	Amazon SageMaker AI 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.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	Pour plus d'informations, consultez la section Amazon SageMaker AI Model Cards dans le manuel Amazon SageMaker AI Developer Guide.				
SageMaker Groupes de packages AI Model `sagemaker:model-package-group`	Avec Amazon SageMaker AI Model Registry, vous pouvez les créer et les gérer de `sagemaker:model-package-group` manière centralisée, et les partager avec d'autres personnes Comptes AWS pour enregistrer des versions de modèles. Pour plus d'informations, consultez Amazon SageMaker AI Model Registry dans le manuel Amazon SageMaker AI Developer Guide.	 Oui	 Oui	 Oui	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Applications pour partenaires AI `sagemaker:PartnerApp`	Avec SageMaker AI Partner AI Apps, vous pouvez créer et gérer des applications SageMaker AI Partner AI de manière centralisée, et partager l'accès à celles-ci avec d'autres personnes Comptes AWS. Pour plus d'informations, consultez la section Configuration du partage entre comptes pour les applications d' SageMaker IA partenaires d'Amazon AI dans le manuel Amazon SageMaker AI Developer Guide.	 O	 O Peut partager avec n'importe qui Compte AW	 N	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
SageMaker Pipelines d'IA `sagemaker:Pipeline`	Avec Amazon SageMaker AI 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 les informations relatives à un pipeline et à ses exécutions avec un accès facultatif pour démarrer, arrêter et réessayer	 O	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Type et code de ressource	Cas d'utilisation	Peut partager 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 partager avec les responsables du service
	des pipelines à partir d'autres comptes. Pour plus d'informations, consultez la section Support entre comptes pour les pipelines d' SageMaker IA dans le manuel Amazon SageMaker AI 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 partager avec les responsables du service
AppRegistry Demandes `servicecatalog:Applications`	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 partager avec les responsables du service
AppRegistry Groupes d'attributs `servicecatalog:AttributeGroups`	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 partager avec les responsables du service
Incident Manager 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. **Note** Actuellement, la possibilité d'ajouter un contact partagé depuis un autre compte à un plan de réponse aux incidents n'est pas prise en charge.	 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 partager avec les responsables du service
	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.				

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 partager avec les responsables du service
Plans de réponse du gestionnaire d'incidents `ssm-incidents:ResponsePlan`	Créez et gérez des plans d'intervention de manière centralisée, et partagez-les avec 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	 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 partager avec les responsables du service
	AWS Systems Manager Incident Manager.				

AWS Systems Manager

Vous pouvez partager les AWS Systems 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 partager avec les responsables du service
Politiques de refus automatique SSM JITNA `ssm:Document`	Créez une politique d'approbation pour l'accès aux just-in-time nœuds avec Systems Manager. Une politique de refus d'accès empêche explicitement l'approbation automatique des demandes d'accès aux nœuds que vous spécifiez.	 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 partager avec les responsables du service
	Partagez la politique de refus d'accès avec d'autres personnes Comptes AWS ou avec votre organisation. Cela garantit que votre politique de refus d'accès pour l'accès aux just-in-time nœuds s'applique à tous les comptes de votre organisation. Pour plus d'informations, consultez la section Accès aux Just-in-time nœuds à l'aide de Systems Manager dans le Guide de AWS Systems Manager l'utilisateur.				

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 partager avec les responsables du service
Paramètres avancés du magasin de paramètres `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 plus d'informations, consultez la section Utilisation de paramètres partagés	 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 partager avec les responsables du service
	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 partager avec les responsables du service
Appartenant au client IPv4pool `ec2:CoipPool`	Au cours du processus AWS Outposts d'installation, AWS crée un pool d'adresses, appelé pool d'adresses IP appartenant au client, sur la base des informations que vous	N	N Ne peut partager qu'avec Comptes AWS le	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 partager avec les responsables du service
	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 des EC2 instances, 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 appartenant au client dans le Guide		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 partager avec les responsables du service
	de l'utilisateur AWS Outposts .				
Piscines 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 CIDRs d'allouer des AWS ressources du pool, par exemple VPCs 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.	 Oui	 Oui Peut partager avec n'importe qui Compte AW	 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 partager avec les responsables du service
Découvertes de ressources de l'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 partager 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 partager avec les responsables du service
Subnets `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 d'entre eux de Comptes AWS lancer leurs ressources applicatives dans une gestion centralisée VPCs. Ces ressources incluent les EC2 instances Amazon, 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	 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 partager avec les responsables du service
	l'utilisateur Amazon VPC. **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				

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 partager avec les responsables du service
	les sous-réseaux que vous avez créés vous-même.				
Groupes de sécurité `ec2:SecurityGroup`	Créez et gérez les groupes de sécurité de manière centralisée, et partagez-les avec d'autres Comptes AWS personnes ou avec votre organisation. Cela permet Comptes AWS à plusieurs d'associer le groupe de sécurité à leurs interfaces réseau Elastic. Pour plus d'informations, consultez Partager un groupe de sécurité dans le guide de l'utilisateur Amazon VPC.	 O	 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 partager avec les responsables du service
Objectifs 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 partager 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 réseaux VPCs et les réseaux locaux 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	 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 partager avec les responsables du service
	lorsque vous 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 partager 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 partager avec les responsables du service
Accès vérifié par AWS groupes `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 partager avec les responsables du service
Configuration des ressources Amazon VPC Lattice `vpc-lattice:ResourceConfiguration`	Créez une configuration de ressources dans Amazon VPC Lattice pour partager les ressources VPC entre les comptes et. VPCs Dans la configuration de la ressource, vous identifiez qui peut accéder à cette ressource et spécifiez la passerelle de ressources par laquelle vous souhaitez partager la ressource. Les consommateurs peuvent accéder à la ressource VPC via un point de terminaison VPC de ressource dans lequel ils créent. AWS PrivateLinkPour plus d'informations, consultez les sections Accès aux ressources VPC AWS PrivateLink dans le guide de l'AWS	 N	 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 partager avec les responsables du service
	PrivateLink utilisateur et Configuration des ressources pour les ressources VPC dans le guide de l'utilisateur VPC Lattice.				

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 partager avec les responsables du service
Services 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

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 partager avec les responsables du service
Réseau de services Amazon VPC Lattice `vpc-lattice:ServiceNetwork`	Créez et gérez les réseaux de services Amazon VPC Lattice de manière centralisée, 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.	 N	 O Peut partager avec n'importe qui Compte AW	 O	 Non

Gestion des autorisations dans AWS RAM

Dans AWS RAM, il existe deux types d'autorisations gérées : les autorisations AWS 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 tout le nécessaire pour une politique basée sur les ressources, à l'exception du principal et de la ressource. Le nom Amazon Resource Name (ARN) de la ressource et l'ARN des principaux associés au partage de ressources complètent les éléments d'une politique basée sur les ressources. AWS RAM rédige ensuite la politique basée sur les ressources qu'il attache 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. AWS Met parfois à jour une autorisation AWS 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 déjà associées à un partage de ressources ne sont pas automatiquement mises à jour. La AWS 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 de l'autorisation AWS gérée dès que possible. Ces mises à jour ajoutent généralement la prise en charge des nouvelles ressources ou des mises à jour Services AWS qui peuvent partager des types de ressources supplémentaires à l'aide de AWS RAM. Une nouvelle version par défaut peut également traiter et corriger les failles de sécurité.

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

Vous pouvez récupérer la liste des autorisations gérées disponibles à tout moment. Pour de plus amples informations, veuillez consulter Afficher les autorisations gérées.

Rubriques

- Afficher les autorisations gérées
- Création et utilisation d'autorisations gérées par le client dans AWS RAM
- Mise à jour des autorisations AWS gérées vers une version plus récente
- Considérations relatives à l'utilisation des autorisations gérées par le client dans AWS RAM
- Comment fonctionnent les autorisations gérées
- Types d'autorisations gérées

Afficher les autorisations gérées

Vous pouvez consulter les détails relatifs aux autorisations gérées qui peuvent être attribuées aux types de ressources dans vos partages de ressources. Vous pouvez identifier les autorisations gérées attribuées aux partages de ressources. Pour consulter ces informations, utilisez la bibliothèque d'autorisations gérées de la AWS RAM console.

Console

Pour consulter les informations relatives aux autorisations gérées disponibles dans AWS RAM

1. Accédez à la page Bibliothèque d'autorisations gérées 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. Bien que toutes les régions partagent les mêmes autorisations AWS 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 l'autorisation gérée dont vous souhaitez consulter les détails. Vous pouvez utiliser le champ de recherche pour filtrer la liste des

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

4. (Facultatif) Pour modifier les préférences d'affichage, choisissez l'icône en forme de roue dentée en haut à droite du panneau des autorisations gérées. Vous pouvez modifier les préférences suivantes :

   - Taille de page : nombre de ressources affichées sur chaque page.
   - Enrouler les lignes : s'il faut enrouler les lignes dans les lignes du tableau.
   - Colonnes : s'il faut afficher ou masquer les informations relatives au type de ressource et aux partages associés.

   Après avoir défini 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 autorisation AWS 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 choisir le numéro 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 d'autorisation gérée : version de l'autorisation gérée attachée à ce partage de ressources.
     - Propriétaire : Compte AWS numéro du propriétaire du partage de ressources.
     - Autoriser les principaux externes : indique si ce partage de ressources permet le partage avec des directeurs extérieurs à l'organisation au sein de. AWS Organizations
     - État : statut actuel de l'association entre le partage de ressources et l'autorisation gérée.
   - État — Décrit 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 d'une autorisation gérée affiche les informations suivantes :

- Type de ressource : type de AWS 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 est donc attribuée automatiquement à tous les nouveaux partages de ressources qui utilisent cette autorisation gérée. Tous les partages de ressources existants qui utilisent des versions différentes sont invités à mettre à jour le partage de ressources vers la version par défaut.
- ARN — Le nom de ressource Amazon (ARN) de l'autorisation gérée. ARNs Pour les autorisations AWS gérées, utilisez 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 désignée par défaut.
- Versions d'autorisations gérées : vous pouvez choisir les informations de version à afficher dans les onglets situés sous cette liste déroulante.
  - Onglet Détails :
    - Heure de création : date et heure auxquelles cette version de l'autorisation gérée a été créée.
    - Heure de la dernière mise à jour : date et heure auxquelles cette version de l'autorisation gérée a été mise à jour pour la dernière fois.
  - Onglet Modèle de politique : liste des actions de service et des conditions, le cas échéant, que cette version de l'autorisation gérée permet aux principaux d'effectuer sur le type de ressource associé.
  - Partage de ressources associé : liste des partages de ressources qui utilisent cette version de l'autorisation gérée.

AWS CLI

Pour consulter les informations relatives aux autorisations gérées disponibles dans AWS RAM

Vous pouvez utiliser la list-permissionscommande pour obtenir une liste des autorisations gérées disponibles à utiliser sur les partages de ressources en cours Région 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 inclure uniquement les éléments du `permissions` tableau de résultats qui correspondent au nom spécifié. Nous précisons également que nous voulons voir uniquement le champ ARN dans les résultats, et ce 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 son texte de 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 dans AWS RAM

AWS Resource Access Manager (AWS RAM) fournit au moins une autorisation AWS gérée pour chaque type de ressource que vous pouvez partager. Cependant, ces autorisations gérées peuvent ne pas fournir l'accès avec le moindre privilège pour votre cas d'utilisation du partage. Lorsque l'une des autorisations AWS 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 dans quelles conditions avec des ressources partagées AWS 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 requises pour effectuer 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

- Création d'une autorisation gérée par le client
- Création d'une nouvelle version d'une autorisation gérée par le client
- Choisissez une version différente comme version par défaut pour une autorisation gérée par le client
- Supprimer une version d'autorisation gérée par le client
- Supprimer une autorisation gérée par le client

Création d'une autorisation gérée par le client

Les autorisations gérées par le client sont spécifiques à un Région 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, puis 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 s'applique cette autorisation gérée.
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 relatives au niveau d'accès en fonction de 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, pour les balises, entrez une clé et une valeur de balise. Ajoutez des balises supplémentaires en choisissant Ajouter une nouvelle étiquette. Répétez cette étape autant de fois que nécessaire.
6. Lorsque vous avez terminé, choisissez Créer une autorisation gérée par le client.

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
    }
}
```

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

Si le cas d'utilisation de l'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, uniquement les nouveaux partages de ressources à venir qui utilisent cette autorisation gérée par le client.

Chaque autorisation gérée peut comporter 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 d'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 des détails des autorisations gérées, dans la section Versions d'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 l'autorisation gérée pour utiliser un modèle de politique existant.
5. Lorsque vous avez terminé, choisissez Créer une version au bas de la page.

AWS CLI

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

1. Trouvez le nom de ressource Amazon (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 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 version différente 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 d'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 Détails des autorisations gérées par le client, sous la section Versions d'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 permet de récupérer 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 aucune sortie en cas de réussite. 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 de chaque autorisation gérée par le client. Lorsqu'une version n'est plus nécessaire et qu'elle 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 le statut de suppression avant d'être complètement supprimées.

Console

Pour supprimer une version d'autorisation gérée par le client

1. Accédez à la bibliothèque d'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, sélectionnez Supprimer pour confirmer que vous souhaitez supprimer cette version de votre autorisation gérée par le client.

   Choisissez Annuler si vous ne souhaitez pas supprimer cette version de l'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, indiquez-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 aucune sortie en cas de réussite. 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 d'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.

   Si des partages de ressources sont toujours 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 des détails des autorisations gérées par le client, choisissez Supprimer les autorisations gérées.
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 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 à jour des autorisations AWS gérées vers une version plus récente

AWS Met parfois à jour les autorisations AWS gérées disponibles pour être associées à un partage de ressources pour un type de ressource spécifique. Lorsque cela est AWS fait, il crée une nouvelle version de l'autorisation AWS gérée. 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 nécessaire 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 celle par défaut pour l'autorisation, la console affiche une bannière en haut de la page de la 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 lancer 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 pour utiliser leur version 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, une fois que vous les avez mises à jour 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 effectué l'une de ces options, vous devez mettre à jour vos partages de ressources pour utiliser la version par défaut qui est désormais utilisée.

AWS CLI

Pour mettre à jour la version d'une autorisation AWS 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'autorisation AWS gérée par défaut pour les réservations EC2 de capacité Amazon.

   ```
   $ 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'autorisation AWS 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 chacune des commandes `ResourceShareArn` que vous avez reçues dans les résultats de la commande de l'étape 1.

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

Les autorisations gérées par le client ne sont disponibles Région AWS que dans le pays dans lequel vous les créez. Tous les types de ressources ne prennent pas en charge les autorisations gérées par le client. Pour obtenir la liste des types de ressources pris en charge dans AWS Resource Access Manager, voirRessources partageables AWS.

Les autorisations gérées par le client avec plusieurs relevés ne sont pas prises en charge. Vous ne pouvez utiliser que des opérateurs uniques non négatifs dans les autorisations gérées par le client.

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

- Clés de condition utilisées pour faire correspondre les propriétés du principal :
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Clés de condition utilisées pour restreindre l'accès aux principaux services :
  - `aws:SourceArn`
  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- Balises du système :
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

> **Note**
>
> La `aws:SourceAccount` valeur est automatiquement renseignée lors du partage avec les responsables du service.

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 de l'accès avec le moindre privilège à vos AWS ressources.

Cette vidéo montre comment créer et associer des autorisations gérées par les clients conformément à la meilleure pratique du moindre privilège. Pour plus d'informations, voir,???.

Lorsque vous créez un partage de ressources, vous associez une autorisation AWS 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 attachée à chaque ressource partagée.

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

Effet

Indique s'il faut `Allow` ou `Deny` non obtenir l'autorisation principale d'effectuer une opération sur une ressource partagée. Pour une autorisation gérée, l'effet est toujours le même`Allow`. Pour plus d'informations, voir Effect dans le guide de l'utilisateur IAM.

Action

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

Condition

Quand et comment un directeur peut interagir avec une ressource dans un partage de ressources. Les conditions ajoutent un niveau de sécurité supplémentaire à vos ressources partagées. Utilisez-les pour limiter l'accès des actions sensibles à vos ressources partagées. 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 soient effectuées par des utilisateurs authentifiés par l'authentification multifactorielle. Pour plus d'informations sur les conditions, voir les clés contextuelles des conditions AWS globales dans le guide de l'utilisateur IAM. Pour plus d'informations sur les conditions spécifiques aux services, consultez la section Actions, ressources et clés de condition pour les AWS services dans la référence d'autorisation de service.

> **Note**
>
> Des conditions sont disponibles pour les autorisations gérées par le client et les types de ressources pris en charge pour les autorisations AWS gérées.
> Pour plus d'informations sur les conditions exclues de l'utilisation avec les autorisations gérées par le client, consultezConsidérations relatives à l'utilisation des autorisations gérées par le client dans AWS 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. AWS les autorisations gérées sont définies par le service AWS propriétaire de la ressource et gérées par. AWS RAM Vous créez et gérez vos propres autorisations gérées par les clients.

- AWS autorisation gérée : une autorisation gérée par défaut est disponible pour chaque type de ressource pris en AWS 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 principaux 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 principaux d'effectuer les actions suivantes :
  - `ec2:RunInstances`

- `ec2:CreateNetworkInterface`
- `ec2:DescribeSubnets`

Les noms des autorisations AWS gérées par défaut utilisent le format suivant :`AWSRAMDefaultPermission`*`ShareableResourceType`*. Par exemple, pour le type de `ec2:Subnet` ressource, le nom de l'autorisation AWS 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 d'autorisations gérées par défaut ou de l'une des autorisations gérées supplémentaires prises en charge par certains types de ressources, sont des autorisations complètes distinctes avec 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 client AWS ou 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 une autorisation d'accès complet (`ReadetWrite`) gérée et 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 les autres développeurs à l'aide de l'autorisation gérée en lecture seule afin de suivre la pratique consistant à accorder le moindre privilège.

> **Note**
>
> Tous les AWS services compatibles AWS RAM prennent en charge au moins une autorisation gérée par défaut. Vous pouvez consulter les autorisations disponibles pour chacune d'entre elles Service AWS sur la page Bibliothèque d'autorisations gérées. Cette page fournit des détails sur chaque autorisation gérée disponible, y compris les partages de ressources actuellement associés à l'autorisation et indique si le partage avec des principaux externes est autorisé, le cas échéant. Pour de plus amples informations, veuillez consulter Afficher les autorisations gérées.

Pour les services qui ne prennent pas en charge les autorisations gérées supplémentaires, lorsque vous créez un partage de ressources, l'autorisation par défaut définie pour le type de ressource que vous choisissez s'applique AWS RAM automatiquement. 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 les 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 dans quelles conditions avec des ressources partagées AWS 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 requises pour effectuer des tâches sur des ressources partagées.

Sécurité dans AWS RAM

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

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

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Resource Access Manager (AWS RAM), consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris 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 son utilisation AWS RAM. Les rubriques suivantes expliquent comment procéder à la configuration AWS RAM pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS RAM ressources.

Rubriques

- Protection des données dans AWS RAM
- Gestion des identités et des accès pour AWS RAM
- Connexion et surveillance AWS RAM
- Résilience dans AWS RAM
- Sécurité de l'infrastructure dans AWS RAM
- Accès AWS Resource Access Manager via un point de terminaison d'interface (AWS PrivateLink)

Protection des données dans AWS RAM

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

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou 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.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec AWS RAM ou d'autres Services AWS

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

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 les personnes qui peuvent être authentifiées (connectées) et autorisées (autorisées) à utiliser AWS les ressources. En utilisant IAM, vous créez des principes, tels que des rôles, des utilisateurs et des groupes dans votre. Compte AWS Vous contrôlez les autorisations dont disposent ces principaux 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

- Comment AWS RAM fonctionne avec IAM
- AWS politiques gérées pour AWS RAM
- Utilisation des rôles liés à un service pour AWS RAM
- Exemples de politiques IAM pour AWS RAM
- Exemples de politiques de contrôle des services pour AWS Organizations et AWS RAM
- Désactiver le partage de ressources avec AWS Organizations

Comment AWS RAM fonctionne avec IAM

Par défaut, les responsables IAM ne sont pas autorisés à créer ou à modifier AWS RAM des ressources. Pour permettre aux responsables IAM de créer ou de modifier des ressources et d'effectuer des tâches, vous devez effectuer l'une des étapes suivantes. Ces actions autorisent l'utilisation de ressources et d'actions d'API 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. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le 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 dans le 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 RAM fournit plusieurs politiques AWS gérées que vous pouvez utiliser pour répondre aux besoins de nombreux utilisateurs. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour AWS RAM.

Si vous avez besoin d'un contrôle plus précis sur 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 dans le Guide de l'AWS Identity and Access Management utilisateur.

Les sections suivantes fournissent les détails AWS RAM spécifiques à la création d'une politique d'autorisation IAM.

Table des matières

- Structure d'une politique
  - Effet
  - Action
  - Ressource
  - Condition

Structure d'une politique

Une politique d'autorisation IAM est un document JSON qui inclut les instructions suivantes : effet, action, ressource et condition. Une politique 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 une autorisation principale pour effectuer une action. Les valeurs possibles sont les suivantes : `Allow` et`Deny`.

Action

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

Ressource

L'instruction Resource indique les AWS RAM ressources concernées par la politique. Pour spécifier une ressource dans l'instruction, vous devez utiliser son Amazon Resource Name (ARN) unique. Pour obtenir la liste complète des ressources autorisées, consultez la section Ressources définies par AWS Resource Access Manager dans le guide de l'utilisateur IAM.

Condition

Les déclarations de condition sont facultatives. Ils peuvent être utilisés pour affiner davantage les conditions dans lesquelles la politique s'applique. AWS RAM prend en charge les clés de condition suivantes :

- `aws:RequestTag/${TagKey}`— Teste si la demande de service inclut une balise dont la clé de balise spécifiée existe et possède la valeur spécifiée.
- `aws:ResourceTag/${TagKey}`— Teste si la ressource traitée par la demande de service possède 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 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 étiqueter un partage de ressources.
- `ram:AllowsExternalPrincipals`— Teste si le partage des ressources dans la demande de service permet le partage avec des principaux externes. Un directeur externe est un Compte AWS externe à votre organisation dans AWS Organizations. Si c'est le cas`False`, vous ne pouvez partager ce partage de ressources qu'avec les comptes de la même organisation.
- `ram:PermissionArn`— Teste 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 en utilisant le format indiqué dans la liste des types de ressources partageables.
- `ram:Principal`— Teste si l'ARN du principal spécifié dans la demande de service correspond à une chaîne d'ARN que vous spécifiez dans la politique.
- `ram:RequestedAllowsExternalPrincipals`— Teste si la demande de service inclut le `allowExternalPrincipals` paramètre et si son argument correspond à la valeur que vous spécifiez dans la politique.
- `ram:RequestedResourceType`— Teste si le type de ressource sur laquelle on agit correspond à une chaîne de type de ressource que vous spécifiez dans la politique. Spécifiez les types de ressources en utilisant le format indiqué dans la liste des types de ressources partageables.
- `ram:ResourceArn`— Teste si l'ARN de la ressource sur laquelle intervient la demande de service correspond à un ARN que vous spécifiez dans la politique.

- `ram:ResourceShareName`— Teste si le nom du partage de ressources concerné par 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 concerné par la demande de service correspond à une chaîne que vous spécifiez dans la politique.

AWS politiques gérées pour AWS RAM

AWS Resource Access Manager fournit actuellement plusieurs politiques AWS RAM gérées, qui sont décrites dans cette rubrique.

AWS politiques gérées

- AWS politique gérée : AWSResource AccessManagerReadOnlyAccess
- AWS politique gérée : AWSResource AccessManagerFullAccess
- AWS politique gérée : AWSResource AccessManagerResourceShareParticipantAccess
- AWS politique gérée : AWSResource AccessManagerServiceRolePolicy
- AWS RAM mises à jour des politiques AWS gérées

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 au AWS RAM rôle lié au service.

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. 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 politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service

AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

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

AWS politique gérée : AWSResource AccessManagerReadOnlyAccess

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

Cette politique fournit des autorisations en lecture seule aux partages de ressources qui vous appartiennent. Compte AWS

Pour ce faire, il autorise l'exécution de n'importe laquelle `Get*` des `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 principaux de consulter les détails sur les parts de ressources détenues par le compte.

JSON

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

AWS politique gérée : AWSResource AccessManagerFullAccess

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

Cette politique fournit un accès administratif complet pour consulter ou modifier les partages de ressources qui vous appartiennent Compte AWS.

Pour ce faire, il autorise l'exécution de toutes `ram` les opérations.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ram`— Permet aux principaux d'afficher ou de modifier toute information concernant les partages de ressources détenus par le Compte AWS.

JSON

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

AWS politique gérée : AWSResource AccessManagerResourceShareParticipantAccess

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

Cette politique permet aux principaux d'accepter ou de rejeter les partages de ressources partagés avec celui-ci Compte AWS, et de consulter les détails de ces partages de ressources. Il ne permet pas de modifier ces partages de ressources.

Pour ce faire, il autorise l'exécution de certaines `ram` opérations.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

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

JSON

```
{
    "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 : AWSResource AccessManagerServiceRolePolicy

La politique AWS gérée ne `AWSResourceAccessManagerServiceRolePolicy` peut être utilisée qu'avec le rôle lié au service pour. AWS RAM Vous ne pouvez pas joindre, détacher, modifier ou supprimer cette politique.

Cette politique fournit un accès AWS RAM en lecture seule à la structure de votre organisation. Lorsque vous activez l'intégration entre AWS RAM et AWS Organizations, crée AWS RAM automatiquement un rôle lié au service nommé AWSServiceRoleForResourceAccessManagerque

le service assume lorsqu'il a besoin de rechercher des informations sur votre organisation et ses comptes, par exemple lorsque vous consultez la structure de l'organisation dans la AWS RAM console.

Pour ce faire, il accorde l'autorisation en lecture seule d'exécuter les `organizations:List` opérations `organizations:Describe` et 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 les informations relatives à la structure de l'organisation, y compris les unités organisationnelles et celles Comptes AWS qu'elles contiennent.

JSON

```
{
    "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/*"
            ]
        }
    ]
}
```

AWS RAM mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS RAM depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS RAM document.

Modification	Description	Date
AWS Resource Access Manager a commencé à suivre les modifications	AWS RAM a 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 AWS Identity and Access Management rôles liés à un service (IAM). 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 RAM définit 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 fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS RAM

AWS RAM utilise 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 AWSResource AccessManagerServiceRolePolicy est attachée à ce rôle lié au service et permet d' AWS RAM effectuer 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 responsable 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 Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le Guide 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 CLI aide 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 RAM ne vous permet pas de modifier le rôle AWSResource AccessManagerServiceRolePolicy 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.

Supprimer un rôle lié à un service pour AWS RAM

Vous pouvez utiliser la console IAM, AWS CLI ou l' AWS API 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, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSResourceAccessManagerServiceRolePolicy` service. 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 AWS RAM liés à un service

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

Exemples de politiques IAM pour AWS RAM

Cette rubrique inclut des exemples de politiques IAM AWS RAM illustrant 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 tiers Comptes AWS

Exemple 1 : Autoriser le partage de ressources spécifiques

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

Par exemple, la politique suivante limite les principaux à partager uniquement la règle de résolution avec le Amazon Resource Name (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, voir... IfExists opérateurs de condition dans le guide de l'utilisateur IAM.

JSON

```
{
    "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 principaux à n'associer que des types de ressources spécifiques aux partages de ressources.

Les actions `AssociateResourceShare` et`CreateResourceShare`, peuvent accepter des principes et en `resourceArns` tant que paramètres d'entrée indépendants. Par conséquent, AWS RAM autorise chaque principal et chaque ressource indépendamment, de sorte qu'il peut y avoir plusieurs contextes de demande. Cela signifie que lorsqu'un principal est associé à un partage de AWS RAM ressources, la clé de `ram:RequestedResourceType` condition n'est pas présente dans le contexte de la demande. De même, lorsqu'une ressource est associée à un partage de AWS RAM ressources, la clé de `ram:Principal` condition n'est pas présente dans le contexte de la demande. Par conséquent, pour autoriser `AssociateResourceShare` et `CreateResourceShare`

associer des principaux au partage de AWS RAM ressources, vous pouvez utiliser l'opérateur de `Null` condition.

Par exemple, la politique suivante limite les principaux à partager uniquement les règles du résolveur Amazon Route 53 et leur permet d'associer n'importe quel principal à ce partage.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "AllowOnlySpecificResourceType",
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    },
    {
    "Sid": "AllowAssociatingPrincipals",
     "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "Null": {
                "ram:Principal": "false"
             }
        }
    }
  ]
}
```

Exemple 3 : Restreindre le partage avec des tiers Comptes AWS

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

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

JSON

```
{
    "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 (SCPs). SCPs sont des politiques que vous associez 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. SCPs offrez un contrôle centralisé sur le maximum d'autorisations 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

Pour l'utiliser SCPs, vous devez d'abord effectuer les opérations suivantes :

- Activez toutes les fonctions de votre organisation. Pour plus d'informations, voir Activation de toutes les fonctionnalités de votre organisation dans le Guide de AWS Organizations l'utilisateur
- Activez SCPs pour une utilisation au sein de votre organisation. Pour plus d'informations, voir Activation et désactivation des types de politiques dans le guide de l'AWS Organizations utilisateur

- Créez SCPs ce dont vous avez besoin. Pour plus d'informations sur la création SCPs, voir Création et mise à jour SCPs dans le Guide de AWS Organizations l'utilisateur.

Exemples de politiques de contrôle des services

Table des matières

- Exemple 1 : empêcher le partage externe
- Exemple 2 : Empêcher les utilisateurs d'accepter des invitations à partager des ressources provenant de comptes externes à votre organisation
- Exemple 3 : Autoriser des comptes spécifiques à partager des types de ressources spécifiques
- Exemple 4 : empêcher le partage avec l'ensemble de l'organisation ou avec des unités organisationnelles
- Exemple 5 : autoriser le partage uniquement avec des principaux spécifiques

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.

AWS RAM autorise APIs séparément pour chaque principal et chaque ressource répertoriés dans l'appel.

JSON

```
{
    "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.

JSON

```
{
    "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 EC2 préfixes Amazon ou d'associer des listes de préfixes à des partages de ressources existants.

AWS RAM autorise APIs séparément pour chaque principal et chaque ressource répertoriés dans l'appel.

L'opérateur `StringEqualsIfExists` autorise une demande si celle-ci n'inclut pas de paramètre de type de ressource ou si elle inclut ce paramètre, si sa valeur correspond exactement au type de ressource spécifié. Si vous incluez un directeur, vous devez en avoir un `...IfExists`.

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

JSON

```
{
    "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.

AWS RAM autorise APIs séparément pour chaque principal et chaque ressource répertoriés dans l'appel.

JSON

```
{
    "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`.

Si vous utilisez un `"Effect": "Deny"` élément avec un opérateur de condition annulé, par exemple`StringNotEqualsIfExists`, la demande est toujours refusée même si la clé de condition n'est pas présente. Utilisez un opérateur de condition `Null` pour vérifier si une clé de condition est absente au moment de l'autorisation.

AWS RAM autorise APIs séparément pour chaque principal et chaque ressource répertoriés dans l'appel.

JSON

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

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 (OUs), vous pouvez désactiver le partage. Lorsque vous désactivez le partage avec toutes les organisations AWS Organizations, OUs celles-ci 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-access AWS CLI commande.

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

> **Important**
>
> Lorsque vous désactivez l'accès sécurisé à AWS 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 IAM AWS 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.

Connexion et surveillance AWS RAM

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS RAM et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller vos AWS RAM ressources et répondre aux incidents potentiels :

Amazon EventBridge

Fournit un near-real-time flux d'événements système décrivant les modifications apportées aux AWS ressources. EventBridge permet une informatique automatisée axée sur les événements, car vous pouvez écrire des règles qui surveillent certains événements et déclenchent des actions automatisées dans d'autres AWS services lorsque ces événements se produisent. Pour de plus amples informations, veuillez consulter Surveillance à AWS RAM l'aide EventBridge.

AWS CloudTrail

Capture les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter Journalisation des appels d' AWS RAM API avec AWS CloudTrail.

Surveillance à AWS RAM l'aide EventBridge

À l'aide d'Amazon EventBridge, vous pouvez configurer des notifications automatiques pour des événements spécifiques dans AWS RAM. Les événements de AWS RAM sont transmis à EventBridge en temps quasi réel. Vous pouvez configurer EventBridge pour surveiller les événements et appeler des cibles en réponse à des événements indiquant des modifications de 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 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 émis dans le meilleur des cas. Si une erreur se produit lors de la AWS RAM tentative d'émission d'un événement, le service essaie plusieurs fois de plus. Cependant, cela peut expirer et entraîner la perte de cet événement spécifique.

Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Exemple : alerte en cas de défaillance du partage des ressources

Envisagez le scénario dans lequel vous souhaitez partager les réservations EC2 de capacité Amazon avec d'autres comptes de votre organisation. Cela constitue un bon moyen de réduire vos coûts.

Toutefois, si vous ne remplissez pas toutes les conditions requises pour partager une réservation de capacité, celle-ci peut échouer silencieusement lors de l'exécution des tâches asynchrones liées au partage des ressources. 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 à la place. Cela peut entraîner des coûts plus élevés que prévu.

Pour surveiller les échecs de partage de ressources, configurez une EventBridge règle Amazon qui vous alerte en cas d'échec d'un partage de AWS RAM ressources. La procédure du didacticiel suivante utilise une rubrique Amazon Simple Notification Service (SNS) pour avertir tous les abonnés à la rubrique chaque fois qu'un échec de partage de ressources est EventBridge découvert. 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, sélectionnez Règles, puis dans la liste Règles, choisissez Créer une règle.
3. Entrez un nom et une description facultative pour votre règle, puis choisissez Next.
4. Faites défiler la page jusqu'à la zone Modèle d'événement, puis sélectionnez Modèles personnalisés (éditeur JSON).
5. Copiez et 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 la cible 1, sous Type de cible, sélectionnez Service AWS.
8. Sous Sélectionnez une cible, choisissez le sujet SNS.
9. Dans le champ Rubrique, choisissez la rubrique SNS dans laquelle vous souhaitez publier la notification. Ce sujet doit déjà exister.
10. Choisissez Next, puis choisissez à nouveau Next pour vérifier votre configuration.
11. Lorsque vous êtes satisfait de vos options, choisissez 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 sélectionnez Activer.

Tant que cette règle est activée, tout partage de AWS RAM ressources défaillant génère une alerte SNS destinée aux destinataires du sujet sur lequel 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 dans la EC2 console Amazon à partir de ces comptes.

Journalisation des appels d' AWS RAM API avec AWS CloudTrail

AWS RAM est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS RAM. CloudTrail capture tous les appels d'API AWS RAM sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS RAM console et des appels de code vers les opérations de l' AWS RAM API. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3 que vous spécifiez, y compris les événements pour lesquels AWS RAM. Si vous ne configurez pas de suivi, vous pouvez toujours consulter 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 faite AWS RAM, l'adresse IP de la demande, le demandeur, la date à laquelle elle a été faite et des informations supplémentaires.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS RAM informations dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS RAM, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS RAM, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal de suivi consigne les événements de toutes

les régions dans la partition AWS , et il livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Création d'un parcours pour votre Compte AWS
- Service AWS intégrations avec des journaux CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les AWS RAM actions sont enregistrées CloudTrail et documentées dans la référence de l'AWS RAM 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 AWS informations d'identification root
- Informations d'identification de sécurité temporaires provenant d'un rôle AWS Identity and Access Management (IAM) ou d'un utilisateur fédéré.
- Informations d'identification de sécurité à long terme d'un utilisateur IAM.
- Un autre AWS service.

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

Comprendre les entrées du fichier AWS RAM journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal 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 AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées,

connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

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

Sécurité de l'infrastructure dans AWS RAM

En tant que service géré, AWS Resource Access Manager il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder 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 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.

Accès AWS Resource Access Manager via un point de terminaison d'interface (AWS PrivateLink)

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

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-

réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à AWS RAM.

Pour plus d'informations, consultez Accès aux Services AWS via AWS PrivateLink dans le Guide AWS PrivateLink .

Considérations relatives à AWS RAM

Avant de configurer un point de terminaison d'interface pour AWS RAM, consultez les considérations du AWS PrivateLink guide.

AWS RAM prend en charge les appels à toutes ses actions d'API via le point de terminaison de l'interface.

Les politiques de point de terminaison VPC sont prises en charge pour. AWS RAM Par défaut, l'accès complet à AWS RAM est autorisé via le point de terminaison de l'interface.

Créez un point de terminaison d'interface pour AWS RAM

Vous pouvez créer un point de terminaison d'interface pour AWS RAM utiliser la console Amazon VPC ou le AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour AWS RAM utiliser le nom de service suivant :

```
com.amazonaws.region.ram
```

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

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

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

Une politique de point de terminaison spécifie les informations suivantes :

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

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

Exemple : politique de point de terminaison VPC pour les actions AWS RAM

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

JSON

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

Résolution des problèmes liés à AWS RAM

Utilisez les informations contenues dans 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 »
- Erreur : « AccessDeniedException »
- Erreur : « UnknownResourceException »
- Erreurs lors de la tentative de partage avec des comptes extérieurs à mon organisation
- Impossible de voir les ressources partagées dans le compte de destination
- Erreur : limite dépassée
- L'autre compte de mon organisation ne reçoit jamais d'invitation
- Vous ne pouvez pas partager un sous-réseau VPC

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 (OUs) 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 et AWS 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.

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

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.

Vous devriez désormais être en mesure de AWS RAM partager vos ressources avec des comptes et OUs au sein 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. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le 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 dans le 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. En outre, les autorisations ne doivent pas être bloquées par celles de votre organisation SCPs.

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.

JSON

```
{
    "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- n'*xxxx*a pas pu être trouvé »
- « CannotUpdateResourceShare: UnknownResourceException : OrganizationalUnit ou- n'*xxxx*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'API Organizations Enable AWSService Access 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 (OUs) de votre organisation.

Solution

Pour résoudre le problème, désactivez l'intégration entre AWS RAM et AWS Organizations. Réactivez-le ensuite en appelant l'opération AWS RAM EnableSharingWithAwsOrganizationAPI ou en utilisant le AWS Management Console pour effectuer les étapes suivantes.

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

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.

Vous devriez désormais être en mesure de AWS RAM partager vos ressources avec des comptes et OUs au sein 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 (VPCs) 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 et AWS 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.

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

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.

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 utilisateurs Comptes 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 de AWS 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 AWS Organizations case Activer le partage avec est 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 cette case. Procédez comme suit pour corriger la situation.

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

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.

Vous devrez peut-être mettre à jour le partage et spécifier les comptes ou les unités organisationnelles de l'organisation avec lesquels le partage doit être effectué.

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 RAM console. 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).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:us-east-1:<Account-A-ID>:<resource-
id>"
        }
    ]
}
```

La ressource est dans un paramètre différent Région AWS de celui de la console actuelle

AWS RAM est un service régional. Les ressources existent dans une région spécifique Région 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, à l' Compte AWS endroit où l'erreur s'affiche, accédez à l'une des pages suivantes, en fonction du type de quota que vous atteignez :
   - La AWS RAM page 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 organisation AWS Organizations, celui-ci ne reçoit aucune invitation.

Cause

Ce comportement est normal si le partage au sein de l' AWS organisation 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' AWS organisation, 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 dans AWS 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 RAM ne 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 liées à AWS Resource Access Manager (AWS RAM). Vous pouvez demander une augmentation de certaines de ces limites. Pour demander une augmentation de limite, contactez Support.

Note

Les définitions suivantes s'appliquent à la description des quotas ci-dessous :

- Ressource : élément Service AWS créé individuellement que vous souhaitez partager, tel qu'un compartiment Amazon S3 ou une EC2 instance Amazon. Chaque ressource référencée dans un partage de ressources compte comme une ressource dans ce quota. Si vous partagez la même ressource dans trois partages de ressources différents, cela augmente de trois votre nombre 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, est comptabilisé dans 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 l'utilisation de votre quota. Si vous partagez avec l'ensemble d'une organisation en faisant référence à son identifiant, celui-ci est pris en compte comme un seul dans ce quota.
- Autorisation gérée par le client : autorisations gérées que vous créez pour répondre à des cas d'utilisation spécifiques en utilisant le moindre privilège d'accès pour gérer la manière 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 maximal 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 entre tous les 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 compte 10 dans la limite.	25 000

Ressource	Limite par défaut
Nombre maximum d'associations principales pour tous les partages de ressources d'un Région AWS **Note** Chaque principal inclus dans une part de ressources est pris en compte dans cette limite. Si un principal est inclus dans 10 parts de ressources différentes, cela 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 qui partagent des comptes avec des comptes qui n'en font pas partie AWS 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 appartenant au même compte AWS Organizations et vous avez activé le partage des ressources au sein du AWS Organizations.	250

Utilisation AWS RAM avec un AWS SDK

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

Documentation SDK	Exemples de code
AWS SDK pour C++	AWS SDK pour C++ exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code

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
Ajout de la prise en charge du partage CloudFront des ressources Amazon	Vous pouvez désormais partager Amazon CloudFront VPC Origins avec d'autres membres de votre Comptes AWS organisation.	6 octobre 2025
Support supplémentaire pour partager les ressources de Billing and Cost Management	Vous pouvez désormais partager les tableaux de bord de Billing and Cost Management avec d'autres Comptes AWS personnes ou avec AWS RAM votre organisation.	19 août 2025
Ajout d'un support pour le partage de AWS Cloud Map ressources	Vous pouvez désormais partager des AWS Cloud Map espaces de noms avec d'autres membres Comptes AWS de votre organisation.	14 août 2025
Ajout de la prise en charge du partage des ressources Amazon Application Recovery Controller (ARC)	Vous pouvez désormais partager les plans Amazon Application Recovery Controller (ARC) avec d'autres Comptes AWS personnes ou	31 juillet 2025

	avec votre organisation AWS RAM.	
Ajout d'un support pour le partage de Oracle Database@ AWS ressources	Vous pouvez désormais partager l'infrastructure Oracle Database@AWS Exadata et les réseaux ODB avec d'autres membres de votre Comptes AWS organisation.	30 juin 2025
Ajout de la prise en charge du partage de ressources d'approbation multipartites	Vous pouvez désormais partager des équipes d'approbation multipartites avec d'autres personnes Comptes AWS ou au sein de votre organisation.	17 juin 2025
Ajout de la prise en charge du partage des ressources Amazon SageMaker AI	Vous pouvez désormais les utiliser AWS RAM pour partager les applicati ons Amazon SageMaker AI Partner avec d'autres Comptes AWS personnes et avec votre organisation.	6 juin 2025
Ajout d'un support pour le partage de AWS Network Firewall ressources	Vous pouvez désormais les utiliser AWS RAM pour partager des AWS Network Firewall pare-feux avec d'autres personnes Comptes AWS et avec votre organisation.	28 mai 2025

Ajout d'un support pour le partage de AWS Systems Manager ressources	Vous pouvez partager une politique de AWS Systems Manager refus d'accès avec d'autres personnes Comptes AWS ou avec vos organisations. AWS RAM	30 avril 2025
Ajout d'un support pour le partage de AWS CodeConnections ressources	Vous pouvez désormais partager des connexions de AWS CodeConnections code avec d'autres Comptes AWS personnes ou au sein de votre organisation.	5 mars 2025
Ajout d'un support pour le partage de AWS Billing ressources	Vous pouvez désormais partager des AWS Billing points de vue avec d'autres Comptes AWS membres de votre organisation.	20 décembre 2024
Ajout de la prise en charge du partage des configurations de ressources Amazon VPC Lattice	Vous pouvez désormais partager les configurations de ressources Amazon VPC Lattice avec d'autres utilisateurs. Comptes AWS	1er décembre 2024
Ajout de la prise en charge du partage des ressources Amazon API Gateway	Vous pouvez désormais partager des noms de domaine API Gateway avec d'autres personnes Comptes AWS ou au sein de votre organisation.	21 novembre 2024

Ajout de la prise en charge du partage des ressources Amazon VPC	Vous pouvez désormais partager des groupes de sécurité Amazon VPC avec d'autres personnes Comptes AWS ou au sein de votre organisation.	30 octobre 2024
Ajout d'un support pour le partage de AWS End User Messaging SMS ressources	Vous pouvez partager AWS End User Messaging SMS des ressources avec d'autres Comptes AWS personnes ou avec vos organisations AWS RAM.	24 septembre 2024
AWS PrivateLink	Avec AWS PrivateLink for AWS RAM, vous pouvez vous connecter directement à la RAM en utilisant un point de terminaison d'interface dans votre cloud privé virtuel (VPC).	9 septembre 2024
Ajout d'un support pour le partage AWS Backup	Vous pouvez partager des coffres-forts espacés de manière logique au sein de votre organisation Comptes AWS ou au sein de celle-ci.	7 août 2024
Ajout de la prise en charge du partage des ressources Elastic Load Balancing	Vous pouvez partager les magasins de confiance Elastic Load Balancing au sein de votre organisation Comptes AWS ou au sein de celle-ci.	5 août 2024

Ajout de la prise en charge du partage de modèles personnalisés Amazon Bedrock	Vous pouvez désormais les utiliser AWS RAM pour partager les modèles personnalisés d'Amazon Bedrock avec d'autres utilisateurs Comptes AWS et avec votre organisation.	1er août 2024
Ajout de la prise en charge du partage AWS CloudHSM des sauvegardes	Vous pouvez partager AWS CloudHSM des sauvegardes avec d'autres Comptes AWS personnes ou avec vos organisations AWS RAM.	28 juin 2024
Ajout de la prise en charge du partage Model Registry des ressources Amazon SageMaker AI.	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.	27 juin 2024
Ajout de la prise en charge du partage d'Amazon SageMaker AI JumpStart	Vous pouvez désormais partager Amazon SageMaker AI JumpStart Hubs avec Comptes AWS ou au sein de votre organisation.	27 juin 2024
Ajout d'un support 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 AWS Systems Manager du 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
Support supplémentaire pour partager les Amazon Simple Storage Service ressources	Vous pouvez désormais partager Amazon Simple Storage Service l'instance Access Grants avec d'autres Comptes AWS personnes ou avec votre organisation AWS RAM.	27 novembre 2023
Ajout d'un support pour partager des points de Explorateur de ressources AWS vue	Vous pouvez désormais partager des Explorateur de ressources AWS points de vue avec d'autres Comptes AWS membres de votre organisat ion.	14 novembre 2023
Ajout de la prise en charge du partage des ressources Amazon Application Recovery Controller (ARC)	Vous pouvez désormais partager des clusters Amazon Application Recovery Controlle r (ARC) avec d'autres Comptes AWS personnes ou avec votre organisation AWS RAM.	18 octobre 2023

Support supplémentaire 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 de la prise en charge du partage du principal de service	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 d'un support pour partager les ressources de la SageMaker 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 fonctionn alités Amazon SageMaker AI Feature Store et du catalogue SageMaker AI en tant que ressources partageables	Vous pouvez désormais partager les groupes de fonctionnalités d'Amazon SageMaker AI Feature Store et les ressources du catalogue SageMaker AI avec d'autres Comptes AWS personnes ou avec votre organisation.	20 juillet 2023
Augmentation de la limite de quota de service pour les invitations en attente	Le nombre maximum d'invitat ions en attente par compte de partage est passé de 20 à 250.	8 juin 2023

Ajout du support pour AWS AppSync GraphQL en APIs tant que ressources partageables	Vous pouvez désormais partager AWS AppSync GraphQL APIs 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 EC2 de placement Amazon en tant que ressources partageables	Vous pouvez désormais partager des groupes de EC2 placement Amazon avec d'autres Comptes AWS personnes pour y lancer leurs instances.	8 novembre 2022
Ajout de liens vers deux vidéos d'introduction sur AWS RAM	Ajout de vidéos de présentat ion 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 pipelines Amazon SageMaker AI	Vous pouvez désormais partager des pipelines d' SageMaker IA avec d'autres 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 ressources Amazon SageMaker AI	Vous pouvez l'utiliser AWS RAM pour partager des groupes de lignées SageMaker IA. 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 AWS RAMAWS politiques d'autorisation IAM gérées	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 autorisations 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

Ajout d'un support 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
Ajout d'un support 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 d'un support pour le partage de AWS Autorité de certification privée ressources	Vous pouvez désormais utiliser AWS RAM pour partager des autorités de certification Autorité de certification privée AWS privées (CAs) avec d'autres Comptes AWS.	17 août 2020

Ajout du support pour le partage des catalogues de données, des bases de données et des tables AWS Glue	Vous pouvez désormais les utiliser AWS RAM pour partager des catalogue s 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 appartenant aux clients IPv4	Vous pouvez désormais les utiliser AWS RAM pour partager les IPv4 adresses 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 AWS RAM partager des hôtes EC2 dédiés Amazon, Groupes de ressources AWS 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 de la prise en charge du 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 de la prise en charge du 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
Ajout de la prise en charge du 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 de la prise en charge du 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.