aws

User Guide

AWS Resource Access Manager

AWS Resource Access Manager: User Guide

Table of Contents

Was ist AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) hilft Ihnen dabei, Ihre Ressourcen sicher zwischen AWS-Konten, innerhalb Ihrer Organisation oder Organisationseinheiten (OUs) und mit AWS Identity and Access Management (IAM-) Rollen und Benutzern für unterstützte Ressourcentypen gemeinsam zu nutzen. Wenn Sie mehrere Ressourcen haben AWS-Konten, können Sie eine Ressource einmal erstellen und sie dann verwenden, AWS RAM um diese Ressource für diese anderen Konten nutzbar zu machen. Wenn Ihr Konto von verwaltet wird AWS Organizations, können Sie Ressourcen mit allen anderen Konten in der Organisation oder nur mit den Konten teilen, die zu einer oder mehreren bestimmten Organisationseinheiten gehören (OUs). Sie können die Daten auch mit bestimmten AWS-Konten Konten teilen, unabhängig davon, ob das Konto Teil einer Organisation ist. Bei einigen unterstützten Ressourcentypen können Sie sie auch mit bestimmten IAM-Rollen und -Benutzern teilen.

Inhalt

Videoübersichten

Das folgende Video bietet eine kurze Einführung in die Erstellung einer Ressourcenfreigabe AWS RAM und beschreibt, wie diese erstellt wird. Weitere Informationen finden Sie unter ???.

Das folgende Video zeigt, wie Sie AWS verwaltete Berechtigungen auf Ihre AWS Ressourcen anwenden. Weitere Informationen finden Sie unter ???.

In diesem Video wird gezeigt, wie vom Kunden verwaltete Berechtigungen nach der bewährten Methode der geringsten Rechte erstellt und verknüpft werden. Weitere Informationen finden Sie unter ???.

Vorteile von AWS RAM

Warum verwenden AWS RAM? Es bietet die folgenden Vorteile:

- Reduziert Ihren Betriebsaufwand — Erstellen Sie eine Ressource einmal und verwenden Sie sie dann, AWS RAM um diese Ressource mit anderen Konten zu teilen. Dadurch müssen Sie keine doppelten Ressourcen in jedem Konto bereitstellen, wodurch sich der Betriebsaufwand verringert. Innerhalb des Kontos, dem die Ressource gehört, AWS RAM wird die Gewährung des Zugriffs für alle Rollen und Benutzer in diesem Konto vereinfacht, ohne dass identitätsbasierte Berechtigungsrichtlinien verwendet werden müssen.
- Sorgt für Sicherheit und Konsistenz — Vereinfachen Sie das Sicherheitsmanagement für Ihre gemeinsam genutzten Ressourcen, indem Sie einen einzigen Satz von Richtlinien und Berechtigungen verwenden. Wenn Sie stattdessen doppelte Ressourcen in all Ihren separaten Konten erstellen würden, hätten Sie die Aufgabe, identische Richtlinien und Berechtigungen zu implementieren und diese dann für all diese Konten identisch zu halten. Stattdessen werden alle Benutzer einer AWS RAM Ressourcenfreigabe durch einen einzigen Satz von Richtlinien und Berechtigungen verwaltet. AWS RAM bietet ein einheitliches Benutzererlebnis für die gemeinsame Nutzung verschiedener Arten von AWS Ressourcen.
- Bietet Transparenz und Überprüfbarkeit — Sehen Sie sich die Nutzungsdetails für Ihre gemeinsam genutzten Ressourcen durch die Integration AWS RAM mit Amazon an CloudWatch und AWS CloudTrail. AWS RAM bietet umfassenden Einblick in gemeinsam genutzte Ressourcen und Konten.

Was ist mit kontenübergreifendem Zugriff mit ressourcenbasierten Richtlinien?

Sie können einige Ressourcentypen gemeinsam mit anderen AWS nutzen, AWS-Konten indem Sie eine ressourcenbasierte Richtlinie anhängen, die AWS Identity and Access Management (IAM-) Prinzipale (IAM-Rollen und Benutzer) außerhalb Ihrer eigenen identifiziert. AWS-Konto Wenn Sie eine Ressource gemeinsam nutzen, indem Sie eine Richtlinie anhängen, werden die zusätzlichen Vorteile, die sich daraus ergeben, jedoch nicht genutzt. AWS RAM Durch die Verwendung erhalten AWS RAM Sie die folgenden Funktionen:

- Sie können Daten mit einer Organisation oder einer Organisationseinheit (OU) teilen, ohne jedes einzelne aufzählen zu müssen. AWS-Konto IDs

- Benutzer können die mit ihnen geteilten Ressourcen direkt in der ursprünglichen AWS-Service Konsole und in den API-Vorgängen sehen, als ob sich diese Ressourcen direkt im Konto des Benutzers befinden würden. Wenn Sie AWS RAM beispielsweise ein Amazon VPC-Subnetz mit einem anderen Konto teilen, können Benutzer dieses Kontos das Subnetz in der Amazon VPC-Konsole und in den Ergebnissen der Amazon VPC-API-Operationen sehen, die in diesem Konto ausgeführt wurden. Ressourcen, die durch das Anhängen einer ressourcenbasierten Richtlinie gemeinsam genutzt werden, sind auf diese Weise nicht sichtbar. Stattdessen müssen Sie die Ressource anhand ihres Amazon-Ressourcennamens (ARN) ermitteln und explizit darauf verweisen.
- Die Besitzer einer Ressource können sehen, welche Principals Zugriff auf jede einzelne Ressource haben, die sie gemeinsam genutzt haben.
- Wenn Sie Ressourcen mit einem Konto teilen, das nicht Teil Ihrer Organisation ist, wird ein AWS RAM Einladungsprozess eingeleitet. Der Empfänger muss die Einladung annehmen, bevor dieser Hauptbenutzer auf die gemeinsam genutzten Ressourcen zugreifen kann. Nachdem Sie die Möglichkeit zur gemeinsamen Nutzung innerhalb Ihrer Organisation aktiviert haben, sind für die gemeinsame Nutzung mit Konten in der Organisation keine Einladungen mehr erforderlich.

Wenn Sie über Ressourcen verfügen, die Sie mithilfe einer ressourcenbasierten Berechtigungsrichtlinie gemeinsam genutzt haben, können Sie diese Ressourcen zu vollständig AWS RAM verwalteten Ressourcen heraufstufen, indem Sie einen der folgenden Schritte ausführen:

- Verwenden Sie die API-Operation PromoteResourceShareCreatedFromPolicy.
- Verwenden Sie das Äquivalent der API-Operation, nämlich den Befehl AWS Command Line Interface (AWS CLI) promote-resource-share-created-from-policy.

Wie funktioniert die gemeinsame Nutzung von Ressourcen

Wenn Sie eine Ressource des Eigentümerkontos mit einem anderen AWS-Konto, dem verbrauchenden Konto, teilen, gewähren Sie den Prinzipalen im verbrauchenden Konto Zugriff auf die gemeinsam genutzte Ressource. Alle Richtlinien und Berechtigungen, die für Rollen und Benutzer des Benutzerkontos gelten, gelten auch für die gemeinsam genutzte Ressource. Bei den Ressourcen in der Freigabe handelt es sich offenbar um systemeigene Ressourcen in der Datei, mit der AWS-Konten Sie sie geteilt haben.

Sie können sowohl globale als auch regionale Ressourcen gemeinsam nutzen. Weitere Informationen finden Sie unter Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.

Teilen Sie Ihre Ressourcen

Mit können Sie Ressourcen AWS RAM, die Sie besitzen, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Um eine Ressourcenfreigabe zu erstellen, geben Sie Folgendes an:

- Die, AWS-Region in der Sie die Ressourcenfreigabe erstellen möchten. In der Konsole wählen Sie aus dem Dropdownmenü Region in der oberen rechten Ecke der Konsole eine Auswahl aus. In der AWS CLI verwenden Sie den Parameter. `--region`
  - Eine Ressourcenfreigabe kann nur regionale Ressourcen enthalten, die sich in derselben AWS-Region Ressourcenfreigabe befinden.
  - Eine Ressourcenfreigabe kann nur globale Ressourcen enthalten, wenn sich die Ressourcenfreigabe in der für globale Ressourcen vorgesehenen Heimatregion, USA Ost (Nord-Virginia), befindet`us-east-1`.
- Ein Name für die Ressourcenfreigabe.
- Die Liste der Ressourcen, auf die Sie im Rahmen dieser Ressourcenfreigabe Zugriff gewähren möchten.
- Die Principals, denen Sie Zugriff auf die Ressourcenfreigabe gewähren. Prinzipale können individuell sein AWS-Konten, die Konten in einer Organisation oder Organisationseinheit (OU) oder einzelne Rollen oder Benutzer AWS Identity and Access Management (IAM). AWS Organizations

  > **Note**
  >
  > Nicht alle Ressourcentypen können mit IAM-Rollen und Benutzern geteilt werden. Informationen zu Ressourcen, die Sie mit diesen Prinzipalen gemeinsam nutzen können, finden Sie unter. Gemeinsam nutzbare Ressourcen AWS

- Eine verwaltete Berechtigung zur Zuordnung zu jedem Ressourcentyp, den Sie in eine Ressourcenfreigabe aufnehmen. Die verwaltete Berechtigung bestimmt, was die Prinzipale in den anderen Konten mit den Ressourcen in der Ressourcenfreigabe tun können.

  Das Verhalten der Berechtigung hängt vom Typ des Hauptbenutzers ab:

  - Befindet sich der Prinzipal in einem anderen Konto als dem Konto, dem die Ressource gehört, sind die mit der Ressourcenfreigabe verknüpften Berechtigungen die maximalen

Berechtigungen, die Rollen und Benutzern in diesen Konten gewährt werden können. Der Administrator dieser Konten muss dann einzelnen Rollen und Benutzern mithilfe identitätsbasierter IAM-Richtlinien Zugriff auf die gemeinsam genutzte Ressource gewähren. Die in diesen Richtlinien gewährten Berechtigungen dürfen die Berechtigungen nicht überschreiten, die in den mit der Ressourcenfreigabe verknüpften Berechtigungen definiert sind.

Das Konto, das die Ressource besitzt, behält das volle Eigentum an den Ressourcen, die es gemeinsam nutzt.

Nutzung gemeinsam genutzter Ressourcen

Wenn der Eigentümer einer Ressource sie mit Ihrem Konto teilt, können Sie auf die gemeinsam genutzte Ressource genauso zugreifen, als ob sie Ihrem Konto gehört. Sie können auf die Ressource zugreifen, indem Sie die Konsole, AWS CLI Befehle und API-Operationen des jeweiligen Dienstes verwenden. Die API-Operationen, die Principals in Ihrem Konto ausführen dürfen, variieren je nach Ressourcentyp und werden durch die der Ressourcenfreigabe zugeordnete AWS RAM Berechtigung spezifiziert. Alle in Ihrem Konto konfigurierten IAM-Richtlinien und Servicesteuerungsrichtlinien gelten ebenfalls weiterhin, sodass Sie Ihre bestehenden Investitionen in Sicherheits- und Governance-Kontrollen nutzen können.

Wenn Sie mithilfe des Dienstes dieser Ressource auf eine gemeinsam genutzte Ressource zugreifen, haben Sie dieselben Fähigkeiten und Einschränkungen wie die Person AWS-Konto , der die Ressource gehört.

- Wenn es sich bei der Ressource um eine regionale Ressource handelt, können Sie nur von dem Konto aus darauf zugreifen, AWS-Region in dem sie im Eigentümerkonto vorhanden ist.
- Wenn es sich um eine globale Ressource handelt, können Sie von jeder Ressource aus darauf zugreifen AWS-Region , die von der Servicekonsole und den Tools der Ressource unterstützt wird. Sie können die gemeinsam genutzte Ressource und ihre globalen Ressourcen in der AWS RAM Konsole und in den Tools nur in der angegebenen Heimatregion, USA Ost (Nord-Virginia), anzeigen und verwaltenus-east-1.

Zugreifen AWS RAM

Sie können auf eine AWS RAM der folgenden Arten damit arbeiten:

AWS RAM Konsole

AWS RAM bietet eine webbasierte Benutzeroberfläche, die AWS RAM Konsole. Wenn Sie sich für eine angemeldet haben AWS-Konto, können Sie auf die AWS RAM Konsole zugreifen, indem Sie sich auf der Startseite der Konsole anmelden AWS-Managementkonsoleund dort eine AWS RAM Auswahl treffen.

Sie können in Ihrem Browser auch direkt zur AWS RAM Konsole navigieren. Wenn Sie noch nicht angemeldet sind, werden Sie aufgefordert, dies zu tun, bevor die Konsole angezeigt wird.

AWS CLI und Tools für Windows PowerShell

Die AWS CLI und AWS -Tools für PowerShell bieten direkten Zugriff auf die AWS RAM öffentlichen API-Operationen. AWS unterstützt diese Tools auf WindowsmacOS, undLinux. Weitere Informationen zu den ersten Schritten finden Sie im AWS Command Line Interface Benutzerhandbuch oder im AWS Tools for Windows PowerShell Benutzerhandbuch. Weitere Informationen zu den Befehlen für AWS RAM finden Sie in der AWS CLI Befehlsreferenz oder der AWS Tools for Windows PowerShell Cmdlet-Referenz.

AWS SDKs

AWS stellt API-Befehle für eine Vielzahl von Programmiersprachen bereit. Weitere Informationen zu den ersten Schritten finden Sie im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.

Abfrage-API

Wenn Sie keine der unterstützten Programmiersprachen verwenden, erhalten Sie mit der AWS RAM HTTPS-Abfrage-API programmatischen Zugriff auf AWS RAM und AWS. Mit der AWS RAM API können Sie HTTPS-Anfragen direkt an den Dienst senden. Wenn Sie die AWS RAM API verwenden, müssen Sie Code hinzufügen, um Anfragen mit Ihren Anmeldeinformationen digital zu signieren. Weitere Informationen finden Sie in der AWS RAM -API-Referenz.

Preisgestaltung für AWS RAM

Es fallen keine zusätzlichen Gebühren für die Nutzung AWS RAM oder Erstellung von Resource Shares und die gemeinsame Nutzung Ihrer Ressourcen für mehrere Konten an. Nutzungsabhängige Gebühren von Ressourcen variieren je nach Ressourcentyp. Weitere Informationen darüber, wie gemeinsam nutzbare Ressourcen in AWS Rechnung gestellt werden, finden Sie in der Dokumentation für den Dienst, der die Ressource besitzt.

Einhaltung der Vorschriften und internationale Standards

PCI DSS

AWS RAM unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstleister und wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert.

Weitere Informationen über PCI DSS, einschließlich der Anforderung einer Kopie des AWS PCI Compliance Package, finden Sie unter PCI DSS Level 1.

FedRAMP

AWS RAM ist in den folgenden Ländern als FedRAMP Moderate zugelassen AWS-Regionen: USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Nordkalifornien) und USA West (Oregon).

AWS RAM ist in den folgenden Ländern als FedRAMP High zugelassen AWS-Regionen: AWS GovCloud (US-West) und AWS GovCloud (US-Ost).

Das Federal Risk and Authorization Management Program (FedRAMP) ist ein US-Bundesprogramm, das einen Standardansatz für die Sicherheitsprüfung, Autorisierung und die laufende Überwachung von Cloud-Produkten und -Services bereitstellt..

Weitere Informationen zur FedRAMP-Konformität finden Sie unter FedRAMP.

SOC und ISO

AWS RAM kann für Workloads verwendet werden, die der Einhaltung von Service Organization Control (SOC) und den Normen ISO 9001, ISO 27001, ISO 27017, ISO 27018 und ISO 27701 der Internationalen Organisation für Normung (ISO) unterliegen. Kunden aus den Bereichen Finanzen, Gesundheitswesen und anderen regulierten Branchen können Einblicke in die Sicherheitsprozesse und -kontrollen zum Schutz von Kundendaten erhalten. Diese Informationen finden Sie in den SOC-Berichten sowie den ISO- und CSA STAR-Zertifikaten unter. AWS AWS Artifact

Weitere Informationen zur SOC-Konformität finden Sie unter SOC.

Weitere Informationen zur ISO-Konformität finden Sie unter ISO 9001, ISO 27001, ISO27017, ISO 27018und ISO 27701.

Erste Schritte mit AWS RAM

Mit können Sie Ressourcen AWS Resource Access Manager, die Sie besitzen, mit anderen Personen teilen AWS-Konten. Wenn Ihr Konto von verwaltet wird AWS Organizations, können Sie Ressourcen auch mit anderen Konten in Ihrer Organisation teilen. Sie können auch Ressourcen verwenden, die von anderen mit Ihnen geteilt wurden AWS-Konten.

Wenn Sie die gemeinsame Nutzung innerhalb nicht aktivieren AWS Organizations, können Sie Ressourcen nicht mit Ihrer Organisation oder mit den Organisationseinheiten (OU) in Ihrer Organisation teilen. Sie können Ressourcen jedoch weiterhin für einzelne Personen AWS-Konten in Ihrer Organisation gemeinsam nutzen. Bei unterstützten Ressourcentypen können Sie Ressourcen auch für einzelne AWS Identity and Access Management (IAM-) Rollen oder Benutzer in Ihrer Organisation gemeinsam nutzen. In diesem Fall werden diese Prinzipale so behandelt, als wären sie externe Konten und nicht als Teil Ihrer Organisation. Sie erhalten eine Einladung, der Resource Share beizutreten, und müssen die Einladung annehmen, um Zugriff auf die gemeinsam genutzten Ressourcen zu erhalten.

Inhalt

Begriffe und Konzepte für AWS RAM

Die folgenden Konzepte erklären, wie Sie AWS Resource Access Manager (AWS RAM) verwenden können, um Ihre Ressourcen gemeinsam zu nutzen.

Ressourcenfreigabe

Sie nutzen Ressourcen gemeinsam, AWS RAM indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe besteht aus den folgenden drei Elementen:

- Eine Liste mit einer oder mehreren AWS Ressourcen, die gemeinsam genutzt werden sollen.
- Eine Liste mit einem oder mehreren Prinzipalen, denen Zugriff auf die Ressourcen gewährt wird.
- Eine verwaltete Berechtigung für jeden Ressourcentyp, den Sie in die Freigabe aufnehmen. Jede verwaltete Berechtigung gilt für alle Ressourcen dieses Typs in dieser Ressourcenfreigabe.

Nachdem Sie sie AWS RAM zum Erstellen einer Ressourcenfreigabe verwendet haben, kann den in der Ressourcenfreigabe angegebenen Prinzipalen Zugriff auf die Ressourcen der Freigabe gewährt werden.

- Wenn Sie das AWS RAM Teilen mit aktivieren und Ihre Prinzipale AWS Organizations, für die Sie die gemeinsame Nutzung nutzen, derselben Organisation angehören wie das Freigabekonto, können diese Prinzipale Zugriff erhalten, sobald ihr Kontoadministrator ihnen mithilfe einer AWS Identity and Access Management (IAM-) Berechtigungsrichtlinie Berechtigungen zur Nutzung der Ressourcen erteilt.
- Wenn Sie das AWS RAM Teilen mit Organizations nicht aktivieren, können Sie Ressourcen trotzdem für AWS-Konten Personen in Ihrer Organisation freigeben. Der Administrator des Benutzerkontos erhält eine Einladung, der Resource Share beizutreten. Er muss die Einladung annehmen, bevor die in der Resource Share angegebenen Principals auf die gemeinsam genutzten Ressourcen zugreifen können.
- Sie können Inhalte auch mit Konten außerhalb Ihrer Organisation teilen, sofern der Ressourcentyp dies unterstützt. Der Administrator des Benutzerkontos erhält eine Einladung zur Teilnahme an der Ressourcenfreigabe. Er muss die Einladung annehmen, bevor die in der Ressourcenfreigabe angegebenen Prinzipale auf die gemeinsam genutzten Ressourcen zugreifen können. Informationen dazu, welche Ressourcentypen diese Art der gemeinsamen Nutzung unterstützen, finden Sie Gemeinsam nutzbare Ressourcen AWS in der Spalte Kann Inhalte mit Konten außerhalb der Organisation teilen.

Konto teilen

Das Freigabekonto enthält die Ressource, die gemeinsam genutzt wird und in der der AWS RAM AWS Administrator mithilfe von AWS RAM.

Ein AWS RAM Administrator ist ein IAM-Prinzipal, der berechtigt ist, Ressourcenfreigaben in der AWS-Konto zu erstellen und zu konfigurieren. Da AWS RAM den Ressourcen in einer Ressourcenfreigabe eine ressourcenbasierte Richtlinie zugewiesen wird, muss der AWS RAM Administrator auch über die erforderlichen Berechtigungen verfügen, um den `PutResourcePolicy` Vorgang AWS-Service für jeden Ressourcentyp, der in einer Ressourcenfreigabe enthalten ist, aufrufen zu können.

Prinzipale werden konsumiert

Das verbrauchende Konto ist das Konto AWS-Konto , für das eine Ressource gemeinsam genutzt wird. Bei der Ressourcenfreigabe kann ein ganzes Konto als Hauptkonto oder für einige Ressourcentypen einzelne Rollen oder Benutzer im Konto angegeben werden. Informationen darüber, welche Ressourcentypen diese Art der gemeinsamen Nutzung unterstützen, finden Sie in der Spalte Kann gemeinsam mit IAM-Rollen Gemeinsam nutzbare Ressourcen AWS und -Benutzern verwendet werden.

AWS RAM unterstützt auch Service Principals als Nutzer von gemeinsam genutzten Ressourcen. Informationen darüber, welche Ressourcentypen diese Art der gemeinsamen Nutzung unterstützen, finden Sie Gemeinsam nutzbare Ressourcen AWS in der Spalte Kann gemeinsam mit Service Principals genutzt werden.

Die Prinzipale des Benutzerkontos können nur die Aktionen ausführen, die mit den beiden folgenden Berechtigungen zulässig sind:

- Die verwalteten Berechtigungen, die mit der Ressource verknüpft sind, werden gemeinsam genutzt. Diese geben die maximalen Berechtigungen an, die den Prinzipalen im verbrauchenden Konto gewährt werden können.
- Die identitätsbasierten IAM-Richtlinien, die einzelnen Rollen oder Benutzern vom IAM-Administrator des Benutzerkontos zugewiesen wurden. Diese Richtlinien müssen `Allow` Zugriff auf bestimmte Aktionen und auf den Amazon-Ressourcennamen (ARN) einer Ressource im Sharing-Konto gewähren.

AWS RAM unterstützt die folgenden IAM-Prinzipaltypen als Nutzer von gemeinsam genutzten Ressourcen:

- Eine weitere AWS-Konto Möglichkeit: Durch die gemeinsame Nutzung von Ressourcen werden die im Sharing-Konto enthaltenen Ressourcen dem Konto zur Verfügung gestellt, das sie nutzt.
- Einzelne IAM-Rollen oder Benutzer in einem anderen Konto — Einige Ressourcentypen unterstützen die direkte gemeinsame Nutzung mit einzelnen IAM-Rollen oder -Benutzern. Geben Sie diesen Prinzipaltyp anhand seines ARN an.
  - IAM-Rolle — `arn:aws:iam::123456789012:role/rolename`
  - IAM-Benutzer — `arn:aws:iam::123456789012:user/username`
- Service Principal — Geben Sie eine Ressource für einen AWS Service frei, um dem Service Zugriff auf eine Resource Share zu gewähren. Durch die gemeinsame Nutzung des AWS Service

Principal kann ein Service in Ihrem Namen Maßnahmen ergreifen, um den betrieblichen Aufwand zu verringern.

Um die gemeinsame Nutzung mit einem Dienstprinzipal zu ermöglichen, aktivieren Sie die gemeinsame Nutzung für alle Benutzer, und wählen Sie dann unter Prinzipaltyp auswählen die Option Dienstprinzipal aus der Dropdownliste aus. Geben Sie den Namen des Dienstprinzipals im folgenden Format an:

- *service-id*.amazonaws.com

Um das Risiko eines verwirrten Stellvertreters zu minimieren, zeigt die Ressourcenrichtlinie die Konto-ID des Ressourcenbesitzers im `aws:SourceAccount` Bedingungsschlüssel an.

- Konten in einer Organisation — Wenn das Sharing-Konto von verwaltet wird AWS Organizations, kann das Resource Sharing die ID der Organisation angeben, die mit allen Konten in der Organisation geteilt werden soll. Die Ressourcenfreigabe kann alternativ eine Organisationseinheit-ID (OU) angeben, die mit allen Konten in dieser Organisationseinheit gemeinsam genutzt werden soll. Ein Sharing-Konto kann nur mit seiner eigenen Organisation oder OU IDs innerhalb seiner eigenen Organisation geteilt werden. Geben Sie Konten in einer Organisation anhand des ARN der Organisation oder der Organisationseinheit an.
  - Alle Konten in einer Organisation — Im Folgenden finden Sie ein Beispiel für einen ARN einer Organisation in AWS Organizations:

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

  - Alle Konten in einer Organisationseinheit — Im Folgenden finden Sie ein Beispiel für einen ARN einer OU-ID:

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

  > **Important**
  >
  > Wenn Sie Daten mit einer Organisation oder einer Organisationseinheit teilen und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im Freigabekonto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet. `"Principal": "*"` Weitere

Informationen finden Sie unter Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie.
Principals in den anderen Accounts, die diese Nutzung nutzen, erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen `Allow` Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

Ressourcenbasierte Richtlinie

Ressourcenbasierte Richtlinien sind JSON-Textdokumente, die die IAM-Richtliniensprache implementieren. Im Gegensatz zu identitätsbasierten Richtlinien, die Sie dem Prinzipal zuordnen, z. B. einer IAM-Rolle oder einem IAM-Benutzer, fügen Sie der Ressource ressourcenbasierte Richtlinien hinzu. AWS RAM erstellt in Ihrem Namen ressourcenbasierte Richtlinien auf der Grundlage der Informationen, die Sie für Ihren Resource Share angeben. Sie müssen ein `Principal` Richtlinienelement angeben, das festlegt, wer auf die Ressource zugreifen kann. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien im IAM-Benutzerhandbuch.

Die von generierten ressourcenbasierten Richtlinien AWS RAM werden zusammen mit allen anderen IAM-Richtlinientypen bewertet. Dazu gehören alle identitätsbasierten IAM-Richtlinien, die den Prinzipalen zugewiesen sind, die versuchen, auf die Ressource zuzugreifen, sowie die Dienststeuerungsrichtlinien (SCPs) für diese Richtlinien, die möglicherweise für die gelten. AWS Organizations AWS-Konto Ressourcenbasierte Richtlinien, die von AWS RAM generiert wurden, unterliegen derselben Richtlinienbewertungslogik wie alle anderen IAM-Richtlinien. Vollständige Informationen zur Richtlinienbewertung und zur Bestimmung der daraus resultierenden Berechtigungen finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

AWS RAM bietet eine einfache und sichere Nutzung von Ressourcen, indem easy-to-use abstrakte, ressourcenbasierte Richtlinien bereitgestellt werden.

Für die Ressourcentypen, die ressourcenbasierte Richtlinien unterstützen, erstellt und verwaltet die ressourcenbasierten Richtlinien AWS RAM automatisch für Sie. AWS RAM Erstellt für eine bestimmte Ressource die ressourcenbasierte Richtlinie, indem es die Informationen aus allen Ressourcenfreigaben kombiniert, zu denen diese Ressource gehört. Stellen Sie sich zum

Beispiel eine Amazon SageMaker AI-Pipeline vor, die Sie mithilfe von zwei verschiedenen Ressourcenfreigaben gemeinsam nutzen AWS RAM und in diese aufnehmen. Sie könnten eine Ressourcenfreigabe verwenden, um Ihrer gesamten Organisation schreibgeschützten Zugriff zu gewähren. Sie könnten dann die andere Ressourcenfreigabe verwenden, um nur einem einzigen SageMaker Konto KI-Ausführungsberechtigungen zu gewähren. AWS RAM kombiniert diese beiden unterschiedlichen Berechtigungssätze automatisch zu einer einzigen Ressourcenrichtlinie mit mehreren Anweisungen. Anschließend wird die kombinierte ressourcenbasierte Richtlinie an die Pipeline-Ressource angehängt. Sie können diese zugrunde liegende Ressourcenrichtlinie anzeigen, indem Sie den Vorgang aufrufen. GetResourcePolicy AWS-Services verwenden Sie dann diese ressourcenbasierte Richtlinie, um jeden Prinzipal zu autorisieren, der versucht, eine Aktion mit der gemeinsam genutzten Ressource auszuführen.

Sie können die ressourcenbasierten Richtlinien zwar manuell erstellen und sie per Anruf an Ihre Ressourcen anhängen`PutResourcePolicy`, wir empfehlen Ihnen jedoch, sie zu verwenden, AWS RAM da sie die folgenden Vorteile bietet:

- Auffindbarkeit für Share-Consumer — Wenn Sie Ressourcen gemeinsam nutzen AWS RAM, können Benutzer alle Ressourcen, die mit ihnen geteilt wurden, direkt in der Konsole und in den API-Vorgängen des Resource Ownering-Dienstes sehen, als ob sich diese Ressourcen direkt im Konto des Benutzers befinden würden. Wenn Sie beispielsweise ein AWS CodeBuild Projekt mit einem anderen Konto teilen, können Benutzer des Benutzerkontos das Projekt in der CodeBuild Konsole und in den Ergebnissen der ausgeführten CodeBuild API-Operationen sehen. Ressourcen, die durch direktes Anhängen einer ressourcenbasierten Richtlinie gemeinsam genutzt werden, sind auf diese Weise nicht sichtbar. Stattdessen müssen Sie die Ressource anhand ihres ARN ermitteln und explizit darauf verweisen.
- Verwaltbarkeit für Share-Inhaber — Wenn Sie Ressourcen gemeinsam nutzen AWS RAM, können Ressourcenbesitzer im Sharing-Konto zentral sehen, welche anderen Konten Zugriff auf ihre Ressourcen haben. Wenn Sie eine Ressource mithilfe einer ressourcenbasierten Richtlinie gemeinsam nutzen, können Sie die Konten, die sie verbrauchen, nur sehen, wenn Sie die Richtlinie für einzelne Ressourcen in der entsprechenden Servicekonsole oder API überprüfen.
- Effizienz — Wenn Sie Ressourcen gemeinsam nutzen AWS RAM, können Sie mehrere Ressourcen gemeinsam nutzen und sie als Einheit verwalten. Für Ressourcen, die nur mithilfe von ressourcenbasierten Richtlinien gemeinsam genutzt werden, müssen für jede Ressource, die Sie gemeinsam nutzen, individuelle Richtlinien gelten.
- Einfachheit — Mit AWS RAM müssen Sie die JSON-basierte IAM-Richtliniensprache nicht verstehen. AWS RAM bietet ready-to-use AWS verwaltete Berechtigungen, aus denen Sie wählen können, um sie an Ihre Ressourcenfreigaben anzuhängen.

Mithilfe AWS RAM von können Sie sogar einige Ressourcentypen gemeinsam nutzen, die noch keine ressourcenbasierten Richtlinien unterstützen. Generiert für solche Ressourcentypen AWS RAM automatisch eine ressourcenbasierte Richtlinie als Darstellung der tatsächlichen Berechtigungen. Benutzer können sich diese Darstellung ansehen, indem sie anrufen. GetResourcePolicy Dies beinhaltet die folgenden Ressourcentypen:

- Amazon Aurora — DB-Cluster
- Amazon EC2 — Kapazitätsreservierungen und dedizierte Hosts
- AWS License Manager — Lizenzkonfigurationen
- AWS Outposts — Routentabellen, Außenposten und Standorte für lokale Gateways
- Amazon Route 53 — Speditionsregeln
- Amazon Virtual Private Cloud — Kundeneigene IPv4 Adressen, Präfixlisten, Subnetze, Traffic Mirror-Ziele, Transit-Gateways und Transit-Gateway-Multicast-Domains

Beispiele für generierte ressourcenbasierte Richtlinien AWS RAM

Wenn Sie eine EC2 Image Builder Builder-Image-Ressource mit einem einzelnen Konto gemeinsam nutzen, AWS RAM generiert es eine Richtlinie, die wie das folgende Beispiel aussieht, und fügt sie allen Bildressourcen hinzu, die in der Ressourcenfreigabe enthalten sind.

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"
        }
    ]
```

```
}
```

Wenn Sie eine EC2 Image Builder Builder-Image-Ressource mit einer IAM-Rolle oder einem anderen Benutzer gemeinsam nutzen AWS-Konto, AWS RAM generiert es eine Richtlinie, die wie im folgenden Beispiel aussieht, und hängt sie an alle Image-Ressourcen an, die in der Ressourcenfreigabe enthalten sind.

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"
        }
    ]
}
```

Wenn Sie eine EC2 Image Builder Builder-Image-Ressource mit allen Konten in einer Organisation oder mit den Konten einer Organisationseinheit gemeinsam nutzen, AWS RAM generiert sie eine Richtlinie, die wie im folgenden Beispiel aussieht, und hängt sie an alle Image-Ressourcen an, die in der Ressourcenfreigabe enthalten sind.

> **Note**
>
> Diese Richtlinie verwendet das `"Condition"` Element `"Principal": "*"` und verwendet es dann, um Berechtigungen auf Identitäten zu beschränken, die den angegebenen

entsprechen. `PrincipalOrgID` Weitere Informationen finden Sie unter [Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie](#).

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"
                }
            }
        }
    ]
}
```

Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie

Wenn Sie `"Principal": "*"` in eine ressourcenbasierte Richtlinie einbeziehen, gewährt die Richtlinie Zugriff auf alle IAM-Prinzipale in dem Konto, das die Ressource enthält, vorbehaltlich aller Einschränkungen, die durch ein `Condition` Element, sofern vorhanden, auferlegt werden. Explizite `Deny` Aussagen in allen Richtlinien, die für den aufrufenden Prinzipal gelten, haben Vorrang vor den durch diese Richtlinie gewährten Berechtigungen. Eine implizite `Deny` (d. h. das Fehlen einer expliziten Angabe`Allow`) in allen geltenden Identitäts-, Berechtigungsgrenzen- oder Sitzungsrichtlinien führt jedoch nicht dazu, dass den Prinzipalen durch eine `Deny` solche ressourcenbasierte Richtlinie Zugriff auf eine Aktion gewährt wird.

Wenn dieses Verhalten für Ihr Szenario nicht erwünscht ist, können Sie dieses Verhalten einschränken, indem Sie einer Identitätsrichtlinie, einer Berechtigungsgrenze oder einer Sitzungsrichtlinie eine explizite `Deny` Anweisung hinzufügen, die sich auf die entsprechenden Rollen und Benutzer auswirkt.

Verwaltete Berechtigungen

Verwaltete Berechtigungen definieren, welche Aktionen Prinzipale unter welchen Bedingungen für unterstützte Ressourcentypen in einer Ressourcenfreigabe ausführen können. Wenn Sie eine Ressourcenfreigabe erstellen, müssen Sie angeben, welche verwalteten Berechtigungen für jeden in der Ressourcenfreigabe enthaltenen Ressourcentyp verwendet werden sollen. In einer verwalteten Berechtigung werden die Gruppen `actions` und Bedingungen aufgeführt, die Prinzipale mit der gemeinsam genutzten AWS RAM Ressource ausführen können.

Sie können jedem Ressourcentyp in einer Ressourcenfreigabe nur eine verwaltete Berechtigung zuordnen. Sie können keine Ressourcenfreigabe erstellen, bei der einige Ressourcen eines bestimmten Typs eine verwaltete Berechtigung und andere Ressourcen desselben Typs eine andere verwaltete Berechtigung verwenden. Dazu müssten Sie zwei verschiedene Ressourcenfreigaben erstellen und die Ressourcen auf diese aufteilen, sodass jeder Gruppe unterschiedliche verwaltete Berechtigungen zugewiesen werden. Es gibt zwei verschiedene Arten von verwalteten Berechtigungen:

AWS verwaltete Berechtigungen

> AWS verwaltete Berechtigungen werden von Kunden erstellt und verwaltet AWS und gewähren Berechtigungen für gängige Kundenszenarien. AWS RAM definiert mindestens eine AWS verwaltete Berechtigung für jeden unterstützten Ressourcentyp. Einige Ressourcentypen unterstützen mehr als eine AWS verwaltete Berechtigung, wobei eine verwaltete Berechtigung als AWS Standard festgelegt ist. Sofern Sie nichts anderes angeben, ist die standardmäßige AWS verwaltete Berechtigung zugeordnet.

Vom Kunden verwaltete Berechtigungen

> Kundenverwaltete Berechtigungen sind verwaltete Berechtigungen, die Sie erstellen und verwalten, indem Sie genau angeben, welche Aktionen unter welchen Bedingungen mit gemeinsam genutzten Ressourcen ausgeführt werden können AWS RAM. Sie möchten beispielsweise den Lesezugriff für Ihre Amazon VPC IP Address Manager (IPAM) -Pools einschränken, die Ihnen helfen, Ihre IP-Adressen in großem Umfang zu verwalten. Sie können kundenverwaltete Berechtigungen für Ihre Entwickler einrichten, um IP-Adressen zuzuweisen,

aber nicht den IP-Adressbereich einsehen, den andere Entwicklerkonten zuweisen. Sie können sich an die bewährte Methode der geringsten Rechte halten und nur die Berechtigungen gewähren, die für die Ausführung von Aufgaben auf gemeinsam genutzten Ressourcen erforderlich sind.

Sie definieren Ihre eigenen Berechtigungen für einen Ressourcentyp in einer gemeinsam genutzten Ressource mit der Option, Bedingungen wie globale Kontextschlüssel und dienstspezifische Schlüssel hinzuzufügen, um die Bedingungen festzulegen, unter denen Prinzipale Zugriff auf die Ressource haben. Diese Berechtigungen können in einer oder mehreren AWS RAM Shares verwendet werden. Die vom Kunden verwalteten Berechtigungen sind regionsspezifisch.

AWS RAM verwendet verwaltete Berechtigungen als Eingabe für die Erstellung der ressourcenbasierten Richtlinien für die Ressourcen, die Sie gemeinsam nutzen.

Version mit verwalteten Berechtigungen

Jede Änderung an einer verwalteten Berechtigung wird als neue Version dieser verwalteten Berechtigung dargestellt. Die neue Version ist die Standardversion für alle neuen Ressourcenfreigaben. Für jede verwaltete Berechtigung ist immer eine Version als Standardversion festgelegt. Wenn Sie eine neue Version mit verwalteten Berechtigungen erstellen oder AWS erstellen, müssen Sie die verwalteten Berechtigungen für jede vorhandene Ressourcenfreigabe explizit aktualisieren. In diesem Schritt können Sie die Änderungen auswerten, bevor Sie sie auf Ihre Ressourcenfreigabe anwenden. Für alle neuen Ressourcenfreigaben wird automatisch die neue Version der verwalteten Berechtigungen für den entsprechenden Ressourcentyp verwendet.

AWS Versionen mit verwalteten Berechtigungen

AWS verarbeitet alle Änderungen an AWS verwalteten Berechtigungen. Solche Änderungen betreffen neue Funktionen oder beheben festgestellte Mängel. Sie können nur die Standardversion mit verwalteten Berechtigungen auf Ihre Ressourcenfreigaben anwenden.

Versionen mit vom Kunden verwalteten Berechtigungen

Sie kümmern sich um alle Änderungen an den vom Kunden verwalteten Berechtigungen. Sie können eine neue Standardversion erstellen, eine ältere Version als Standardversion festlegen oder Versionen löschen, die keinen Ressourcenfreigaben mehr zugeordnet sind. Jede vom Kunden verwaltete Berechtigung kann bis zu fünf Versionen haben.

Wenn Sie eine Ressourcenfreigabe erstellen oder aktualisieren, können Sie nur die Standardversion der angegebenen verwalteten Berechtigung anhängen. Weitere Informationen finden Sie unter Aktualisierung AWS verwalteter Berechtigungen auf eine neuere Version.

Teilen Sie Ihre AWS Ressourcen

Gehen Sie wie folgt vor, um eine Ressource, deren Eigentümer Sie sind AWS RAM, gemeinsam zu nutzen:

- Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations (optional)
- Erstellen einer Ressourcen-Freigabe

Hinweise

- Die gemeinsame Nutzung einer Ressource mit Prinzipalen außerhalb des AWS-Konto Eigentümers der Ressource hat keine Auswirkung auf die Berechtigungen oder Kontingente, die für die Ressource innerhalb des Kontos gelten, mit dem sie erstellt wurde.
- AWS RAM ist ein regionaler Dienst. Die Prinzipale, mit denen Sie die Ressourcen gemeinsam nutzen, können nur auf die Ressourcenfreigaben zugreifen, AWS-Regionen in denen die Ressourcen erstellt wurden.
- Bei einigen Ressourcen gelten besondere Überlegungen und Voraussetzungen für die gemeinsame Nutzung. Weitere Informationen finden Sie unter Gemeinsam nutzbare Ressourcen AWS.

Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations

Wenn Ihr Konto von verwaltet wird AWS Organizations, können Sie dies nutzen, um Ressourcen einfacher gemeinsam zu nutzen. Mit oder ohne Organizations kann ein Benutzer Inhalte mit einzelnen Konten teilen. Wenn sich Ihr Konto jedoch in einer Organisation befindet, können Sie Inhalte für einzelne Konten oder für alle Konten in der Organisation oder in einer Organisationseinheit freigeben, ohne jedes Konto aufzählen zu müssen.

Um Ressourcen innerhalb einer Organisation gemeinsam zu nutzen, müssen Sie zuerst die AWS RAM Konsole verwenden oder AWS Command Line Interface (AWS CLI), um das Teilen mit zu

aktivieren. AWS Organizations Wenn Sie Ressourcen in Ihrer Organisation gemeinsam nutzen, sendet AWS RAM keine Einladungen an Schulleiter. Principals in Ihrer Organisation erhalten Zugriff auf gemeinsam genutzte Ressourcen, ohne Einladungen austauschen zu müssen.

Wenn Sie die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation aktivieren, AWS RAM wird eine dienstbezogene Rolle mit dem Namen erstellt. **`AWSServiceRoleForResourceAccessManager`** Diese Rolle kann nur vom AWS RAM Dienst übernommen werden und erteilt die AWS RAM Berechtigung, mithilfe der AWS verwalteten Richtlinie `AWSResourceAccessManagerServiceRolePolicy` Informationen über die Organisation abzurufen, der er angehört.

> **Note**
>
> Wenn Sie das Teilen mit AWS Organizations aktivieren, schränkt die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation standardmäßig den Zugriff auf Nutzer innerhalb derselben Organisation ein. Wenn ein Benutzerkonto die Organisation verlässt, verliert dieses Konto den Zugriff auf Ressourcen in der Ressourcenfreigabe. Diese Einschränkung gilt unabhängig davon, ob Sie Ressourcen mit einer Organisationseinheit, der gesamten Organisation oder einem einzelnen Konto in der Organisation gemeinsam nutzen.
> Für die account-to-account gemeinsame Nutzung innerhalb Ihrer Organisation können Sie den Freigabezugriff auch dann beibehalten, wenn Konten verlassen werden`RetainSharingOnAccountLeaveOrganization`, indem Sie `True` beim Erstellen einer neuen Ressourcenfreigabe die Einstellung auf einstellen. Wenn diese Einstellung aktiviert ist, wird eine Einladung an das Nutzerkonto AWS RAM gesendet (ähnlich wie beim Teilen mit externen Konten). Das Konto behält auch dann Zugriff auf gemeinsam genutzte Ressourcen, wenn es die Organisation verlässt.
> Für die `RetainSharingOnAccountLeaveOrganization` Einstellung gelten die folgenden Anforderungen und Einschränkungen:
>
> - `allowExternalPrincipals`Muss sein `True`
> - Kann nur festgelegt werden, wenn neue Ressourcenfreigaben erstellt werden
> - Gilt nicht für die gemeinsame Nutzung mit OUs oder für die gesamte Organisation
> - Wenn auf gesetzt `RetainSharingOnAccountLeaveOrganization` ist`True`, können Sie Ressourcenfreigaben nicht verwenden, um Ressourcen gemeinsam zu nutzen, die nur innerhalb einer Organisation gemeinsam genutzt werden können.

Wenn Sie Ressourcen nicht mehr mit Ihrer gesamten Organisation teilen müssen oder OUs können Sie die gemeinsame Nutzung von Ressourcen deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der gemeinsamen Nutzung von Ressourcen mit AWS Organizations.

Mindestberechtigungen

Um die folgenden Verfahren ausführen zu können, müssen Sie sich als Principal im Verwaltungskonto der Organisation anmelden, das über die folgenden Berechtigungen verfügt:

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

Voraussetzungen

- Sie können diese Schritte nur ausführen, wenn Sie als Principal im Verwaltungskonto der Organisation angemeldet sind.
- In der Organisation müssen alle Funktionen aktiviert sein. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Alle Funktionen in Ihrer Organisation aktivieren.

> **Important**
>
> Sie müssen das Teilen mit AWS Organizations mithilfe der AWS RAM Konsole oder des AWS CLI Befehls enable-sharing-with-aws-organization aktivieren. Dadurch wird sichergestellt, dass die `AWSServiceRoleForResourceAccessManager`-serviceverknüpfte Rolle erstellt wird. Wenn Sie den vertrauenswürdigen Zugriff über die AWS Organizations Konsole oder den enable-aws-service-access AWS CLI Befehl aktivieren, AWS Organizations wird die `AWSServiceRoleForResourceAccessManager` dienstbezogene Rolle nicht erstellt, und Sie können Ressourcen innerhalb Ihrer Organisation nicht gemeinsam nutzen.

Console

Um die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation zu ermöglichen

1. Öffnen Sie die Seite „Einstellungen“ in der AWS RAM Konsole.
2. Wählen Sie „Teilen mit AWS Organizations aktivieren“ und anschließend „Einstellungen speichern“.

AWS CLI

Um die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation zu aktivieren

Verwenden Sie den Befehl enable-sharing-with-aws-organization.

Dieser Befehl kann in allen AWS-Region Bereichen verwendet werden und ermöglicht die gemeinsame Nutzung AWS Organizations in allen Regionen, in denen er unterstützt AWS RAM wird.

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

Erstellen einer Ressourcen-Freigabe

Um Ressourcen, die Ihnen gehören, gemeinsam zu nutzen, erstellen Sie eine Ressourcenfreigabe. Es folgt eine Übersicht über den Prozess:

1. Fügen Sie die Ressourcen hinzu, die Sie teilen möchten.
2. Geben Sie für jeden Ressourcentyp, den Sie in die gemeinsame Nutzung aufnehmen, die verwaltete Berechtigung an, die für diesen Ressourcentyp verwendet werden soll.
   - Sie können zwischen einer der verfügbaren AWS verwalteten Berechtigungen, einer vorhandenen vom Kunden verwalteten Berechtigung wählen oder eine neue vom Kunden verwaltete Berechtigung erstellen.
   - AWS verwaltete Berechtigungen werden von erstellt AWS , um Standardanwendungsfälle abzudecken.
   - Mit vom Kunden verwalteten Berechtigungen können Sie Ihre eigenen verwalteten Berechtigungen an Ihre Sicherheits- und Geschäftsanforderungen anpassen.

> **Note**
>
> Wenn die ausgewählte verwaltete Berechtigung mehrere Versionen hat, wird AWS RAM automatisch die Standardversion angehängt. Sie können nur die Version anhängen, die als Standardversion festgelegt ist.

3. Geben Sie die Prinzipale an, die Zugriff auf die Ressourcen haben sollen.

Überlegungen

- Wenn Sie später eine AWS Ressource löschen müssen, die Sie in eine Freigabe aufgenommen haben, empfehlen wir, die Ressource zunächst entweder aus einer Ressourcenfreigabe zu entfernen, die sie enthält, oder die Ressourcenfreigabe zu löschen.
- Die Ressourcentypen, die Sie in eine Ressourcenfreigabe aufnehmen können, sind unter aufgeführtGemeinsam nutzbare Ressourcen AWS.
- Sie können eine Ressource nur gemeinsam nutzen, wenn Sie Eigentümer dieser Ressource sind. Sie können eine Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- AWS RAM ist ein regionaler Dienst. Wenn Sie eine Ressource mit Prinzipalen in anderen teilen AWS-Konten, müssen diese Prinzipale auf jede Ressource von derselben Seite aus zugreifen AWS-Region , in der sie erstellt wurde. Auf unterstützte globale Ressourcen können Sie von allen AWS-Region Ressourcen aus zugreifen, die von der Servicekonsole und den Tools der jeweiligen Ressource unterstützt werden. Sie können solche gemeinsam genutzten Ressourcen und ihre globalen Ressourcen in der AWS RAM Konsole und in den Tools nur in der angegebenen Heimatregion, USA Ost (Nord-Virginia), einsehen`us-east-1`. Weitere Informationen zu AWS RAM und globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
- Wenn das Konto, von dem aus Sie Inhalte teilen, Teil einer Organisation ist AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten alle Prinzipale in der Organisation, für die Sie Inhalte freigeben, automatisch Zugriff auf die Ressourcenfreigaben, ohne dass Einladungen erforderlich sind. Ein Hauptbenutzer in einem Konto, mit dem Sie Inhalte außerhalb des Unternehmenskontextes teilen, erhält eine Einladung zur Teilnahme an der Resource Share und erhält erst dann Zugriff auf die gemeinsam genutzten Ressourcen, wenn sie die Einladung annehmen.
- Wenn Sie die Ressource mit einem Dienstprinzipal teilen, können Sie der Ressourcenfreigabe keine anderen Prinzipale zuordnen.

- Wenn die gemeinsame Nutzung zwischen Konten oder Prinzipalen erfolgt, die Teil einer Organisation sind, wirken sich alle Änderungen an der Organisationsmitgliedschaft dynamisch auf den Zugriff auf die gemeinsam genutzte Ressource aus.
  - Wenn Sie der Organisation oder Organisationseinheit ein Konto hinzufügen, das Zugriff auf eine Ressourcenfreigabe hat, erhält dieses neue Mitgliedskonto automatisch Zugriff auf die Ressourcenfreigabe. AWS-Konto Der Administrator des Kontos, für das Sie eine gemeinsame Nutzung vorgenommen haben, kann dann einzelnen Prinzipalen in diesem Konto Zugriff auf die Ressourcen in dieser Freigabe gewähren.
  - Wenn Sie ein Konto aus der Organisation oder einer Organisationseinheit entfernen, die Zugriff auf eine Ressourcenfreigabe hat, verlieren alle Prinzipale in diesem Konto automatisch den Zugriff auf Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.
  - Wenn Sie Rollen oder Benutzer im Mitgliedskonto direkt für ein Mitgliedskonto oder für IAM freigegeben haben und dann dieses Konto aus der Organisation entfernen, verlieren alle Principals in diesem Konto den Zugriff auf die Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.

  Important

  Wenn Sie Daten für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Principals im gemeinsam genutzten Konto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet. `"Principal": "*"` Weitere Informationen finden Sie unter Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie.
  Principals in den anderen Accounts, die diese Nutzung nutzen, erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen `Allow` Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

- Sie können Ihren Ressourcenfreigaben nur die Organisation hinzufügen, der Ihr Konto OUs angehört, und aus dieser Organisation stammen. Sie können einer Ressourcenfreigabe keine

Organisationen OUs oder Organisationen von außerhalb Ihrer eigenen Organisation als Prinzipale hinzufügen. Sie können jedoch einzelne AWS-Konten oder, bei unterstützten Diensten, IAM-Rollen und Benutzer von außerhalb Ihrer Organisation als Principals zu einer Ressourcenfreigabe hinzufügen.

> **Note**
>
> Nicht alle Ressourcentypen können mit IAM-Rollen und Benutzern geteilt werden. Informationen zu Ressourcen, die Sie mit diesen Prinzipalen gemeinsam nutzen können, finden Sie unter. Gemeinsam nutzbare Ressourcen AWS

- Für die folgenden Ressourcentypen haben Sie sieben Tage Zeit, um die Einladung zur Teilnahme an der Share für die folgenden Ressourcentypen anzunehmen. Wenn du die Einladung nicht annimmst, bevor sie abläuft, wird die Einladung automatisch abgelehnt.

> **Important**
>
> Für gemeinsam genutzte Ressourcentypen, die nicht in der folgenden Liste aufgeführt sind, haben Sie 12 Stunden Zeit, um die Einladung zur Teilnahme an der Resource Share anzunehmen. Nach 12 Stunden läuft die Einladung ab und die Zuordnung des Endbenutzer-Hauptbenutzers zur Resource Share wird aufgehoben. Die Einladung kann von Endbenutzern nicht mehr angenommen werden.

  - Amazon Aurora — DB-Cluster
  - Amazon EC2 — Kapazitätsreservierungen und dedizierte Hosts
  - AWS License Manager — Lizenzkonfigurationen
  - AWS Outposts — Routentabellen, Außenposten und Standorte für lokale Gateways
  - Amazon Route 53 — Speditionsregeln
  - Amazon VPC — Kundeneigene IPv4 Adressen, Präfixlisten, Subnetze, Traffic Mirror-Ziele, Transit-Gateways, Transit-Gateway-Multicast-Domänen

Console

Um eine Ressourcenfreigabe zu erstellen

1. Öffnen Sie die AWS RAM -Konsole.

2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen. Wenn Sie globale Ressourcen in die gemeinsame Nutzung von Ressourcen einbeziehen möchten, müssen Sie die angegebene Heimatregion, USA Ost (Nord-Virginia), auswählen`us-east-1`.
3. Wenn Sie noch keine Erfahrung damit haben AWS RAM, wählen Sie auf der Startseite die Option Ressourcenfreigabe erstellen aus. Wählen Sie andernfalls auf der Seite Von mir geteilt: Gemeinsam genutzte Ressourcen die Option Ressourcenfreigabe erstellen aus.
4. Gehen Sie in Schritt 1: Angaben zur Ressourcenfreigabe angeben wie folgt vor:

   a. Geben Sie für Name einen beschreibenden Namen für die Ressourcenfreigabe ein.

   b. Wählen Sie unter Ressourcen wie folgt Ressourcen aus, die der Ressourcenfreigabe hinzugefügt werden sollen:

      - Wählen Sie unter Ressourcentyp auswählen den Ressourcentyp aus, den Sie gemeinsam nutzen möchten. Dadurch wird die Liste der gemeinsam nutzbaren Ressourcen auf die Ressourcen des ausgewählten Typs gefiltert.
      - Aktivieren Sie in der resultierenden Ressourcenliste die Kontrollkästchen neben den einzelnen Ressourcen, die Sie gemeinsam nutzen möchten. Die ausgewählten Ressourcen werden unter Ausgewählte Ressourcen verschoben.

        Wenn Sie Ressourcen gemeinsam nutzen, die einer bestimmten Availability Zone zugeordnet sind, können Sie mithilfe der Availability Zone ID (AZ ID) den relativen Standort dieser Ressourcen zwischen Konten ermitteln. Weitere Informationen finden Sie unter Availability Zone IDs für Ihre AWS Ressourcen.

   c. (Optional) Um der Ressourcenfreigabe Tags hinzuzufügen, geben Sie unter Tags einen Tag-Schlüssel und einen Tag-Wert ein. Fügen Sie weitere hinzu, indem Sie Neues Tag hinzufügen wählen. Wiederholen Sie diesen Schritt nach Bedarf. Diese Tags gelten nur für die Ressourcenfreigabe selbst, nicht für die Ressourcen in der Ressourcenfreigabe.
5. Wählen Sie Weiter aus.
6. In Schritt 2: Ordnen Sie jedem Ressourcentyp eine verwaltete Berechtigung zu, können Sie wählen, ob Sie dem Ressourcentyp eine verwaltete Berechtigung zuordnen, eine bestehende

vom AWS Kunden verwaltete Berechtigung auswählen oder Ihre eigene vom Kunden verwaltete Berechtigung für unterstützte Ressourcentypen erstellen möchten. Weitere Informationen finden Sie unter Arten von verwalteten Berechtigungen.

Wählen Sie Vom Kunden verwaltete Berechtigung erstellen aus, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls zum Teilen entspricht. Weitere Informationen finden Sie unter Erstellen Sie eine vom Kunden verwaltete Berechtigung. Wählen Sie

nach Abschluss des Vorgangs Ihre neue vom Kunden verwaltete Berechtigung aus der Dropdownliste Verwaltete Berechtigungen aus.

> **Note**
>
> Wenn die ausgewählte verwaltete Berechtigung mehrere Versionen hat, wird AWS RAM automatisch die Standardversion angehängt. Sie können nur die Version anhängen, die als Standardversion festgelegt wurde.

Um die Aktionen anzuzeigen, die die verwaltete Berechtigung zulässt, erweitern Sie die Option Richtlinienvorlage für diese verwaltete Berechtigung anzeigen.

7. Wählen Sie Weiter aus.
8. Gehen Sie in Schritt 3: Prinzipalen Zugriff gewähren wie folgt vor:

   a. Standardmäßig ist Freigabe für alle zulassen aktiviert, was bedeutet, dass Sie für die Ressourcentypen, die dies unterstützen, Ressourcen mit Ressourcen teilen können, AWS-Konten die sich außerhalb Ihrer Organisation befinden. Dies wirkt sich nicht auf Ressourcentypen aus, die nur innerhalb einer Organisation gemeinsam genutzt werden können, wie z. B. Amazon VPC-Subnetze. Sie können einige unterstützte Ressourcentypen auch für IAM-Rollen und -Benutzer freigeben.

      Um die gemeinsame Nutzung von Ressourcen auf Konten und Prinzipale in Ihrer Organisation zu beschränken, wählen Sie Freigabe nur innerhalb Ihrer Organisation zulassen aus.

   b. Gehen Sie für Principals wie folgt vor:

- Um die Organisation, eine Organisationseinheit (OU) oder eine Organisation, AWS-Konto die Teil einer Organisation ist, hinzuzufügen, aktivieren Sie die Option Organisationsstruktur anzeigen. Dadurch wird eine Strukturansicht Ihrer Organisation angezeigt. Aktivieren Sie dann das Kontrollkästchen neben jedem Prinzipal, den Sie hinzufügen möchten.

  > **Important**
  >
  > Wenn Sie Inhalte für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im Freigabekonto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet. `"Principal": "*"` Weitere Informationen finden Sie unter Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie. Principals in den anderen Accounts, die diese Nutzung nutzen, erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen `Allow` Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

  - Wenn Sie die Organisation auswählen (die ID beginnt mito-), können Prinzipale in der gesamten AWS-Konten Organisation auf die Ressourcenfreigabe zugreifen.
  - Wenn Sie eine Organisationseinheit auswählen (die ID beginnt mitou-), OUs können alle Prinzipale AWS-Konten in dieser Organisationseinheit und der zugehörigen untergeordneten Organisationseinheit auf die Ressourcenfreigabe zugreifen.
  - Wenn Sie eine Einzelperson auswählen AWS-Konto, können nur Principals in diesem Konto auf die Ressourcenfreigabe zugreifen.

> **Note**
>
> Die Option „Organisationsstruktur anzeigen“ wird nur angezeigt, wenn „Teilen mit“ aktiviert AWS Organizations ist und Sie beim Verwaltungskonto der Organisation angemeldet sind.
> Sie können diese Methode nicht verwenden, um eine Rolle oder einen Benutzer AWS-Konto außerhalb Ihrer Organisation oder eines IAM-Benutzers anzugeben. Stattdessen müssen Sie die Option Organisationsstruktur anzeigen deaktivieren und die Dropdownliste und das Textfeld verwenden, um die ID oder den ARN einzugeben.

- Um einen Prinzipal nach ID oder ARN anzugeben, einschließlich Prinzipalen, die sich außerhalb der Organisation befinden, wählen Sie für jeden Prinzipal den Prinzipaltyp aus. Geben Sie als Nächstes die ID (für eine AWS-Konto Organisation oder OU) oder den ARN (für eine IAM-Rolle oder einen IAM-Benutzer) ein und wählen Sie dann Hinzufügen aus. Die verfügbaren Prinzipaltypen sowie ID- ARN ARN-Formate lauten wie folgt:
  - AWS-Konto— Um eine hinzuzufügen AWS-Konto, geben Sie die 12-stellige Konto-ID ein. Beispiel:

    ```
    123456789012
    ```

  - Organisation — Um alle zu Ihrer Organisation hinzuzufügen, geben Sie die ID der Organisation ein. AWS-Konten Beispiel:

    ```
    o-abcd1234
    ```

  - Organisationseinheit (OU) — Um eine OU hinzuzufügen, geben Sie die ID der OU ein. Beispiel:

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

  - IAM-Rolle — Um eine IAM-Rolle hinzuzufügen, geben Sie den ARN der Rolle ein. Verwenden Sie die folgende Syntax:

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

    Beispiel:

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

> **Note**
>
> Um den eindeutigen ARN für eine IAM-Rolle abzurufen, zeigen Sie die Rollenliste in der IAM-Konsole an, verwenden Sie den AWS CLI Befehl get-role oder die GetRoleAPI-Aktion.

- IAM-Benutzer — Um einen IAM-Benutzer hinzuzufügen, geben Sie den ARN des Benutzers ein. Verwenden Sie die folgende Syntax:

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

  Beispiel:

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

> **Note**
>
> Um den eindeutigen ARN für einen IAM-Benutzer zu erhalten, zeigen Sie die Benutzerliste in der IAM-Konsole an, verwenden Sie den get-user AWS CLI Befehl oder die GetUserAPI-Aktion.

- Service Principal — Um einen Service Principal hinzuzufügen, wählen Sie Service Principal aus der Dropbox Select Principal Type aus. Geben Sie den Namen des AWS Dienstprinzipals ein. Verwenden Sie die folgende Syntax:
  - *`service-id`*`.amazonaws.com`

    Beispiel:

    `pca-connector-ad.amazonaws.com`

c. Stellen Sie unter Ausgewählte Prinzipale sicher, dass die von Ihnen angegebenen Prinzipale in der Liste angezeigt werden.

9. Wählen Sie Weiter aus.
10. Überprüfen Sie in Schritt 4: Überprüfen und erstellen die Konfigurationsdetails für Ihre Ressourcenfreigabe. Um die Konfiguration für einen beliebigen Schritt zu ändern, wählen Sie den Link, der dem Schritt entspricht, zu dem Sie zurückkehren möchten, und nehmen Sie die erforderlichen Änderungen vor.

11. Nachdem Sie die Überprüfung der Ressourcenfreigabe abgeschlossen haben, wählen Sie Ressourcenfreigabe erstellen aus.

    Es kann einige Minuten dauern, bis die Ressourcen- und Prinzipal-Zuordnungen abgeschlossen ist. Warten Sie, bis dieser Vorgang abgeschlossen ist, bevor Sie versuchen, die Ressourcenfreigabe zu verwenden.

12. Sie können jederzeit Ressourcen und Principals hinzufügen und entfernen oder benutzerdefinierte Tags auf Ihre Resource Share anwenden. Sie können die verwalteten Berechtigungen für Ressourcentypen ändern, die in Ihrer Ressourcenfreigabe enthalten sind, und zwar für Typen, die mehr als die standardmäßige verwaltete Berechtigung unterstützen. Sie können Ihre Ressourcenfreigabe löschen, wenn Sie die Ressourcen nicht mehr gemeinsam nutzen möchten. Weitere Informationen finden Sie unter Teilen Sie AWS Ressourcen, die Ihnen gehören.

AWS CLI

Um eine gemeinsame Nutzung einer Ressource zu erstellen

Verwenden Sie den Befehl create-resource-share. Mit dem folgenden Befehl wird eine Ressourcenfreigabe erstellt, die von allen Mitgliedern der AWS-Konten Organisation gemeinsam genutzt wird. Die gemeinsame Nutzung enthält eine AWS License Manager Lizenzkonfiguration und gewährt die standardmäßigen verwalteten Berechtigungen für diesen Ressourcentyp.

> **Note**
>
> Wenn Sie eine vom Kunden verwaltete Berechtigung mit einem Ressourcentyp in dieser Ressourcenfreigabe verwenden möchten, können Sie entweder eine vorhandene vom Kunden verwaltete Berechtigung verwenden oder eine neue vom Kunden verwaltete Berechtigung erstellen. Notieren Sie sich den ARN für die vom Kunden verwaltete Berechtigung und erstellen Sie dann die Ressourcenfreigabe. Weitere Informationen finden Sie unter Erstellen Sie eine vom Kunden verwaltete Berechtigung.

```
$ 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"
    }
}
```

Nutzung gemeinsam genutzter AWS Ressourcen

Führen Sie die folgenden Aufgaben aus, um mit der Nutzung von Ressourcen zu beginnen AWS Resource Access Manager, die mit Ihrem Konto geteilt wurden.

Aufgaben

- Antworten Sie auf die Einladung zur gemeinsamen Nutzung von Ressourcen
- Verwenden Sie die Ressourcen, die mit Ihnen gemeinsam genutzt werden

Antworten Sie auf die Einladung zur gemeinsamen Nutzung von Ressourcen

Wenn Sie eine Einladung erhalten, einer Resource Share beizutreten, müssen Sie diese annehmen, um Zugriff auf die gemeinsam genutzten Ressourcen zu erhalten.

Einladungen werden in den folgenden Szenarien nicht verwendet:

- Wenn Sie Teil einer Organisation in Ihrer Organisation sind AWS Organizations und das Teilen in Ihrer Organisation aktiviert ist, erhalten Prinzipale in der Organisation automatisch ohne Einladungen Zugriff auf die gemeinsam genutzten Ressourcen.

- Wenn Sie die Ressource mit dem teilen AWS-Konto , dem die Ressource gehört, erhalten die Prinzipale in diesem Konto automatisch und ohne Einladungen Zugriff auf die gemeinsam genutzten Ressourcen.

Console

Um auf Einladungen zu antworten

1. Öffnen Sie in der AWS RAM Konsole die Seite Für mich freigegeben: Gemeinsam genutzte Ressourcen.

   > **Note**
   >
   > Eine gemeinsam genutzte Ressource ist nur in der Datei sichtbar, AWS-Region in der sie erstellt wurde. Wenn eine erwartete Ressourcenfreigabe nicht in der Konsole angezeigt wird, müssen Sie möglicherweise AWS-Region mithilfe des Dropdown-Steuerelements in der oberen rechten Ecke zu einer anderen wechseln.

2. Sehen Sie sich die Liste der Ressourcenfreigaben an, auf die Sie Zugriff erhalten haben.

   In der Spalte Status wird Ihr aktueller Teilnahmestatus für die Ressourcenfreigabe angezeigt. Der `Pending` Status gibt an, dass Sie zu einer Resource Share hinzugefügt wurden, die Einladung jedoch noch nicht angenommen oder abgelehnt haben.

3. Um auf die Einladung zur Ressourcenfreigabe zu antworten, wählen Sie die Resource Share-ID aus und wählen Sie Resource Share annehmen, um die Einladung anzunehmen, oder Resource Share ablehnen, um die Einladung abzulehnen. Wenn Sie die Einladung ablehnen, erhalten Sie keinen Zugriff auf die Ressourcen. Wenn Sie die Einladung annehmen, erhalten Sie Zugriff auf die Ressourcen.

AWS CLI

Besorgen Sie sich zunächst eine Liste der Resource Share-Einladungen, die Ihnen zur Verfügung stehen. Der folgende Beispielbefehl wurde in der `us-west-2` Region ausgeführt und zeigt, dass eine Ressourcenfreigabe im `PENDING` Bundesstaat verfügbar ist.

```
$ 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"
        }
    ]
}
```

Sie können den Amazon-Ressourcennamen (ARN) der Einladung aus dem vorherigen Befehl als Parameter im nächsten Befehl verwenden, um diese Einladung anzunehmen.

```
$ 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"
    }
}
```

Die Ausgabe zeigt, dass der geändert `status` wurde zu`ACCEPTED`. Die Ressourcen, die in dieser Ressourcenfreigabe enthalten sind, stehen nun den Prinzipalen im akzeptierenden Konto zur Verfügung.

Verwenden Sie die Ressourcen, die mit Ihnen gemeinsam genutzt werden

Nachdem Sie die Einladung zum Beitritt zu einer gemeinsamen Ressource angenommen haben, können Sie bestimmte Aktionen für die gemeinsam genutzten Ressourcen ausführen. Diese Aktionen variieren je nach Ressourcentyp. Weitere Informationen finden Sie unter Gemeinsam nutzbare Ressourcen AWS. Die Ressourcen sind direkt in der Servicekonsole und in den API/CLI Betriebsabläufen der einzelnen Ressourcen verfügbar. Wenn es sich um eine regionale Ressource handelt, müssen Sie den richtigen Befehl AWS-Region in der Servicekonsole oder im API/CLI-Befehl verwenden. Wenn es sich um eine globale Ressource handelt, müssen Sie die angegebene Heimatregion USA Ost (Nord-Virginia) verwenden. `us-east-1` Um die Ressource anzuzeigen AWS RAM, müssen Sie die AWS RAM Konsole öffnen, in der AWS-Region die Ressourcenfreigabe erstellt wurde.

Mit gemeinsam genutzten AWS Ressourcen arbeiten

Sie können AWS Resource Access Manager (AWS RAM) verwenden, um AWS Ressourcen, die Ihnen gehören, gemeinsam zu nutzen und auf AWS Ressourcen zuzugreifen, die mit Ihnen geteilt wurden.

Inhalt

Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen

In diesem Thema werden die Unterschiede bei der Verwendung von AWS Resource Access Manager (AWS RAM) mit regionalen und globalen Ressourcen erörtert.

Ressourcen sind entweder regional oder global. Sie können das vierte Feld im Amazon-Ressourcennamen (ARN) verwenden, um zu identifizieren, ob es sich um eine regionale oder globale Ressource handelt. Regionale Ressourcen zeigen die AWS-Region. Wenn es leer ist, ist die Ressource global.

Was sind die Unterschiede zwischen regionalen und globalen Ressourcen?

Regionale Ressourcen

Die meisten Ressourcen, mit denen Sie Inhalte teilen können, AWS RAM sind regional. Sie erstellen sie in einer bestimmten AWS-Region und sie sind dann in dieser Region vorhanden. Um diese Ressourcen aufzurufen oder mit ihnen zu interagieren, müssen Sie Ihre Aktivitäten auf diese Region ausrichten. Um beispielsweise eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance mit dem zu erstellen AWS-Managementkonsole, wählen Sie AWS-Region die aus, in der Sie die Instance erstellen möchten. Wenn Sie das AWS Command Line Interface (AWS CLI) verwenden, um die Instance zu erstellen, fügen Sie den `--region` Parameter hinzu. Sie verfügen AWS SDKs jeweils über einen eigenen, äquivalenten Mechanismus zur Angabe der Region, die von der Operation verwendet wird.

Es gibt mehrere Gründe für die Nutzung regionaler Ressourcen. Ein guter Grund besteht darin, sicherzustellen, dass sich die Ressourcen und die Service-Endpunkte, über die Sie auf sie zugreifen, so nah wie möglich am Kunden befinden. Dies verbessert die Leistung, indem die Latenz minimiert wird. Ein weiterer Grund ist die Bereitstellung einer Isolationsgrenze. Auf diese Weise können Sie unabhängige Kopien von Ressourcen in mehreren Regionen erstellen, um die Last zu verteilen und die Skalierbarkeit zu verbessern. Gleichzeitig werden die Ressourcen voneinander isoliert, um die Verfügbarkeit zu verbessern.

Wenn Sie AWS-Region in der Konsole oder in einem AWS CLI Befehl einen anderen Wert angeben, können Sie die Ressourcen, die Sie in der vorherigen Region sehen konnten, nicht mehr sehen oder mit ihnen interagieren.

Wenn Sie den Amazon-Ressourcennamen (ARN) für eine regionale Ressource betrachten, wird die Region, die die Ressource enthält, als viertes Feld im ARN angegeben. Eine Amazon-

EC2-Instance ist beispielsweise eine regionale Ressource. Solche Ressourcen haben ARNs ein ähnliches Aussehen wie das folgende Beispiel für eine VPC, die in der `us-east-1` Region existiert.

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

Globale Ressourcen

Einige AWS Dienste unterstützen Ressourcen, auf die Sie global zugreifen können, was bedeutet, dass Sie die Ressource von überall aus verwenden können. Sie geben AWS-Region in der Konsole eines globalen Dienstes keine an. Um auf eine globale Ressource zuzugreifen, geben Sie bei der Verwendung der Service AWS CLI - und AWS SDK-Operationen keinen `--region` Parameter an.

Globale Ressourcen unterstützen Fälle, in denen es entscheidend ist, dass jeweils nur eine Instanz einer bestimmten Ressource existieren kann. In solchen Szenarien ist die Replikation oder Synchronisation zwischen Kopien in verschiedenen Regionen nicht ausreichend. Dass auf einen einzigen globalen Endpunkt zugegriffen werden muss und dadurch potenziell die Latenz erhöht wird, wird als akzeptabel angesehen, um sicherzustellen, dass alle Änderungen für die Nutzer der Ressource sofort sichtbar sind. Wenn Sie beispielsweise ein AWS Cloud-WAN-Kernnetzwerk als globale Ressource erstellen, ist es für alle Benutzer konsistent. Es erscheint als ein einziges, zusammenhängendes globales Netzwerk in allen Regionen.

Der Amazon-Ressourcenname (ARN) für eine globale Ressource enthält keine Region. Das vierte Feld eines solchen ARN ist leer, z. B. der folgende Beispiel-ARN für ein Cloud-WAN-Kernnetzwerk.

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

Gemeinsam genutzte Ressourcen und ihre Regionen

AWS RAM ist ein regionaler Dienst, und ein Resource Share ist Regional. Daher kann eine Ressourcenfreigabe Ressourcen aus derselben Ressource AWS-Region wie die Ressourcenfreigabe und alle unterstützten globalen Ressourcen enthalten. Die Region, in der Sie die Ressourcenfreigabe erstellen, ist die Heimatregion der Ressourcenfreigabe.

> **Important**
>
> Derzeit können Sie Ressourcenfreigaben mit globalen Ressourcen nur in der ausgewiesenen Heimatregion USA Ost (Nord-Virginia), erstellen`us-east-1`. Sie können die Ressourcenfreigabe zwar nur in dieser einzelnen Heimatregion erstellen, aber jede gemeinsam genutzte globale Ressource wird als globale Standardressource angezeigt, wenn sie in der Konsole oder in den CLI- und SDK-Vorgängen dieses Dienstes angezeigt wird. Die Beschränkung auf die Heimatregion gilt nur für die gemeinsam genutzte Ressource, nicht für die darin enthaltenen Ressourcen.

Um eine regionale Ressource, die Sie in der `us-west-2` Region erstellt haben, gemeinsam zu nutzen, müssen Sie die AWS RAM Konsole so konfigurieren, dass die Ressourcenfreigabe dort verwendet `us-west-2` und erstellt wird. Sie können keine Ressourcenfreigabe erstellen, die regionale Ressourcen aus anderen Ländern umfasst AWS-Regionen. Das bedeutet, dass Sie zwei unterschiedliche Ressourcenfreigaben erstellen müssen`eu-north-1`, um Ressourcen aus beiden `us-west-2` Quellen gemeinsam zu nutzen. Sie können Ressourcen aus zwei verschiedenen Regionen nicht zu einer einzigen gemeinsamen Nutzung kombinieren.

Um eine globale Ressource in der AWS RAM Konsole gemeinsam zu nutzen, müssen Sie die AWS RAM Konsole so konfigurieren, dass sie die angegebene Heimatregion USA Ost (Nord-Virginia) verwendet`us-east-1`. Erstellen Sie dann die gemeinsame Nutzung der Ressource in der angegebenen Heimatregion. Sie können globale Ressourcen in einer Ressourcenfreigabe nur mit Ressourcen aus der `us-east-1` Region kombinieren.

Auch wenn die globale Ressource nur in der angegebenen Heimatregion in einer gemeinsamen AWS RAM Ressource sichtbar ist, handelt es sich auch nach der gemeinsamen Nutzung um eine globale Ressource. Sie können in der geteilten Version AWS-Konten von jeder Region aus darauf zugreifen, von der aus Sie auch im Original darauf zugreifen konnten AWS-Konto.

Überlegungen

- Um eine Ressourcenfreigabe in der AWS RAM Konsole zu erstellen, müssen Sie die Region verwenden, die die Ressourcen enthält, die Sie teilen möchten. Wenn Sie eine globale Ressource hinzufügen möchten, müssen Sie die angegebene Heimatregion verwenden, um die gemeinsame Nutzung zu erstellen. Um beispielsweise ein AWS Cloud-WAN-Kernnetzwerk gemeinsam zu nutzen, müssen Sie die Ressourcenfreigabe in der `us-east-1` Region erstellen.

- Um eine Ressourcenfreigabe in der AWS RAM Konsole anzuzeigen oder zu ändern, müssen Sie die Region verwenden, die die Ressourcenfreigabe enthält. In ähnlicher Weise können Sie mit den SDK-Vorgängen AWS RAM AWS CLI und nur mit Ressourcenfreigaben interagieren, die sich in der Region befinden, die Sie in Ihrem Vorgang angegeben haben. Um Ressourcenfreigaben, die globale Ressourcen enthalten, anzuzeigen oder zu ändern, müssen Sie die angegebene Heimatregion, USA Ost (Nord-Virginia), verwenden`us-east-1`.
- Um eine regionale Ressource in der AWS RAM Konsole anzuzeigen und sie in eine Ressourcenfreigabe aufzunehmen, müssen Sie die Region verwenden, in der sich die regionale Ressource befindet.
- Um eine globale Ressource in der AWS RAM Konsole anzuzeigen und sie in eine Ressourcenfreigabe aufzunehmen, müssen Sie die angegebene Heimatregion, USA Ost (Nord-Virginia), angeben`us-east-1`.
- Sie können eine gemeinsame Nutzung von Ressourcen sowohl mit regionalen als auch mit globalen Ressourcen nur in der angegebenen Heimatregion, USA Ost (Nord-Virginia), erstellen`us-east-1`.

Teilen Sie AWS Ressourcen, die Ihnen gehören

Sie können AWS Resource Access Manager (AWS RAM) verwenden, um die von Ihnen angegebenen Ressourcen mit den von Ihnen angegebenen Prinzipalen gemeinsam zu nutzen. In diesem Abschnitt wird beschrieben, wie Sie neue Ressourcenfreigaben erstellen, bestehende Ressourcenfreigaben ändern und nicht mehr benötigte Ressourcenfreigaben löschen können.

Themen

Ressourcenfreigaben anzeigen, die Sie erstellt haben in AWS RAM

Sie können eine Liste der von Ihnen erstellten Ressourcenfreigaben anzeigen. Sie können sehen, welche Ressourcen Sie gemeinsam nutzen und mit welchen Prinzipalen sie gemeinsam genutzt werden.

Console

Um deine gemeinsam genutzten Ressourcen einzusehen

1. Öffnen Sie in der AWS RAM Konsole die Seite Von mir geteilt: Ressourcenfreigaben.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wenn für eine der verwalteten Berechtigungen, die von den Ressourcenfreigaben in den Ergebnissen verwendet werden, eine neue Version der verwalteten Berechtigung vorhanden ist, die als Standard festgelegt wurde, wird auf der Seite ein Banner angezeigt, um Sie darauf hinzuweisen. Sie können alle Versionen mit verwalteten Berechtigungen gleichzeitig aktualisieren, indem Sie oben auf der Seite auf Alle überprüfen und aktualisieren klicken.

   Alternativ wird für einzelne gemeinsam genutzte Ressourcen mit einer oder mehreren neuen Versionen verwalteter Berechtigungen in der Spalte Status der Eintrag Update verfügbar angezeigt. Wenn Sie auf diesen Link klicken, werden die aktualisierten Versionen mit verwalteten Berechtigungen überprüft. Sie können sie dann als Versionen für die relevanten Ressourcentypen in dieser einen Ressourcenfreigabe zuweisen.
4. (Optional) Wenden Sie einen Filter an, um nach bestimmten Ressourcenfreigaben zu suchen. Sie können mehrere Filter anwenden, um die Suche zu verfeinern. Sie können ein Schlüsselwort eingeben, z. B. einen Teil eines Ressourcenfreigabenamens, um nur die Ressourcenfreigaben aufzulisten, die diesen Text im Namen enthalten. Wählen Sie das Textfeld aus, um eine Dropdownliste mit vorgeschlagenen Attributfeldern anzuzeigen. Nachdem Sie einen ausgewählt haben, können Sie aus der Liste der verfügbaren Werte für dieses Feld auswählen. Sie können weitere Attribute oder Schlüsselwörter hinzufügen, bis Sie die gewünschte Ressource gefunden haben.

5. Wählen Sie den Namen der Ressourcenfreigabe, die Sie überprüfen möchten. In der Konsole werden die folgenden Informationen zur Ressourcenfreigabe angezeigt:

   - Zusammenfassung — Listet den Namen, die ID, den Besitzer, den Amazon-Ressourcennamen (ARN), das Erstellungsdatum, ob die gemeinsame Nutzung mit externen Konten zulässig ist und ihren aktuellen Status auf.
   - Verwaltete Berechtigungen — Listet die verwalteten Berechtigungen auf, die mit dieser Ressourcenfreigabe verknüpft sind. Pro Ressourcentyp kann in der Ressourcenfreigabe maximal eine verwaltete Berechtigung enthalten sein. Jede verwaltete Berechtigung zeigt die Version der verwalteten Berechtigung an, die der Ressourcenfreigabe zugeordnet ist. Wenn es sich nicht um die Standardversion handelt, zeigt die Konsole den Link Auf Standardversion aktualisieren an. Wenn Sie diesen Link wählen, haben Sie die Möglichkeit, die Ressourcenfreigabe so zu aktualisieren, dass sie die Standardversion verwendet.
   - Gemeinsam genutzte Ressourcen — Listet die einzelnen Ressourcen auf, die in der Ressourcenfreigabe enthalten sind. Wählen Sie die ID einer Ressource, um einen neuen Browser-Tab zu öffnen und die Ressource in der Konsole des nativen Dienstes anzuzeigen.
   - Gemeinsam genutzte Principals — Listet die Principals auf, mit denen die Ressourcen gemeinsam genutzt werden.
   - Tags — Listet die Tag-Schlüssel-Wert-Paare auf, die der Resource Share selbst zugeordnet sind. Dabei handelt es sich nicht um die Tags, die den einzelnen in der Resource Share enthaltenen Ressourcen zugeordnet sind.

AWS CLI

Um Ihre Ressourcenfreigaben einzusehen

Sie können den get-resource-sharesBefehl mit dem `--resource-owner` Parameter auf verwenden, `SELF` um Details zu den in Ihrem erstellten Ressourcenfreigaben anzuzeigen AWS-Konto.

Das folgende Beispiel zeigt die Ressourcenfreigaben, die in der aktuellen AWS-Region (`us-east-1`) Datei für den Aufruf gemeinsam genutzt AWS-Konto werden. Verwenden Sie den `--region <region-code>` Parameter, um die in einer anderen Region erstellten Ressourcenfreigaben abzurufen. Um Ressourcenfreigaben einzubeziehen, die globale Ressourcen enthalten, müssen Sie die Region USA Ost (Nord-Virginia), angeben`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"
        }
    ]
}
```

Einen Ressourcenanteil erstellen in AWS RAM

Um Ressourcen, die Ihnen gehören, gemeinsam zu nutzen, erstellen Sie eine Ressourcenfreigabe. Es folgt eine Übersicht über den Prozess:

1. Fügen Sie die Ressourcen hinzu, die Sie teilen möchten.
2. Geben Sie für jeden Ressourcentyp, den Sie in die gemeinsame Nutzung aufnehmen, die verwaltete Berechtigung an, die für diesen Ressourcentyp verwendet werden soll.
   - Sie können zwischen einer der verfügbaren AWS verwalteten Berechtigungen, einer vorhandenen vom Kunden verwalteten Berechtigung wählen oder eine neue vom Kunden verwaltete Berechtigung erstellen.

- AWS verwaltete Berechtigungen werden von erstellt AWS , um Standardanwendungsfälle abzudecken.
- Mit vom Kunden verwalteten Berechtigungen können Sie Ihre eigenen verwalteten Berechtigungen an Ihre Sicherheits- und Geschäftsanforderungen anpassen.

> **Note**
>
> Wenn die ausgewählte verwaltete Berechtigung mehrere Versionen hat, wird AWS RAM automatisch die Standardversion angehängt. Sie können nur die Version anhängen, die als Standardversion festgelegt ist.

3. Geben Sie die Prinzipale an, die Zugriff auf die Ressourcen haben sollen.

Überlegungen

- Wenn Sie später eine AWS Ressource löschen müssen, die Sie in eine Freigabe aufgenommen haben, empfehlen wir, die Ressource zunächst entweder aus einer Ressourcenfreigabe zu entfernen, in der sie enthalten ist, oder die Ressourcenfreigabe zu löschen.
- Die Ressourcentypen, die Sie in eine Ressourcenfreigabe aufnehmen können, sind unter aufgeführtGemeinsam nutzbare Ressourcen AWS.
- Sie können eine Ressource nur gemeinsam nutzen, wenn Sie Eigentümer dieser Ressource sind. Sie können eine Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- AWS RAM ist ein regionaler Dienst. Wenn Sie eine Ressource mit Prinzipalen in anderen teilen AWS-Konten, müssen diese Prinzipale auf jede Ressource von derselben Seite aus zugreifen AWS-Region , in der sie erstellt wurde. Auf unterstützte globale Ressourcen können Sie von allen AWS-Region Ressourcen aus zugreifen, die von der Servicekonsole und den Tools der jeweiligen Ressource unterstützt werden. Sie können solche gemeinsam genutzten Ressourcen und ihre globalen Ressourcen in der AWS RAM Konsole und in den Tools nur in der angegebenen Heimatregion, USA Ost (Nord-Virginia), einsehen`us-east-1`. Weitere Informationen zu AWS RAM und globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
- Wenn das Konto, von dem aus Sie Inhalte teilen, Teil einer Organisation in Ihrer Organisation ist AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten alle Prinzipale in der Organisation, für die Sie Inhalte freigeben, automatisch Zugriff auf die Ressourcenfreigaben, ohne dass Einladungen erforderlich sind. Ein Hauptbenutzer in einem Konto, mit dem Sie Inhalte außerhalb des Unternehmenskontextes teilen, erhält eine Einladung

zur Teilnahme an der Resource Share und erhält erst dann Zugriff auf die gemeinsam genutzten Ressourcen, wenn er die Einladung akzeptiert hat.

- Wenn Sie die Ressource mit einem Dienstprinzipal teilen, können Sie der Ressourcenfreigabe keine anderen Prinzipale zuordnen.
- Wenn die gemeinsame Nutzung zwischen Konten oder Prinzipalen erfolgt, die Teil einer Organisation sind, wirken sich alle Änderungen an der Organisationsmitgliedschaft dynamisch auf den Zugriff auf die gemeinsam genutzte Ressource aus.
  - Wenn Sie der Organisation oder Organisationseinheit ein Konto hinzufügen, das Zugriff auf eine Ressourcenfreigabe hat, erhält dieses neue Mitgliedskonto automatisch Zugriff auf die Ressourcenfreigabe. AWS-Konto Der Administrator des Kontos, für das Sie eine gemeinsame Nutzung vorgenommen haben, kann dann einzelnen Prinzipalen in diesem Konto Zugriff auf die Ressourcen in dieser Freigabe gewähren.
  - Wenn Sie ein Konto aus der Organisation oder einer Organisationseinheit entfernen, die Zugriff auf eine Ressourcenfreigabe hat, verlieren alle Prinzipale in diesem Konto automatisch den Zugriff auf Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.
  - Wenn Sie Rollen oder Benutzer im Mitgliedskonto direkt für ein Mitgliedskonto oder für IAM freigegeben haben und dann dieses Konto aus der Organisation entfernen, verlieren alle Principals in diesem Konto den Zugriff auf die Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.

> **Important**
>
> Wenn Sie Daten für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Principals im gemeinsam genutzten Konto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet. `"Principal": "*"` Weitere Informationen finden Sie unter Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie.
>
> Principals in den anderen Accounts, die diese Nutzung nutzen, erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen `Allow` Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der

verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

- Sie können Ihren Ressourcenfreigaben nur die Organisation hinzufügen, der Ihr Konto OUs angehört, und aus dieser Organisation stammen. Sie können einer Ressourcenfreigabe keine Organisationen OUs oder Organisationen von außerhalb Ihrer eigenen Organisation als Prinzipale hinzufügen. Sie können jedoch einzelne AWS-Konten oder, bei unterstützten Diensten, IAM-Rollen und Benutzer von außerhalb Ihrer Organisation als Principals zu einer Ressourcenfreigabe hinzufügen.

  Note

  Nicht alle Ressourcentypen können mit IAM-Rollen und Benutzern geteilt werden. Informationen zu Ressourcen, die Sie mit diesen Prinzipalen gemeinsam nutzen können, finden Sie unter. Gemeinsam nutzbare Ressourcen AWS

- Für die folgenden Ressourcentypen haben Sie sieben Tage Zeit, um die Einladung zur Teilnahme an der Share für die folgenden Ressourcentypen anzunehmen. Wenn du die Einladung nicht annimmst, bevor sie abläuft, wird die Einladung automatisch abgelehnt.

  Important

  Für gemeinsam genutzte Ressourcentypen, die nicht in der folgenden Liste aufgeführt sind, haben Sie 12 Stunden Zeit, um die Einladung zur Teilnahme an der Resource Share anzunehmen. Nach 12 Stunden läuft die Einladung ab und die Zuordnung des Endbenutzer-Hauptbenutzers zur Resource Share wird aufgehoben. Die Einladung kann von Endbenutzern nicht mehr angenommen werden.

  - Amazon Aurora — DB-Cluster
  - Amazon EC2 — Kapazitätsreservierungen und engagierte Gastgeber
  - AWS License Manager — Lizenzkonfigurationen
  - AWS Outposts — Routentabellen, Außenposten und Standorte für lokale Gateways
  - Amazon Route 53 — Speditionsregeln
  - Amazon VPC — Kundeneigene IPv4 Adressen, Präfixlisten, Subnetze, Traffic Mirror-Ziele, Transit-Gateways, Transit-Gateway-Multicast-Domänen

Console

Um eine Ressourcenfreigabe zu erstellen

1. Öffnen Sie die AWS RAM -Konsole.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen. Wenn Sie globale Ressourcen in die gemeinsame Nutzung von Ressourcen einbeziehen möchten, müssen Sie die angegebene Heimatregion, USA Ost (Nord-Virginia), auswählen`us-east-1`.
3. Wenn Sie noch keine Erfahrung damit haben AWS RAM, wählen Sie auf der Startseite die Option Ressourcenfreigabe erstellen aus. Wählen Sie andernfalls auf der Seite Von mir geteilt: Gemeinsam genutzte Ressourcen die Option Ressourcenfreigabe erstellen aus.
4. Gehen Sie in Schritt 1: Angaben zur Ressourcenfreigabe angeben wie folgt vor:

   a. Geben Sie unter Name einen beschreibenden Namen für die Ressourcenfreigabe ein.

   b. Wählen Sie unter Ressourcen wie folgt Ressourcen aus, die der Ressourcenfreigabe hinzugefügt werden sollen:

      - Wählen Sie unter Ressourcentyp auswählen den Ressourcentyp aus, den Sie gemeinsam nutzen möchten. Dadurch wird die Liste der gemeinsam nutzbaren Ressourcen auf die Ressourcen des ausgewählten Typs gefiltert.
      - Aktivieren Sie in der resultierenden Ressourcenliste die Kontrollkästchen neben den einzelnen Ressourcen, die Sie gemeinsam nutzen möchten. Die ausgewählten Ressourcen werden unter Ausgewählte Ressourcen verschoben.

        Wenn Sie Ressourcen gemeinsam nutzen, die einer bestimmten Availability Zone zugeordnet sind, können Sie mithilfe der Availability Zone ID (AZ-ID) den relativen Standort dieser Ressourcen zwischen Konten ermitteln. Weitere Informationen finden Sie unter Availability Zone IDs für Ihre AWS Ressourcen.

   c. (Optional) Um der Ressourcenfreigabe Tags hinzuzufügen, geben Sie unter Tags einen Tag-Schlüssel und einen Tag-Wert ein. Fügen Sie weitere hinzu, indem Sie Neues Tag hinzufügen wählen. Wiederholen Sie diesen Schritt nach Bedarf. Diese Tags gelten nur für die Ressourcenfreigabe selbst, nicht für die Ressourcen in der Ressourcenfreigabe.

5. Wählen Sie Weiter aus.
6. In Schritt 2: Ordnen Sie jedem Ressourcentyp eine verwaltete Berechtigung zu, können Sie wählen, ob Sie dem Ressourcentyp eine verwaltete Berechtigung zuordnen, eine bestehende vom AWS Kunden verwaltete Berechtigung auswählen oder Ihre eigene vom Kunden verwaltete Berechtigung für unterstützte Ressourcentypen erstellen möchten. Weitere Informationen finden Sie unter Arten von verwalteten Berechtigungen.

   Wählen Sie Vom Kunden verwaltete Berechtigung erstellen aus, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls für das Teilen entspricht. Weitere Informationen finden Sie unter Erstellen Sie eine vom Kunden verwaltete Berechtigung. Wählen Sie nach Abschluss des Vorgangs Ihre neue vom Kunden verwaltete Berechtigung aus der Dropdownliste Verwaltete Berechtigungen aus

   und wählen Sie anschließend Ihre neue vom Kunden verwaltete Berechtigung aus.

   > **Note**
   >
   > Wenn die ausgewählte verwaltete Berechtigung mehrere Versionen hat, wird AWS RAM automatisch die Standardversion angehängt. Sie können nur die Version anhängen, die als Standardversion festgelegt wurde.

   Um die Aktionen anzuzeigen, die die verwaltete Berechtigung zulässt, erweitern Sie die Option Richtlinienvorlage für diese verwaltete Berechtigung anzeigen.
7. Wählen Sie Weiter aus.
8. Gehen Sie in Schritt 3: Prinzipalen Zugriff gewähren wie folgt vor:

   a. Standardmäßig ist Freigabe für alle zulassen aktiviert, was bedeutet, dass Sie für die Ressourcentypen, die dies unterstützen, Ressourcen mit Ressourcen teilen können, AWS-Konten die sich außerhalb Ihrer Organisation befinden. Dies wirkt sich nicht auf Ressourcentypen aus, die nur innerhalb einer Organisation gemeinsam genutzt werden können, wie z. B. Amazon VPC-Subnetze. Sie können einige unterstützte Ressourcentypen auch für IAM-Rollen und -Benutzer freigeben.

Um die gemeinsame Nutzung von Ressourcen auf Konten und Prinzipale in Ihrer Organisation zu beschränken, wählen Sie Freigabe nur innerhalb Ihrer Organisation zulassen aus.

b. Gehen Sie für Principals wie folgt vor:

- Um die Organisation, eine Organisationseinheit (OU) oder eine Organisation, AWS-Konto die Teil einer Organisation ist, hinzuzufügen, aktivieren Sie die Option Organisationsstruktur anzeigen. Dadurch wird eine Strukturansicht Ihrer Organisation angezeigt. Aktivieren Sie dann das Kontrollkästchen neben jedem Prinzipal, den Sie hinzufügen möchten.

  > **Important**
  >
  > Wenn Sie Inhalte für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im Freigabekonto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet. `"Principal": "*"` Weitere Informationen finden Sie unter Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie. Principals in den anderen Accounts, die diese Nutzung nutzen, erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen `Allow` Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

- Wenn Sie die Organisation auswählen (die ID beginnt mito-), können Prinzipale in der gesamten AWS-Konten Organisation auf die Ressourcenfreigabe zugreifen.
- Wenn Sie eine Organisationseinheit auswählen (die ID beginnt mitou-), OUs können alle Prinzipale AWS-Konten in dieser Organisationseinheit und der

zugehörigen untergeordneten Organisationseinheit auf die Ressourcenfreigabe zugreifen.

- Wenn Sie eine Einzelperson auswählen AWS-Konto, können nur Principals in diesem Konto auf die Ressourcenfreigabe zugreifen.

> **Note**
>
> Die Option „Organisationsstruktur anzeigen“ wird nur angezeigt, wenn „Teilen mit“ aktiviert AWS Organizations ist und Sie beim Verwaltungskonto der Organisation angemeldet sind.
> Sie können diese Methode nicht verwenden, um eine Rolle oder einen Benutzer AWS-Konto außerhalb Ihrer Organisation oder eines IAM-Benutzers anzugeben. Stattdessen müssen Sie die Option Organisationsstruktur anzeigen deaktivieren und die Dropdownliste und das Textfeld verwenden, um die ID oder den ARN einzugeben.

- Um einen Prinzipal nach ID oder ARN anzugeben, einschließlich Prinzipalen, die sich außerhalb der Organisation befinden, wählen Sie für jeden Prinzipal den Prinzipaltyp aus. Geben Sie als Nächstes die ID (für eine AWS-Konto Organisation oder OU) oder den ARN (für eine IAM-Rolle oder einen IAM-Benutzer) ein und wählen Sie dann Hinzufügen aus. Die verfügbaren Prinzipaltypen sowie ID- ARN ARN-Formate lauten wie folgt:
  - AWS-Konto— Um eine hinzuzufügen AWS-Konto, geben Sie die 12-stellige Konto-ID ein. Zum Beispiel:

    ```
    123456789012
    ```

  - Organisation — Um alle zu Ihrer Organisation hinzuzufügen, geben Sie die ID der Organisation ein. AWS-Konten Zum Beispiel:

    ```
    o-abcd1234
    ```

  - Organisationseinheit (OU) — Um eine OU hinzuzufügen, geben Sie die ID der OU ein. Zum Beispiel:

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

  - IAM-Rolle — Um eine IAM-Rolle hinzuzufügen, geben Sie den ARN der Rolle ein. Verwenden Sie die folgende Syntax:

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

Zum Beispiel:

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

> **Note**
>
> Um den eindeutigen ARN für eine IAM-Rolle abzurufen, zeigen Sie die Rollenliste in der IAM-Konsole an, verwenden Sie den AWS CLI Befehl get-role oder die GetRoleAPI-Aktion.

- IAM-Benutzer — Um einen IAM-Benutzer hinzuzufügen, geben Sie den ARN des Benutzers ein. Verwenden Sie die folgende Syntax:

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

  Zum Beispiel:

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

  > **Note**
  >
  > Um den eindeutigen ARN für einen IAM-Benutzer zu erhalten, zeigen Sie die Benutzerliste in der IAM-Konsole an, verwenden Sie den get-user AWS CLI Befehl oder die GetUserAPI-Aktion.

- Service Principal — Um einen Service Principal hinzuzufügen, wählen Sie Service Principal aus der Dropbox Select Principal Type aus. Geben Sie den Namen des AWS Dienstprinzipals ein. Verwenden Sie die folgende Syntax:
  - `service-id.amazonaws.com`

    Zum Beispiel:

    `pca-connector-ad.amazonaws.com`

c. Stellen Sie unter Ausgewählte Prinzipale sicher, dass die von Ihnen angegebenen Prinzipale in der Liste angezeigt werden.

9. Wählen Sie Weiter aus.
10. Überprüfen Sie in Schritt 4: Überprüfen und erstellen die Konfigurationsdetails für Ihre Ressourcenfreigabe. Um die Konfiguration für einen beliebigen Schritt zu ändern, wählen Sie den Link, der dem Schritt entspricht, zu dem Sie zurückkehren möchten, und nehmen Sie die erforderlichen Änderungen vor.
11. Nachdem Sie die Überprüfung der Ressourcenfreigabe abgeschlossen haben, wählen Sie Ressourcenfreigabe erstellen aus.

    Es kann einige Minuten dauern, bis die Ressourcen- und Prinzipal-Zuordnungen abgeschlossen ist. Warten Sie, bis dieser Vorgang abgeschlossen ist, bevor Sie versuchen, die Ressourcenfreigabe zu verwenden.
12. Sie können jederzeit Ressourcen und Principals hinzufügen und entfernen oder benutzerdefinierte Tags auf Ihre Resource Share anwenden. Sie können die verwalteten Berechtigungen für Ressourcentypen ändern, die in Ihrer Ressourcenfreigabe enthalten sind, und zwar für die Typen, die mehr als die standardmäßige verwaltete Berechtigung unterstützen. Sie können Ihre Ressourcenfreigabe löschen, wenn Sie die Ressourcen nicht mehr gemeinsam nutzen möchten. Weitere Informationen finden Sie unter Teilen Sie AWS Ressourcen, die Ihnen gehören.

AWS CLI

Um eine gemeinsame Nutzung einer Ressource zu erstellen

Verwenden Sie den create-resource-share-Befehl. Mit dem folgenden Befehl wird eine Ressourcenfreigabe erstellt, die von allen Mitgliedern der AWS-Konten Organisation gemeinsam genutzt wird. Die gemeinsame Nutzung enthält eine AWS License Manager Lizenzkonfiguration und gewährt die standardmäßigen verwalteten Berechtigungen für diesen Ressourcentyp.

> **Note**
>
> Wenn Sie eine vom Kunden verwaltete Berechtigung mit einem Ressourcentyp in dieser Ressourcenfreigabe verwenden möchten, können Sie entweder eine vorhandene vom Kunden verwaltete Berechtigung verwenden oder eine neue vom Kunden verwaltete Berechtigung erstellen. Notieren Sie sich den ARN für die vom Kunden verwaltete Berechtigung und erstellen Sie dann die Ressourcenfreigabe. Weitere Informationen finden Sie unter Erstellen Sie eine vom Kunden verwaltete Berechtigung.

```
$ 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"
    }
}
```

Aktualisieren Sie eine Ressourcenfreigabe in AWS RAM

Sie können eine Ressourcenfreigabe AWS RAM jederzeit auf folgende Weise aktualisieren:

- Sie können einer von Ihnen erstellten Ressourcenfreigabe Prinzipale, Ressourcen oder Tags hinzufügen.
- Bei Ressourcentypen, die mehr als die standardmäßigen AWS verwalteten Berechtigungen unterstützen, können Sie auswählen, welche verwaltete Berechtigung für die einzelnen Ressourcen gilt.
- Wenn eine verwaltete Berechtigung, die mit der Ressourcenfreigabe verknüpft ist, eine neue Standardversion hat, können Sie die verwaltete Berechtigung aktualisieren, sodass sie die neue Version verwendet.
- Sie können den Zugriff auf gemeinsam genutzte Ressourcen widerrufen, indem Sie Prinzipale oder Ressourcen aus einer Ressourcenfreigabe entfernen. Wenn Sie den Zugriff widerrufen, haben Prinzipale keinen Zugriff mehr auf die gemeinsam genutzten Ressourcen.

> **Note**
>
> Principals, mit denen Sie Ressourcen gemeinsam nutzen, können Ihre Ressourcenfreigabe verlassen, wenn die Freigabe leer ist oder nur Ressourcentypen enthält, die das Verlassen einer Ressourcenfreigabe unterstützen. Wenn die Ressourcenfreigabe Ressourcentypen enthält, die das Verlassen der Ressource nicht unterstützen, wird eine Meldung angezeigt, in der die Hauptbenutzer darüber informiert werden, dass sie sich an den Eigentümer der gemeinsamen Nutzung wenden müssen. In diesem Fall müssen Sie als Eigentümer der Ressourcenfreigabe die Prinzipale aus Ihrer Ressourcenfreigabe entfernen. Eine Liste der Ressourcentypen, die diese Aktion nicht unterstützen, finden Sie unterVoraussetzungen für das Verlassen einer Ressourcenfreigabe.

Console

So aktualisieren Sie eine Ressourcenfreigabe

1. Navigieren Sie in der AWS RAM Konsole zur Seite Von mir geteilt: Ressourcenfreigaben.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wählen Sie die gemeinsam genutzte Ressource aus und klicken Sie dann auf Ändern.
4. Schritt 1: Geben Sie Details zur Ressourcenfreigabe an, überprüfen Sie die Details zur Ressourcenfreigabe und aktualisieren Sie bei Bedarf eine der folgenden Angaben:

   a. (Optional) Um den Namen der Ressourcenfreigabe zu ändern, bearbeiten Sie den Namen.

   b. (Optional) Um der Ressourcenfreigabe eine Ressource hinzuzufügen, wählen Sie unter Ressourcen den Ressourcentyp aus und aktivieren Sie dann das Kontrollkästchen neben der Ressource, um sie der Ressourcenfreigabe hinzuzufügen. Globale Ressourcen werden nur angezeigt, wenn Sie in der die Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzen AWS-Managementkonsole.

c. (Optional) Um eine Ressource aus der Ressourcenfreigabe zu entfernen, suchen Sie die Ressource unter Ausgewählte Ressourcen und wählen Sie dann das X neben der Ressourcen-ID aus.

d. (Optional) Um der Ressourcenfreigabe ein Tag hinzuzufügen, geben Sie unter Tags einen Tag-Schlüssel und einen Tag-Wert in die leeren Textfelder ein. Um mehr als ein Tag-Schlüssel-Wert-Paar hinzuzufügen, wählen Sie Neues Tag hinzufügen aus. Sie können bis zu 50 Tags hinzufügen.

e. Um ein Tag aus der Resource Share zu entfernen, suchen Sie unter Tags das Tag und wählen Sie neben dem Tag die Option Entfernen aus.

5. Wählen Sie Weiter aus.

6. (Optional) In Schritt 2: Ordnen Sie jedem Ressourcentyp eine verwaltete Berechtigung zu, können Sie wählen, ob Sie AWS dem Ressourcentyp eine verwaltete Berechtigung zuordnen, eine bestehende vom Kunden verwaltete Berechtigung auswählen oder Ihre eigene vom Kunden verwaltete Berechtigung erstellen möchten. Weitere Informationen finden Sie unter Arten von verwalteten Berechtigungen.

   Sie können auch vom Kunden verwaltete Berechtigung erstellen auswählen, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls für das Teilen entspricht. Weitere Informationen finden Sie unter Erstellen Sie eine vom Kunden verwaltete Berechtigung. Nachdem Sie den Vorgang abgeschlossen haben wählen Sie und dann können Sie Ihre neue vom Kunden verwaltete Berechtigung aus der Dropdownliste Verwaltete Berechtigungen auswählen.

   Um die Aktionen anzuzeigen, die die verwaltete Berechtigung zulässt, erweitern Sie die Option Richtlinienvorlage für diese verwaltete Berechtigung anzeigen.

7. Wenn es sich bei der Version der verwalteten Berechtigung, die derzeit der Ressourcenfreigabe zugewiesen ist, nicht um die aktuelle Standardversion handelt, können Sie auf die Standardversion aktualisieren, indem Sie Auf Standardversion aktualisieren klicken.

> **Note**
>
> Bis Sie Ihre Änderungen an der Ressourcenfreigabe nach dem letzten Schritt gespeichert haben, können Sie das Versionsupdate abbrechen, indem Sie Auf

vorherige Version zurücksetzen klicken. Bei AWS verwalteten Berechtigungen ist die Änderung jedoch nach dem Speichern der Ressourcenfreigabe endgültig und Sie können nicht mehr zur vorherigen Version zurückkehren.

8. Wählen Sie Weiter aus.
9. Schritt 3: Wählen Sie die Principals aus, die Zugriff haben, überprüfen Sie die ausgewählten Principals und aktualisieren Sie bei Bedarf eines der folgenden Elemente:

   a. (Optional) Um zu ändern, ob die gemeinsame Nutzung für Prinzipale innerhalb oder außerhalb Ihrer Organisation aktiviert ist, wählen Sie eine der folgenden Optionen:

      - Um Ressourcen mit AWS-Konten oder einzelnen IAM-Rollen oder Benutzern außerhalb Ihrer Organisation gemeinsam zu nutzen, wählen Sie Gemeinsame Nutzung mit externen Prinzipalen zulassen aus.
      - Um die gemeinsame Nutzung von Ressourcen auf Prinzipale in Ihrer Organisation zu beschränken AWS Organizations, wählen Sie Nur gemeinsame Nutzung mit Prinzipalen in Ihrer Organisation zulassen aus.

   b. Gehen Sie für Principals wie folgt vor:

      - (Optional) Um eine Organisation, eine Organisationseinheit (OU) oder ein Mitglied AWS-Konto innerhalb Ihrer Organisation hinzuzufügen, aktivieren Sie die Option Organisationsstruktur anzeigen, um eine Strukturansicht Ihrer Organisation anzuzeigen. Aktivieren Sie dann das Kontrollkästchen neben jedem Prinzipal, den Sie hinzufügen möchten.

        Important

        Wenn Sie Daten für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im Freigabekonto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet. `"Principal": "*"` Weitere Informationen finden Sie unter Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten Richtlinie.

Principals in den anderen Accounts, die diese Nutzung nutzen, erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen `Allow` Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

> **Note**
>
> Die Option Organisationsstruktur anzeigen wird nur angezeigt, wenn das Teilen mit aktiviert AWS Organizations ist und Sie als Hauptbenutzer im Verwaltungskonto der Organisation angemeldet sind.
> Sie können diese Methode nicht verwenden, um eine Rolle oder einen Benutzer AWS-Konto außerhalb Ihrer Organisation oder eines IAM-Benutzers anzugeben. Stattdessen müssen Sie diese Hauptbenutzer hinzufügen, indem Sie ihre Kennungen eingeben, die im Textfeld unter dem Schalter Organisationsstruktur anzeigen angezeigt werden. Sehen Sie sich den nächsten Aufzählungspunkt an.

- (Optional) Um einen Prinzipal anhand seiner ID hinzuzufügen, wählen Sie den Prinzipaltyp aus der Dropdownliste aus und geben Sie dann die ID oder den ARN für den Prinzipal ein. Wählen Sie abschließend Hinzufügen aus.

  Wenn Sie eine Einzelperson auswählen AWS-Konto, kann nur dieses Konto auf den Resource Share zugreifen. Sie können eine der folgenden Optionen wählen.

  - Andere AWS-Konto (nicht der Besitzer der Ressource) — Macht die Ressource für das andere Konto verfügbar. Der Administrator dieses Kontos muss den Vorgang abschließen, indem er einzelnen Rollen und Benutzern mithilfe identitätsbasierter Berechtigungsrichtlinien Zugriff auf die gemeinsam genutzte Ressource gewährt. Diese Berechtigungen dürfen nicht höher sein als diejenigen, die in den verwalteten Berechtigungen definiert sind, die der Ressourcenfreigabe zugeordnet sind.

- Dieser AWS-Konto (Ressourcenbesitzer) — Alle Rollen und Benutzer im Konto, dem die Ressource gehört, erhalten automatisch den Zugriff, der durch die verwalteten Berechtigungen definiert ist, die der Ressourcenfreigabe zugeordnet sind.
- Der Zusatz wird sofort in der Liste Ausgewählte Hauptbenutzer angezeigt.

  Sie können dann weitere Konten oder Ihre Organisation hinzufügen OUs, indem Sie diesen Schritt wiederholen.
- (Optional) Um einen Hauptbenutzer zu entfernen, suchen Sie ihn unter Ausgewählte Hauptbenutzer, aktivieren Sie das entsprechende Kontrollkästchen und wählen Sie dann Abwählen aus.

10. Wählen Sie Weiter aus.
11. Überprüfen Sie in Schritt 4: Überprüfen und aktualisieren die Konfigurationsdetails für Ihre Ressourcenfreigabe.
12. Um die Konfiguration für einen beliebigen Schritt zu ändern, wählen Sie den Link, der dem Schritt entspricht, zu dem Sie zurückkehren möchten, und nehmen Sie dann die erforderlichen Änderungen vor.

    Wenn verwaltete Berechtigungen immer noch andere Versionen als die Standardversion verwenden, haben Sie eine weitere Möglichkeit, dies zu beheben, indem Sie Auf Standardversion aktualisieren klicken.
13. Wählen Sie „Ressourcenfreigabe aktualisieren“, wenn Sie mit den Änderungen fertig sind.

AWS CLI

Um eine Ressourcenfreigabe zu aktualisieren

Sie können die folgenden AWS CLI Befehle verwenden, um eine Ressourcenfreigabe zu ändern:

- Verwenden Sie den Befehl update-resource-share, um eine Ressourcenfreigabe umzubenennen oder um zu ändern, ob externe Principals zulässig sind. Das folgende Beispiel benennt die angegebene Ressourcenfreigabe um und legt fest, dass nur Prinzipale aus ihrer Organisation zugelassen werden. Sie müssen den Dienstendpunkt für den verwenden AWS-Region , der die Ressourcenfreigabe enthält.

```
$ 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
    }
}
```

- Verwenden Sie den Befehl, um einer Ressourcenfreigabe eine Ressource hinzuzufügen associate-resource-share. Das folgende Beispiel fügt der angegebenen Ressourcenfreigabe ein Subnetz hinzu.

```
$ 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
    ]
}
```

- Verwenden Sie die Befehle list-permissionsund, um eine verwaltete Berechtigung für einen Ressourcentyp in einer Ressourcenfreigabe hinzuzufügen oder zu ersetzen. associate-resource-share-permission Sie können nur eine verwaltete Berechtigung pro Ressourcentyp in einer Ressourcenfreigabe zuweisen. Wenn Sie versuchen, einem Ressourcentyp, der bereits

über eine verwaltete Berechtigung verfügt, eine verwaltete Berechtigung hinzuzufügen, müssen Sie die `--replace` Option angeben, andernfalls schlägt der Befehl mit einem Fehler fehl.

Der folgende Beispielbefehl listet die vier verwalteten Berechtigungen auf, die ARNs für ein Amazon Elastic Compute Cloud (Amazon EC2) -Subnetz verfügbar sind, und verwendet dann eine davon, ARNs um die aktuell zugewiesene AWS verwaltete Berechtigung für diesen Ressourcentyp in der angegebenen Ressourcenfreigabe zu ersetzen.

```
$ 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
}
```

- Verwenden Sie den Befehl disassociate-resource-share, um eine Ressource aus einer Ressourcenfreigabe zu entfernen. Im folgenden Beispiel wird das EC2 Amazon-Subnetz mit dem angegebenen ARN aus der angegebenen Ressourcenfreigabe entfernt.

```
$ 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
    ]
}
```

- Verwenden Sie die Befehle tag-resourceund, um die an eine Ressourcenfreigabe angehängten Tags zu ändern. untag-resource Im folgenden Beispiel wird das Tag `project=lima` zur angegebenen Ressourcenfreigabe hinzugefügt.

  ```
  $ 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
  ```

  Im folgenden Beispiel wird das Tag mit dem Schlüssel von `project` aus der angegebenen Ressourcenfreigabe entfernt.

  ```
  $ 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
  ```

  Die Tagging-Befehle erzeugen keine Ausgabe, wenn sie erfolgreich sind.

Ihre geteilten Ressourcen anzeigen in AWS RAM

Sie können die Liste der einzelnen Ressourcen, die Sie gemeinsam genutzt haben, für alle gemeinsam genutzten Ressourcen einsehen. Anhand der Liste können Sie feststellen, welche Ressourcen Sie derzeit gemeinsam nutzen, in wie vielen Ressourcenfreigaben sie enthalten sind und wie viele Prinzipale Zugriff darauf haben.

Console

Um die Ressourcen anzuzeigen, die Sie derzeit gemeinsam nutzen

1. Öffnen Sie in der AWS RAM Konsole die Seite Von mir geteilt: Gemeinsam genutzte Ressourcen.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Für jede freigegebene Ressource sind die folgenden Informationen verfügbar:

   - Ressourcen-ID — Die ID der Ressource. Wählen Sie die ID einer Ressource, um einen neuen Browser-Tab zu öffnen und die Ressource in der nativen Servicekonsole anzuzeigen.
   - Ressourcentyp — Der Ressourcentyp.
   - Datum der letzten gemeinsamen Nutzung — Das Datum, an dem die Ressource zuletzt gemeinsam genutzt wurde.
   - Ressourcenfreigaben — Die Anzahl der Ressourcenfreigaben, zu denen die Ressource gehört. Um die Liste der Ressourcenfreigaben zu sehen, wählen Sie die Anzahl aus.
   - Principals — Die Anzahl der Principals, die auf die Ressource zugreifen können. Wählen Sie den Wert, um die Principals anzuzeigen.

AWS CLI

Um die Ressourcen anzuzeigen, die Sie gerade teilen

Sie können den Befehl list-resources verwenden, wobei der Parameter auf `--resource-owner` gesetzt ist, um Details `SELF` zu den Ressourcen anzuzeigen, die Sie derzeit gemeinsam nutzen.

Das folgende Beispiel zeigt die Ressourcen, die in den Ressourcenfreigaben in der AWS-Region (`us-east-1`) für den Aufruf enthalten sind. AWS-Konto Verwenden Sie den `--region` *`<region-code>`* Parameter, um die Ressourcen abzurufen, die Sie in einer anderen Region gemeinsam nutzen.

```
$ 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"
        }
    ]
}
```

Prinzipale anzeigen, mit denen Sie Ressourcen teilen, in AWS RAM

Sie können die Principals, mit denen Sie Ihre Ressourcen teilen, für alle gemeinsam genutzten Ressourcen anzeigen. Anhand dieser Prinzipalliste können Sie feststellen, wer Zugriff auf Ihre gemeinsam genutzten Ressourcen hat.

Console

Um die Principals anzuzeigen, mit denen Sie Ressourcen teilen

1. Navigieren Sie in der Konsole zur Seite Von mir geteilt: Prinzipale. AWS RAM
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere

Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.

3. Wenden Sie einen Filter an, um bestimmte Hauptbenutzer zu finden. Sie können mehrere Filter anwenden, um die Suche zu verfeinern. Wählen Sie das Textfeld aus, um eine Dropdownliste mit vorgeschlagenen Attributfeldern anzuzeigen. Nachdem Sie einen ausgewählt haben, können Sie aus der Liste der verfügbaren Werte für dieses Feld auswählen. Sie können weitere Attribute oder Schlüsselwörter hinzufügen, bis Sie die gewünschte Ressource gefunden haben.
4. Für jeden Prinzipal in der Liste zeigt die Konsole die folgenden Informationen an:

   - Prinzipal-ID — Die ID des Prinzipals. Wählen Sie die ID, um einen neuen Browser-Tab zu öffnen, auf dem der Principal in der nativen Konsole angezeigt wird.
   - Ressourcenfreigaben — Die Anzahl der Ressourcenfreigaben, die Sie mit dem angegebenen Prinzipal gemeinsam genutzt haben. Wählen Sie die Anzahl, um die Liste der gemeinsam genutzten Ressourcen anzuzeigen.
   - Ressourcen — Die Anzahl der Ressourcen, die Sie mit dem Principal geteilt haben. Wählen Sie die Anzahl, um die Liste der gemeinsam genutzten Ressourcen anzuzeigen.

AWS CLI

Um die Principals anzuzeigen, mit denen Sie Ressourcen teilen

Sie können den Befehl list-principals verwenden, um eine Liste der Principals abzurufen, auf die Sie in Resource Shares verweisen, die Sie in der aktuellen AWS-Region Version für das aufrufende Konto erstellt haben.

Im folgenden Beispiel werden die Principals aufgeführt, die Zugriff auf Shares haben, die in der Standardregion für das aufrufende Konto erstellt wurden. In diesem Beispiel handelt es sich bei den Hauptbenutzern um die Organisation des anrufenden Accounts und um ein separates AWS-Konto, als Teil von zwei verschiedenen Ressourcenfreigaben. Sie müssen den Dienstendpunkt für den verwenden AWS-Region , der die Ressourcenfreigabe enthält.

```
$ 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
        }
    ]
}
```


Löschen einer Ressourcenfreigabe in AWS RAM

Sie können eine Ressourcenfreigabe jederzeit löschen. Wenn Sie eine Ressourcenfreigabe löschen, verlieren alle Prinzipale, die der Ressourcenfreigabe zugeordnet waren, den Zugriff auf die gemeinsam genutzten Ressourcen. Durch das Löschen einer Ressourcenfreigabe werden die gemeinsam genutzten Ressourcen nicht gelöscht.

> **Um eine AWS Ressource zu löschen**
>
> Wenn Sie eine AWS Ressource löschen müssen, die Sie in eine Ressourcenfreigabe aufgenommen haben, AWS empfiehlt es sich, zunächst sicherzustellen, dass Sie die Ressource entweder aus allen Ressourcenfreigaben entfernen, die sie enthalten, oder die Ressourcenfreigabe löschen.

Die gelöschte Ressourcenfreigabe bleibt nach dem Löschen noch für kurze Zeit in der AWS RAM Konsole sichtbar, ihr Status ändert sich jedoch in`Deleted`.

Console

So löschen Sie eine Ressourcenfreigabe

1. Öffnen Sie in der AWS RAM Konsole die Seite Von mir geteilt: Ressourcenfreigaben.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wählen Sie die Ressourcenfreigabe aus, die Sie löschen möchten.

   > **Warning**
   >
   > Achten Sie darauf, die richtige Ressourcenfreigabe auszuwählen. Sie können eine Ressourcenfreigabe nicht wiederherstellen, nachdem Sie sie gelöscht haben.

4. Wählen Sie Löschen und dann in der Bestätigungsnachricht Löschen aus.
5. Die gelöschte Ressourcenfreigabe verschwindet nach zwei Stunden. Bis dahin bleibt sie in der Konsole mit dem Status Gelöscht sichtbar.

AWS CLI

So löschen Sie eine Ressourcenfreigabe

Sie können den delete-resource-shareBefehl verwenden, um eine Ressourcenfreigabe zu löschen, die Sie nicht mehr benötigen.

Im folgenden Beispiel wird zunächst der get-resource-sharesBefehl verwendet, um den Amazon-Ressourcennamen (ARN) der Ressourcenfreigabe abzurufen, die Sie löschen möchten. Anschließend wird delete-resource-sharedie angegebene Ressourcenfreigabe gelöscht.

```
$  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
}
```

Greifen Sie auf mit Ihnen geteilte AWS Ressourcen zu

Mit AWS Resource Access Manager (AWS RAM) können Sie die Ressourcenfreigaben anzeigen, zu denen Sie hinzugefügt wurden, die gemeinsam genutzten Ressourcen, auf die Sie zugreifen können, und die, für AWS-Konten die Sie Ressourcen gemeinsam genutzt haben. Sie können eine Ressourcenfreigabe auch verlassen, wenn Sie keinen Zugriff mehr auf die gemeinsam genutzten Ressourcen benötigen.

Inhalt

Empfangen und Ablehnen von Resource Share-Einladungen

Um auf gemeinsam genutzte Ressourcen zugreifen zu können, muss der Besitzer der Resource Share Sie als Principal hinzufügen. Der Besitzer kann der Ressourcenfreigabe eine der folgenden Optionen als Principal hinzufügen.

- Die Organisation, der Ihr Konto angehört
- Eine Organisationseinheit (OU), die Ihr Konto enthält
- Ihr individuelles Konto
- Für unterstützte Ressourcentypen Ihre spezifische IAM-Rolle oder Ihr IAM-Benutzer

Wenn Sie der Ressourcenfreigabe durch eine Person hinzugefügt werden AWS-Konto , die Mitglied einer Organisation ist AWS Organizations, und die gemeinsame Nutzung innerhalb der Organisation aktiviert ist, erhalten Sie automatisch Zugriff auf die gemeinsam genutzten Ressourcen, ohne eine Einladung annehmen zu müssen. Service Principals erhalten außerdem automatischen Zugriff auf gemeinsam genutzte Ressourcen, ohne eine Einladung annehmen zu müssen. Wenn das Konto, über das Sie Zugriff erhalten, später aus der Organisation entfernt wird, verlieren alle Principals in diesem Konto automatisch den Zugriff auf die Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.

Wenn Sie durch einen der folgenden Gründe zu einer Ressourcenfreigabe hinzugefügt werden, erhalten Sie eine Einladung, der Ressourcenfreigabe beizutreten:

- Ein Konto außerhalb Ihrer Organisation in AWS Organizations
- Ein Konto innerhalb Ihrer Organisation, für das Teilen mit nicht aktiviert AWS Organizations ist

Wenn Sie eine Einladung erhalten, einer Resource Share beizutreten, müssen Sie diese annehmen, um auf die gemeinsam genutzten Ressourcen zugreifen zu können. Wenn Sie die Einladung ablehnen, können Sie nicht auf die gemeinsam genutzten Ressourcen zugreifen.

Für die folgenden Ressourcentypen haben Sie sieben Tage Zeit, um die Einladung zur Teilnahme an der Share für die folgenden Ressourcentypen anzunehmen. Wenn du die Einladung nicht annimmst, bevor sie abläuft, wird die Einladung automatisch abgelehnt.

> **Important**
>
> Für gemeinsam genutzte Ressourcentypen, die nicht in der folgenden Liste aufgeführt sind, haben Sie 12 Stunden Zeit, um die Einladung zur Teilnahme an der Resource Share anzunehmen. Nach 12 Stunden läuft die Einladung ab und die Zuordnung des Endbenutzer-Hauptbenutzers zur Resource Share wird aufgehoben. Die Einladung kann von Endbenutzern nicht mehr angenommen werden.

- Amazon Aurora — DB-Cluster
- Amazon EC2 — Kapazitätsreservierungen und dedizierte Hosts
- AWS License Manager — Lizenzkonfigurationen
- AWS Outposts — Routentabellen, Außenposten und Standorte für lokale Gateways
- Amazon Route 53 — Speditionsregeln
- Amazon VPC — Kundeneigene IPv4 Adressen, Präfixlisten, Subnetze, Traffic Mirror-Ziele, Transit-Gateways, Transit-Gateway-Multicast-Domänen

Console

Um auf eine Einladung zu einer gemeinsamen Nutzung von Ressourcen zu antworten

1. Navigieren Sie in der AWS RAM Konsole zur Seite Mit mir geteilt: Gemeinsam genutzte Ressourcen.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Sehen Sie sich die Liste der gemeinsam genutzten Ressourcen an, zu denen Sie hinzugefügt wurden.

   In der Spalte Status wird Ihr aktueller Teilnahmestatus für die Ressourcenfreigabe angezeigt. Der `Pending` Status gibt an, dass Sie zu einer Resource Share hinzugefügt wurden, die Einladung jedoch noch nicht angenommen oder abgelehnt haben.

4. Um auf die Einladung zur Ressourcenfreigabe zu antworten, wählen Sie die Resource Share-ID aus und wählen Sie Resource Share annehmen, um die Einladung anzunehmen, oder Resource Share ablehnen, um die Einladung abzulehnen. Wenn Sie die Einladung ablehnen, erhalten Sie keinen Zugriff auf die Ressourcen. Wenn Sie die Einladung annehmen, erhalten Sie Zugriff auf die Ressourcen.

AWS CLI

Um auf eine Einladung zu einer gemeinsamen Nutzung von Ressourcen zu antworten

Sie können die folgenden Befehle verwenden, um Einladungen zu einer Ressourcenfreigabe anzunehmen oder abzulehnen:

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

1. Im folgenden Beispiel wird zunächst der get-resource-share-invitationsBefehl verwendet, um eine Liste aller für den Benutzer verfügbaren Einladungen abzurufen AWS-Konto. Mit dem AWS CLI `query` Parameter können Sie die Ausgabe auf nur die Einladungen beschränken, für die der Wert auf `status` festgelegt ist`PENDING`. Dieses Beispiel zeigt, dass eine Einladung vom Konto `111111111` derzeit `PENDING` für das aktuelle Konto im angegebenen Konto gilt. `123456789012` AWS-Region

```
$ 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. Nachdem Sie die Einladung gefunden haben, die Sie annehmen möchten, notieren Sie sich die `resourceShareInvitationArn` in der Ausgabe enthaltenen Informationen, um sie im nächsten Befehl anzunehmen.

```
$ 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"
    }
}
```

   Falls erfolgreich, beachten Sie, dass die Antwort zeigt, dass der von `PENDING` zu geändert `status` wurde`ACCEPTED`.

Wenn Sie die Einladung stattdessen ablehnen möchten, führen Sie den reject-resource-share-invitationBefehl mit denselben Parametern aus.

```
$ 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"
    }
}
```


Für Sie geteilte Ressourcen anzeigen

Sie können die Ressourcenfreigaben anzeigen, auf die Sie Zugriff haben. Sie können sehen, welche Prinzipale Ressourcen mit Ihnen teilen und welche Ressourcen sie gemeinsam nutzen.

Console

Um die gemeinsam genutzten Ressourcen einzusehen

1. Navigieren Sie in der AWS RAM Konsole zur Seite Für mich freigegeben: Ressourcenfreigaben.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. (Optional) Wenden Sie einen Filter an, um nach bestimmten Ressourcenfreigaben zu suchen. Sie können mehrere Filter anwenden, um die Suche zu verfeinern. Sie können ein Schlüsselwort eingeben, z. B. einen Teil eines Ressourcenfreigabenamens, um nur die Ressourcenfreigaben aufzulisten, die diesen Text im Namen enthalten. Wählen Sie das Textfeld aus, um eine Dropdownliste mit vorgeschlagenen Attributfeldern anzuzeigen. Nachdem Sie einen ausgewählt haben, können Sie aus der Liste der verfügbaren Werte für dieses Feld auswählen. Sie können weitere Attribute oder Schlüsselwörter hinzufügen, bis Sie die gewünschte Ressource gefunden haben.
4. Die AWS RAM Konsole zeigt die folgenden Informationen an:

- Name — Der Name der Ressourcenfreigabe.
- ID — Die ID der Ressourcenfreigabe. Wählen Sie die ID, um die Detailseite für die Ressourcenfreigabe anzuzeigen.
- Besitzer — Die ID desjenigen AWS-Konto , der die Ressourcenfreigabe erstellt hat.
- Status – Der aktuelle Status der Ressourcenfreigabe. Mögliche Werte sind:
  - `Active`— Die Ressourcenfreigabe ist aktiv und kann verwendet werden.
  - `Deleted`— Die Ressourcenfreigabe wurde gelöscht und kann nicht mehr verwendet werden.
  - `Pending`— Eine Einladung zur Annahme der Ressourcenfreigabe wartet auf eine Antwort.

AWS CLI

Um die Resource Shares einzusehen

Verwenden Sie den get-resource-sharesBefehl, wobei der `--resource-owner` Parameter auf gesetzt ist`OTHER-ACCOUNTS`.

Das folgende Beispiel zeigt die Liste der Ressourcenfreigaben, die im angegebenen Konto von anderen gemeinsam AWS-Region mit dem aufrufenden Konto genutzt wurden AWS-Konten.

```
$ 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"
        }
    ]
}
```


Mit Ihnen geteilte Ressourcen anzeigen

Sie können die freigegebenen Ressourcen anzeigen, auf die Sie Zugriff haben. Sie können sehen, welche Prinzipale die Ressourcen für Sie freigegeben haben und welche Ressourcenfreigaben die Ressourcen enthalten.

Console

Um Ressourcen anzuzeigen, die mit Ihnen geteilt wurden

1. Navigieren Sie in der AWS RAM Konsole zur Seite Mit mir geteilt: Gemeinsam genutzte Ressourcen.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wenden Sie einen Filter an, um bestimmte freigegebene Ressourcen zu suchen. Sie können mehrere Filter anwenden, um die Suche zu verfeinern.
4. Die folgenden Informationen stehen zur Verfügung:

   - Ressourcen-ID — Die ID der Ressource. Wählen Sie die ID der Ressource aus, um sie in ihrer Service-Konsole anzuzeigen.
   - Ressourcentyp — Der Ressourcentyp.

- Datum der letzten Freigabe — Das Datum, an dem die Ressource für Sie freigegeben wurde.
- Ressourcenfreigaben — Die Anzahl der Ressourcenfreigaben, in denen die Ressource enthalten ist. Wählen Sie den Wert, um die Ressourcenanteile anzuzeigen.
- Besitzer-ID — Die ID des Prinzipals, dem die Ressource gehört.

AWS CLI

Um Ressourcen anzuzeigen, die mit Ihnen geteilt wurden

Sie können den Befehl list-resources verwenden, um Ressourcen anzuzeigen, die mit Ihnen gemeinsam genutzt wurden.

Der folgende Beispielbefehl zeigt Details zu der Ressource an, auf die über eine Ressourcenfreigabe in der angegebenen Ressource AWS-Region von einer anderen Ressource zugegriffen werden kann. AWS-Konto

```
$ 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"
        }
    ]
}
```

Principals anzeigen, die mit Ihnen geteilt werden

Sie können sich eine Liste aller Principals anzeigen lassen, die Ressourcen mit Ihnen teilen. Sie können sehen, welche Ressourcen und Ressourcenfreigaben sie mit Ihnen teilen.

Console

Um die Principals anzuzeigen, die Ressourcen mit Ihnen teilen

1. Öffnen Sie die AWS RAM Konsole zu https://console.aws.amazon.com/ram/Hause.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wählen Sie im Navigationsbereich Shared with me (Für mich freigegeben) und Principals (Prinzipale).
4. (Optional) Sie können einen Filter anwenden, um nach bestimmten Hauptbenutzern zu suchen. Sie können mehrere Filter anwenden, um die Suche zu verfeinern.
5. Die Konsole zeigt die folgenden Informationen an:
   - Prinzipal-ID — Die ID des Prinzipals, der die Daten mit Ihnen teilt.
   - Ressourcenfreigaben — Die Anzahl der Ressourcenfreigaben, zu denen der Prinzipal Sie hinzugefügt hat. Wählen Sie die Anzahl, um die Liste der Ressourcenfreigaben anzuzeigen.
   - Ressourcen — Die Anzahl der Ressourcen, die der Schulleiter mit Ihnen teilt. Wählen Sie den Wert, um die Liste der Ressourcen anzuzeigen.

AWS CLI

Um die Principals anzuzeigen, die Ressourcen mit Ihnen gemeinsam nutzen

Sie können den Befehl list-principals verwenden, um die Liste der Prinzipale abzurufen, die Ressourcen mit Ihnen gemeinsam nutzen. AWS-Konto

Der folgende Beispielbefehl zeigt Details zu dem Benutzer an AWS-Konto , der eine gemeinsame Ressource mit dem Konto geteilt hat, das zum Aufrufen des Vorgangs in dem angegebenen Konto verwendet wurde. AWS-Region

```
$  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
        }
    ]
}
```

Einen Ressourcenanteil hinterlassen

Wenn Sie keinen Zugriff mehr auf Ressourcen benötigen, die mit Ihnen geteilt wurden, können Sie eine Ressourcenfreigabe jederzeit verlassen. Wenn Sie eine Ressourcenfreigabe verlassen, verlieren Sie den Zugriff auf die gemeinsam genutzten Ressourcen.

Voraussetzungen für das Verlassen einer Ressourcenfreigabe

- Sie können eine Ressourcenfreigabe nur verlassen, wenn sie für Sie als Einzelperson AWS-Konto und nicht im Rahmen einer Organisation freigegeben wurde. Sie können eine Ressourcenfreigabe nicht verlassen, wenn Sie von einem Mitarbeiter AWS-Konto innerhalb Ihrer Organisation hinzugefügt wurden und das Teilen mit aktiviert AWS Organizations ist. Der Zugriff auf gemeinsam genutzte Ressourcen innerhalb einer Organisation erfolgt automatisch.
- Um eine Ressourcenfreigabe zu verlassen, stellen Sie sicher, dass die Ressourcenfreigabe entweder leer ist oder dass sie nur Ressourcentypen enthält, die das Verlassen einer gemeinsamen Nutzung unterstützen.

  Im Folgenden sind die einzigen Ressourcentypen aufgeführt, die das Verlassen einer Ressourcenfreigabe unterstützen.

Service	Ressourcentyp
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation`

Service	Ressourcentyp
	`ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

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

Amazon Route 53	`route53resolver:ResolverRule`

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

Wie verlasse ich eine Ressourcenfreigabe

Console

Um eine gemeinsame Nutzung einer Ressource zu verlassen

1. Navigieren Sie in der AWS RAM Konsole zur Seite Für mich freigegeben: Ressourcenfreigaben.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen

Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.

3. Wählen Sie die gemeinsame Nutzung der Ressource aus, die Sie verlassen möchten.
4. Wählen Sie „Ressourcenfreigabe verlassen“ und wählen Sie im Bestätigungsdialogfeld die Option „Verlassen“.

AWS CLI

Um eine Ressourcenfreigabe zu verlassen

Sie können den disassociate-resource-shareBefehl verwenden, um eine Ressourcenfreigabe zu verlassen.

Die folgenden Beispielbefehle führen dazu AWS-Konto , dass der, der den Befehl aufruft, den Zugriff auf die Ressourcen verliert, die von der im ARN angegebenen Ressourcenfreigabe gemeinsam genutzt werden. Sie müssen die Anfrage an den Dienstendpunkt in dem Ordner weiterleiten AWS-Region , der die Ressourcenfreigabe enthält, die Sie verlassen möchten.

1. Rufen Sie zunächst die Liste der Ressourcenfreigaben ab, um den ARN der Ressourcenfreigabe abzurufen, die Sie verlassen möchten.

```
$ 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"
        }
    ]
}
```

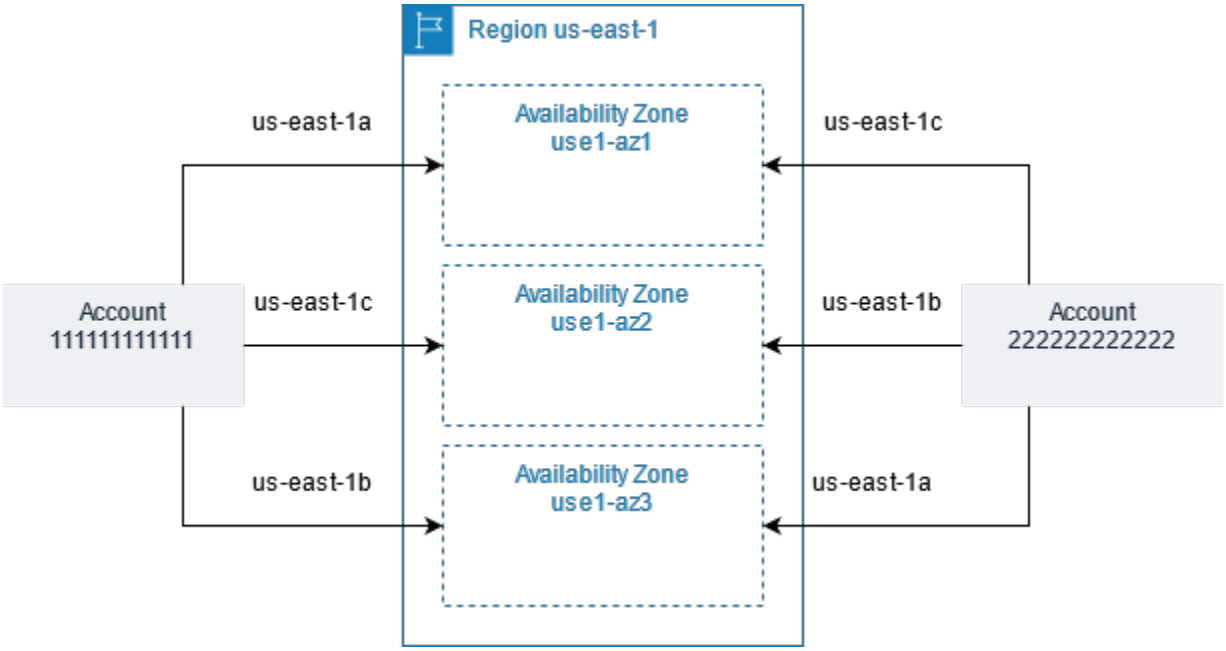
2. Anschließend können Sie den Befehl ausführen, um diese Ressourcenfreigabe zu verlassen. Beachten Sie, dass Sie auch Ihre Konto-ID als Principal angeben müssen`123456789012`, um die Verbindung zu der angegebenen Ressourcenfreigabe zu trennen, die von den Konten `111111111111` gemeinsam genutzt wird.

```
$ 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
        }
    ]
}
```

Availability Zone IDs für Ihre AWS Ressourcen

AWS ordnet die physischen Availability Zones nach dem Zufallsprinzip den jeweiligen Availability Zonen-Namen zu AWS-Konto. Dieser Ansatz hilft dabei, Ressourcen auf die Availability Zones in einer zu verteilen AWS-Region, anstatt dass Ressourcen wahrscheinlich in der Availability Zone „a“ für jede Region konzentriert werden. Daher entspricht die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht dem gleichen physischen Standort wie `us-east-1a` für ein anderes AWS Konto. Weitere Informationen finden Sie unter Regionen und Availability Zones im EC2 Amazon-Benutzerhandbuch.

Die folgende Abbildung zeigt, dass die IDs AZs für jedes Konto gleich sind, obwohl die Namen der Availability Zone für jedes Konto unterschiedlich zugeordnet werden können.



Bei einigen Ressourcen müssen Sie nicht nur die Availability Zone AWS-Region, sondern auch die Availability Zone identifizieren. Zum Beispiel ein Amazon VPC-Subnetz. Innerhalb eines einzelnen Kontos ist die Zuordnung einer Availability Zone zu einem bestimmten Namen nicht wichtig. Wenn Sie AWS RAM eine solche Ressource jedoch mit anderen teilen AWS-Konten, ist die Zuordnung wichtig. Diese zufällige Zuordnung erschwert es dem Konto, das auf die gemeinsam genutzte Ressource zugreift, zu wissen, auf welche Availability Zone verwiesen werden soll. Um Ihnen dabei zu helfen, ermöglichen Ihnen diese Ressourcen auch, mithilfe der AZ-ID den tatsächlichen Standort Ihrer Ressourcen im Verhältnis zu Ihren Konten zu ermitteln. Eine AZ-ID ist eine eindeutige und konsistente Kennung für eine Availability Zone in allen Bereichen AWS-Konten. Dies `use1-az1` ist beispielsweise eine AZ-ID für eine Availability Zone in der `us-east-1` Region und steht für denselben physischen Standort in jedem AWS Konto.

Sie können AZ verwenden IDs , um den Standort von Ressourcen in einem Konto im Verhältnis zu den Ressourcen in einem anderen Konto zu bestimmen. Wenn Sie beispielsweise ein Subnetz in der Availability Zone mit der AZ-ID `use1-az2` mit einem anderen Konto teilen, steht dieses Subnetz dem Konto in der Availability Zone zur Verfügung, dessen AZ-ID ebenfalls `use1-az2` ist. Die AZ-ID für jedes Subnetz wird in der Amazon VPC-Konsole angezeigt und kann mit dem abgefragt werden. AWS CLI

Console

Um die AZ IDs für die Availability Zones in Ihrem Konto anzuzeigen

1. Navigieren Sie in der AWS RAM Konsole zur AWS RAM Konsolenseite.
2. Sie können die aktuelle AZ IDs AWS-Region unter Ihrer AZ-ID einsehen.

AWS CLI

Um die AZ IDs für die Availability Zones in Ihrem Konto einzusehen

Der folgende Beispielbefehl zeigt die AZ IDs für die Availability Zones in der Region us-west-2 und wie sie für den Anruf zugeordnet sind. AWS-Konto

```
$ 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"
        }
    ]
}
```

Gemeinsam nutzbare Ressourcen AWS

Mit AWS Resource Access Manager (AWS RAM) können Sie Ressourcen teilen, die von anderen erstellt und verwaltet wurden AWS-Services. Sie können Ressourcen mit Einzelpersonen teilen AWS-Konten. Sie können Ressourcen auch mit den Konten in einer Organisation oder mit Organisationseinheiten (OUs) in teilen AWS Organizations. Bei einigen unterstützten Ressourcentypen können Sie Ressourcen auch für einzelne AWS Identity and Access Management (IAM-) Rollen und Benutzer gemeinsam nutzen.

In den folgenden Abschnitten sind die Ressourcentypen, gruppiert nach AWS-Service, aufgeführt, die Sie gemeinsam nutzen AWS RAM können. Die Spalten in den Tabellen geben an, welche Funktionen die einzelnen Ressourcentypen unterstützen:

Kann mit IAM-Benutzern und -Rollen geteilt werden	 — Sie können Ressourcen dieses Typs nicht nur mit Konten, sondern auch mit einzelnen Rollen und Benutzern AWS Identity and Access Management (IAM) teilen.	Ja
	 — Sie können Ressourcen dieses Typs nur mit Konten teilen.	Nein
Kann mit Konten außerhalb der eigenen Organisation teilen	 Du darfst Ressourcen dieses Typs nur mit einzelnen Konten innerhalb oder außerhalb der Organisation teilen. Weitere Informationen finden Sie unter Überlegungen.	Ja.

	 — Sie können Ressourcen dieses Typs nur mit Konten teilen, die Mitglieder derselben Organisation sind.	Nein
Kann vom Kunden verwaltete Berechtigungen verwenden	Alle Ressourcentypen, die von unterstützt werden, AWS RAM unterstützen AWS verwaltete Berechtigungen. Ein Ja in dieser Spalte bedeutet jedoch, dass vom Kunden verwaltete Berechtigungen auch für diesen Ressourcentyp unterstützt werden.	
	 — Ressourcen dieses Typs unterstützen die Verwendung von vom Kunden verwalteten Berechtigungen.	Ja
	 — Ressourcen dieses Typs unterstützen die Verwendung von vom Kunden verwalteten Berechtigungen nicht.	Nein
Kann mit Service Principals geteilt werden	 — Sie können Ressourcen dieses Typs mit AWS-Services teilen.	Ja
	 — Sie können Ressourcen dieses Typs nicht mit anderen teilen AWS-Services.	Nein

AWS App Mesh

Sie können die folgenden AWS App Mesh Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Gitter `appmesh:Mesh`	Erstellen und verwalten Sie ein Mesh zentral und teilen Sie es mit anderen Personen AWS-Konten oder Ihrer Organisation. Ein gemeinsames Mesh ermöglicht es Ressourcen, die von verschiedenen erstellt wurden, im selben Mesh miteinander AWS-Konten zu kommunizieren. Weitere Informationen finden Sie im AWS App Mesh Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Netzen.	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Nein	 Nein

AWS AppSync GraphQL-API

Sie können die folgenden AWS AppSync GraphQL-API-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AppSync GraphyQL APIs `appsync:APIs`	Verwalte AWS AppSync GraphQL APIs zentral und teile sie mit anderen AWS-Konten oder deiner Organisation. Auf diese Weise können mehrere Konten gemeinsam AWS AppSync APIs genutzt werden, um eine einheitliche AWS AppSync zusammengeführte API zu erstellen, die auf Daten aus mehreren Subschemas APIs über verschiedene Konten in derselben Region zugreifen kann. Weitere Informationen finden Sie unter Zusammengeführt APIs im AWS AppSync Entwicklerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Amazon API Gateway

Sie können die folgenden Amazon API Gateway Gateway-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Private benutzerdefinierte Domänen für API Gateway `apigateway:Domainnames`	Erstellen und verwalten Sie Domainnamen zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten Ihre Domainnamen aufrufen, die privat zugeordnet sind. APIs Weitere Informationen finden Sie unter Benutzerdefinierte Domainnamen für private APIs in API Gateway im Amazon API Gateway Developer Guide.	N	Ja Kann mit jedem geteilt werden AWS-Konto.	N	Nein

Amazon Application Recovery Controller (ARC)

Sie können die folgenden Amazon Application Recovery Controller (ARC) -Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
ARC-Cluster weiterleiten `route53-recovery-control:Cluster`	Erstellen und verwalten Sie ARC-Cluster zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten Control Panels und Routing-Steuerelemente in einem einzigen gemeinsam genutzten Cluster einrichten, wodurch die Komplexität und die Gesamtzahl der Cluster, die ein Unternehmen benötigt, reduziert werden. Weitere Informationen finden Sie unter Kontenübergreifendes Teilen von Clustern im Amazon Application Recovery Controller	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	r (ARC) Developer Guide.				
Wechselpläne für die ARC-Region `arc-region-switch:Plan`	Erstellen und verwalten Sie Pläne zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten Ressourcen von einem Konto nutzen, das sich von dem Konto unterscheidet, das den Plan hostet. Weitere Informationen finden Sie unter Region Switch im Amazon Application Recovery Controller (ARC) Developer Guide.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Amazon Aurora

Sie können die folgenden Amazon Aurora Aurora-Ressourcen mit anderen teilen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Aurora-DB-Cluster `rds:Cluster`	Erstellen und verwalten Sie einen DB-Cluster zentral und teilen Sie ihn mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer einen gemeinsam genutzten, zentral verwalteten DB-Cluster klonen. Weitere Informationen finden Sie unter Kontoüber greifendes Klonen mit AWS RAM und Amazon Aurora im Amazon Aurora Aurora-Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden. AWS-Konto	 N	 Nein

AWS Backup

Sie können die folgenden AWS Backup Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Sicherungstresore `backup:BackupVault`	Sie können Tresore mit logischen Air-Gaps zentral erstellen und verwalten und sie gemeinsam mit anderen Personen oder Ihrer Organisation nutzen. AWS-Konten Mit dieser Option können mehrere Konten auf Backups aus den Tresoren zugreifen und diese wiederherstellen. Weitere Informationen finden Sie im Entwicklerhandbuch unter Überblick über Tresore mit logischem Air-Gapped.AWS Backup	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Amazon Bedrock

Sie können die folgenden Amazon Bedrock-Ressourcen mit anderen teilen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Kundenspezifisches Modell von Bedrock `bedrock:CustomModel`	Erstellen und verwalten Sie ein benutzerdefiniertes Modell zentral und teilen Sie es mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten dasselbe benutzerdefinierte Modell für generative KI-Anwendungen verwenden. Weitere Informationen finden Sie unter Ein Modell für ein anderes Konto teilen im Amazon Bedrock-Benutzerhandbuch.	 Ja	 Nein Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	 Ja	 Nein

Billing and Cost Management

Sie können die folgenden Ressourcen für Billing and Cost Management gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
BCM-Dashboards `bcm-dashboards:dashboard`	Erstellen und verwalten Sie Billing and Cost Management Kostenmanagement-Dashboards und teilen Sie sie mit anderen AWS-Konten innerhalb oder außerhalb Ihres Unternehmens. Wenn Sie ein Dashboard teilen, werden nur die Dashboard-Konfigurationen gemeinsam genutzt, nicht die zugrunde liegenden Daten. Empfänger erhalten Zugriff auf das Dashboard-Layout und die Widget-Konfigurationen und sehen die Daten auf der Grundlage ihrer eigenen Zugriffsberechtigungen. Diese gemeinsame Nutzung ermöglicht es Unternehmen, gemeinsame Verfahren	N	Ja Kann mit jedem AWS-Konto geteilt werden.	Ja	Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	zur Kostenberichterstattung festzulegen, und unterstützt verschiedene Teams dabei, Kostendaten einheitlich zu betrachten. Weitere Informationen finden Sie unter Teilen von Dashboards im Billing and Cost Management-Benutzerhandbuch.				

AWS Billing Service anzeigen

Sie können die folgenden AWS Billing View Service-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Ansichten zur Abrechnung	Erstellen und verwalten Sie benutzerdefinierte Abrechnungsansicht	N	N	Ja	Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
`billing:billingview`	en zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Inhaber von Anwendungen und Geschäftsbereichen von einem Mitgliedskonto aus auf AWS Ausgaben auf Geschäftseinheitsebene zugreifen. Weitere Informationen finden Sie im AWS Cost Management Benutzerhandbuch unter Teilen von benutzerdefinierten Abrechnungsansichten.		Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.		

AWS Cloud Map

Sie können die folgenden AWS Cloud Map Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS Cloud Map Namespaces `servicediscovery:Namespace`	Erstellen und verwalten Sie Namespaces zentral und teilen Sie sie mit anderen innerhalb Ihrer Organisation. AWS-Konten Auf diese Weise können mehrere Dienste und Instanzen im gemeinsam genutzten Namespace AWS-Konten erkennen, ohne dass temporäre Anmeldeinformationen erforderlich sind. Weitere Informationen finden Sie unter Gemeinsam genutzte AWS Cloud Map Namespaces im Entwicklerhandbuch .AWS Cloud Map	 Ja	 Nein Kann nur innerhalb der eigenen Organisation geteilt AWS-Konten werden.	 Ja	 Nein

AWS Cloud-WAN

Sie können die folgenden AWS Cloud-WAN-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Kernnetzwerke `networkmanager:CoreNetwork`	Erstellen und verwalten Sie ein Cloud-WAN-Kernnetzwerk zentral und teilen Sie es mit anderen AWS-Konten. Auf diese Weise können mehrere Hosts in einem einzigen Cloud-WAN-Kernnetzwerk AWS-Konten aufrufen und bereitstellen. Weitere Informationen finden Sie unter Gemeinsame Nutzung eines Kernnetzwerks im AWS Cloud WAN-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Nein	 Nein

Amazon CloudFront

Sie können die folgenden CloudFront Amazon-Ressourcen teilen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Amazon CloudFront VpcOrigin `cloudfront:VpcOrigin`	Erstellen und verwalten Sie CloudFront VPC-Ursprünge zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere gemeinsam AWS-Konten genutzte VPC-Ursprünge für CloudFront Distributionen verwenden. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Ressourcen CloudFront im Amazon CloudFront Developer Guide.	N	Ja Kann mit jedem geteilt werden AWS-Konto.	N	Nein

AWS CloudHSM

Sie können die folgenden AWS CloudHSM Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS CloudHSM Backups `cloudhsm:Backup`	Verwalten Sie AWS CloudHSM Backups zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen über das Backup einsehen und sie zur Wiederherstellung eines AWS CloudHSM Clusters verwenden. Weitere Informationen finden Sie im AWS CloudHSM Benutzerhandbuch unter AWS CloudHSM Backups verwalten.	 Ja	 Ja	 Ja	 Nein

AWS CodeBuild

Sie können die folgenden AWS CodeBuild Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
CodeBuild Projekte `codebuild:Project`	Erstellen Sie ein Projekt und verwenden Sie es, um Builds auszuführen. Teilen Sie das Projekt mit anderen AWS-Konten Personen oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen zu einem Projekt einsehen und dessen Builds analysieren. Weitere Informationen finden Sie im AWS CodeBuild Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Projekten.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein
CodeBuild Gruppen melden `codebuild:ReportGroup`	Erstellen Sie eine Berichtsgruppe und verwenden Sie sie, um Berichte zu erstellen, wenn Sie ein Projekt erstellen. Teilen Sie die Berichtsgruppe mit	 Ja	 Ja Kann mit jedem geteilt werden	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	anderen AWS-Konten Personen oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer die Berichtsgruppe und ihre Berichte sowie die Testfallergebnisse für jeden Bericht einsehen. Ein Bericht kann nach seiner Erstellung 30 Tage lang angezeigt werden. Danach läuft er ab und kann nicht mehr angezeigt werden. Weitere Informationen finden Sie im AWS CodeBuild Benutzerhandbuch unter Arbeiten mit geteilten Projekten.		AWS-Konto.		

AWS CodeConnections

Sie können die folgenden CodeConnections Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Verbindungen codieren `codeconnections:Connection`	Verwalten Sie die Wiederverwendung von Codeverbindungen in mehreren Konten. Mit anderen Worten, die gemeinsame Nutzung von Codeverbindungen reduziert den Verwaltungsaufwand und den Bedarf an Administratorzugriff für jedes Konto, für das eine Codeverbindung erforderlich ist. Weitere Informationen finden Sie unter Verbindungen teilen mit AWS-Konten im Developer Tools Console-Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Amazon DataZone

Sie können die folgenden DataZone Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
DataZone Domänen `datazone:Domain`	Erstellen und verwalten Sie Domains zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten DataZone Amazon-Domains erstellen. Weitere Informationen finden Sie unter Was ist Amazon DataZone im DataZone Amazon-Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

Amazon EC2

Sie können die folgenden Amazon EC2 EC2-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Kapazitätsreservierungen `ec2:CapacityReservation`	Sie können Kapazitätsreservierungen zentral erstellen und verwalten und die reservierte Kapazität gemeinsam mit anderen Personen AWS-Konten oder Ihrer Organisation nutzen. Auf diese Weise können mehrere ihre Amazon EC2 EC2-Instances in zentral verwalteten reservierten Kapazitäten AWS-Konten starten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsamen Kapazitätsreservierungen im Amazon EC2 EC2-Benutzerhandbuch. Teilen Sie Kapazitätsblöcke für ML (UltraServer CBs werden noch nicht unterstützt) mit anderen	 N	Ja für Kapazitätsreservierungen (kann mit allen geteilt werden AWS-Konto). Nein für Kapazitätsblöcke (kann nur innerhalb AWS-Konten der eigenen Organisation geteilt werden).	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	AWS-Konten oder Ihrer Organisation. Diese Funktion ermöglicht es Workloads, die in verschiedenen Umgebungen ausgeführt werden AWS-Konten , Amazon EC2 EC2-Instances in Ihren eigenen Kapazitätsblöcken zu starten, sodass Sie Ihre reservierte Kapazität besser nutzen und Kosten sparen können. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Kapazitätsblöcken im Amazon EC2 EC2-Benutzerhandbuch. **Important** Wenn Sie nicht alle Voraussetzungen für die gemeinsam				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	e Nutzung einer Kapazitätsreservierung erfüllen, kann die gemeinsame Nutzung fehlschlagen. Wenn dies passiert und ein Benutzer versucht, eine Amazon EC2 EC2-Instance mit dieser Kapazitätsreservierung zu starten, wird sie als On-Demand-Instance gestartet, für die höhere Kosten anfallen können. Wir empfehlen Ihnen, zu überprüfen, ob Sie auf die gemeinsam				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	e Kapazitätsreservierung zugreifen können, indem Sie versuchen, sie in der Amazon EC2 EC2-Konsole anzuzeigen. Sie können auch nach ausgefallenen Ressourcenfreigaben suchen, sodass Sie Korrekturmaßnahmen ergreifen können, bevor Benutzer Instances auf eine Weise starten, die Ihre Kosten in die Höhe treibt. Weitere Informationen finden Sie unter Beispiel:				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Warnung bei Ausfällen bei der gemeinsamen Nutzung von Ressourcen.				
Dedicated Hosts `ec2:DedicatedHost`	Weisen Sie Amazon EC2 EC2-Dedicated Hosts zentral zu und verwalten Sie sie und teilen Sie die Instance-Kapazität des Hosts mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere ihre Amazon EC2 EC2-Instances auf zentral verwalteten dedizierten Hosts AWS-Konten starten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Dedicated Hosts im Amazon EC2 EC2-Benutzerhandbuch.	 N	 Ja Kann mit jedem AWS-Konto geteilt werden.	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Placement-Gruppen `ec2:PlacementGroup`	Teilen Sie die Platzierungsgruppen, die Sie besitzen AWS-Konten, innerhalb und außerhalb Ihrer Organisation mit anderen. Sie können Amazon EC2 EC2-Instances von jedem Konto aus starten, mit dem Sie sich eine gemeinsame Platzierungsgruppe teilen. Weitere Informationen finden Sie unter Eine Platzierungsgruppe teilen im Amazon EC2 EC2-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Nein	 Nein

EC2 Image Builder

Sie können die folgenden EC2 Image Builder Builder-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Image Builder Builder-Komponenten `imagebuilder:Component`	Erstellen und verwalten Sie Komponenten zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Verwalten Sie, wer vordefinierte Build- und Testkomponenten in seinen Image-Rezepten verwenden kann. Weitere Informationen finden Sie unter Share EC2 Image Builder Builder-Ressourcen im EC2 Image Builder Builder-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein
Container-Rezepte von Image Builder `imagebuilder:ContainerRecipe`	Erstellen und verwalten Sie Ihre Container-Rezepte zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Sie verwalten, wer vordefinierte	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Dokumente verwenden kann, um Container-Image-Builds zu duplizieren. Weitere Informationen finden Sie unter Share EC2 Image Builder Builder-Ressourcen im EC2 Image Builder Builder-Benutzerhandbuch.				
Image Builder Builder-Bilder `imagebuilder:Image`	Erstellen und verwalten Sie Ihre Golden Images zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Verwalten Sie, wer mit EC2 Image Builder erstellte Images in Ihrem Unternehmen verwenden kann. Weitere Informationen finden Sie unter Share EC2 Image Builder Builder-Ressourcen im EC2 Image Builder Builder-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Image-Rezepte von Image Builder `imagebuilder:ImageRecipe`	Erstellen und verwalten Sie Ihre Image-Rezepte zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Sie verwalten, wer vordefinierte Dokumente verwenden kann, um AMI-Builds zu duplizieren. Weitere Informationen finden Sie unter Share EC2 Image Builder Builder-Ressourcen im EC2 Image Builder Builder-Benutzerhandbuch.	Ja	Ja Kann mit jedem geteilt werden. AWS-Konto	Ja	Nein

Elastic Load Balancing

Sie können die folgenden Elastic Load Balancing Balancing-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
ELB Trust-Stores `elasticloadbalancing:TrustStore`	Erstellen und verwalten Sie Elastic Load Balancing Trust Stores zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Sicherheitsadministratoren können eine einzelne oder eine kleinere Anzahl von Trust Stores verwalten und Mutual TLS-Konfigurationen für alle Application Load Balancer aktivieren. Weitere Informationen finden Sie unter Teilen Ihres Elastic Load Balancing Balancing-Trustspeichers für Application Load Balancers im Benutzerhandbuch für Application Load Balancers.	 Ja	 Ja	 Nein	 Nein

AWS End User Messaging SMS

Sie können die folgende AWS End User Messaging SMS Ressource mit anderen teilen, indem Sie. AWS RAM

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS SMS Listen zum Abmelden per Spracheingabe `sms-voice:OptOutList`	Erstellen Sie eine Abmeldeliste und teilen Sie sie mit anderen AWS-Konten Personen in Ihrer Organisation. Sie können die Abmeldeliste teilen, sodass die anderen Anwendungen die Rufnummern anderer Benutzer abbestellen können, AWS-Konten oder sie können den Status der Telefonnummer des Benutzers überprüfen. Weitere Informationen finden Sie im AWS End User Messaging SMS Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Ressourcen.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS SMS Telefonnummern für Sprachanrufe `sms-voice:PhoneNumber`	Erstellen und verwalten Sie Telefonnummern, um sie mit anderen AWS-Konten oder Ihrer Organisation zu teilen. Auf diese Weise können mehrere AWS-Konten Personen Nachrichten unter Verwendung der gemeinsam genutzten Telefonnummer senden. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Ressourcen im AWS End User Messaging SMS internen Benutzerhandbuch.	 N	 Kann mit jedem geteilt werden AWS-Konto. Ja	 Ja	 Ja

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS SMS Sprachpool `sms-voice:Pool`	Erstellen und verwalten Sie Pools, um sie mit anderen AWS-Konten oder Ihrer Organisation zu teilen. Auf diese Weise können mehrere Benutzer Nachrichten über den gemeinsamen Pool AWS-Konten senden. Weitere Informationen finden Sie im AWS End User Messaging SMS Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Ressourcen.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Ja

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS SMS Sprachsender IDs `sms-voice:SenderId`	Erstellen und verwalten Sie Absender IDs und teilen Sie sie mit anderen AWS-Konten Personen oder Ihrer Organisation. Auf diese Weise können mehrere Nachrichten unter Verwendung der gemeinsamen Absender-ID AWS-Konten senden. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Ressourcen im AWS End User Messaging SMS internen Benutzerhandbuch.	N	Ja Kann mit jedem geteilt werden AWS-Konto.	Ja	Ja

Amazon FSx für OpenZFS

Sie können die folgenden Ressourcen von Amazon FSx für OpenZFS mit anderen teilen, indem Sie. AWS RAM

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
FSx Volumen `fsx:Volume`	Erstellen und verwalten Sie FSx OpenZFS-Volumes zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten die Datenreplikation mithilfe von OpenZfs Snapshots auf gemeinsam genutzten Volumes über oder durchführen. FSx APIs `CreateVolume` `CopySnapshotAndUpdateVolume` Weitere Informationen finden Sie unter On-Demand-Datenreplikation im Amazon FSx for OpenZFS-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

AWS Glue

Sie können die folgenden AWS Glue Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS Glue Katalog `glue:Catalog`	Verwalten Sie einen zentralen Datenkatalog und teilen Sie Metadaten zu Datenbanken und Tabellen mit AWS-Konten oder Ihrer Organisation. Auf diese Weise können Benutzer Abfragen zu Daten über mehrere Konten hinweg ausführen. Weitere Informationen finden Sie unter AWS Konten übergreifendes Teilen von Datenkatalogtabellen und Datenbanken im AWS Lake Formation Entwicklerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein
AWS Glue Datenbanken `glue:Database`	Erstellen und verwalten Sie Datenkatalogdatenbanken zentral und teilen Sie sie mit AWS-Konten oder Ihrer Organisat	 N	 Ja	 N	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	ion. Datenbanken sind Sammlungen von Datenkatalogtabellen. Auf diese Weise können Benutzer Abfragen ausführen und ETL-Jobs (Extrahieren, Transformieren und Laden) ausführen, mit denen Daten aus mehreren Konten verknüpft und abgefragt werden können. Weitere Informationen finden Sie unter AWS Kontenübergreifendes Teilen von Datenkatalogtabellen und Datenbanken im AWS Lake Formation Entwicklerhandbuch.		Kann mit jedem geteilt werden AWS-Konto.		

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS Glue Tische `glue:Table`	Erstellen und verwalten Sie Datenkatalogtabellen zentral und teilen Sie sie mit AWS-Konten Ihrer Organisation. Datenkatalogtabellen enthalten Metadaten zu Datentabellen in Amazon S3, JDBC-Datenquellen, Amazon Redshift, Streaming-Quellen und anderen Datenspeichern. Auf diese Weise können Benutzer Abfragen und ETL-Jobs ausführen, mit denen Daten mehrerer Konten verknüpft und abgefragt werden können. Weitere Informationen finden Sie unter AWS Kontenübergreifendes Teilen von Datenkatalogtabellen und Datenbanken im AWS Lake Formation Entwicklerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

AWS License Manager

Sie können die folgenden AWS License Manager Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Lizenzkonfigurationen `license-manager:LicenseConfiguration`	Sie können Lizenzkonfigurationen zentral erstellen und verwalten und sie mit anderen Personen AWS-Konten oder Ihrer Organisation teilen. Auf diese Weise können Sie zentral verwaltete Lizenzregeln, die auf den Bedingungen Ihrer Unternehmensvereinbarungen basieren, für mehrere durchsetzen AWS-Konten. Weitere Informationen finden Sie unter Lizenzkonfigurationen in License Manager im License Manager Manager-Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

AWS Marketplace

Sie können die folgenden AWS Marketplace Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Entitäten im Marketplace-Katalog `aws-marketplace:Entity`	Erstellen, verwalten und teilen Sie Entitäten innerhalb AWS-Konten oder innerhalb Ihrer Organisation in AWS Marketplace. Weitere Informationen finden Sie AWS RAM in der AWS Marketplace Catalog API Referenz unter Gemeinsame Nutzung von Ressourcen.	Ja	Ja Kann mit jedem geteilt werden AWS-Konto.	N	Nein

AWS Migration Hub Refactor Spaces

Sie können die folgenden AWS Migration Hub Refactor Spaces Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Refactor Spaces-Umgebung `refactor-spaces:Environment`	Erstellen Sie eine Refactor Spaces-Umgebung und verwenden Sie sie, um Ihre Refactor Spaces-Anwendungen zu enthalten. Teilen Sie die Umgebung mit anderen AWS-Konten oder allen Konten in Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen über die Umgebung und die darin enthaltenen Anwendungen einsehen. Weitere Informationen finden Sie unter Gemeinsame Nutzung von Refactor Spaces-Umgebungen AWS RAM im AWS Migration Hub Refactor Spaces Benutzerhandbuch.	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Ja	 Nein

Mehrparteien-Genehmigung

Sie können die folgenden Ressourcen zur Genehmigung durch mehrere Parteien gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Genehmigungsteam mit mehreren Parteien `mpa:ApprovalTeam`	Erstellen und verwalten Sie Genehmigungsteams und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können andere AWS-Konten ein Genehmigungsteam verwenden, das einem geschützten Vorgang zugeordnet ist. Ein geschützter Vorgang ist eine vordefinierte Liste von Vorgängen, für deren Ausführung die Genehmigung durch das Team erforderlich ist. Weitere Informationen finden Sie unter Begriffe und Konzepte im Benutzerhandbuch zur	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Genehmigung durch mehrere Parteien.				

AWS Network Firewall

Sie können die folgenden AWS Network Firewall Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Netzwerk-Firewalls `network-firewall:Firewall`	Erstellen und verwalten Sie Firewalls zentral und teilen Sie sie mit anderen, AWS-Konten sodass diese Firewall-Endpunkte einrichten können. Auf diese Weise können mehrere Konten den Schutz einer einzigen Firewall nutzen. Weitere Informati	Ja	Ja Kann mit jedem geteilt werden AWS-Konto.	N	Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	onen finden Sie im AWS Network Firewall Entwicklerhandbuch unter AWS Network Firewall Ressourcen gemeinsam nutzen.				
Netzwerk-Firewall-Richtlinien `network-firewall:FirewallPolicy`	Erstellen und verwalten Sie Firewall-Richtlinien zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten in einer Organisation dieselben Verhaltensmuster für Netzwerküberwachung, Schutz und Filterung nutzen. Weitere Informationen finden Sie im AWS Network Firewall Entwicklerhandbuch unter AWS Network Firewall Ressourcen gemeinsam nutzen.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Nein	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen

Regelgruppen für Network Firewall
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Sie können statusfreie und statusbehaftete Regelgruppen zentral erstellen und verwalten und sie gemeinsam mit anderen AWS-Konten oder Ihrer Organisation nutzen. Auf diese Weise können mehrere Konten in einer Organisation eine Reihe von Kriterien für die Überprüfung und Bearbeitung des Netzwerkverkehrs gemeinsam nutzen. AWS Organizations Weitere Informationen finden Sie im AWS Network Firewall Entwicklerhandbuch unter [AWS Network Firewall Ressourcen gemeinsam nutzen]().	 Ja	 Ja
			
			Kann mit jedem geteilt werden AWS-Konto.
				 Nein	 Nein

Oracle Database@AWS

Sie können die folgenden Oracle Database@AWS Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Oracle Database@AWS Exadata-Infrastruktur `odb:CloudExadataInfrastructure`	Mit Oracle Database@AWS können Sie Ihre Exadata-Infrastruktur und Ihr ODB-Netzwerk für mehrere AWS-Konten Personen in derselben Organisation gemeinsam nutzen. AWS Auf diese Weise können Sie die Infrastruktur einmal bereitstellen und sie für alle vertrauenswürdigen Konten wiederverwenden. So können Sie Kosten senken und gleichzeitig die Verantwortlichkeiten trennen. Weitere Informationen finden Sie Oracle Database@AWS im Oracle Database@AWS Benutzerhandbuch	N	N Kann nur innerhalb AWS-Konten der eigenen Organisation geteilt werden.	N	Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	unter Gemeinsame Nutzung von Ressourcen.				

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Oracle Database@AWS ODB-Netzwerk `odb:OdbNetwork`	Mit Oracle Database@AWS können Sie Ihre Exadata-Infrastruktur und Ihr ODB-Netzwerk für mehrere Personen AWS-Konten in derselben Organisation gemeinsam nutzen. AWS Auf diese Weise können Sie die Infrastruktur einmal bereitstellen und sie für alle vertrauenswürdigen Konten wiederverwenden. So können Sie Kosten senken und gleichzeitig die Verantwortlichkeiten trennen. Weitere Informationen finden Sie Oracle Database@AWS im Oracle Database@AWS Benutzerhandbuch unter Gemeinsame Nutzung von Ressourcen.	 N	 N Kann nur innerhalb AWS-Konten der eigenen Organisation geteilt werden.	 N	 Nein

AWS Outposts

Sie können die folgenden AWS Outposts Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Outposts `outposts:Outpost`	Erstellen und verwalten Sie Outposts zentral und teilen Sie sie mit anderen AWS-Konten in Ihrer Organisation. Auf diese Weise können mehrere Konten Subnetze und EBS-Volumes auf Ihren gemeinsam genutzten, zentral verwalteten Outposts erstellen. Weitere Informationen finden Sie im AWS Outposts Benutzerhandbuch unter Arbeiten mit gemeinsam AWS genutzten Outposts-Ressourcen.	 N	 N Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	 Ja	 Nein
Routing-Tabellen für das lokale Gateway	Erstellen und verwalten Sie VPC-Verknüpfungen zu einem lokalen Gateway zentral und teilen Sie sie mit	 N	 N	 N	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
`ec2:LocalGatewayRouteTable`	anderen Personen AWS-Konten in Ihrer Organisation. Auf diese Weise können mehrere Konten VPC-Verknüpfungen zu einem lokalen Gateway erstellen und die Routentabelle und die Konfiguration der virtuellen Schnittstelle anzeigen. Weitere Informationen finden Sie im Benutzerhandbuch unter Gemeinsam nutzbare Outpost-Ressourcen.AWS Outposts		Kann nur mit der eigenen AWS-Konten Organisation geteilt werden.		

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Websites von Outposts `outposts:Site`	Erstellen und verwalten Sie Outpost-Websites und teilen Sie sie mit anderen Mitgliedern Ihrer AWS-Konten Organisation. Auf diese Weise können mehrere Konten Outposts auf der gemeinsam genutzten Site erstellen und verwalten, und es wird eine geteilte Steuerung zwischen den Outpost-Ressourcen und der Site unterstützt. Weitere Informationen finden Sie im AWS Outposts Benutzerhandbuch unter Arbeiten mit gemeinsam AWS genutzten Outposts-Ressourcen.	 N	 Ja Kann mit jedem AWS-Konto geteilt werden.	 N	 Nein

Amazon S3 on Outposts

Sie können die folgende Amazon S3 on Outposts-Ressource mit anderen teilen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
S3 auf Outpost `s3-outposts:Outpost`	Erstellen und verwalten Sie Amazon S3 S3-Buckets, Access Points und Endpoints auf dem Outpost. Auf diese Weise können mehrere Konten Outposts auf der gemeinsam genutzten Site erstellen und verwalten, und es wird eine geteilte Steuerung zwischen den Outpost-Ressourcen und der Site unterstützt. Weitere Informationen finden Sie im AWS Outposts Benutzerhandbuch unter Arbeiten mit gemeinsam AWS genutzten Outposts-Ressourcen.	 N	 N Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	 Ja	 Nein

AWS Private Certificate Authority

Sie können die folgenden AWS Private CA Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Private Zertifizierungsstelle () CAs `acm-pca:CertificateAuthority`	Erstellen und verwalten Sie private Zertifizierungsstellen (CAs) für die interne Public-Key-Infrastruktur (PKI) Ihrer Organisation und teilen Sie diese CAs mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können AWS Certificate Manager Benutzer in anderen Konten X.509-Zertifikate ausstellen, die von Ihrer gemeinsamen Zertifizierungsstelle signiert wurden. Weitere Informationen finden Sie im AWS Private Certificate Authority Benutzerhandbuch unter Steuern des Zugriffs auf eine private Zertifizierungsstelle.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Nein	 Ja

AWS Resource Explorer

Sie können die folgenden AWS Resource Explorer Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Ansichten des Resource Explorers `resource-explorer-2:View`	Erstellen und konfigurieren Sie Resource Explorer-Ansichten zentral und geben Sie sie für andere Benutzer AWS-Konten in Ihrer Organisation frei. Auf diese Weise können Rollen und Benutzer in mehreren Gruppen AWS-Konten nach den Ressourcen suchen und diese entdecken, auf die über die Ansicht zugegriffen werden kann. Weitere Informationen finden Sie im AWS Resource Explorer Benutzerhandbuch unter Teilen von Resource Explorer-Ansichten.	 N	 N Kann nur innerhalb AWS-Konten der eigenen Organisation geteilt werden.	 N	 Nein

AWS -Ressourcengruppen

Sie können die folgenden AWS -Ressourcengruppen Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Ressourcengruppen `resource-groups:Group`	Erstellen und verwalten Sie eine Host-Ressourcengruppe zentral und teilen Sie sie mit anderen Personen AWS-Konten in Ihrer Organisation. Auf diese Weise können sich mehrere eine Gruppe von Amazon EC2 Dedicated Hosts AWS-Konten teilen, die mit AWS License Manager erstellt wurden. Weitere Informationen finden Sie unter Host-Ressourcengruppen AWS License Manager im AWS License Manager Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

Amazon Route 53

Sie können die folgenden Amazon Route 53-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Route 53 Resolver Firewall-Regelgruppen `route53resolver:FirewallRuleGroup`	Erstellen und verwalten Sie die Route 53 Resolver DNS-Firewall-Regelgruppen zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten gemeinsam eine Reihe von Kriterien für die Prüfung und Bearbeitung ausgehender DNS-Abfragen verwenden, die über den Route 53 Resolver gesendet werden. Weitere Informationen finden Sie unter Gemeinsame Nutzung von Route 53-Resolver-DNS-Firewall-Regelgruppen AWS-Konte	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Nein	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	n im Amazon Route 53-Entwicklerhandbuch.				
Route 53 Profiles `route53profiles:Profile`	Erstellen und verwalten Sie Route 53 Profiles zentral und teilen Sie sie mit anderen Personen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten die in Route 53 angegebenen DNS-Konfigurationen Profiles auf mehrere Konten anwenden VPCs. Weitere Informationen finden Sie unter Amazon Route 53 Profiles im Amazon Route 53 Developer Guide.	 Ja	 Ja Kann mit jedem teilen AWS-Konto.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Resolver-Regeln `route53resolver:ResolverRule`	Erstellen und verwalten Sie Resolver-Regeln zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten DNS-Abfragen von ihren virtuellen privaten Clouds (VPCs) an die Ziel-IP-Adressen weiterleiten, die in gemeinsamen, zentral verwalteten Resolver-Regeln definiert sind. Weitere Informationen finden Sie unter Resolver-Regeln mit anderen teilen AWS-Konten und gemeinsame Regeln verwenden im Amazon Route 53 Developer Guide.	 N	 Ja Kann mit jedem AWS-Konto geteilt werden.	 N	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Konfigurationen für die Protokollierung von Resolver-Abfragen `route53resolver:ResolverQueryLogConfig`	Erstellen und verwalten Sie Abfrageprotokolle zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer DNS-Abfragen, die ihren VPCs Ursprung haben, in einem zentral verwalteten Abfrageprotokoll protokollieren. Weitere Informationen finden Sie unter Gemeinsame Nutzung von Resolver-Abfrageprotokollierungskonfigurationen mit anderen AWS-Konten im Amazon Route 53-Entwicklerhandbuch.	Ja	Ja Kann mit jedem AWS-Konto geteilt werden.	Ja	Nein

Amazon Simple Storage Service

Sie können die folgenden Amazon Simple Storage Service Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
S3-Zugriffsberechtigungen `s3:AccessGrants`	Erstellen und verwalten Sie die S3 Access Grants Instance zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten gemeinsam genutzte Ressourcen anzeigen und löschen. Weitere Informationen finden Sie im Amazon Simple Storage Service Benutzerhandbuch unter S3 Access gewährt kontoüber greifenden Zugriff.	Ja	Ja Kann mit jedem AWS-Konto geteilt werden.	Ja	Ja

Amazon SageMaker KI

Sie können die folgenden Amazon SageMaker AI-Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker KI-Ressourcenkatalog `sagemaker:SagemakerCatalog`	Aus Gründen der Auffindbarkeit — ermöglicht es Kontoinhabern, anderen Konten für alle Featuregruppen-Ressourcen im AI-Katalog Auffindbarkeitsberechtigungen zu gewähren. SageMaker Sobald der Zugriff gewährt wurde, können Benutzer dieser Konten die Funktionsgruppen, die mit ihnen geteilt wurden, im Katalog einsehen. Weitere Informationen finden Sie unter Kontenübergreifende Auffindbarkeit und Zugriff auf Funktionsgruppen im Amazon SageMaker AI Developer Guide. **Note** Auffindbarkeit und Zugriff	N	Ja Kann mit jedem AWS-Konto geteilt werden.	Ja	Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	sind separate Berechtigungen in KI. SageMaker				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker KI-Funktionsgruppen `sagemaker:FeatureGroup`	Für den Zugriff — ermöglicht Kontoinhabern, anderen Konten Zugriffsberechtigungen für ausgewählte Featuregruppenressourcen zu gewähren. Sobald der Zugriff gewährt wurde, können Benutzer dieser Konten die Funktionsgruppen verwenden, die mit ihnen geteilt wurden. Weitere Informationen finden Sie unter Kontenübergreifende Auffindbarkeit und Zugriff auf Funktionsgruppen im Amazon SageMaker AI Developer Guide. **Note** Auffindbarkeit und Zugriff sind separate Berechtig	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	ungen in KI. SageMaker				
SageMaker KI-Hubs `sagemaker:Hub`	Mit Amazon SageMaker AI JumpStart können Sie sie `sagemaker:Hub` zentral erstellen und verwalten und mit anderen innerhalb AWS-Konten derselben Organisation teilen. Weitere Informationen finden Sie unter Steuern des Zugriffs auf das Foundation-Modell mithilfe von privaten kuratierten Hubs in Amazon SageMaker AI JumpStart im Amazon SageMaker AI Developer Guide.	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker AI Lineage-Gruppen `sagemaker:LineageGroup`	Mit Amazon SageMaker AI können Sie Abstammungsgruppen Ihrer Pipeline-Metadaten erstellen, um ein tieferes Verständnis ihrer Geschichte und ihrer Beziehungen zu erhalten. Teilen Sie die Abstammungsgruppe mit anderen AWS-Konten oder mit den Konten in Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen über die Herkunftsgruppe einsehen und die darin enthaltenen Tracking-Entitäten abfragen. Weitere Informationen finden Sie unter Accountübergreifendes Lineage Tracking im Amazon SageMaker AI Developer Guide.	 Ja	 Ja Kann mit jedem teilen. AWS-Konto	 Nein	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker KI-Modellkarten `sagemaker:ModelCard`	Amazon SageMaker AI erstellt Modellkarten, um wichtige Details zu Ihren Machine-Learning-Modellen (ML) an einem zentralen Ort zu dokumentieren und so die Verwaltung und Berichterstattung zu optimieren. Teilen Sie Ihre Model Cards mit anderen AWS-Konten oder mit den Konten in Ihrem Unternehmen, um eine Strategie für mehrere Konten für Ihre Machine-Learning-Operationen zu erreichen. Auf diese Weise können AWS-Konten Sie den Zugriff auf die Modellkarten für ihre ML-Aktivitäten mit anderen Konten teilen. Weitere Informationen finden Sie unter Amazon SageMaker AI Model Cards im	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Nein	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Amazon SageMaker AI Developer Guide.				
SageMaker AI Model-Paketgruppen `sagemaker:model-package-group`	Mit Amazon SageMaker AI Model Registry können Sie sie `sagemaker:model-package-group` zentral erstellen und verwalten und mit anderen teilen, AWS-Konten um Modellversionen zu registrieren. Weitere Informationen finden Sie unter Amazon SageMaker AI Model Registry im Amazon SageMaker AI Developer Guide.	 Ja	 Ja	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker Apps von KI-Partnern `sagemaker:PartnerApp`	Mit SageMaker KI-Partner-Apps können Sie SageMaker KI-Partner-KI-Apps zentral erstellen und verwalten und den Zugriff darauf mit anderen teilen AWS-Konten. Weitere Informationen finden Sie unter Einrichtung von kontoübergreifendem Teilen für SageMaker KI-Apps von Amazon AI-Partnern im Amazon SageMaker AI Developer Guide.	 Ja	 Ja Kann mit jedem AWS-Konto teilen.	 Nein	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker KI-Pipelines `sagemaker:Pipeline`	Mit Amazon SageMaker AI Model Building Pipelines können Sie end-to-end Machine-Learning-Workflows in großem Umfang erstellen, automatisieren und verwalten. Teilen Sie Ihre Pipelines mit anderen AWS-Konten oder den Konten in Ihrer Organisation, um eine Strategie mit mehreren Konten für Ihre Machine-Learning-Operationen zu erreichen. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen über eine Pipeline und ihre Ausführungen einsehen und haben optional Zugriff darauf, Pipelines von anderen Konten aus zu starten, zu beenden und	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	erneut zu versuchen. Weitere Informationen finden Sie unter Kontoübergreifender Support für SageMaker KI-Pipelines im Amazon SageMaker AI Developer Guide.				

AWS Service Catalog AppRegistry

Sie können die folgenden AWS Service Catalog AppRegistry Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AppRegistry Anwendungen `servicecatalog:Applications`	Erstellen Sie eine Anwendung und verwenden Sie sie, um die zu dieser Anwendung gehörenden Ressourcen in	N	N Kann nur mit AWS-	Ja	Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Ihrer gesamten AWS Umgebung zu verfolgen. Teilen Sie die Anwendung mit anderen AWS-Konten Personen oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen über die Anwendung und die damit verbundenen Ressourcen lokal einsehen. Weitere Informationen finden Sie unter Erstellen von Anwendungen im Service Catalog-Benutzerhandbuch.		Konten der eigenen Organisation geteilt werden.		

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AppRegistry Attributgruppen `servicecatalog:AttributeGroups`	Erstellen Sie eine Attributgruppe und verwenden Sie sie, um Metadaten zu Ihren Anwendungen zu speichern. Teilen Sie die Attributgruppen mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen zu den Attributgruppen einsehen. Weitere Informationen finden Sie unter Erstellen von Attributgruppen im Service Catalog-Benutzerhandbuch.	N	N Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	Ja	Nein

AWS Systems Manager Incident Manager

Sie können die folgenden AWS Systems Manager Incident Manager Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Incident-Manager-Kontakte `ssm-contacts:Contact`	Erstellen und verwalten Sie Kontakte und Eskalationspläne zentral und geben Sie die Kontaktdaten an andere Personen AWS-Konten oder Ihre Organisation weiter. Auf diese Weise können sich viele Nutzer die Interaktionen AWS-Konten ansehen, die während eines Vorfalls stattgefunden haben. **Note** Derzeit wird die Möglichkeit, einen Kontakt, der von einem anderen Konto aus geteilt wurde, zu einem Notfallplan hinzuzufügen, nicht unterstützt.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Weitere Informationen finden Sie unter Arbeiten mit gemeinsamen Kontakten und Reaktionsplänen im AWS Systems Manager Incident Manager-Benutzerhandbuch.				

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Reaktionspläne des Incident Managers `ssm-incidents:ResponsePlan`	Erstellen und verwalten Sie Reaktionspläne zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können diese CloudWatch Amazon-Alarme und EventBridge Amazon-Ereignisregeln mit Reaktionsplänen AWS-Konten verbinden und automatisch einen Vorfall erstellen, wenn er erkannt wird. Der Vorfall hat auch Zugriff auf die Metriken dieser anderen AWS-Konten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsamen Kontakten und Reaktionsplänen im AWS Systems Manager Incident Manager-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

AWS Systems Manager

Sie können die folgenden AWS Systems Manager Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Richtlinien für automatische Ablehnung von SSM JITNA `ssm:Document`	Erstellen Sie mit Systems Manager eine Genehmigungsrichtlinie für den just-in-time Knotenzugriff. Eine Zugriffsverweigerungsrichtlinie verhindert ausdrücklich die automatische Genehmigung von Zugriffsanforderungen an die von Ihnen angegebenen Knoten. Teilen Sie die Richtlinie zur Zugriffsverweigerung mit anderen AWS-Konten oder Ihrer Organisation. Dadurch wird sichergestellt, dass Ihre Richtlinie zur Zugriffsverweigerung für den just-in-time Knotenzugriff für alle Konten in Ihrer	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Organisation gilt. Weitere Informationen finden Sie unter Just-in-time Knotenzugriff mit Systems Manager im AWS Systems Manager Benutzerhandbuch.				

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Parameter > Erweiterte Parameter speichern `ssm:Parameter`	Erstellen Sie einen Parameter und verwenden Sie ihn, um Konfigurationsdaten zu speichern, auf die Sie in Ihren Skripten, Befehlen, SSM-Dokumenten sowie Konfigurations- und Automatisierungsworkflows verweisen können. Teilen Sie den Parameter mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer Informationen über die Zeichenfolge einsehen und die Sicherheit erhöhen, indem Ihre Daten von Ihrem Code getrennt werden. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Arbeiten mit	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	gemeinsam genutzten Parametern.				

Amazon VPC

Sie können die folgenden Amazon Virtual Private Cloud (Amazon VPC) -Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Im Besitz des Kunden IPv4pool `ec2:CoipPool`	AWS Erstellt während des AWS Outposts Installationsvorgangs auf der Grundlage der von Ihnen bereitgestellten Informationen zu Ihrem lokalen Netzwerk einen Adresspool, der als kundeneigener IP-Adresspool bezeichnet wird.	 N	 N Kann nur AWS-Konten mit der eigenen Organisation geteilt werden.	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Kundeneigene IP-Adressen bieten lokale oder externe Konnektivität zu Ressourcen in Ihren Outposts-Subnetzen über Ihr lokales Netzwerk. Sie können diese Adressen Ressourcen auf Ihrem Outpost zuweisen, z. B. EC2-Instances, indem Sie Elastic IP-Adressen verwenden oder die Subnetzeinstellung verwenden, die automatisch kundeneigene IP-Adressen zuweist. Weitere Informationen finden Sie unter Kundeneigene IP-Adressen im AWS Outposts -Benutzerhandbuch.				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
IPAM-Pools `ec2:IpamPool`	Teilen Sie Amazon VPC IPAM-Pools zentral mit anderen AWS-Konten IAM-Rollen oder -Benutzern oder einer ganzen Organisation oder Organisationseinheit (OU) in. AWS Organizations Auf diese Weise können diese Principals Ressourcen CIDRs aus dem Pool AWS Ressourcen zuweisen, z. B. VPCs in ihren jeweiligen Konten. Weitere Informationen finden Sie unter Einen IPAM-Pool gemeinsam nutzen AWS RAM im Amazon VPC IP Address Manager-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Entdeckungen von IPAM-Ressourcen `ec2:IpamResourceDiscovery`	Teilen Sie Ressourcenentdeckungen mit anderen AWS-Konten. Eine Ressourcenerkennung ist eine Amazon VPC IPAM-Komponente, die es IPAM ermöglicht, Ressourcen zu verwalten und zu überwachen, die zum Eigentümerkonto gehören. Weitere Informationen finden Sie unter Arbeiten mit Ressourcenerkennungen im Benutzerhandbuch für Amazon VPC IPAM.	 N	 Ja Kann mit jedem geteilt werden. AWS-Konto	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Präfixliste `ec2:PrefixList`	Erstellen und verwalten Sie Präfixlisten zentral und teilen Sie sie mit anderen AWS-Konten Personen oder Ihrer Organisation. Dadurch können mehrere Präfixlisten in ihren Ressourcen AWS-Konten referenziert werden, z. B. VPC-Sicherheitsgruppen und Subnetz-Routetabellen. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Präfixlisten im Amazon VPC-Benutzerhandbuch.	 N	 Ja Kann mit jedem AWS-Konto geteilt werden.	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Subnets `ec2:Subnet`	Erstellen und verwalten Sie Subnetze zentral und geben Sie sie AWS-Konten innerhalb Ihrer Organisation frei. Auf diese Weise können mehrere AWS-Konten Benutzer ihre Anwendungsressourcen in zentral verwalteten VPCs starten. Zu diesen Ressourcen gehören Amazon EC2 EC2-Instances, Amazon Relational Database Service (RDS) -Datenbanken, Amazon Redshift Redshift-Cluster und Funktionen. AWS Lambda Weitere Informationen finden Sie unter Arbeiten mit VPC-Sharing im Amazon VPC-Benutzerhandbuch.	 N	 N Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Note Um bei der Erstellung einer Ressourcenfreigabe ein Subnetz einzubeziehen, benötigen Sie zusätzlich zu die `ec2:DescribeVpcs` Berechtigungen `ec2:DescribeSubnets` und. `ram:CreateResourceShare` Standard-Subnetze können nicht gemeinsam genutzt werden. Sie können nur Subnetze teilen, die Sie selbst erstellt haben.				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Sicherheitsgruppen `ec2:SecurityGroup`	Erstellen und verwalten Sie Sicherheitsgruppen zentral und teilen Sie sie mit anderen Personen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Benutzer die Sicherheitsgruppe ihren Elastic Network-Schnittstellen AWS-Konten zuordnen. Weitere Informationen finden Sie unter Eine Sicherheitsgruppe teilen im Amazon VPC-Benutzerhandbuch.	 Ja	 Nein Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Ziele von Traffic Mirror `ec2:TrafficMirrorTarget`	Erstellen und verwalten Sie Traffic-Mirror-Ziele zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Benutzer gespiegelten Netzwerkverkehr von Traffic Mirror-Quellen in ihren Konten an ein gemeinsames, zentral verwaltetes Traffic Mirror-Ziel senden. Weitere Informationen finden Sie unter Kontenübergreifende Traffic-Spiegelungsziele im Traffic Mirroring Guide.	 N	 Ja Kann mit jedem geteilt werden. AWS-Konto	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Transit Gateways `ec2:TransitGateway`	Erstellen und verwalten Sie Transit-Gateways zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Personen den Verkehr zwischen ihren VPCs und lokalen Netzwerken über ein gemeinsam genutztes, zentral verwaltetes Transit-Gateway weiterleiten. Weitere Informationen finden Sie unter Gemeinsame Nutzung eines Transit-Gateways in den Amazon VPC Transit Gateways. **Note** Um bei der Erstellung einer Ressource nfreigabe ein Transit-	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Gateway einzubeziehen, benötigen Sie zusätzlich zu die `ec2:DescribeTransitGateway` entsprechende Berechtigung. `ram:CreateResourceShare`				

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Transit-Gateway-Multicast-Domänen `ec2:TransitGatewayMulticastDomain`	Erstellen und verwalten Sie Transit-Gateway-Multicast-Domänen zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Gruppenmitglieder oder Gruppenquellen in der AWS-Konten Multicast-Domäne an- und abmelden. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Multicast-Domänen im Transit Gateways Guide.	 N	 Ja Kann mit jedem geteilt werden. AWS-Konto	 N	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
AWS Verified Access Gruppen `ec2:VerifiedAccessGroup`	Erstellen und verwalten Sie AWS Verified Access Gruppen zentral und teilen Sie sie dann mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Anwendungen in mehreren Konten einen einzigen, gemeinsamen Satz von AWS Verified Access Endpunkten verwenden. Weitere Informationen finden Sie AWS Resource Access Manager im AWS Verified Access Benutzerhandbuch unter Ihre AWS Verified Access Gruppe teilen.	Ja	Ja Kann mit jedem geteilt werden AWS-Konto.	N	Nein

Amazon VPC Lattice

Sie können die folgenden Amazon VPC Lattice-Ressourcen gemeinsam nutzen, indem Sie. AWS RAM

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Konfiguration der Amazon VPC Lattice-Ressourcen `vpc-lattice:ResourceConfiguration`	Erstellen Sie eine Ressourcenkonfiguration in Amazon VPC Lattice, um VPC-Ressourcen für mehrere Konten gemeinsam zu nutzen und. VPCs In der Ressourcenkonfiguration geben Sie an, wer auf diese Ressource zugreifen kann, und geben das Ressource n-Gateway an, über das Sie die Ressource gemeinsam nutzen möchten. Verbraucher können über einen Ressourcen-VPC-Endpunkt, den sie erstellen, auf die VPC-Ressource zugreifen. AWS PrivateLink Weitere Informationen finden Sie unter Zugreifen auf VPC-Ressourcen durch AWS PrivateLink im AWS PrivateLink Benutzerhandbuch	 N	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	und unter Ressourcenkonfiguration für VPC-Ressourcen im VPC Lattice-Benutzerhandbuch.				
Amazon VPC Lattice-Dienste `vpc-lattice:Service`	Erstellen und verwalten Sie Amazon VPC Lattice-Dienste zentral und teilen Sie sie mit Einzelpersonen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Servicebetreiber die service-to-service Kommunikation in einer Umgebung mit mehreren Konten verbinden, sichern und beobachten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Ressourcen im VPC Lattice-Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM-Benutzern und -Rollen geteilt werden	Kann mit Konten außerhalb der eigenen Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Amazon VPC Lattice-Servicenetzwerk `vpc-lattice:ServiceNetwork`	Erstellen und verwalten Sie Amazon VPC Lattice-Servicenetzwerke zentral und teilen Sie sie mit Einzelpersonen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Besitzer von Servicenetzwerken die service-to-service Kommunikation in einer Umgebung mit mehreren Konten verbinden, sichern und beobachten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Ressourcen im Amazon VPC Lattice-Benutzerhandbuch.	 Nein	 Ja Kann mit jedem geteilt werden. AWS-Konto	 Ja	 Nein

Verwaltung von Berechtigungen in AWS RAM

In AWS RAM gibt es zwei Arten von verwalteten Berechtigungen:AWS verwaltete Berechtigungen und vom Kunden verwaltete Berechtigungen.

Verwaltete Berechtigungen definieren, wie ein Verbraucher auf die Ressourcen in einer gemeinsam genutzten Ressource reagieren kann. Wenn Sie eine Ressourcenfreigabe erstellen, müssen Sie angeben, welche verwalteten Berechtigungen für jeden in der Ressourcenfreigabe enthaltenen Ressourcentyp verwendet werden sollen. Die Richtlinienvorlage in der verwalteten Berechtigung enthält alles, was für eine ressourcenbasierte Richtlinie erforderlich ist, mit Ausnahme des Prinzipals und der Ressource. Der Amazon-Ressourcenname (ARN) der Ressource und der ARN der Principals, die der Ressourcenfreigabe zugeordnet sind, vervollständigen die Elemente einer ressourcenbasierten Richtlinie.AWS RAM verfasst dann die ressourcenbasierte Richtlinie, die allen Ressourcen in dieser Ressourcenfreigabe zugewiesen wird.

Jede verwaltete Berechtigung kann eine oder mehrere Versionen haben. Eine Version wird als Standardversion für diese verwaltete Berechtigung festgelegt. Gelegentlich AWS aktualisiert eine AWS verwaltete Berechtigung für einen Ressourcentyp, indem eine neue Version erstellt und diese neue Version als Standardversion festgelegt wird. Sie können Ihre vom Kunden verwalteten Berechtigungen auch aktualisieren, indem Sie neue Versionen erstellen. Verwaltete Berechtigungen, die bereits mit einer Ressourcenfreigabe verknüpft sind, werden nicht automatisch aktualisiert. Die AWS RAM Konsole zeigt an, wann eine neue Standardversion verfügbar ist, und Sie können die Änderungen in der neuen Standardversion im Vergleich zur vorherigen überprüfen.

> **Note**
>
> Wir empfehlen, so bald wie möglich auf die neue Version der AWS verwalteten Berechtigung zu aktualisieren. Diese Updates bieten in der Regel Unterstützung für neue oder aktualisierte Ressourcentypen, mit AWS-Services denen weitere Ressourcentypen gemeinsam genutzt werden können AWS RAM. Eine neue Standardversion kann auch Sicherheitslücken beheben und korrigieren.

> **Important**
>
> Sie können nur die Standardversion der verwalteten Berechtigung an eine neue Ressourcenfreigabe anhängen.

Sie können die Liste der verfügbaren verwalteten Berechtigungen jederzeit abrufen. Weitere Informationen finden Sie unter Verwaltete Berechtigungen anzeigen.

Themen

Verwaltete Berechtigungen anzeigen

In Ihren Ressourcenfreigaben können Sie sich Details zu verwalteten Berechtigungen anzeigen lassen, die Sie Ressourcentypen zuweisen können. Sie können die verwalteten Berechtigungen identifizieren, die Ressourcenfreigaben zugewiesen sind. Um diese Details einzusehen, verwenden Sie die Bibliothek für verwaltete Berechtigungen in der AWS RAM Konsole.

Console

Einzelheiten zu verwalteten Berechtigungen finden Sie unter AWS RAM

1. Navigieren Sie in der AWS RAM Konsole zur Seite mit der Bibliothek für verwaltete Berechtigungen.
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. `us-east-1` Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen. Zwar verfügen alle Regionen über dieselben verfügbaren AWS verwalteten Berechtigungen, dies wirkt sich jedoch auf die Anzahl der zugehörigen Ressourcenfreigaben aus, die für jede verwaltete Berechtigung in angezeigt werdenStep 5. Vom Kunden verwaltete Berechtigungen sind nur in der Region verfügbar, in der sie erstellt wurden.
3. Wählen Sie in der Liste Verwaltete Berechtigungen die verwaltete Berechtigung aus, für die Sie Details anzeigen möchten. Sie können das Suchfeld verwenden, um die Liste der

verwalteten Berechtigungen zu filtern, indem Sie einen Teil eines Namens oder eines Ressourcentyps eingeben oder einen verwalteten Berechtigungstyp aus der Dropdownliste auswählen.

4. (Optional) Um die Anzeigeeinstellungen zu ändern, wählen Sie das Zahnradsymbol oben rechts im Bereich Verwaltete Berechtigungen. Sie können die folgenden Einstellungen ändern:

   - Seitengröße — Die Anzahl der Ressourcen, die auf jeder Seite angezeigt werden.
   - Zeilen umbrechen — Gibt an, ob Zeilen in Tabellenzeilen umgebrochen werden sollen.
   - Spalten — Gibt an, ob Informationen über den Ressourcentyp und die zugehörigen Anteile ein- oder ausgeblendet werden sollen.

   Wenn Sie mit der Einstellung der Anzeigeeinstellungen fertig sind, wählen Sie Bestätigen.

5. Für jede verwaltete Berechtigung werden in der Liste die folgenden Informationen angezeigt:

   - Name der verwalteten Berechtigung — Der Name der verwalteten Berechtigung.
   - Ressourcentyp — Der Ressourcentyp, der der verwalteten Berechtigung zugeordnet ist.
   - Verwalteter Berechtigungstyp — Gibt an, ob es sich bei der AWS verwalteten Berechtigung um eine verwaltete oder eine vom Kunden verwaltete Berechtigung handelt.
   - Zugeordnete Freigaben — Die Anzahl der Ressourcenfreigaben, die der verwalteten Berechtigung zugeordnet sind. Wenn eine Zahl angezeigt wird, können Sie die Zahl auswählen, um eine Tabelle mit Ressourcenfreigaben mit den folgenden Informationen anzuzeigen:
     - Name der Ressourcenfreigabe — Der Name der Ressourcenfreigabe, die der verwalteten Berechtigung zugeordnet ist.
     - Version der verwalteten Berechtigung — Die Version der verwalteten Berechtigung, die mit dieser Ressourcenfreigabe verknüpft ist.
     - Besitzer — Die AWS-Konto Nummer des Besitzers der Ressourcenfreigabe.
     - Externe Prinzipale zulassen — Gibt an, ob diese Ressourcenfreigabe die gemeinsame Nutzung mit Prinzipalen außerhalb der Organisation innerhalb der Organisation ermöglicht. AWS Organizations
     - Status — Der aktuelle Status der Zuordnung zwischen der Ressourcenfreigabe und der verwalteten Berechtigung.
   - Status — Beschreibt, ob die verwaltete Berechtigung wie folgt lautet:

- Anfügbar — Sie können die verwaltete Berechtigung an Ihre Ressourcenfreigaben anhängen.
- Nicht anfügbar — Sie können die verwaltete Berechtigung nicht an Ihre Ressourcenfreigaben anhängen.
- Löschen — Die verwaltete Berechtigung ist nicht mehr aktiv und wird bald gelöscht.
- Gelöscht — Die verwaltete Berechtigung wurde gelöscht. Sie bleibt zwei Stunden lang sichtbar, bevor sie aus der Bibliothek mit verwalteten Berechtigungen verschwindet.

Sie können den Namen der verwalteten Berechtigung wählen, um weitere Informationen zu dieser verwalteten Berechtigung anzuzeigen. Auf der Detailseite für eine verwaltete Berechtigung werden die folgenden Informationen angezeigt:

- Ressourcentyp — Der AWS Ressourcentyp, für den diese verwaltete Berechtigung gilt.
- Anzahl der Versionen — Sie können bis zu fünf Versionen einer vom Kunden verwalteten Berechtigung haben.
- Standardversion — Gibt an, welche Version die Standardversion ist und daher automatisch allen neuen Ressourcenfreigaben zugewiesen wird, die diese verwaltete Berechtigung verwenden. Bei allen vorhandenen Ressourcenfreigaben, die unterschiedliche Versionen verwenden, werden Sie aufgefordert, die Ressourcenfreigabe auf die Standardversion zu aktualisieren.
- ARN — Der Amazon-Ressourcenname (ARN) der verwalteten Berechtigung. Die ARNs vier AWS verwalteten Berechtigungen verwenden das folgende Format:

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

  Die Teilzeichenfolge *[DefaultPermission]* (ohne die Klammern in einem tatsächlichen ARN) ist nur im Namen der einen verwalteten Berechtigung für diesen Ressourcentyp enthalten, der als Standard festgelegt ist.
- Versionen mit verwalteten Berechtigungen — Sie können wählen, welche Versionsinformationen in den Tabs unter dieser Dropdownliste angezeigt werden sollen.
  - Registerkarte „Details“:
    - Erstellungszeit — Datum und Uhrzeit der Erstellung dieser Version der verwalteten Berechtigung.

- Uhrzeit der letzten Aktualisierung — Datum und Uhrzeit der letzten Aktualisierung dieser Version der verwalteten Berechtigung.

- Registerkarte „Richtlinienvorlage“ — Die Liste der Dienstaktionen und -bedingungen, sofern zutreffend, die Prinzipale mit dieser Version der verwalteten Berechtigung für den zugehörigen Ressourcentyp ausführen können.
- Zugeordnete Ressourcenfreigaben — Die Liste der Ressourcenfreigaben, die diese Version der verwalteten Berechtigung verwenden.

AWS CLI

Um Details zu verwalteten Berechtigungen anzuzeigen, die in verfügbar sind AWS RAM

Sie können den list-permissionsBefehl verwenden, um eine Liste der verwalteten Berechtigungen abzurufen, die aktuell AWS-Region für das anrufende Konto zur Verwendung auf gemeinsam genutzten Ressourcen verfügbar sind.

```
$ 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"
        }
    ]
}
```

Sie können den ARN einer bestimmten verwalteten Berechtigung auch anhand ihres Namens im `--query` Parameter des `list-permissions` AWS CLI Befehls finden. Im folgenden Beispiel wird die Ausgabe so gefiltert, dass nur Elemente in den `permissions` Array-Ergebnissen enthalten sind, die dem angegebenen Namen entsprechen. Wir geben auch an, dass wir nur das ARN-Feld in den Ergebnissen und im Klartextformat anstelle des Standard-JSON sehen möchten.

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

Nachdem Sie den ARN der spezifischen verwalteten Berechtigung gefunden haben, an der Sie interessiert sind, können Sie deren Details, einschließlich des JSON-Richtlinientexts, abrufen, indem Sie den Befehl ausführen 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"
    }
}
```

Erstellen und Verwenden von kundenverwalteten Berechtigungen in AWS RAM

AWS Resource Access Manager (AWS RAM) bietet mindestens eine AWS verwaltete Berechtigung für jeden Ressourcentyp, den Sie gemeinsam nutzen können. Diese verwalteten Berechtigungen bieten jedoch möglicherweise keinen Zugriff mit den geringsten Rechten für Ihren Anwendungsfall

beim Teilen. Wenn eine der bereitgestellten AWS verwalteten Berechtigungen nicht funktioniert, können Sie Ihre eigene vom Kunden verwaltete Berechtigung erstellen.

Kundenverwaltete Berechtigungen sind verwaltete Berechtigungen, die Sie erstellen und verwalten, indem Sie genau angeben, welche Aktionen unter welchen Bedingungen mit gemeinsam genutzten Ressourcen ausgeführt werden können AWS RAM. Sie möchten beispielsweise den Lesezugriff für Ihre Amazon VPC IP Address Manager (IPAM) -Pools einschränken, die Ihnen helfen, Ihre IP-Adressen in großem Umfang zu verwalten. Sie können kundenverwaltete Berechtigungen für Ihre Entwickler einrichten, um IP-Adressen zuzuweisen, aber nicht den IP-Adressbereich einsehen, den andere Entwicklerkonten zuweisen. Sie können sich an die bewährte Methode der geringsten Rechte halten und nur die Berechtigungen gewähren, die für die Ausführung von Aufgaben auf gemeinsam genutzten Ressourcen erforderlich sind.

Darüber hinaus können Sie vom Kunden verwaltete Berechtigungen nach Bedarf aktualisieren oder löschen.

Themen

Erstellen Sie eine vom Kunden verwaltete Berechtigung

Vom Kunden verwaltete Berechtigungen sind spezifisch für eine AWS-Region. Stellen Sie sicher, dass Sie diese vom Kunden verwaltete Berechtigung in der entsprechenden Region erstellen.

Console

Um eine vom Kunden verwaltete Berechtigung zu erstellen

1. Führen Sie eine der folgenden Aktionen aus:
   - Navigieren Sie zur Bibliothek mit verwalteten Berechtigungen und wählen Sie Eine vom Kunden verwaltete Berechtigung erstellen aus.
   - Navigieren Sie in der Konsole direkt zur Seite „Vom Kunden verwaltete Rechte erstellen“.

2. Geben Sie für Details zur vom Kunden verwalteten Berechtigung einen Namen für die vom Kunden verwaltete Berechtigung ein.
3. Wählen Sie den Ressourcentyp aus, für den diese verwaltete Berechtigung gilt.
4. Für die Richtlinienvorlage definieren Sie, welche Operationen mit diesem Ressourcentyp ausgeführt werden dürfen.

   - Sie können „Verwaltete Berechtigung importieren“ wählen, um Aktionen aus einer vorhandenen verwalteten Berechtigung zu verwenden.
   - Wählen oder deaktivieren Sie Informationen zur Zugriffsebene, um Ihren Anforderungen im Visual Editor zu entsprechen.
   - Fügen Sie Bedingungen mit dem JSON-Editor hinzu oder ändern Sie sie.
5. (Optional) Um der verwalteten Berechtigung Tags anzuhängen, geben Sie unter Tags einen Tag-Schlüssel und einen Tag-Wert ein. Fügen Sie weitere Tags hinzu, indem Sie Neues Tag hinzufügen wählen. Wiederholen Sie diesen Schritt nach Bedarf.
6. Wenn Sie fertig sind, wählen Sie Vom Kunden verwaltete Berechtigung erstellen aus.

AWS CLI

Um eine vom Kunden verwaltete Berechtigung zu erstellen

- Führen Sie den Befehl create-permission aus und geben Sie einen Namen, den Ressourcentyp, für den die vom Kunden verwaltete Berechtigung gilt, und den Haupttext der Richtlinienvorlage an.

  Der folgende Beispielbefehl erstellt eine verwaltete Berechtigung für den `imagebuilder:Component` Ressourcentyp.

```
$ 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
    }
}
```

Erstellen Sie eine neue Version einer vom Kunden verwalteten Berechtigung

Wenn sich der Anwendungsfall für Ihre vom Kunden verwaltete Berechtigung ändert, können Sie eine neue Version der verwalteten Berechtigung erstellen. Dies wirkt sich nicht auf Ihre vorhandenen Ressourcenfreigaben aus, sondern nur auf die zukünftigen neuen Ressourcenfreigaben, die diese vom Kunden verwaltete Berechtigung verwenden.

Jede verwaltete Berechtigung kann bis zu fünf Versionen haben, aber Sie können nur die Standardversion zuordnen.

Console

Um eine neue Version einer vom Kunden verwalteten Berechtigung zu erstellen

1. Navigieren Sie zur Bibliothek mit verwalteten Berechtigungen.
2. Filtern Sie die Liste der verwalteten Berechtigungen nach Vom Kunden verwaltet, oder suchen Sie nach dem Namen der vom Kunden verwalteten Berechtigung, die Sie ändern möchten.
3. Wählen Sie auf der Seite mit den Details zu verwalteten Berechtigungen im Abschnitt Versionen mit verwalteten Berechtigungen die Option Version erstellen aus.
4. Für die Richtlinienvorlage können Sie Aktionen und Bedingungen mit dem visuellen Editor oder dem JSON-Editor hinzufügen oder entfernen.

   Sie haben auch die Möglichkeit, Verwaltete Berechtigungen importieren auszuwählen, um eine vorhandene Richtlinienvorlage zu verwenden.
5. Wenn Sie fertig sind, wählen Sie unten auf der Seite Version erstellen aus.

AWS CLI

Um eine neue Version einer vom Kunden verwalteten Berechtigung zu erstellen

1. Suchen Sie den Amazon-Ressourcennamen (ARN) der verwalteten Berechtigung, für die Sie eine neue Version erstellen möchten. Rufen Sie dazu list-permissions mit dem `--permission-type CUSTOMER_MANAGED` Parameter auf, um nur vom Kunden verwaltete Berechtigungen einzubeziehen.

```
$ 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. Nachdem Sie den ARN haben, können Sie den create-permission-versionVorgang aufrufen und die aktualisierte Richtlinienvorlage bereitstellen.

```
$ 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
    }
}
```

Die Ausgabe enthält die Versionsnummer der neuen Version.

Wählen Sie eine andere Version als Standard für eine vom Kunden verwaltete Berechtigung

Sie können eine andere vom Kunden verwaltete Berechtigungsversion als neue Standardversion festlegen.

Console

Um eine neue Standardversion für eine vom Kunden verwaltete Berechtigung festzulegen

1. Navigieren Sie zur Bibliothek mit verwalteten Berechtigungen.
2. Filtern Sie die Liste der verwalteten Berechtigungen nach Vom Kunden verwaltet, oder suchen Sie nach dem Namen der vom Kunden verwalteten Berechtigung, die Sie ändern möchten.
3. Wählen Sie auf der Seite mit den vom Kunden verwalteten Berechtigungen im Abschnitt Versionen verwalteter Berechtigungen mithilfe der Dropdownliste die Version aus, die Sie als neue Standardversion festlegen möchten.
4. Wählen Sie Als Standardversion festlegen aus.
5. Wenn das Dialogfeld angezeigt wird, bestätigen Sie, dass diese Version die Standardversion für alle neuen Ressourcenfreigaben sein soll, die diese vom Kunden verwaltete Berechtigung verwenden. Wenn Sie damit einverstanden sind, wählen Sie Als Standardversion festlegen.

AWS CLI

Um eine neue Standardversion für eine vom Kunden verwaltete Berechtigung festzulegen

1. Suchen Sie die Versionsnummer, die Sie als Standardversion festlegen möchten, indem Sie anrufen list-permission-versions.

   Mit dem folgenden Beispielbefehl werden die aktuellen Versionen für die angegebene verwaltete Berechtigung abgerufen.

```
$ 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. Nachdem Sie die Versionsnummer als Standard festgelegt haben, können Sie den set-default-permission-versionVorgang aufrufen.

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

   Dieser Befehl gibt bei Erfolg keine Ausgabe zurück. Sie können den list-permission-versionsVorgang erneut ausführen und überprüfen, ob das `defaultVersion` Feld der ausgewählten Version jetzt auf gesetzt ist`true`.

Löschen Sie eine vom Kunden verwaltete Berechtigungsversion

Sie können bis zu fünf Versionen jeder vom Kunden verwalteten Berechtigung haben. Wenn eine Version nicht mehr benötigt wird und nicht verwendet wird, können Sie sie löschen. Sie können die Standardversion einer vom Kunden verwalteten Berechtigung nicht löschen. Gelöschte Versionen bleiben bis zu zwei Stunden in der Konsole sichtbar und haben den Status Gelöscht, bevor sie vollständig entfernt werden.

Console

Um eine vom Kunden verwaltete Berechtigungsversion zu löschen

1. Navigieren Sie zur Bibliothek mit verwalteten Berechtigungen.
2. Filtern Sie die Liste der verwalteten Berechtigungen nach Vom Kunden verwaltet, oder suchen Sie nach dem Namen der vom Kunden verwalteten Berechtigung mit der Version, die Sie löschen möchten.
3. Stellen Sie sicher, dass die Version, die Sie löschen möchten, derzeit nicht die Standardversion ist.
4. Wählen Sie für den Abschnitt Versionen der Seite den Tab Zugeordnete Ressourcenfreigaben aus, um zu sehen, ob Freigaben diese Version verwenden.

   Wenn Shares verknüpft sind, müssen Sie die Version mit vom Kunden verwalteten Berechtigungen ändern, bevor Sie diese Version löschen können.
5. Wählen Sie auf der rechten Seite des Abschnitts Version die Option Version löschen aus.
6. Wählen Sie im Bestätigungsdialogfeld die Option Löschen aus, um zu bestätigen, dass Sie diese Version Ihrer vom Kunden verwalteten Berechtigung löschen möchten.

Wählen Sie Abbrechen, wenn Sie diese Version Ihrer vom Kunden verwalteten Berechtigung nicht löschen möchten.

AWS CLI

Um eine Version einer vom Kunden verwalteten Berechtigung zu löschen

1. Rufen Sie den list-permission-versionsVorgang auf, um die verfügbaren Versionsnummern abzurufen.
2. Nachdem Sie die Versionsnummer erhalten haben, geben Sie sie als Parameter für an delete-permission-version.

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

Dieser Befehl gibt bei Erfolg keine Ausgabe zurück. Sie können den Vorgang list-permission-versionserneut ausführen und überprüfen, ob die Version nicht mehr in der Ausgabe enthalten ist.

Löschen Sie eine vom Kunden verwaltete Berechtigung

Wenn eine vom Kunden verwaltete Berechtigung nicht mehr benötigt wird und nicht verwendet wird, können Sie sie löschen. Eine vom Kunden verwaltete Berechtigung, die einer Ressourcenfreigabe zugeordnet ist, kann nicht gelöscht werden. Die gelöschte vom Kunden verwaltete Berechtigung verschwindet nach zwei Stunden. Bis dahin bleibt sie in der Bibliothek mit verwalteten Berechtigungen mit dem Status Gelöscht sichtbar.

Console

Um eine vom Kunden verwaltete Berechtigung zu löschen

1. Navigieren Sie zur Bibliothek mit verwalteten Berechtigungen.
2. Filtern Sie die Liste der verwalteten Berechtigungen nach Vom Kunden verwaltet, oder suchen Sie nach dem Namen der vom Kunden verwalteten Berechtigung, die Sie löschen möchten.

3. Vergewissern Sie sich, dass in der Liste der verwalteten Berechtigungen 0 zugeordnete Shares vorhanden sind, bevor Sie die vom Kunden verwaltete Berechtigung auswählen.

   Wenn der verwalteten Berechtigung noch Ressourcenfreigaben zugeordnet sind, müssen Sie allen Ressourcenfreigaben eine weitere verwaltete Berechtigung zuweisen, bevor Sie fortfahren können.

4. Wählen Sie in der oberen rechten Ecke der Seite mit den vom Kunden verwalteten Berechtigungen die Option Verwaltete Berechtigung löschen aus.
5. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie Löschen, um die verwaltete Berechtigung zu löschen.

AWS CLI

Um eine vom Kunden verwaltete Berechtigung zu löschen

1. Suchen Sie den ARN der verwalteten Berechtigung, die Sie löschen möchten, indem Sie list-permissions mit dem `--permission-type CUSTOMER_MANAGED` Parameter aufrufen, um nur vom Kunden verwaltete Berechtigungen einzubeziehen.

```
$ 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. Nachdem Sie den ARN der verwalteten Löschberechtigung haben, geben Sie ihn als Parameter für delete-permission an.

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

Aktualisierung AWS verwalteter Berechtigungen auf eine neuere Version

Gelegentlich AWS werden die verwalteten Berechtigungen AWS aktualisiert, die für das Anhängen an eine Ressourcenfreigabe für einen bestimmten Ressourcentyp verfügbar sind. In AWS diesem Fall wird eine neue Version der AWS verwalteten Berechtigung erstellt. Ressourcenfreigaben, die den angegebenen Ressourcentyp enthalten, werden nicht automatisch aktualisiert, sodass sie die neueste Version der verwalteten Berechtigung verwenden. Sie müssen die verwalteten Berechtigungen für jede Ressourcenfreigabe explizit aktualisieren. Dieser zusätzliche Schritt ist erforderlich, damit Sie die Änderungen bewerten können, bevor Sie sie auf Ihre Ressourcenfreigaben anwenden.

Console

Immer wenn in der Konsole eine Seite angezeigt wird, auf der die mit einer Ressourcenfreigabe verknüpften Berechtigungen aufgeführt sind, und eine oder mehrere dieser Berechtigungen eine andere Version als die Standardversion für die Berechtigung verwenden, zeigt die Konsole oben auf der Konsolenseite ein Banner an. Das Banner weist darauf hin, dass Ihre Ressourcenfreigabe eine andere Version als die Standardversion verwendet.

Darüber hinaus kann bei individuellen Berechtigungen die Schaltfläche Auf Standardversion aktualisieren neben der aktuellen Versionsnummer angezeigt werden, wenn es sich bei dieser Version nicht um die Standardversion handelt.

Wenn Sie auf diese Schaltfläche klicken, wird der Assistent zum Aktualisieren von Ressourcenfreigaben gestartet. In Schritt 2 des Assistenten können Sie die Version aller nicht standardmäßigen Berechtigungen aktualisieren, sodass sie ihre Standardversionen verwenden.

Die Änderungen werden erst gespeichert, wenn Sie den Assistenten abgeschlossen haben, indem Sie auf der letzten Seite des Assistenten auf Absenden klicken.

> **Note**
>
> Sie können nur die Standardversion anhängen und nicht zu einer anderen Version zurückkehren.
> Bei vom Kunden verwalteten Berechtigungen können Sie nach dem Aktualisieren der Berechtigungen auf die Standardversion keine weitere Version auf eine Ressourcenfreigabe anwenden, es sei denn, Sie haben diese andere Version zuerst als Standardversion festgelegt. Wenn Sie beispielsweise eine Berechtigung auf die Standardversion aktualisiert haben und dann einen Fehler gefunden haben, den Sie rückgängig machen wollten, können Sie die vorherige Version als Standardversion festlegen. Sie können auch eine andere neue Version erstellen und diese dann als Standardversion festlegen. Nachdem Sie eine dieser Optionen ausgeführt haben, würden Sie Ihre Ressourcenfreigaben so aktualisieren, dass sie die aktuelle Standardversion verwenden.

AWS CLI

Um die Version einer AWS verwalteten Berechtigung zu aktualisieren

1. Führen Sie den Befehl get-resource-sharesmit dem `--permission-arn` Parameter aus, um den Amazon-Ressourcennamen (ARN) der verwalteten Berechtigung anzugeben, die Sie aktualisieren möchten. Dies führt dazu, dass der Befehl nur die Ressourcenfreigaben zurückgibt, die diese verwaltete Berechtigung verwenden.

   Der folgende Beispielbefehl gibt beispielsweise Details für jede Ressourcenfreigabe zurück, die die standardmäßige AWS verwaltete Berechtigung für Amazon EC2 EC2-Kapazitätsreservierungen verwendet.

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

   Die Ausgabe umfasst den ARN aller gemeinsam genutzten Ressourcen mit mindestens einer Ressource, deren Zugriff durch diese verwaltete Berechtigung gesteuert wird.

2. Führen Sie für jede im vorherigen Befehl angegebene Ressourcenfreigabe den Befehl aus associate-resource-share-permission. Fügen Sie den Parameter ein, `--resource-`

`share-arn` um die zu aktualisierende Ressourcenfreigabe anzugeben, den Parameter, `--permission-arn` um anzugeben, welche AWS verwaltete Berechtigung Sie aktualisieren möchten, und den `--replace` Parameter, um anzugeben, dass Sie die Freigabe aktualisieren möchten, sodass sie die neueste Version dieser verwalteten Berechtigung verwendet. Sie müssen die Versionsnummer nicht angeben. Die Standardversion wird automatisch verwendet.

```
$ 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. Wiederholen Sie den Befehl im vorherigen Schritt für jeden Befehl`ResourceShareArn`, den Sie in den Ergebnissen des Befehls in Schritt 1 erhalten haben.

Überlegungen zur Verwendung von vom Kunden verwalteten Berechtigungen in AWS RAM

Vom Kunden verwaltete Berechtigungen sind nur in dem Land verfügbar AWS-Region , in dem Sie sie erstellen. Nicht alle Ressourcentypen unterstützen vom Kunden verwaltete Berechtigungen. Eine Liste der unterstützten Ressourcentypen finden Sie unterGemeinsam nutzbare Ressourcen AWS. AWS Resource Access Manager

Vom Kunden verwaltete Berechtigungen mit mehreren Kontoauszügen werden nicht unterstützt. In vom Kunden verwalteten Berechtigungen können Sie nur einzelne Operatoren verwenden, die nicht negieren.

Die folgenden Bedingungen werden in vom Kunden verwalteten Berechtigungen nicht unterstützt:

- Bedingungsschlüssel, die verwendet werden, um die Eigenschaften des Prinzipals abzugleichen:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Bedingungsschlüssel, die verwendet werden, um den Zugriff für Dienstprinzipale einzuschränken:
  - `aws:SourceArn`

  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- System-Tags:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

> **Note**
>
> Der `aws:SourceAccount` Wert wird automatisch aufgefüllt, wenn er für Service Principals freigegeben wird.

Wie funktionieren verwaltete Berechtigungen

Sehen Sie sich für einen schnellen Überblick das folgende Video an, das zeigt, wie Sie mit verwalteten Berechtigungen die bewährte Methode des Zugriffs mit den geringsten Rechten auf Ihre AWS Ressourcen anwenden können.

In diesem Video wird gezeigt, wie vom Kunden verwaltete Berechtigungen nach der bewährten Methode der geringsten Rechte erstellt und verknüpft werden. Weitere Informationen finden Sie unter ???.

Wenn Sie eine Ressourcenfreigabe erstellen, ordnen Sie jedem Ressourcentyp, den Sie teilen möchten, eine AWS verwaltete Berechtigung zu. Wenn es für die verwaltete Berechtigung mehrere Versionen gibt, verwendet die neue Ressourcenfreigabe immer die Version, die als Standard festgelegt wurde.

Nachdem Sie die Ressourcenfreigabe erstellt haben,AWS RAM verwendet die verwaltete Berechtigung, um eine ressourcenbasierte Richtlinie zu generieren, die jeder gemeinsam genutzten Ressource zugewiesen wird.

Die Richtlinienvorlage in einer verwalteten Berechtigung gibt Folgendes an:

Auswirkung

Gibt an, ob `Allow` oder ob `Deny` die Hauptberechtigung zur Ausführung eines Vorgangs auf einer gemeinsam genutzten Ressource besteht. Bei einer verwalteten Berechtigung gilt die Wirkung immer`Allow`. Weitere Informationen finden Sie unter Effekt im IAM-Benutzerhandbuch.

Action

Die Liste der Vorgänge, zu deren Ausführung der Principal berechtigt ist. Dies kann eine Aktion in der AWS-Managementkonsole oder eine Operation in der AWS Command Line Interface(AWS CLI) oder AWS API sein. Die Aktionen werden durch die AWS Berechtigung definiert. Weitere Informationen finden Sie unter Aktion im IAM-Benutzerhandbuch.

Bedingung

Wann und wie ein Principal mit einer Ressource in einer Resource Share interagieren kann. Bedingungen fügen Ihren gemeinsam genutzten Ressourcen eine zusätzliche Sicherheitsebene hinzu. Verwenden Sie sie, um den Zugriff für vertrauliche Aktionen auf Ihre gemeinsam genutzten Ressourcen zu beschränken. Sie können beispielsweise Bedingungen angeben, nach denen die Aktionen aus einem bestimmten IP-Adressbereich des Unternehmens stammen müssen oder dass die Aktionen von Benutzern ausgeführt werden müssen, die mit Multi-Faktor-Authentifizierung authentifiziert wurden. Weitere Informationen zu Bedingungen finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch. Weitere Informationen zu dienstspezifischen Bedingungen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste in der Service Authorization Reference.

> **Note**
>
> Bedingungen sind für vom Kunden verwaltete Berechtigungen und unterstützte Ressourcentypen für AWS verwaltete Berechtigungen verfügbar.
> Informationen zu Bedingungen, die von der Verwendung mit vom Kunden verwalteten Berechtigungen ausgeschlossen sind, finden Sie unterÜberlegungen zur Verwendung von vom Kunden verwalteten Berechtigungen in AWS RAM.

Arten von verwalteten Berechtigungen

Wenn Sie eine Ressourcenfreigabe erstellen, wählen Sie eine verwaltete Berechtigung aus, um sie jedem Ressourcentyp zuzuordnen, den Sie in die Ressourcenfreigabe aufnehmen.AWS verwaltete Berechtigungen werden vom Dienst definiert, der die AWS Ressource besitzt, und sie

werden von verwaltet.AWS RAM Sie erstellen und verwalten Ihre eigenen, vom Kunden verwalteten Berechtigungen.

- AWS verwaltete Berechtigung — Für jeden Ressourcentyp, der diese Funktion AWS RAM unterstützt, ist eine verwaltete Standardberechtigung verfügbar. Die verwaltete Standardberechtigung ist diejenige, die für einen Ressourcentyp verwendet wird, sofern Sie nicht ausdrücklich eine der zusätzlichen verwalteten Berechtigungen auswählen. Die standardmäßige verwaltete Berechtigung soll die gängigsten Kundenszenarien für die gemeinsame Nutzung von Ressourcen des angegebenen Typs unterstützen. Die standardmäßige verwaltete Berechtigung ermöglicht es Prinzipalen, bestimmte Aktionen auszuführen, die vom Dienst für den Ressourcentyp definiert werden. Für den `ec2:Subnet` Ressourcentyp Amazon VPC können Principals mit der standardmäßigen verwalteten Berechtigung beispielsweise die folgenden Aktionen ausführen:
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  Die Namen der AWS verwalteten Standardberechtigungen verwenden das folgende Format:. `AWSRAMDefaultPermission`*`ShareableResourceType`* Für den `ec2:Subnet` Ressourcentyp lautet der Name der standardmäßigen AWS verwalteten Berechtigung beispielsweise`AWSRAMDefaultPermissionSubnet`.

  > **Note**
  >
  > Die verwaltete Standardberechtigung unterscheidet sich von der Standardversion einer verwalteten Berechtigung. Alle verwalteten Berechtigungen, unabhängig davon, ob es sich um Standardberechtigungen oder um eine der zusätzlichen verwalteten Berechtigungen handelt, die von einigen Ressourcentypen unterstützt werden, sind separate, vollständige Berechtigungen mit unterschiedlichen Auswirkungen und Aktionen, die unterschiedliche Freigabeszenarien unterstützen, z. B. Lese-/Schreibzugriff oder Nur-Lese-Zugriff.
  > Jede verwaltete Berechtigung, unabhängig davon, ob sie vom Kunden verwaltet AWS oder vom Kunden verwaltet wird, kann mehrere Versionen haben, von denen eine die Standardversion für diese Berechtigung ist.

  Wenn Sie beispielsweise einen Ressourcentyp gemeinsam nutzen, der sowohl eine verwaltete `Read` Vollzugriffsberechtigung `Write` als auch eine verwaltete Leseberechtigung unterstützt, können Sie eine Ressourcenfreigabe für den Administrator mit der verwalteten

Vollzugriffsberechtigung erstellen. Sie können dann eine separate Ressourcenfreigabe für andere Entwickler erstellen, indem Sie die verwaltete Leseberechtigung verwenden, um der Praxis der Gewährung der geringsten Rechte zu folgen.

> **Note**
>
> Alle AWS Dienste, die mit funktionieren,AWS RAM unterstützen mindestens eine verwaltete Standardberechtigung. Sie können die verfügbaren Berechtigungen für die einzelnen Berechtigungen AWS-Service auf der Bibliotheksseite für verwaltete Berechtigungen einsehen. Auf dieser Seite finden Sie Einzelheiten zu allen verfügbaren verwalteten Berechtigungen, einschließlich aller Ressourcenfreigaben, die derzeit mit der Berechtigung verknüpft sind, und gegebenenfalls, ob die gemeinsame Nutzung mit externen Prinzipalen zulässig ist. Weitere Informationen finden Sie unter Verwaltete Berechtigungen anzeigen.
>
> Bei Diensten, die keine zusätzlichen verwalteten Berechtigungen unterstützen, wird beim Erstellen einer Ressourcenfreigabe AWS RAM automatisch die Standardberechtigung angewendet, die für den von Ihnen ausgewählten Ressourcentyp definiert ist. Falls unterstützt, haben Sie auch die Möglichkeit, auf der Seite Verwaltete Berechtigungen zuordnen die Option Vom Kunden verwaltete Berechtigungen erstellen auszuwählen.

- Vom Kunden verwaltete Berechtigungen — Kundenverwaltete Berechtigungen sind verwaltete Berechtigungen, die Sie erstellen und verwalten, indem Sie genau angeben, welche Aktionen unter welchen Bedingungen mit Ressourcen ausgeführt werden können, die gemeinsam genutzt werden AWS RAM. Sie möchten beispielsweise den Lesezugriff für Ihre Amazon VPC IP Address Manager (IPAM) -Pools einschränken, die Ihnen helfen, Ihre IP-Adressen in großem Umfang zu verwalten. Sie können kundenverwaltete Berechtigungen für Ihre Entwickler einrichten, um IP-Adressen zuzuweisen, aber nicht den IP-Adressbereich einsehen, den andere Entwicklerkonten zuweisen. Sie können sich an die bewährte Methode der geringsten Rechte halten und nur die Berechtigungen gewähren, die für die Ausführung von Aufgaben auf gemeinsam genutzten Ressourcen erforderlich sind.

Sicherheit in AWS Resource Access Manager

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für AWS Resource Access Manager (AWS RAM) gelten, finden Sie unter Vom Compliance-Programm abgedeckte AWS -Services.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS RAM. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS RAM , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS RAM Ressourcen unterstützen.

Topics

Datenschutz in AWS Resource Access Manager

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Resource Access Manager. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der AWS RAM API oder auf andere AWS-Services Weise arbeiten oder diese verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die

für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Identitäts- und Zugriffsmanagement für AWS Resource Access Manager

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. Administratoren in IAM kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Mithilfe von IAM erstellen Sie Prinzipale wie Rollen, Benutzer und Gruppen in Ihrem. AWS-Konto Sie kontrollieren die Berechtigungen, die diese Prinzipale haben, um Aufgaben mithilfe von Ressourcen auszuführen. AWS Sie können IAM ohne zusätzliche Kosten nutzen. Weitere Informationen zur Verwaltung und Erstellung benutzerdefinierter IAM-Richtlinien finden Sie unter Verwaltung von IAM-Richtlinien im IAM-Benutzerhandbuch.

Topics

Wie AWS RAM funktioniert mit IAM

Standardmäßig sind IAM-Prinzipale nicht berechtigt, Ressourcen zu erstellen oder zu ändern. AWS RAM Um es IAM-Prinzipalen zu ermöglichen, Ressourcen zu erstellen oder zu ändern und Aufgaben auszuführen, führen Sie einen der folgenden Schritte aus. Diese Aktionen gewähren die Erlaubnis, bestimmte Ressourcen und API-Aktionen zu verwenden.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

AWS RAM bietet mehrere AWS verwaltete Richtlinien, die Sie verwenden können, um den Bedürfnissen vieler Benutzer gerecht zu werden. Weitere Informationen dazu finden Sie unter AWS verwaltete Richtlinien für AWS Resource Access Manager.

Wenn Sie eine genauere Kontrolle über die Berechtigungen benötigen, die Sie Ihren Benutzern gewähren, können Sie in der IAM-Konsole Ihre eigenen Richtlinien erstellen. Informationen zum Erstellen von Richtlinien und zum Anhängen dieser Richtlinien an Ihre IAM-Rollen und -Benutzer finden Sie im Benutzerhandbuch unter Richtlinien und Berechtigungen in IAM.AWS Identity and Access Management

Die folgenden Abschnitte enthalten die AWS RAM spezifischen Details zum Erstellen einer IAM-Berechtigungsrichtlinie.

Inhalt

Richtlinienstruktur

Eine IAM-Berechtigungsrichtlinie ist ein JSON-Dokument, das die folgenden Aussagen enthält: Effect, Action, Resource und Condition. Eine IAM-Richtlinie hat in der Regel die folgende Form.

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

Auswirkung

Die Effect-Anweisung gibt an, ob die Richtlinie einem Hauptbenutzer die Erlaubnis zur Ausführung einer Aktion gewährt oder verweigert. Zu den möglichen Werten gehören: `Allow` und`Deny`.

Action

Die Action-Anweisung gibt die AWS RAM API-Aktionen an, für die die Richtlinie die Genehmigung zulässt oder verweigert. Eine vollständige Liste der zulässigen Aktionen finden Sie AWS Resource Access Manager im IAM-Benutzerhandbuch unter Definierte Aktionen von.

Ressource

In der Ressourcenanweisung werden die AWS RAM Ressourcen angegeben, die von der Richtlinie betroffen sind. Um eine Ressource in der Anweisung anzugeben, müssen Sie ihren eindeutigen Amazon-Ressourcennamen (ARN) verwenden. Eine vollständige Liste der zulässigen Ressourcen finden Sie unter Resources defined by AWS Resource Access Manager im IAM-Benutzerhandbuch.

Bedingung

Zustandsanweisungen sind optional. Sie können verwendet werden, um die Bedingungen, unter denen die Richtlinie gilt, weiter zu verfeinern. AWS RAM unterstützt die folgenden Bedingungsschlüssel:

- `aws:RequestTag/${TagKey}`— Testet, ob die Serviceanfrage ein Tag mit dem angegebenen Tag-Schlüssel enthält, existiert und den angegebenen Wert hat.
- `aws:ResourceTag/${TagKey}`— Testet, ob der Ressource, auf die die Serviceanfrage reagiert hat, ein Tag mit einem Tag-Schlüssel angehängt ist, den Sie in der Richtlinie angeben.

  Mit der folgenden Beispielbedingung wird überprüft, ob der Ressource, auf die in der Serviceanfrage verwiesen wird, ein Tag mit dem Schlüsselnamen „Owner“ und dem Wert „Dev Team“ angehängt ist.

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

- `aws:TagKeys`— Gibt die Tag-Schlüssel an, die verwendet werden müssen, um eine Ressourcenfreigabe zu erstellen oder zu kennzeichnen.
- `ram:AllowsExternalPrincipals`— Testet, ob die Ressourcenfreigabe in der Serviceanfrage die gemeinsame Nutzung mit externen Prinzipalen ermöglicht. Bei AWS Organizations einem externen Principal handelt es sich um einen AWS-Konto externen Principal innerhalb Ihrer Organisation. Wenn das Ergebnis ergibt`False`, können Sie diese Ressourcenfreigabe nur mit Konten in derselben Organisation teilen.
- `ram:PermissionArn`— Testet, ob der in der Serviceanfrage angegebene Berechtigungs-ARN mit einer ARN-Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.
- `ram:PermissionResourceType`— Testet, ob die in der Serviceanfrage angegebene Berechtigung für den Ressourcentyp gültig ist, den Sie in der Richtlinie angeben. Geben Sie Ressourcentypen in dem Format an, das in der Liste der gemeinsam nutzbaren Ressourcentypen angezeigt wird.
- `ram:Principal`— Testet, ob der ARN des in der Serviceanfrage angegebenen Principals mit einer ARN-Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.
- `ram:RequestedAllowsExternalPrincipals`— Testet, ob die Serviceanfrage den `allowExternalPrincipals` Parameter enthält und ob sein Argument mit dem Wert übereinstimmt, den Sie in der Richtlinie angeben.
- `ram:RequestedResourceType`— Testet, ob der Ressourcentyp der Ressource, auf die reagiert wird, mit einer Ressourcentyp-Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.

Geben Sie Ressourcentypen in dem Format an, das in der Liste der gemeinsam nutzbaren Ressourcentypen angezeigt wird.

- `ram:ResourceArn`— Testet, ob der ARN der Ressource, auf die die Serviceanfrage reagiert, mit einem ARN übereinstimmt, den Sie in der Richtlinie angeben.
- `ram:ResourceShareName`— Testet, ob der Name der Ressourcenfreigabe, auf die die Serviceanfrage reagiert, mit einer Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.
- `ram:ShareOwnerAccountId`— Prüft, ob die Konto-ID-Nummer der Ressourcenfreigabe, auf die die Serviceanfrage reagiert, mit einer Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.

AWS verwaltete Richtlinien für AWS Resource Access Manager

AWS Resource Access Manager bietet derzeit mehrere AWS RAM verwaltete Richtlinien, die in diesem Thema beschrieben werden.

AWS verwaltete Richtlinien

- AWS verwaltete Richtlinie: AWSResource AccessManagerReadOnlyAccess
- AWS verwaltete Richtlinie: AWSResource AccessManagerFullAccess
- AWS verwaltete Richtlinie: AWSResource AccessManagerResourceShareParticipantAccess
- AWS verwaltete Richtlinie: AWSResource AccessManagerServiceRolePolicy
- AWS RAM Aktualisierungen der AWS verwalteten Richtlinien

In der obigen Liste können Sie die ersten drei Richtlinien Ihren IAM-Rollen, -Gruppen und -Benutzern zuordnen, um Berechtigungen zu gewähren. Die letzte Richtlinie in der Liste ist für die dienstbezogene Rolle des AWS RAM Dienstes reserviert.

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSResource AccessManagerReadOnlyAccess

Sie können die `AWSResourceAccessManagerReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen für die Ressourcenfreigaben, deren Eigentümer Sie sind. AWS-Konto

Zu diesem Zweck wird die Berechtigung zum Ausführen aller OR-Operationen erteilt. `Get*` `List*` Es bietet keine Möglichkeit, eine Ressourcenfreigabe zu ändern.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ram`— Ermöglicht Prinzipalen das Einsehen von Details zu den Ressourcenfreigaben, die dem Konto gehören.

JSON

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

AWS verwaltete Richtlinie: AWSResource AccessManagerFullAccess

Sie können die `AWSResourceAccessManagerFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie bietet vollen Administratorzugriff zum Anzeigen oder Ändern der Ressourcenfreigaben, deren Eigentümer Sie sind AWS-Konto.

Zu diesem Zweck erteilt sie die Erlaubnis, alle `ram` Operationen auszuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ram`— Ermöglicht es Prinzipalen, alle Informationen über die Ressourcenfreigaben anzuzeigen oder zu ändern, die Eigentum von sind. AWS-Konto

JSON

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

AWS verwaltete Richtlinie: AWSResource AccessManagerResourceShareParticipantAccess

Sie können die `AWSResourceAccessManagerResourceShareParticipantAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie bietet Principals die Möglichkeit, gemeinsam genutzte Ressourcenfreigaben zu akzeptieren oder abzulehnen und Details zu diesen Ressourcenfreigaben einzusehen. AWS-Konto Sie bietet keine Möglichkeit, diese Ressourcenfreigaben zu ändern.

Dazu wird die Erlaubnis erteilt, einige `ram` Operationen auszuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ram`— Ermöglicht Prinzipalen, Einladungen zur gemeinsamen Nutzung von Ressourcen anzunehmen oder abzulehnen und Details zu den gemeinsam genutzten Ressourcen für das Konto einzusehen.

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 verwaltete Richtlinie: AWSResource AccessManagerServiceRolePolicy

Die AWS verwaltete Richtlinie `AWSResourceAccessManagerServiceRolePolicy` kann nur mit der serviceverknüpften Rolle für AWS RAM verwendet werden. Sie können diese Richtlinie nicht anhängen, trennen, ändern oder löschen.

Diese Richtlinie AWS RAM bietet nur Lesezugriff auf die Struktur Ihrer Organisation. Wenn Sie die Integration zwischen AWS RAM und aktivieren AWS Organizations, AWS RAM wird automatisch eine dienstbezogene Rolle mit dem Namen erstellt AWSServiceRoleForResourceAccessManager, die der Dienst annimmt, wenn er Informationen über Ihre Organisation und deren Konten nachschlagen muss, z. B. wenn Sie die Struktur der Organisation in der Konsole anzeigen. AWS RAM

Zu diesem Zweck wird nur Lesezugriff für die Ausführung der `organizations:List` Vorgänge `organizations:Describe` und gewährt, die Einzelheiten zur Struktur und zu den Konten der Organisation bereitstellen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations`— Ermöglicht es den Schulleitern, Informationen über die Struktur der Organisation, einschließlich der Organisationseinheiten und der AWS-Konten darin enthaltenen Informationen, einzusehen.

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 Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS RAM seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS RAM Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Date
AWS Resource Access Manager hat begonnen, Änderungen zu verfolgen	AWS RAM dokumentierte die bestehenden verwaltet en Richtlinien und begann, Änderungen nachzuverfolgen.	16. September 2021

Verwenden von serviceverknüpften Rollen für AWS RAM

AWS Resource Access Manager verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit dem Dienst verknüpft ist. AWS RAM Mit Diensten verknüpfte Rollen sind vordefiniert AWS und enthalten alle Berechtigungen, die erforderlich sind, AWS RAM um in Ihrem Namen andere AWS Dienste aufzurufen.

Eine dienstverknüpfte Rolle AWS RAM erleichtert die Konfiguration, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS RAM definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS RAM kann, sofern nicht anders definiert, nur ihre dienstbezogenen Rollen übernehmen. Die definierten Berechtigungen umfassen sowohl eine Vertrauensrichtlinie als auch eine Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM-Entität zugeordnet werden.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS RAM

AWS RAM verwendet die dienstverknüpfte Rolle, die benannt wird`AWSServiceRoleForResourceAccessManager`, wenn Sie das Teilen mit aktivieren. AWS Organizations Diese Rolle gewährt dem AWS RAM Dienst die Berechtigung, Organisationsdetails einzusehen, z. B. die Liste der Mitgliedskonten und die Organisationseinheiten, in denen sich die einzelnen Konten befinden.

Diese dienstbezogene Rolle vertraut darauf, dass der folgende Dienst die Rolle übernimmt:

- `ram.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen AWSResource AccessManagerServiceRolePolicy ist an diese dienstbezogene Rolle angehängt und ermöglicht AWS RAM die Ausführung der folgenden Aktionen für die angegebenen Ressourcen:

- Aktionen: schreibgeschützte Aktionen, mit denen Details zur Struktur Ihrer Organisation abgerufen werden. Die vollständige Liste der Aktionen finden Sie in der Richtlinie in der IAM-Konsole:. AWSResourceAccessManagerServiceRolePolicy

Damit ein Principal die AWS RAM gemeinsame Nutzung innerhalb Ihrer Organisation aktivieren kann, muss dieser Principal (eine IAM-Entität wie ein Benutzer, eine Gruppe oder eine Rolle) über die Berechtigung verfügen, eine dienstbezogene Rolle zu erstellen. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer dienstbezogenen Rolle für AWS RAM

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie das AWS RAM Teilen innerhalb Ihrer Organisation in der AWS-Managementkonsole aktivieren oder EnableSharingWithAwsOrganizationin Ihrem Konto mithilfe der AWS CLI oder einer AWS API ausführen, AWS RAM wird die dienstbezogene Rolle für Sie erstellt.

Rufen Sie an`enable-sharing-with-aws-organizations`, um die serviceverknüpfte Rolle in Ihrem Konto zu erstellen.

Wenn Sie diese dienstbezogene Rolle löschen, ist sie nicht AWS RAM mehr berechtigt, die Details der Struktur Ihrer Organisation einzusehen.

Bearbeitung einer dienstbezogenen Rolle für AWS RAM

AWS RAM erlaubt es Ihnen nicht, die AWSResource AccessManagerServiceRolePolicy dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS RAM

Sie können die IAM-Konsole, die AWS CLI oder die AWS API verwenden, um die serviceverknüpfte Rolle manuell zu löschen.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die serviceverknüpfte Rolle zu löschen. `AWSResourceAccessManagerServiceRolePolicy` Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Rollen AWS RAM

AWS RAM unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Beispiele für IAM-Richtlinien für AWS RAM

Dieses Thema enthält Beispiele für IAM-Richtlinien AWS RAM , die die gemeinsame Nutzung bestimmter Ressourcen und Ressourcentypen sowie die Einschränkung der gemeinsamen Nutzung veranschaulichen.

Beispiele für IAM-Richtlinien

- Beispiel 1: Erlauben Sie die gemeinsame Nutzung bestimmter Ressourcen
- Beispiel 2: Erlauben Sie die gemeinsame Nutzung bestimmter Ressourcentypen
- Beispiel 3: Beschränken Sie die gemeinsame Nutzung mit externen AWS-Konten

Beispiel 1: Erlauben Sie die gemeinsame Nutzung bestimmter Ressourcen

Sie können eine IAM-Berechtigungsrichtlinie verwenden, um Prinzipale darauf zu beschränken, nur bestimmte Ressourcen Ressourcenfreigaben zuzuordnen.

Die folgende Richtlinie beschränkt beispielsweise Principals darauf, nur die Resolver-Regel mit dem angegebenen Amazon-Ressourcennamen (ARN) zu teilen. Der Operator `StringEqualsIfExists` lässt eine Anfrage zu, wenn entweder die Anfrage keinen `ResourceArn` Parameter enthält oder wenn sie diesen Parameter enthält, wenn sein Wert genau dem angegebenen ARN entspricht.

Weitere Informationen darüber, wann und warum `...IfExists` Operatoren verwendet werden sollten, finden Sie unter... IfExists Bedingungsoperatoren im IAM-Benutzerhandbuch.

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"
            }
        }
    }]
```

```
}
```

Beispiel 2: Erlauben Sie die gemeinsame Nutzung bestimmter Ressourcentypen

Sie können eine IAM-Richtlinie verwenden, um Prinzipale darauf zu beschränken, Ressourcenfreigaben nur bestimmte Ressourcentypen zuzuordnen.

Die Aktionen `AssociateResourceShare` und `CreateResourceShare` können Prinzipale und `resourceArns` als unabhängige Eingabeparameter akzeptieren. AWS RAM Autorisiert daher jeden Prinzipal und jede Ressource unabhängig voneinander, sodass es mehrere Anforderungskontexte geben kann. Das heißt, wenn ein Prinzipal einer AWS RAM Ressourcenfreigabe zugeordnet wird, ist der `ram:RequestedResourceType` Bedingungsschlüssel im Anforderungskontext nicht vorhanden. In ähnlicher Weise ist der `ram:Principal` Bedingungsschlüssel im Anforderungskontext nicht vorhanden, wenn eine AWS RAM Ressource einer Ressourcenfreigabe zugeordnet wird. Daher können Sie den `AssociateResourceShare` `Null`Bedingungsoperator `CreateResourceShare` verwenden, um der Ressourcenfreigabe Prinzipale zuzuweisen und sie der AWS RAM Ressourcenfreigabe zuzuordnen.

Die folgende Richtlinie beschränkt beispielsweise Principals darauf, nur Amazon Route 53-Resolver-Regeln gemeinsam zu nutzen, und ermöglicht es ihnen, dieser Freigabe jeden Prinzipal zuzuordnen.

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"
             }
        }
    }
  ]
}
```

Beispiel 3: Beschränken Sie die gemeinsame Nutzung mit externen AWS-Konten

Sie können eine IAM-Richtlinie verwenden, um zu verhindern, dass Prinzipale Ressourcen mit Personen teilen AWS-Konten , die sich außerhalb ihrer AWS Organisation befinden.

Die folgende IAM-Richtlinie verhindert beispielsweise, dass Prinzipale externe AWS-Konten Ressourcen gemeinsam nutzen.

JSON

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

Beispiele für Dienststeuerungsrichtlinien für AWS Organizations und AWS RAM

AWS RAM unterstützt Richtlinien zur Dienststeuerung (SCPs). SCPs sind Richtlinien, die Sie an Elemente in einer Organisation anhängen, um Berechtigungen innerhalb dieser Organisation zu

verwalten. Ein SCP gilt für alle AWS-Konten Unterkategorien des Elements, an das Sie den SCP anhängen. SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation. Sie können Ihnen dabei helfen, sicherzustellen, dass Sie die Richtlinien Ihrer Organisation für die Zugriffskontrolle einhalten. AWS-Konten Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

Voraussetzungen

Um sie verwenden zu können SCPs, müssen Sie zunächst wie folgt vorgehen:

- Aktivieren aller Funktionen in der Organisation. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Alle Funktionen in Ihrer Organisation aktivieren
- SCPs Für die Verwendung in Ihrer Organisation aktivieren. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinientypen aktivieren und deaktivieren
- Erstellen Sie das SCPs , was Sie benötigen. Weitere Informationen zum Erstellen SCPs finden Sie unter Erstellen und Aktualisieren SCPs im AWS Organizations Benutzerhandbuch.

Beispiel für Service-Kontrollrichtlinien

Inhalt

In den folgenden Beispielen wird veranschaulicht, wie Sie verschiedene Aspekte der Ressourcenfreigabe in einer Organisation steuern können.

Beispiel 1: Externes Teilen verhindern

Das folgende SCP verhindert, dass Benutzer Ressourcenfreigaben erstellen, die die gemeinsame Nutzung mit Prinzipalen ermöglichen, die sich außerhalb der Organisation des gemeinsam genutzten Benutzers befinden.

AWS RAM autorisiert APIs separat für jeden Prinzipal und jede Ressource, die im Anruf aufgeführt sind.

JSON

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

Beispiel 2: Verhindern Sie, dass Benutzer Einladungen zur gemeinsamen Nutzung von Ressourcen von externen Konten außerhalb Ihrer Organisation annehmen

Der folgende SCP verhindert, dass alle Benutzer in einem betroffenen Konto eine Einladung zur Nutzung eines Resource Shares annehmen. Ressourcenfreigaben, die für andere Konten in derselben Organisation wie das Sharing-Konto gemeinsam genutzt werden, generieren keine Einladungen und sind daher von diesem SCP nicht betroffen.

JSON

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

Beispiel 3: Erlauben Sie bestimmten Konten, bestimmte Ressourcentypen gemeinsam zu nutzen

Das folgende SCP erlaubt nur Konten `111111111111` und `222222222222` das Erstellen neuer Ressourcenfreigaben, die Amazon EC2-Präfixlisten gemeinsam nutzen, oder das Zuordnen von Präfixlisten zu bestehenden Ressourcenfreigaben.

AWS RAM autorisiert APIs separat für jeden Prinzipal und jede Ressource, die im Call aufgeführt sind.

Der Operator `StringEqualsIfExists` lässt eine Anfrage zu, wenn entweder die Anforderung keinen Ressourcentypparameter enthält oder wenn sie diesen Parameter enthält, wenn sein Wert genau dem angegebenen Ressourcentyp entspricht. Wenn Sie einen Schulleiter einbeziehen, müssen Sie ihn haben`...IfExists`.

Weitere Informationen darüber, wann und warum `...IfExists` Operatoren verwendet werden sollten, finden Sie unter... IfExists Bedingungsoperatoren im IAM-Benutzerhandbuch.

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"
                }
            }
        }
    ]
}
```

Beispiel 4: Verhindern Sie die gemeinsame Nutzung mit der gesamten Organisation oder mit Organisationseinheiten

Das folgende SCP verhindert, dass Benutzer Ressourcenfreigaben erstellen, die Ressourcen mit einer gesamten Organisation oder mit beliebigen Organisationseinheiten gemeinsam nutzen. Benutzer können Daten mit einzelnen Personen AWS-Konten in der Organisation oder mit IAM-Rollen oder -Benutzern teilen.

AWS RAM autorisiert APIs separat für jeden Prinzipal und jede Ressource, die im Call aufgeführt sind.

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

Beispiel 5: Erlaube die gemeinsame Nutzung nur mit bestimmten Principals

Das folgende Beispiel mit SCP ermöglicht es Benutzern, Ressourcen nur mit der `o-12345abcdef`, Organisationseinheit `ou-98765fedcba` der Organisation und gemeinsam zu nutzen. AWS-Konto `111111111111`

Wenn Sie beispielsweise `StringNotEqualsIfExists` ein `"Effect": "Deny"` Element mit einem negierten Bedingungsoperator verwenden, wird die Anfrage auch dann abgelehnt, wenn der Bedingungsschlüssel nicht vorhanden ist. Verwenden Sie einen Bedingungsoperator `Null`, um zu prüfen, ob ein Bedingungsschlüssel zum Zeitpunkt der Autorisierung abwesend ist.

AWS RAM autorisiert APIs separat für jeden Prinzipal und jede Ressource, die im Call aufgeführt sind.

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"
        }
      }
    }
  ]
}
```

Beispiel 6: Verhindern Sie gemeinsame Nutzung von Ressourcen, wenn diese Option aktiviert RetainSharingOnAccountLeaveOrganization ist

Der folgende SCP verhindert, dass Benutzer Ressourcenfreigaben erstellen oder ändern, wenn der `ram:RetainSharingOnAccountLeaveOrganization` Bedingungsschlüssel auf `true` gesetzt ist.

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

Deaktivieren der gemeinsamen Nutzung von Ressourcen mit AWS Organizations

Wenn Sie zuvor das Teilen mit aktiviert haben AWS Organizations und Sie Ressourcen nicht mehr mit Ihrer gesamten Organisation oder Ihren Organisationseinheiten teilen müssen (OUs), können Sie das Teilen deaktivieren. Wenn Sie die gemeinsame Nutzung für deaktivieren AWS Organizations, OUs werden alle Organisationen oder Organisationen aus den von Ihnen erstellten Ressourcenfreigaben entfernt und sie verlieren den Zugriff auf die gemeinsam genutzten Ressourcen. Externe Konten (Konten, die per Einladung zur Resource Share hinzugefügt wurden) sind davon nicht betroffen und werden weiterhin mit der Resource Share verknüpft.

Um das Teilen mit zu deaktivieren AWS Organizations

1. Deaktivieren Sie den vertrauenswürdigen Zugriff auf die AWS Organizations Verwendung des AWS Organizations disable-aws-service-access AWS CLI Befehls.

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

   > **Important**
   >
   > Wenn Sie den vertrauenswürdigen Zugriff auf deaktivieren AWS Organizations, werden Prinzipale in Ihren Organisationen aus allen gemeinsam genutzten Ressourcen entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

2. Verwenden Sie die IAM-Konsole, die oder die IAM-API-Operationen AWS CLI, um die dienstverknüpfte Rolle zu löschen. AWSServiceRoleForResourceAccessManager Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Einloggen und Überwachen AWS RAM

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS RAM und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. AWS bietet mehrere Tools zur Überwachung Ihrer AWS RAM Ressourcen und zur Reaktion auf potenzielle Vorfälle:

Amazon EventBridge

Liefert eine near-real-time Reihe von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Computing, da Sie Regeln schreiben können, die auf bestimmte Ereignisse achten und automatische Aktionen in anderen AWS Diensten auslösen können, wenn diese Ereignisse eintreten. Weitere Informationen finden Sie unter Überwachung AWS RAM mit EventBridge.

AWS CloudTrail

Erfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie unter AWS RAM API-Aufrufe protokollieren mit AWS CloudTrail.

Überwachung AWS RAM mit EventBridge

Mit Amazon EventBridge können Sie automatische Benachrichtigungen für bestimmte Ereignisse in einrichten AWS RAM. Ereignisse von AWS RAM werden nahezu EventBridge in Echtzeit zugestellt. Sie können so konfigurieren EventBridge , dass Ereignisse überwacht und Ziele als Reaktion auf Ereignisse aufgerufen werden, die auf Änderungen an Ihren Ressourcenfreigaben hinweisen. Änderungen an einer Ressourcenfreigabe lösen Ereignisse sowohl für den Eigentümer der Ressourcenfreigabe als auch für die Prinzipale aus, denen Zugriff auf die Ressourcenfreigabe gewährt wurde.

Wenn Sie ein Ereignismuster erstellen, ist `aws.ram` die Quelle.

> **Note**
>
> Achten Sie darauf, Code zu schreiben, der von diesen Ereignissen abhängt. Diese Ereignisse sind nicht garantiert, werden aber nach bestem Wissen und Gewissen ausgegeben. Wenn beim AWS RAM Versuch, ein Ereignis auszulösen, ein Fehler auftritt, versucht der Dienst es noch mehrmals. Es kann jedoch zu einem Timeout kommen und zum Verlust dieses bestimmten Ereignisses führen.

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Beispiel: Warnung bei Ausfällen bei der gemeinsamen Nutzung von Ressourcen

Stellen Sie sich das Szenario vor, in dem Sie Amazon EC2 EC2-Kapazitätsreservierungen mit anderen Konten in Ihrer Organisation teilen möchten. Dies ist eine gute Möglichkeit, Ihre Kosten zu senken.

Wenn Sie jedoch nicht alle Voraussetzungen für die gemeinsame Nutzung einer Kapazitätsreservierung erfüllen, kann es sein, dass die asynchrone Ausführung der Aufgaben, die mit der gemeinsamen Nutzung von Ressourcen verbunden sind, stillschweigend fehlschlägt. Wenn der Share-Vorgang fehlschlägt und Ihre Benutzer in anderen Konten versuchen, Instances mit einer dieser Kapazitätsreservierungen zu starten, verhält sich Amazon EC2 so, als ob die Kapazitätsreservierung voll wäre, und startet die Instance stattdessen als On-Demand-Instance. Dies kann zu höheren Kosten als erwartet führen.

Um Fehler bei der gemeinsamen Nutzung von Ressourcen zu überwachen, richten Sie eine EventBridge Amazon-Regel ein, die Sie benachrichtigt, wenn eine gemeinsame AWS RAM Nutzung einer Ressource ausfällt. Das folgende Tutorial-Verfahren verwendet ein Amazon Simple Notification Service (SNS) -Thema, um alle Abonnenten des Themas zu benachrichtigen, wenn ein Fehler bei der gemeinsamen Nutzung von Ressourcen EventBridge entdeckt wird. Weitere Informationen zu Amazon SNS finden Sie im Amazon-Simple-Notification-Service-Entwicklerhandbuch.

Um eine Regel zu erstellen, die Sie benachrichtigt, wenn die gemeinsame Nutzung von Ressourcen fehlschlägt

1. Öffnen Sie die EventBridge Amazon-Konsole.
2. Wählen Sie im Navigationsbereich Regeln und dann in der Liste Regeln die Option Regel erstellen aus.
3. Geben Sie einen Namen und optional eine Beschreibung für Ihre Regel ein und wählen Sie dann Weiter aus.
4. Scrollen Sie nach unten zum Feld Ereignismuster und wählen Sie Benutzerdefinierte Muster (JSON-Editor) aus.
5. Kopieren Sie das folgende Ereignismuster und fügen Sie es ein:

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

```
    "status": ["failed"]
  }
}
```

6. Wählen Sie Weiter aus.
7. Wählen Sie für Ziel 1 unter Zieltyp die Option AWS-Service.
8. Wählen Sie unter Ziel auswählen die Option SNS-Thema aus.
9. Wählen Sie unter Thema das SNS-Thema aus, zu dem Sie die Benachrichtigung veröffentlichen möchten. Dieses Thema muss bereits existieren.
10. Wählen Sie Weiter und klicken Sie dann erneut auf Weiter, um Ihre Konfiguration zu überprüfen.
11. Wenn Sie mit Ihren Optionen zufrieden sind, wählen Sie Regel erstellen aus.
12. Vergewissern Sie sich, dass Ihre neue Regel wieder auf der Seite Regeln als Aktiviert markiert ist. Wählen Sie bei Bedarf das Optionsfeld neben Ihrem Regelnamen und wählen Sie dann Aktivieren aus.

Solange diese Regel aktiviert ist, generiert jede AWS RAM fehlgeschlagene Ressourcenfreigabe eine SNS-Warnung an die Empfänger des Themas, für das Sie das Thema veröffentlicht haben.

Sie können auch überprüfen, ob Reservierungen für gemeinsame Kapazitäten für die Konten zugänglich sind, mit denen Sie sie geteilt haben, indem Sie versuchen, sie von diesen Konten aus in der Amazon EC2 EC2-Konsole anzuzeigen.

AWS RAM API-Aufrufe protokollieren mit AWS CloudTrail

AWS RAM ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS RAM. CloudTrail erfasst alle API-Aufrufe AWS RAM als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS RAM Konsole und Codeaufrufen für die AWS RAM API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen von Ihnen angegebenen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS RAM. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Ermitteln Sie anhand der von CloudTrail gesammelten Informationen die Anfrage AWS RAM, die anfragende IP-Adresse, den Anfragenden, den Zeitpunkt der Anfrage und weitere Informationen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS RAM Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS RAM, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS RAM, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Erstellen Sie einen Trail für Ihren AWS-Konto
- AWS-Service Integrationen mit Protokollen CloudTrail
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS RAM Aktionen werden von der AWS RAM API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Zum Beispiel werden durch Aufrufe der `CreateResourceShare`-, `AssociateResourceShare`- und `EnableSharingWithAwsOrganization`-Aktionen Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen, anhand derer Sie feststellen können, wer die Anfrage gestellt hat.

- AWS-Konto Root-Anmeldeinformationen
- Temporäre Sicherheitsanmeldedaten von einer AWS Identity and Access Management (IAM-) Rolle oder einem Verbundbenutzer.
- Langfristige Sicherheits-Anmeldeinformation eines IAM-Benutzers.
- Ein weiterer Dienst AWS .

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

AWS RAM Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für die `CreateResourceShare` Aktion.

```
{
    "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"
}
```

Konformitätsvalidierung für AWS Resource Access Manager

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz in AWS Resource Access Manager

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS Resource Access Manager

Als verwalteter Dienst AWS Resource Access Manager ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter

Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS RAM über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Zugriff AWS Resource Access Manager über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können AWS PrivateLink damit eine private Verbindung zwischen Ihrer VPC und AWS Resource Access Manager herstellen. Sie können darauf zugreifen, AWS RAM als ob es in Ihrer VPC wäre, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen für den Zugriff AWS RAM keine öffentlichen IP-Adressen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für AWS RAM bestimmt ist.

Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Überlegungen zu AWS RAM

Bevor Sie einen Schnittstellen-Endpunkt für einrichten AWS RAM, lesen Sie die Überlegungen im AWS PrivateLink Handbuch.

AWS RAM unterstützt Aufrufe aller API-Aktionen über den Schnittstellenendpunkt.

VPC-Endpunktrichtlinien werden unterstützt für AWS RAM. Standardmäßig AWS RAM ist der vollständige Zugriff auf über den Schnittstellenendpunkt zulässig.

Erstellen Sie einen Schnittstellenendpunkt für AWS RAM

Sie können einen Schnittstellenendpunkt für die AWS RAM Verwendung entweder der Amazon VPC-Konsole oder der AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für die AWS RAM Verwendung des folgenden Servicenamens:

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

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an die AWS RAM Verwendung des standardmäßigen regionalen DNS-Namens stellen. Beispiel, `ram.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff AWS RAM über den Schnittstellenendpunkt. Um den Zugriff AWS RAM von Ihrer VPC aus zu kontrollieren, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für Aktionen AWS RAM

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten AWS RAM Aktionen.

JSON

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

Behebung von Problemen mit AWS RAM

Mithilfe der Informationen in diesem Abschnitt des Handbuchs können Sie häufig auftretende Probleme diagnostizieren und beheben, wenn Sie mit AWS Resource Access Manager (AWS RAM) arbeiten.

Themen

Fehler: „Ihre Konto-ID ist in einer AWS Organisation nicht vorhanden“

Szenario

Wenn Sie versuchen, eine Ressource für Konten oder Organisationseinheiten (OUs) in Ihrer AWS Organisation gemeinsam zu nutzen, wird die Fehlermeldung "Ihre Konto-ID existiert nicht in einer Organisation" angezeigt.

Ursache

Dieser Fehler kann auftreten, wenn die serviceverknüpfte Rolle AWSServiceRoleForResourceAccessManagernicht erfolgreich erstellt wurde, wenn Sie die Integration zwischen AWS Resource Access Manager und AWS Organizations aktivieren.

Lösung

Um die erforderliche dienstverknüpfte Rolle neu zu erstellen, führen Sie die folgenden Schritte aus, um die Integration zu deaktivieren und sie dann wieder zu aktivieren.

> **Important**
>
> Wenn Sie den vertrauenswürdigen Zugriff auf deaktivieren AWS Organizations, werden Prinzipale innerhalb Ihrer Organisation aus allen gemeinsam genutzten Ressourcen entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie in der AWS Organizations Konsole zur Seite Dienste.
3. Wählen Sie RAM.
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie in der AWS RAM Konsole zur Seite „Einstellungen“.
6. Markieren Sie das Kästchen Teilen mit AWS Organizations aktivieren und wählen Sie dann Einstellungen speichern aus.

Sie sollten nun in der Lage sein AWS RAM , Ihre Ressourcen mit Konten und innerhalb OUs der Organisation zu teilen.

Fehler: "AccessDeniedException“

Szenario

Wenn Sie versuchen, eine Ressource gemeinsam zu nutzen oder eine Ressourcenfreigabe anzuzeigen, wird die Ausnahme „Zugriff verweigert“ angezeigt.

Ursache

Dieser Fehler kann auftreten, wenn Sie versuchen, eine Ressourcenfreigabe zu erstellen, obwohl Sie nicht über die erforderlichen Berechtigungen verfügen. Dies kann durch unzureichende Berechtigungen in Richtlinien verursacht werden, die Ihrem AWS Identity and Access Management (IAM-) Principal zugeordnet sind. Dies kann auch auf Einschränkungen aufgrund einer AWS Organizations Service Control Policy (SCP) zurückzuführen sein, die sich auf Ihren Computer auswirken. AWS-Konto

Lösung

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Um den Fehler zu beheben, müssen Sie sicherstellen, dass die Berechtigungen durch `Allow` Anweisungen in der Berechtigungsrichtlinie erteilt werden, die vom Prinzipal verwendet wird, der die Anfrage stellt. Darüber hinaus dürfen die Berechtigungen nicht durch die Berechtigungen Ihrer Organisation blockiert werden SCPs.

Um eine Ressourcenfreigabe zu erstellen, benötigen Sie die folgenden zwei Berechtigungen:

- `ram:CreateResourceShare`

- `ram:AssociateResourceShare`

Um eine Ressourcenfreigabe anzuzeigen, benötigen Sie die folgende Berechtigung:

- `ram:GetResourceShares`

Um einer Ressourcenfreigabe Berechtigungen zuzuweisen, benötigen Sie die folgende Berechtigung:

- *`resourceOwningService`*`:`*`PutPolicyAction`*

Das ist ein Platzhalter. Sie müssen ihn durch die "PutPolicy" -Berechtigung (oder eine gleichwertige) für den Dienst ersetzen, dem die Ressource gehört, die Sie teilen möchten. Wenn Sie beispielsweise eine Route 53-Resolver-Regel gemeinsam nutzen, wäre die erforderliche Berechtigung wie folgt erforderlich:`route53resolver:PutResolverRulePolicy`. Wenn Sie die Erstellung einer Ressourcenfreigabe zulassen möchten, die mehrere Ressourcentypen enthält, müssen Sie die entsprechenden Berechtigungen für jeden Ressourcentyp angeben, den Sie zulassen möchten.

Das folgende Beispiel zeigt, wie eine solche IAM-Berechtigungsrichtlinie aussehen könnte.

JSON

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

Fehler: "“ UnknownResourceException

Szenario

Sie erhalten einen der folgenden Fehler:

- "CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit Sie- *xxxx* konnten nicht gefunden werden“

- "CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit Sie- *xxxx* konnte nicht gefunden werden“.

Ursache

Diese Fehler können auftreten, wenn Sie die Integration zwischen AWS RAM und AWS Organizations mithilfe der Organisationskonsole oder der Organizations Enable AWSService Access API aktivieren, anstatt die AWS RAM Konsole zu verwenden. Wenn Sie die Integration mithilfe der Organisationskonsole oder der API aktivieren, erstellt der Dienst die `AWSServiceRoleForResourceAccessManager` Rolle nicht in Ihrem Konto. Diese Rolle wird benötigt, um auf Informationen über Ihre Organisation zuzugreifen. Da die Rolle nicht erstellt wurde, AWS RAM kann nicht auf Details zu den Konten oder Organisationseinheiten (OUs) in Ihrer Organisation zugegriffen werden.

Lösung

Um das Problem zu beheben, deaktivieren Sie die Integration zwischen AWS RAM und AWS Organizations. Schalten Sie es dann wieder ein, indem Sie den AWS RAM EnableSharingWithAwsOrganizationAPI-Vorgang aufrufen oder AWS-Managementkonsole die folgenden Schritte mithilfe von ausführen.

> **Important**
>
> Wenn Sie den vertrauenswürdigen Zugriff auf deaktivieren AWS Organizations, werden Prinzipale innerhalb Ihrer Organisation aus allen gemeinsam genutzten Ressourcen entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie in der AWS Organizations Konsole zur Seite Dienste.
3. Wählen Sie RAM.
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie in der AWS RAM Konsole zur Seite „Einstellungen“.
6. Markieren Sie das Kästchen Teilen mit AWS Organizations aktivieren und wählen Sie dann Einstellungen speichern aus.

Sie sollten nun in der Lage sein AWS RAM , Ihre Ressourcen mit Konten und innerhalb OUs der Organisation zu teilen.

Fehler beim Versuch, Inhalte mit Konten außerhalb meiner Organisation zu teilen

Szenario

Wenn Sie versuchen, Ressourcen mit Konten außerhalb Ihrer Organisation gemeinsam zu nutzen, wird einer der folgenden Fehler angezeigt:

- „Sie können die Ressource nicht außerhalb Ihrer Organisation gemeinsam nutzen. “
- „Die Ressource, die Sie teilen möchten, kann nur innerhalb Ihrer AWS Organisation gemeinsam genutzt werden. “
- "InvalidParameterException: Die Hauptkonto-ID befindet sich nicht in Ihrer AWS Organisation. Sie sind nicht berechtigt, externe Ressourcen AWS-Konten zu einer Ressourcenfreigabe hinzuzufügen. “
- "OperationNotPermittedException: Die Ressource, die Sie teilen möchten, kann nur innerhalb Ihrer AWS Organisation gemeinsam genutzt werden. “

Mögliche Ursachen und Lösungen

Einige Ressourcentypen können nur mit Konten in derselben Organisation gemeinsam genutzt werden

Einige Ressourcentypen können nicht mit Konten geteilt werden, die nicht Mitglied dieser Organisation sind. Ein Beispiel für einen Ressourcentyp mit dieser Einschränkung sind virtuelle private Verbindungen (VPCs), die Teil von Amazon Elastic Compute Cloud (Amazon EC2) sind.

Informationen darüber, ob Sie einen bestimmten Ressourcentyp mit Konten und Prinzipalen außerhalb Ihrer Organisation teilen können, finden Sie unter Gemeinsam nutzbare Ressourcen. AWS

Die mit dem Dienst verknüpfte Rolle wurde nicht erfolgreich erstellt

Dieses Problem kann auftreten, wenn die serviceverknüpfte Rolle `AWSServiceRoleForResourceAccessManager` nicht erfolgreich erstellt wurde, als Sie die Integration zwischen und AWS RAM aktiviert haben. AWS Organizations

Wenn Sie versuchen, eine Ressource mit einem Konto zu teilen, das Teil Ihrer Organisation ist, einer dieser Fehler angezeigt wird, führen Sie die folgenden Schritte aus, um die dienstverknüpfte Rolle zu löschen und neu zu erstellen.

> **Important**
>
> Wenn Sie den vertrauenswürdigen Zugriff auf deaktivieren AWS Organizations, werden Prinzipale innerhalb Ihrer Organisation aus allen gemeinsam genutzten Ressourcen entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie in der AWS Organizations Konsole zur Seite Dienste.
3. Wählen Sie RAM.
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie in der AWS RAM Konsole zur Seite „Einstellungen“.
6. Markieren Sie das Kästchen Teilen mit AWS Organizations aktivieren und wählen Sie dann Einstellungen speichern aus.

Geteilte Ressourcen werden im Zielkonto nicht angezeigt

Szenario

Benutzer können die Ressourcen nicht sehen, von denen sie glauben, dass sie von anderen mit ihnen geteilt wurden AWS-Konten.

Mögliche Ursachen und Lösungen

Teilen mit AWS Organizations wurde aktiviert, indem Organizations verwendet wurden, anstatt AWS RAM

Wenn statt mithilfe von Organizations aktiviert AWS Organizations wurde AWS RAM, schlägt das Teilen innerhalb der Organisation fehl. Um zu überprüfen, ob dies die Ursache des Problems ist, navigieren Sie in der AWS RAM Konsole zur Seite „Einstellungen“ und stellen Sie sicher, dass das AWS Organizations Kontrollkästchen Teilen aktivieren mit aktiviert ist.

- Wenn das Kontrollkästchen aktiviert ist, ist dies nicht die Ursache.
- Wenn das Kontrollkästchen nicht aktiviert ist, ist dies möglicherweise die Ursache. Markieren Sie das Kontrollkästchen noch nicht. Gehen Sie wie folgt vor, um die Situation zu korrigieren.

> **Important**
>
> Wenn Sie den vertrauenswürdigen Zugriff auf deaktivieren AWS Organizations, werden Prinzipale innerhalb Ihrer Organisation aus allen gemeinsam genutzten Ressourcen entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie in der AWS Organizations Konsole zur Seite Dienste.
3. Wählen Sie RAM.
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie in der AWS RAM Konsole zur Seite „Einstellungen“.
6. Markieren Sie das Kästchen Teilen mit AWS Organizations aktivieren und wählen Sie dann Einstellungen speichern aus.

Möglicherweise müssen Sie die Freigabe aktualisieren und die Konten oder Organisationseinheiten innerhalb der Organisation angeben, für die das Teilen verwendet werden soll.

Die Ressourcenfreigabe gibt dieses Konto nicht als Hauptbenutzer an

Sehen Sie sich in der AWS-Konto Datei, die die Ressourcenfreigabe erstellt hat, die Ressourcenfreigabe in der AWS RAM Konsole an. Vergewissern Sie sich, dass das Konto, das nicht auf die Ressourcen zugreifen kann, als Principal aufgeführt ist. Ist dies nicht der Fall, aktualisieren Sie den Share, um das Konto als Principal hinzuzufügen.

Für die Rolle oder den Benutzer im Konto sind keine Mindestberechtigungen erforderlich

Wenn Sie eine Ressource in Konto A mit einem anderen Konto B teilen, erhalten Rollen und Benutzer in Konto B nicht automatisch Zugriff auf die Ressourcen in der Freigabe. Der Administrator von Konto B muss zunächst den IAM-Rollen und Benutzern in Konto B, die auf die Ressource zugreifen

müssen, die entsprechenden Berechtigungen erteilen. Als Beispiel zeigt die folgende Richtlinie, wie Sie Rollen und Benutzern in Konto B für eine Ressource von Konto A schreibgeschützten Zugriff gewähren können. Die Richtlinie spezifiziert die Ressource anhand ihres Amazon-Ressourcennamens (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>"
        }
    ]
}
```

Die Ressource hat eine andere AWS-Region als die aktuelle Konsoleneinstellung

AWS RAM ist ein regionaler Dienst. Ressourcen sind in einer bestimmten Region vorhanden AWS-Region, und um sie sehen zu können, AWS-Managementkonsole müssen sie so konfiguriert sein, dass sie die Ressourcen in dieser Region anzeigen.

Die AWS-Region Datei, auf die die Konsole gerade zugreift, wird in der oberen rechten Ecke der Konsole angezeigt. Um ihn zu ändern, wählen Sie den Namen der aktuellen Region und dann im Dropdownmenü die Region aus, deren Ressourcen Sie sehen möchten.

Fehler: Limit überschritten

Szenario

Sie erhalten die Meldung "Sie haben das Limit für die Anzahl der Ressourcen erreicht, die Sie teilen können" oder "ResourceShareLimitExceededException", wenn Sie versuchen, Ressourcen gemeinsam zu nutzen.

Ursache

Diese Fehler treten auf, wenn Sie die maximale Anzahl an Ressourcen erreichen, die Sie gemeinsam nutzen können, entweder mit dem AWS RAM Dienst oder mit dem Dienst AWS-Service , der die Ressource erstellt hat, die Sie teilen möchten. Dieses Kontingent (früher als Limit bezeichnet) kann sich sowohl auf das Sharing-Konto als auch auf das Konto auswirken, mit dem Sie die Ressource teilen.

Lösung

1. Um Ihre Kontingente einzusehen, rufen Sie an der AWS-Konto Stelle, an der der Fehler angezeigt wird, je nachdem, welche Art von Kontingent Sie erreicht haben, zu einer der folgenden Seiten auf:
   - Die AWS RAM Seite in der Service Quotas Quotas-Konsole
   - Die Seite für diejenigen AWS-Service, deren Ressourcen vom Kontingent betroffen sind
2. Scrollen Sie nach unten und wählen Sie das entsprechende Kontingent aus.
3. Wenn es für dieses Kontingent verfügbar ist, wählen Sie Kontingenterhöhung beantragen.
4. Geben Sie einen neuen Wert für das Kontingent ein und wählen Sie dann „Anfrage“.
5. Die Anfrage wird auf der Seite mit dem Verlauf der Kontingentanträge angezeigt, auf der Sie den Status der Anfrage überprüfen können, bis sie abgeschlossen ist.

Das andere Konto in meiner Organisation erhält nie eine Einladung

Szenario

Wenn Sie Ressourcen mit einem anderen Konto in derselben Organisation teilen, das von verwaltet wird AWS Organizations, erhält dieser keine Einladungen.

Ursache

Dieses Verhalten ist zu erwarten, wenn für Ihr Konto die gemeinsame Nutzung innerhalb der AWS Organisation aktiviert ist.

Wenn diese Option aktiviert ist und Sie Inhalte mit einem anderen Konto in Ihrer Organisation teilen, werden keine Einladungen gesendet und es ist auch keine Annahme erforderlich. Alle Organisationskonten, auf die Sie in der Ressourcenfreigabe als Hauptbenutzer verweisen, können sofort auf die Ressourcen in der Freigabe zugreifen.

Wenn Ihr Konto die gemeinsame Nutzung innerhalb der AWS Organisation nicht aktiviert hat, werden die Inhalte, die Sie mit anderen Konten teilen, als eigenständige Konten behandelt, auch wenn sich diese in derselben AWS Organisation befinden. Einladungen werden gesendet und müssen akzeptiert werden, bevor Benutzer auf die Ressourcen in den Shares zugreifen können.

Sie können ein VPC-Subnetz nicht gemeinsam nutzen

Szenario

Wenn Sie versuchen, ein VPC-Subnetz mit einem anderen Konto gemeinsam AWS RAM zu nutzen, ist der Freigabevorgang erfolgreich. Das verbrauchende Konto wird jedoch `LIMIT EXCEEDED` für diese Ressource in der Konsole angezeigt. AWS RAM

Ursache

Für einige einzelne Ressourcentypen gelten dienstspezifische Einschränkungen, die sich von den Einschränkungen unterscheiden, die von durchgesetzt wurden. AWS RAM Einige dieser Einschränkungen können die gemeinsame Nutzung effektiv verhindern, selbst wenn Sie eine der Einschränkungen von noch nicht erreicht haben. AWS RAM Grenzwerte sind ein Beispiel für diese Einschränkungen. Amazon Virtual Private Cloud (Amazon VPC) begrenzt die Anzahl der Subnetze, die Sie mit einem anderen individuellen Konto teilen können. Wenn Sie versuchen, ein Subnetz mit einem verbrauchenden Konto gemeinsam zu nutzen, das bereits die maximale Anzahl von Subnetzen enthält, wird dieses verbrauchende Konto `LIMIT EXCEEDED` in der Konsole für diese Ressource angezeigt. Weitere Informationen zu diesem Limit finden Sie unter Amazon VPC Quotas — VPC Sharing im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Um dieses Problem zu beheben, suchen Sie zunächst nach anderen Ressourcenfreigaben, die die angegebene Ressource möglicherweise gemeinsam mit dem betroffenen Konto nutzen, und entfernen Sie die Freigaben, die Sie möglicherweise nicht mehr benötigen. Sie können auch eine Erhöhung für ein Limit beantragen, das Anpassungen unterstützt. Verwenden Sie die Service Quotas Quotas-Konsole, um eine Erhöhung des Limits anzufordern.

> **Note**
>
> AWS RAM erkennt Änderungen der Limiterhöhung nicht automatisch. Sie müssen die Ressource oder den Prinzipal erneut der Ressourcenfreigabe zuordnen, damit RAM die Änderung erkennt.

Servicekontingenten für AWS RAM

Ihr AWS-Konto hat die folgenden Beschränkungen in Bezug auf AWS Resource Access Manager (AWS RAM). Sie können eine Erhöhung einiger dieser Limits beantragen. Um eine Erhöhung des Limits zu beantragen, wenden Sie sich an Support.

> **Note**
>
> Die folgenden Definitionen gelten für die Beschreibung in den folgenden Kontingenten:
>
> - Ressource — Ein individuell AWS-Service erstelltes Element, das Sie teilen möchten, z. B. ein Amazon S3 S3-Bucket oder eine EC2 Amazon-Instance. Jede Ressource, auf die in einer Ressourcenfreigabe verwiesen wird, wird als eine Ressource auf dieses Kontingent angerechnet. Wenn Sie dieselbe Ressource in drei verschiedenen Ressourcenanteilen gemeinsam nutzen, erhöht sich Ihre Anzahl für dieses Kontingent um drei.
> - Gemeinsam genutzte Ressourcen — Ein AWS RAM erstellter Container, den Sie verwenden können, um Ressourcen gemeinsam zu nutzen. Jede gemeinsame Nutzung einer Ressource, unabhängig davon, wie viele Ressourcen sie enthält, wird auf Ihr Kontingent angerechnet.
> - Gemeinsamer Hauptbenutzer — Eine Kennung, die Sie einer Ressourcenfreigabe zugeordnet haben. Dabei kann es sich um eine AWS Identity and Access Management (IAM-) Rolle oder einen Benutzer, eine AWS-Konto Kennung, eine Organisationseinheit oder eine gesamte Organisation handeln. Jeder gemeinsam genutzte Hauptbenutzer, auf den Sie in einer Ressourcenfreigabe verweisen, erhöht Ihre Kontingentnutzung um einen. Wenn Sie eine gemeinsame Nutzung für eine gesamte Organisation verwenden, indem Sie auf deren ID verweisen, wird dieser Wert bei diesem Kontingent nur als eine Person gewertet.
> - Vom Kunden verwaltete Berechtigungen — Verwaltete Berechtigungen, die Sie für bestimmte Anwendungsfälle erstellen, indem Sie den geringsten Zugriff verwenden, um zu verwalten, wie Ihre gemeinsam genutzten Ressourcen verwendet werden.

Ressource	Standardlimit
Maximale Anzahl von Ressourcenfreigaben pro AWS-Region	25,000

Ressource	Standardlimit
Maximale Anzahl von Ressourcenzuordnungen pro Ressourcenfreigabe	5,000
Maximale Anzahl von Hauptverbänden pro Ressourcenanteil	5,000
Maximale Anzahl von vom Kunden verwalteten Berechtigungen	1.500
Maximale Anzahl von vom Kunden verwalteten Berechtigungen pro Ressourcentyp	10
Maximale Anzahl von Versionen pro vom Kunden verwalteter Berechtigung	5
Maximale Anzahl von Ressourcenzuordnungen für alle gemeinsam genutzten Ressourcen in einem AWS-Region **Note** Jede Ressource, die in einer Ressourcenfreigabe enthalten ist, wird auf dieses Limit angerechnet. Wenn eine Ressource in 10 verschiedenen Ressourcenanteilen enthalten ist, wird dies auf den Grenzwert angerechnet.	25,000

Ressource	Standardlimit
Maximale Anzahl von Hauptzuordnungen für alle Ressourcenanteile in einem AWS-Region **Note** Jeder Hauptbenutzer, der in einer Ressourcenfreigabe enthalten ist, wird auf dieses Limit angerechnet. Wenn ein Hauptbenutzer in 10 verschied enen Ressourcenanteilen enthalten ist, wird dieser Wert auf die Obergrenze angerechnet.	25,000
Maximale Anzahl ausstehender Einladungen pro Sharing-Konto • Dieses Kontingent gilt nur für das Senden von Konten, die Inhalte mit Konten teilen, die nicht Teil desselben sind AWS Organizat ions. • Es gibt kein Kontingent, das begrenzt, wie viele ausstehende Einladungen ein Empfangskonto haben kann. • Einladungen werden nicht verwendet, wenn sie zwischen Konten geteilt werden, die Teil desselben sind AWS Organizations und Sie die gemeinsame Nutzung von Ressourcen innerhalb von aktiviert haben AWS Organizat ions.	250

Verwendung AWS RAM mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die Entwicklern helfen, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK für C++	AWS SDK für C++ Codebeispiele
AWS SDK für Go	AWS SDK für Go Code-Beispiele
AWS SDK für Java	AWS SDK für Java Code-Beispiele
AWS SDK für JavaScript	AWS SDK für JavaScript Code-Beispiele
AWS SDK für .NET	AWS SDK für .NET Code-Beispiele
AWS SDK für PHP	AWS SDK für PHP Code-Beispiele
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto3) Code-Beispiele
AWS SDK für Ruby	AWS SDK für Ruby Code-Beispiele

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie über den Feedback-Link ein Code-Beispiel an.

Dokumentenverlauf für das AWS RAM Benutzerhandbuch

In der folgenden Tabelle werden wichtige Ergänzungen der AWS Resource Access Manager Dokumentation beschrieben. Wir aktualisieren die Dokumentation auch, um das Feedback zu berücksichtigen, das Sie uns senden.

Um über diese Updates informiert zu werden, können Sie den AWS RAM RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Unterstützung für die gemeinsame Nutzung von CloudFront Amazon-Ressourcen hinzugefügt	Sie können Amazon CloudFront VPC Origins jetzt mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	6. Oktober 2025
Unterstützung für die gemeinsame Nutzung von Ressourcen für Billing and Cost Management hinzugefügt	Sie können jetzt Billing and Cost Management Kostenmanagement-Dashboards mit anderen AWS-Konten oder Ihrer Organisation teilen. AWS RAM	19. August 2025
Unterstützung für die gemeinsame Nutzung AWS Cloud Map von Ressourcen wurde hinzugefügt	Sie können jetzt AWS Cloud Map Namespaces mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	14. August 2025
Unterstützung für die gemeinsame Nutzung von Amazon Application Recovery Controller (ARC) -Ressourcen hinzugefügt	Sie können jetzt Amazon Application Recovery Controller (ARC) -Pläne mit anderen AWS-Konten oder Ihrer Organisation teilen AWS RAM.	31. Juli 2025
Unterstützung für die gemeinsame Nutzung von Oracle Database@AWS	Sie können jetzt die Oracle Database@AWS Exadata-Infrastruktur und ODB-Netzwerke mit anderen AWS-Konte	30. Juni 2025

Ressourcen wurde hinzugefügt	n innerhalb Ihrer Organisation gemeinsam nutzen.	
Unterstützung für die gemeinsame Nutzung von Genehmigungsressourcen durch mehrere Parteien wurde hinzugefügt	Sie können jetzt Genehmigungsteams mit mehreren Parteien gemeinsam mit anderen Parteien AWS-Konten oder innerhalb Ihrer Organisation verwenden.	17. Juni 2025
Unterstützung für die gemeinsame Nutzung von Amazon SageMaker AI-Ressourcen hinzugefügt	Sie können Amazon SageMaker AI-Partner-Apps jetzt mit anderen AWS-Konten und mit Ihrer Organisation teilen. AWS RAM	6. Juni 2025
Unterstützung für die gemeinsame Nutzung von AWS Network Firewall Ressourcen wurde hinzugefügt	Sie können AWS Network Firewall Firewalls jetzt AWS RAM für andere Benutzer AWS-Konten und für Ihre Organisation verwenden.	28. Mai 2025
Unterstützung für die gemeinsame Nutzung von AWS Systems Manager Ressourcen wurde hinzugefügt	Sie können eine AWS Systems Manager Zugriffsverweigerungsrichtlinie mit anderen AWS-Konten oder Ihren Organisationen teilen. AWS RAM	30. April 2025
Unterstützung für die gemeinsame Nutzung von Ressourcen hinzugefügt AWS CodeConnections	Sie können jetzt AWS CodeConnections Codeverbindungen mit anderen Personen AWS-Konten oder innerhalb Ihrer Organisation teilen.	5. März 2025

Unterstützung für die gemeinsame Nutzung von AWS Billing Ressourcen hinzugefügt	Sie können jetzt AWS Billing Ansichten mit anderen AWS-Konten in Ihrer Organisation teilen.	20. Dezember 2024
Unterstützung für die gemeinsame Nutzung von Amazon VPC Lattice-Ressourcenkonfigurationen hinzugefügt	Sie können jetzt Amazon VPC Lattice-Ressourcenkonfigurationen mit anderen teilen. AWS-Konten	01. Dezember 2024
Unterstützung für die gemeinsame Nutzung von Amazon API Gateway Gateway-Ressourcen hinzugefügt	Sie können jetzt API Gateway Gateway-Domainnamen mit anderen AWS-Konten oder innerhalb Ihrer Organisation teilen.	21. November 2024
Unterstützung für die gemeinsame Nutzung von Amazon VPC-Ressourcen hinzugefügt	Sie können Amazon VPC Security-Gruppen jetzt mit anderen AWS-Konten oder innerhalb Ihrer Organisation teilen.	30. Oktober 2024
Unterstützung für die gemeinsame Nutzung AWS End User Messaging SMS von Ressourcen hinzugefügt	Sie können AWS End User Messaging SMS Ressourcen mit anderen AWS-Konten oder Ihren Organisationen teilen AWS RAM.	24. September 2024
AWS PrivateLink	Mit AWS PrivateLink for können Sie eine direkte Verbindung zum RAM herstellen AWS RAM, indem Sie einen Schnittstellenendpunkt in Ihrer Virtual Private Cloud (VPC) verwenden.	9. September 2024

Unterstützung für das Teilen wurde hinzugefügt AWS Backup	Sie können Tresore mit logischem Air-Gap innerhalb AWS-Konten oder innerhalb Ihrer Organisation gemeinsam nutzen.	7. August 2024
Unterstützung für die gemeinsame Nutzung von Elastic Load Balancing Balancing-Ressourcen hinzugefügt	Sie können Elastic Load Balancing Trust Stores innerhalb AWS-Konten oder innerhalb Ihrer Organisation gemeinsam nutzen.	5. August 2024
Unterstützung für das Teilen von Amazon Bedrock Custom Models hinzugefügt	Sie können es jetzt verwenden AWS RAM , um benutzerd efinierte Amazon Bedrock-M odelle mit anderen AWS-Konte n und mit Ihrer Organisation zu teilen.	1. August 2024
Unterstützung für das Teilen AWS CloudHSM von Backups hinzugefügt	Sie können AWS CloudHSM Backups mit anderen AWS-Konten oder Ihren Organisat ionen teilen AWS RAM.	28. Juni 2024
Unterstützung für die gemeinsame Nutzung von Amazon SageMaker Model Registry AI-Ressourcen hinzugefügt.	Sie können jetzt erweiterte Parameter sicher und effizient innerhalb Ihrer Organisation AWS-Konten oder innerhalb Ihrer Organisation teilen.	27. Juni 2024
Unterstützung für die gemeinsame Nutzung von Amazon SageMaker AI hinzugefügt JumpStart	Sie können Amazon SageMaker AI JumpStart Hubs jetzt mit AWS-Konten oder innerhalb Ihrer Organisat ion teilen.	27. Juni 2024

Unterstützung für das Teilen hinzugefügt Amazon Route 53 ResolverProfiles	Sie können es jetzt verwenden AWS RAM , um es Amazon Route 53 Resolver Profiles mit anderen AWS-Konten innerhalb Ihrer Organisation zu teilen.	22. April 2024
Unterstützung für die gemeinsame Nutzung von AWS Systems Manager Parameter Store-Ressourcen wurde hinzugefügt	Sie können jetzt erweiterte Parameter sicher und effizient innerhalb Ihrer Organisation AWS-Konten oder innerhalb Ihrer Organisation teilen.	21. Februar 2024
Unterstützung für die gemeinsame Nutzung von Amazon FSx für OpenZFS-Snapshots hinzugefügt	Sie können jetzt Amazon FSx for OpenZFS-Snapshots mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	19. Dezember 2023
Unterstützung für die gemeinsame Nutzung von Ressourcen hinzugefügt Amazon Simple Storage Service	Sie können die Amazon Simple Storage Service Access Grants-Instanz jetzt mit anderen Personen AWS-Konten oder mit Ihrer Organisation teilen AWS RAM.	27. November 2023
Unterstützung für das Teilen von AWS Resource Explorer Ansichten hinzugefügt	Sie können jetzt AWS Resource Explorer Ansichten mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	14. November 2023
Unterstützung für die gemeinsame Nutzung von Amazon Application Recovery Controller (ARC) -Ressourcen hinzugefügt	Sie können jetzt Amazon Application Recovery Controller (ARC) -Cluster mit anderen AWS-Konten oder Ihrer Organisation teilen AWS RAM.	18. Oktober 2023

Unterstützung für die gemeinsame Nutzung von DataZone Amazon-Ressourcen hinzugefügt	Sie können jetzt DataZone Amazon-Ressourcen mit anderen AWS-Konten oder Ihrer Organisation teilen.	04. Oktober 2023
Unterstützung für die gemeinsame Nutzung von Service Principal hinzugefügt	Sie können nun Service Principals mit Ressource nfreigaben verknüpfen. Auf diese Weise können bestimmte Dienste die erforderlichen Aktionen für Kundenressourcen in Ihrem Namen verwalten.	29. August 2023
Unterstützung für die gemeinsame Nutzung von SageMaker Model Card-Ressourcen wurde hinzugefügt	Sie können SageMaker Model Card-Ressourcen jetzt mit anderen AWS-Konten oder Ihrer Organisation teilen.	18. August 2023
Unterstützung für Amazon SageMaker AI Feature Store-Funktionsgruppen und SageMaker KI-Katalog als gemeinsam nutzbare Ressourcen hinzugefügt	Sie können jetzt Amazon SageMaker AI Feature Store-Funktionsgruppen und SageMaker KI-Katalogressourcen mit anderen AWS-Konten oder Ihrer Organisation teilen.	20. Juli 2023
Erhöhung des Servicekontingents für ausstehende Einladungen	Die maximale Anzahl ausstehender Einladungen pro Sharing-Konto wurde von 20 auf 250 erhöht.	08. Juni 2023
Unterstützung für AWS AppSync GraphQL APIs als gemeinsam nutzbare Ressourcen hinzugefügt	Sie können AWS AppSync GraphQL jetzt APIs AWS-Konten mit AWS RAM anderen teilen.	24. Mai 2023

Unterstützung für AWS Verified Access Gruppen als gemeinsam nutzbare Ressourcen hinzugefügt	Sie können jetzt AWS Verified Access Gruppen zentral erstellen und verwalten und sie dann mit anderen AWS-Konten oder Ihrer Organisation teilen.	27. April 2023
Unterstützung für vom Kunden verwaltete Berechtigungen in der AWS RAM Konsole hinzugefügt	Sie können jetzt auf sichere Weise detaillierte Ressource nzugriffskontrollen für unterstützte Ressourcentypen erstellen und verwalten.	19. April 2023
Unterstützung für Amazon VPC Lattice Service und gemeinsam nutzbare Service-Netzwerkressourcen hinzugefügt	Sie können jetzt die Service- und Service-Netzwerkressourcen von Amazon VPC Lattice mit anderen teilen. AWS-Konten	31. März 2023
Unterstützung für AWS Marketplace Katalog-Entitäten als gemeinsam nutzbare Ressourcen hinzugefügt	Sie können Ihre Entitäten jetzt mit anderen AWS-Konten im Marketplace teilen.	27. März 2023
Unterstützung für die Verwaltung von Berechtigungsversionen in der AWS RAM Konsole hinzugefügt	Sie können jetzt die AWS RAM Konsole verwenden, um Versionsdetails anzuzeigen und die Berechtigungen auf die Version zu aktualisieren, die als Standardversion festgelegt ist.	16. Januar 2023

Aktualisierung der bewährten Methoden für IAM	Aktualisierung des Leitfadens zur Ausrichtung an bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM.	3. Januar 2023
Unterstützung für Amazon EC2-Placement-Gruppen als gemeinsam nutzbare Ressourcen hinzugefügt	Sie können Amazon EC2-Placement-Gruppen jetzt mit anderen teilen AWS-Konten , um deren Instances zu starten.	08. November 2022
Es wurden Links zu zwei Einführungsvideos hinzugefügt über AWS RAM	Es wurden Übersichtsvideos hinzugefügt, die das Teilen einer Ressource mit anderen beschreiben AWS RAM und erläutern. AWS-Konten	2p. August 2022
Unterstützung für Amazon SageMaker AI-Pipelines hinzugefügt	Sie können SageMaker KI-Pipelines jetzt mit anderen teilen. AWS-Konten	2.August 2022
Unterstützung für AWS Service Catalog AppRegistry Anwendungen und Attributgruppen als gemeinsam nutzbare Ressourcentypen hinzugefügt	Sie können jetzt AppRegistry Anwendungen und Attributgruppen mit anderen AWS-Konten teilen.	17. Juni 2022
AWS Resource Access Manager erhält die SOC- und ISO-Zertifizierung	AWS RAM wurde als konform mit den Normen Service Organization Control (SOC) und ISO 9001, ISO 27001, ISO 27017, ISO 27018 und ISO 27701 der Internationalen Organisation für Normung (ISO) validiert.	31. Mai 2022

AWS Resource Access Manager erhält die FedRAMP-Zertifizierung	AWS RAM wurde als konform mit dem Federal Risk and Authorization Management Program (FedRAMP) validiert.	8. April 2022
AWS Resource Access Manager erhält die PCI DSS-Zertifizierung	AWS RAM wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert.	27. Februar 2022
Unterstützung für Amazon VPC IPAM-Ressourcenentdeckungen als gemeinsam nutzbare Ressourcen hinzugefügt. Außerdem können Sie jetzt IPAM-Pools mit Konten außerhalb einer Organisation teilen	Sie können jetzt IPAM-Ressourcenentdeckungen mit anderen teilen. AWS-Konten	25 Januar 2022
Unterstützung für die gemeinsame Nutzung globaler Ressourcen wurde hinzugefügt	Sie können jetzt globale Ressourcen mit anderen teilen AWS-Konten.	2. Dezember 2021
Unterstützung für AWS Cloud-WAN-Kernnetzwerke als gemeinsam nutzbare globale Ressourcen hinzugefügt	Sie können jetzt Cloud WAN-Kernnetzwerke mit anderen AWS-Konten teilen.	2. Dezember 2021
Support für die gemeinsame Nutzung von Amazon VPC IP Address Manager (IPAM) - Pools	Sie können Amazon VPC IPAM-Pools verwenden, AWS RAM um sie gemeinsam zu nutzen. Weitere Informationen finden Sie unter Gemeinsam nutzbare AWS Ressourcen im AWS RAM Benutzerhandbuch.	1. Dezember 2021

Support für die gemeinsame Nutzung von Amazon SageMaker AI-Ressourcen	Sie können es verwenden AWS RAM , um SageMaker KI-Abstammungsgruppen gemeinsam zu nutzen. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Gemeinsam nutzbare AWS Ressourcen.	30. November 2021
Support für die gemeinsame Nutzung von AWS Migration Hub Refactor Spaces-Ressourcen	Sie können es verwenden AWS RAM , um Migration Hub Hub-Umgebungen gemeinsam zu nutzen. Weitere Informationen finden Sie unter Gemeinsam nutzbare AWS Ressourcen im AWS RAM Benutzerhandbuch.	29. November 2021
Es wurden Informationen zu AWS RAMAWS-verwalteten IAM-Berechtigungsrichtlinien hinzugefügt	Veröffentlichte Details zu den verfügbaren AWS-verwalteten Berechtigungsrichtlinien, auf die Sie in der IAM-Konsole zugreifen und die Sie an die IAM-Prinzipale in Ihrem anhängen können. AWS-Konto	16. September 2021
Unterstützung für die gemeinsame Nutzung von S3 auf Outposts-Ressourcen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um S3 auf Outposts mit anderen AWS-Konten zu teilen.	05. August 2021

Unterstützung für zusätzliche verwaltete Berechtigungen und die gemeinsame Nutzung von Ressourcen mit IAM-Prinzipalen hinzugefügt	Für unterstützte Ressourcentypen können Sie aus zusätzlichen AWS RAM verwalteten Berechtigungen wählen und Ressourcen für einzelne IAM-Rollen und -Benutzer gemeinsam nutzen.	10. Juni 2021
Unterstützung für die gemeinsame Nutzung von AWS Systems Manager Incident Manager-Ressourcen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Kontakte und Reaktionspläne von AWS Systems Manager Incident Manager mit anderen zu teilen AWS-Konten.	10. Mai 2021
Unterstützung für die gemeinsame Nutzung von Amazon Route 53-Ressourcen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Amazon Route 53 Resolver DNS-Firewall-Regelgruppen mit anderen AWS-Konten zu teilen.	31. März 2021
Unterstützung für die gemeinsame Nutzung AWS Transit Gateway von Ressourcen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Transit-Gateway-Multicast-Domänen mit anderen AWS-Konten zu teilen.	10. Dezember 2020
Unterstützung für die gemeinsame Nutzung AWS Network Firewall von Ressourcen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um AWS Network Firewall Firewall-Richtlinien und Regelgruppen mit anderen zu teilen AWS-Konten.	17. November 2020

Unterstützung für die gemeinsame Nutzung von Outposts und lokalen Gateway-Routentabellen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Outposts und lokale Gateway-Routentabellen mit anderen AWS-Konten zu teilen.	15. Oktober 2020
Unterstützung für die gemeinsame Nutzung von Route 53-Abfrageprotokollen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Route 53-Abfrageprotokolle mit anderen zu teilen AWS-Konten.	7. September 2020
Unterstützung für die gemeinsame Nutzung von AWS Private Certificate Authority Ressourcen wurde hinzugefügt	Sie können es jetzt verwenden AWS RAM , um AWS Private CA private Zertifizierungsstellen (CAs) mit anderen zu teilen AWS-Konten.	17. August 2020
Unterstützung für die gemeinsame Nutzung von AWS Glue-Datenkatalogen, Datenbanken und -Tabellen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um AWS Glue-Datenkataloge, Datenbanken und Tabellen mit anderen AWS-Konten zu teilen.	7. Juli 2020
Unterstützung für die gemeinsame Nutzung von Amazon VPC-Präfixlisten hinzugefügt	Sie können sie jetzt AWS RAM zum Teilen von Präfixlisten verwenden.	29. Juni 2020
Unterstützung für die gemeinsame Nutzung von AWS Outposts kundeneigenen Adressen IPv4 hinzugefügt	Sie können es jetzt verwenden AWS RAM , um AWS Outposts kundeneigene IPv4 Adressen mit anderen zu teilen. AWS-Konten	22. April 2020
Unterstützung für das Teilen AWS App Mesh von Meshes hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Meshes mit anderen zu teilen. AWS-Konten	17. Januar 2020

Unterstützung für das Teilen von AWS CodeBuild Projekten und Berichtsgruppen wurde hinzugefügt	Sie können es jetzt verwenden AWS RAM , um AWS CodeBuild Projekte und Berichtsgruppen mit anderen zu teilen AWS-Konten.	13. Dezember 2019
Unterstützung für die gemeinsame Nutzung zusätzlicher Ressourcen hinzugefügt	Sie können es jetzt verwenden , AWS RAM um Amazon EC2 Dedicated Hosts, AWS -Ressourcengruppen Ressourcengruppen und Amazon EC2 Image Builder Builder-Komponenten, Images und Image-Rezepte mit anderen zu teilen. AWS-Konte n	02. Dezember 2019
Unterstützung für die gemeinsame Nutzung von Kapazitätsreservierungen auf Abruf hinzugefügt	Sie können es jetzt verwenden AWS RAM , um On-Demand-Kapazitätsreservierungen mit anderen zu teilen AWS-Konte n.	29. Juli 2019
Unterstützung für die gemeinsame Nutzung von Aurora-DB-Clustern hinzugefü gt	Sie können es jetzt verwenden AWS RAM , um Aurora-DB-Cluster mit anderen zu teilen AWS-Konten.	2. Juli 2019
Unterstützung für die gemeinsame Nutzung von Traffic Mirroring-Zielen wurde hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Traffic Mirroring-Ziele mit anderen zu teilen. AWS-Konten	25. Juni 2019

Unterstützung für die gemeinsame Nutzung von Lizenzkonfigurationen wurde hinzugefügt	Sie können es jetzt verwenden AWS RAM , um AWS License Manager Manager-Lizenzkonfigurationen mit anderen zu teilen AWS-Konten.	5. Dezember 2018
Unterstützung für die gemeinsame Nutzung von Subnetzen hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Amazon VPC-Subnetze mit anderen zu teilen. AWS-Konten	27. November 2018
Unterstützung für die gemeinsame Nutzung von Transit-Gateways hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Amazon VPC Transit Gateways mit anderen zu teilen. AWS-Konten	26. November 2018
Unterstützung für die gemeinsame Nutzung von Resolver-Regeln hinzugefügt	Sie können es jetzt verwenden AWS RAM , um Route 53-Resolver-Regeln mit anderen zu teilen. AWS-Konten	20. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.