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 zwischenAWS-Konten, innerhalb Ihrer Organisation oder Organisationseinheiten (OUs) sowie mitAWS Identity and Access Management (IAM-) Rollen und Benutzern für unterstützte Ressourcentypen zu teilen. Wenn Sie mehrere habenAWS-Konten, können Sie eine Ressource einmal erstellen und verwenden,AWS RAM um diese Ressource für diese anderen Konten nutzbar zu machen. Wenn Ihr Konto von verwaltet wirdAWS Organizations, können Sie Ressourcen mit allen anderen Konten in der Organisation oder nur mit den Konten teilen, die zu einer oder mehreren bestimmten Organisationseinheiten (OUs) gehören. Sie können Inhalte auch mit einer bestimmtenAWS-Konten Konto-ID teilen, unabhängig davon, ob das Konto Teil einer Organisation ist. Bei einigen unterstützten Ressourcentypen können Sie sie auch für bestimmte IAM-Rollen und -Benutzer freigeben.

Inhalt

Videoübersichten

Das folgende Video stellt eine kurze EinführungAWS RAM und beschreibt, wie ein Ressourcenfreigabe erstellt wird. Weitere Informationen finden Sie unter ???.

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

Dieses Video zeigt, wie kundenverwaltete Rechte nach der bewährten Methode der geringsten Rechte erstellt und zugeordnet werden. Weitere Informationen finden Sie unter ???.

Vorteile von AWS RAM

Warum AWS RAM verwenden? Sie bietet die folgenden Vorteile:

- Reduziert Ihren betrieblichen Aufwand — 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 es vereinfacht, allen Rollen und Benutzern in diesem Konto Zugriff zu gewähren, ohne identitätsbasierte Berechtigungsrichtlinien verwenden zu 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 einerAWS RAM Ressourcennutzung durch einen einzigen Satz von Richtlinien und Berechtigungen verwaltet. AWS RAMbietet ein einheitliches Erlebnis für die gemeinsame Nutzung verschiedener Arten vonAWS Ressourcen.
- Sorgt für Transparenz und Überprüfbarkeit — Durch die Integration vonAWS RAM Amazon CloudWatch und können Sie sich die Nutzungsdetails Ihrer gemeinsam genutzten Ressourcen anzeigen lassenAWS CloudTrail. AWS RAMbietet einen umfassenden Überblick über gemeinsam genutzte Ressourcen und Konten.

Wie steht es mit kontenübergreifenden Zugriffen mit ressourcenbasierten Richtlinien?

Sie können einige Arten vonAWS Ressourcen mit anderen teilen,AWS-Konten indem Sie eine ressourcenbasierte Richtlinie anhängen, dieAWS Identity and Access Management (IAM-) Prinzipale (IAM-Rollen und Benutzer) außerhalb Ihrer Ressourcen identifiziertAWS-Konto. Wenn Sie eine Ressource gemeinsam nutzen, indem Sie eine Richtlinie anhängen, werden die zusätzlichen Vorteile, die sich darausAWS RAM ergeben, jedoch nicht genutzt. Durch die Verwendung erhaltenAWS RAM Sie folgende Funktionen:

- Sie können die Daten für eine Organisation oder eine Organisationseinheit (OE) freigeben, ohne jede einzelne derAWS-Konto IDs aufzählen zu müssen.

- Benutzer können die für sie freigegebenen Ressourcen direkt in der ursprünglichenAWS-Service Konsole und in den API-Vorgängen sehen, als ob sich diese Ressourcen direkt im Konto des Benutzers befinden würden. Wenn SieAWS 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 zu Ihrer Organisation gehört, wird einAWS RAM Einladungsprozess eingeleitet. Der Empfänger muss die Einladung annehmen, bevor der Prinzipal auf die freigegebenen Ressourcen zugreifen kann. Nachdem Sie die Funktion zum Teilen innerhalb Ihrer Organisation aktiviert haben, sind für die gemeinsame Nutzung mit Konten in der Organisation keine Einladungen erforderlich.

Wenn Sie über Ressourcen verfügen, die Sie mithilfe einer ressourcenbasierten Berechtigungsrichtlinie gemeinsam genutzt haben, können Sie diese Ressourcen zu vollständigAWS RAM verwalteten Ressourcen heraufstufen, indem Sie eine der folgenden Aktionen ausführen:

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

Funktionsweise der Ressourcenfreigabe

Wenn Sie eine Ressource im Eigentümerkonto mit einer anderen RessourceAWS-Konto, dem Verbraucherkonto, teilen, gewähren Sie den Hauptbenutzern des Benutzerkontos Zugriff auf die gemeinsam genutzte Ressource. Alle Richtlinien und Berechtigungen, die für Rollen und Benutzer im Nutzerkonto gelten, gelten auch für die gemeinsam genutzte Ressource. Die Ressourcen in der Freigabe sehen aus, als wären sie native Ressourcen in dem, mit demAWS-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 AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Um eine Ressourcenfreigabe zu erstellen, geben Sie Folgendes an:

- Der,AWS-Region in der Sie den Ressourcenfreigabe anlegen möchten. In der Konsole wählen Sie aus dem Dropdown-Menü Region in der oberen rechten Ecke der Konsole. In derAWS CLI verwenden Sie den`--region` Parameter.
  - Ein Ressourcenfreigabe kann nur regionale Ressourcen enthalten, die mit dem Ressourcenfreigabe übereinstimmen.AWS-Region
  - Ein Ressourcenanteil kann nur globale Ressourcen enthalten, wenn sich der Ressourcenanteil in der ausgewiesenen Heimatregion für globale Ressourcen, 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 Prinzipale, denen Sie Zugriff auf die Ressource gewähren. Principals können EinzelpersonenAWS-Konten, die Konten einer Organisation oder einer Organisationseinheit (OU) inAWS Organizations oder einzelne Rollen oder BenutzerAWS Identity and Access Management (IAM) sein.

  > **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 unterGemeinsam nutzbare Ressourcen AWS.

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

  Das Verhalten der Erlaubnis ist abhängig vom Typ des Prinzipals:

- Wenn der Principal ein anderes Konto hat als das, dem die Ressource gehört, dann sind die mit der Ressourcennutzung 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 Zugriff auf die gemeinsam genutzte Ressource mit identitätsbasierten IAM-Richtlinien gewähren. Die in diesen Richtlinien gewährten Berechtigungen dürfen nicht über die Berechtigungen hinausgehen, die in den mit der Ressourcennutzung verknüpften Berechtigungen definiert sind.

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

Verwenden gemeinsam genutzter Ressourcen

Wenn der Besitzer einer Ressource diese mit Ihrem Konto teilt, können Sie auf die geteilte Ressource zugreifen, als ob sie Ihrem Konto gehört hätte. Sie können auf die Ressource zugreifen, indem Sie die Konsole,AWS CLI Befehle und API-Operationen des entsprechenden Dienstes verwenden. Die API-Operationen, die die Principals in Ihrem Konto ausführen dürfen, variieren je nach Ressourcentyp und werden durch die der Ressourcennutzung zugewieseneAWS RAM Berechtigung festgelegt. Alle in Ihrem Konto konfigurierten IAM-Richtlinien und Servicekontrollrichtlinien gelten ebenfalls weiterhin, sodass Sie Ihre vorhandenen Investitionen in Sicherheits- und Governance-Kontrollen nutzen können.

Wenn Sie über den Dienst dieser Ressource auf eine gemeinsam genutzte Ressource zugreifen, haben Sie dieselben Fähigkeiten und Einschränkungen wieAWS-Konto der Besitzer der Ressource.

- Wenn es sich bei der Ressource um eine regionale Ressource handelt, können Sie nur von der Ressource aus zugreifen,AWS-Region in der sie im eigenen Konto vorhanden ist.
- Wenn die Ressource global ist, können Sie von jedem Ort aus darauf zugreifenAWS-Region, den die Servicekonsole und die Tools der Ressource unterstützen. Sie können die Ressourcenfreigabe und die zugehörigen globalen Ressourcen in derAWS RAM Konsole und den Tools nur in der dafür vorgesehenen Heimatregion USA Ost (Nord-Virginia) anzeigen und verwaltenus-east-1.

Zugriff auf AWS RAM

Sie können AWS RAM auf folgende Art und Weise nutzen:

AWS RAM-Konsole

AWS RAM bietet eine Web-basierte Benutzeroberfläche, die AWS RAM-Konsole. Nach der Registrierung einer können Sie auf dieAWS RAM -Konsole zugreifenAWS-Konto, indem Sie sich bei der anmelden AWS Management Consoleund aufAWS RAM der Konsolenstartseite auswählen.

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

AWS CLIund Tools für Windows PowerShell

DieAWS CLI undAWS Tools for PowerShell bieten direkten Zugriff auf dieAWS RAM öffentlichen API-Operationen. AWSunterstützt diese Tools aufWindowsmacOS, undLinux. Weitere Informationen zu den ersten Schritten finden Sie im AWS Command Line Interface-Benutzerhandbuch oder AWS Tools for Windows PowerShell-Benutzerhandbuch. Weitere Informationen zu den Befehlen fürAWS RAM finden Sie in der AWS CLI-Befehlsreferenz oder in der AWS Tools for Windows PowerShellCmdletreferenz.

AWS-SDKs

AWSstellt API-Befehle für zahlreiche Programmiersprachen bereit. Weitere Informationen zu den ersten Schritten finden Sie im -Benutzerhandbuch fürAWS SDKs und Tools.

Abfrage-API

Wenn Sie keine der unterstützten Programmiersprachen verwenden, erhalten Sie mit derAWS RAM HTTPS-Abfrage-API programmatischen Zugriff aufAWS RAM undAWS. Mit derAWS RAM API können Sie HTTPS-Anfragen direkt an den Service richten. Wenn Sie die AWS RAM-API nutzen, müssen Sie Code zur digitalen Signierung von Anfragen mittels Ihrer Anmeldeinformationen einschließen. Weitere Informationen finden Sie in der AWS RAM-API-Referenz.

Preise für AWS RAM

Für die NutzungAWS RAM oder Erstellung von Ressourcenfreigaben und die gemeinsame Nutzung Ihrer Ressourcen für mehrere Konten fallen keine zusätzlichen Gebühren an. Nutzungsabhängige Gebühren von Ressourcen variieren je nach Ressourcentyp. Weitere Informationen zur AbrechnungAWS freigegebener Ressourcen finden Sie in der Dokumentation für den Dienst, der der die Ressource gehört.

Konformität und internationale Standards

PCI-DSS

AWS RAMunterstützt 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 RAMist als FedRAMP Moderate in den folgenden Ländern zugelassenAWS-Regionen: US East (Nord-Virginia), USA East (Ohio), USA West (Nordkalifornien) und USA West (Oregon).

AWS RAMist in den folgenden Ländern als FedRAMP High zugelassenAWS-Regionen:AWS GovCloud (US-West) undAWS 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 RAMkann für Workloads verwendet werden, die den Normen Service Organization Control (SOC) und ISO 9001, ISO 27001, ISO 27017, ISO 27018 und ISO 27701 der International Organization for Standardization (ISO) entsprechen. Kunden aus den Bereichen Finanzen, Gesundheitswesen und anderen regulierten Branchen können Einblicke in die Sicherheitsprozesse und -kontrollen zum Schutz von Kundendaten erhalten. Diese finden Sie in den SOC-Berichten sowie in denAWS ISO- und CSA STAR-Zertifikaten unter AWS Artifact.

Weitere Informationen zur SOC-Konformität finden Sie unter SOC.

Weitere Informationen zur ISO-Konformität finden Sie unter ISO 9001, ISO 27001, ISO 27017, ISO 27018 und ISO 27701.

Erste Schritte mit AWS RAM

MitAWS Resource Access Manager, Sie können Ressourcen, die Sie besitzen, mit anderen gewährt.AWS-Konten. Wenn Ihr Konto verwaltet wird vonAWS Organizations, können Sie Ressourcen auch mit den anderen Konten in Ihrer Organisation teilen. Sie können auch Ressourcen verwenden, die von anderen mit Ihnen geteilt wurdenAWS-Konten.

Wenn Sie das Teilen innerhalb von nicht aktivierenAWS Organizations, können Sie Ressourcen nicht mit Ihrer Organisation oder den Organisationseinheiten (OU) in Ihrer Organisation teilen. Sie können Ressourcen jedoch weiterhin mit Einzelpersonen gewährt.AWS-Kontenin Ihrer Organisation. Fürunterstützte Ressourcenfreigabe, Sie können Ressourcen auch mit einzelnen Personen teilenAWS Identity and Access Management(IAM) Rollen oder Benutzer in Ihrer Organisation. In diesem Fall werden diese Prinzipale so behandelt, als wären sie externe Konten und nicht als Teil Ihrer Organisation. Sie erhalten eine Einladung zur Teilnahme an der Ressourcenfreigabe und sie müssen die Einladung zur Teilnahme an der Ressourcenfreigabe und sie müssen die Einladung zur Teilnahme an der Ressourcenfreigabe und die Einladung wird ihnen Zugriff auf die freigegebene gewährt.

Inhalt

Begriffe und Konzepte fürAWS RAM

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

Ressourcenfreigabe

Sie teilen Ressourcen mitAWS RAMdurch Erstellen einesgemeinsam genutzte Ressourcen. Ein Ressourcenanteil besteht aus den folgenden drei Elementen:

- Eine Liste mit einem oder mehrerenAWSRessourcen, die gemeinsam genutzt werden sollen.
- Eine Liste mit einem oder mehrerenPrinzipaledenen der Zugang zu den Ressourcen gewährt wird.

- EINverwaltete Erlaubnisfür jeden Ressourcentyp, den Sie in den Share aufnehmen. Jede verwaltete Berechtigung gilt für alle Ressourcen dieses Typs in dieser Ressourcenfreigabe.

Nach der VerwendungAWS RAMUm eine Ressourcenfreigabe zu erstellen, kann den in der Ressourcenfreigabe angegebenen Prinzipalen Zugriff auf die Ressourcen der Freigabe gewährt werden.

- Wenn du einschaltestAWS RAMteilen mitAWS Organizations, und Ihre Prinzipale, für die Sie etwas teilen, gehören derselben Organisation an wie das Sharing-Konto. Diese Prinzipale können Zugriff erhalten, sobald ihr Kontoadministrator ihnen die Erlaubnis erteilt, die Ressourcen mithilfe einesAWS Identity and Access Management(IAM) -Berechtigungsrichtlinie.
- Wenn Sie nicht einschaltenAWS RAMWenn Sie Ressourcen mit Organizations teilen, können Sie weiterhin Ressourcen mit Einzelpersonen teilenAWS-Kontendie in Ihrer Organisation vorhanden sind. 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 die Daten auch an Konten außerhalb Ihrer Organisation anfügen können, 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 darüber, welche Ressourcentypen diese Art der gemeinsamen Nutzung unterstützen, finden Sie unterGemeinsam nutzbare Ressourcen AWSund schauen Sie sich den anKann mit Konten außerhalb seiner Organisation teilenSpalte.

Konto teilen

DasKonto teilenenthält die Ressource, die gemeinsam genutzt wird und in derAWS RAMAdministrator erstellt denAWSgemeinsame Nutzung von Ressourcen mithilfe vonAWS RAM.

EinAWS RAMAdministrator ist ein IAM-Principal, der über die Rechte zum Erstellen und Konfigurieren von Ressourcenfreigaben in derAWS-Konto. WeilAWS RAMfunktioniert, indem es an die Ressourcen in einer Ressourcenfreigabe anfügen kann, dieAWS RAMDer Administrator muss auch über Berechtigungen zum Aufrufen von verfügen`PutResourcePolicy`Betrieb in`AWS-Service`für jeden Ressourcentyp, der in einer Ressourcenfreigabe enthalten ist.

Principals konsumieren

Dasverbrauchendes Kontoist derAWS-Kontofür die 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 unterGemeinsam nutzbare Ressourcen AWSund schauen Sie sich den anKann Rollen und Benutzer mit IAM teilenSpalte.

AWS RAMunterstützt auch Service Principals als Nutzer von Resource Shares. Informationen darüber, welche Ressourcentypen diese Art der gemeinsamen Nutzung unterstützen, finden Sie unterGemeinsam nutzbare Ressourcen AWSund schauen Sie sich den anKann mit Service Principals teilenSpalte.

Die Hauptbenutzer des Benutzerkontos können nur die Aktionen ausführen, die vonbeidesder folgenden Berechtigungen:

- Die verwalteten Berechtigungen, die mit der Ressourcenfreigabe verknüpft sind. Diese spezifizierenmaximalBerechtigungen, die den Hauptbenutzern des Benutzerkontos erteilt werden können.
- Die identitätsbasierten IAM-Richtlinien, die vom IAM-Administrator im Nutzerkonto einzelnen Rollen oder Benutzern zugewiesen wurden. Diese Richtlinien müssen Folgendes gewährenAllowZugriff auf bestimmte Aktionen und aufAmazon-Ressourcenname (ARN)einer Ressource im Sharing-Konto.

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

- Ein weitererAWS-Konto— Die gemeinsame Nutzung von Ressourcen stellt die im Sharing-Konto enthaltenen Ressourcen dem nutzenden Konto zur Verfügung.
- 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`
- Leiter des Dienstes— Teilen Sie eine Ressource mit einemAWSDienst, um dem Dienst Zugriff auf eine gemeinsame Ressource zu gewähren. Die gemeinsame Nutzung von Service Principal

ermöglicht eineAWSService, der in Ihrem Namen Maßnahmen zur Verringerung der betrieblichen Belastung ergreift.

Um die gemeinsame Nutzung mit einem Dienstprinzipal zu ermöglichen, wählen Sie aus, ob Sie die gemeinsame Nutzung für alle zulassen möchten, und klicken Sie dann unterWählen Sie den Haupttyp, wählenLeiter des Dienstesaus der Drop-down-Liste. Geben Sie den Namen des Dienstprinzipals im folgenden Format an:

- *service-id*.amazonaws.com

Um das Risiko zu verringern, dass der Stellvertreter verwirrt wird, zeigt die Ressourcenrichtlinie die Konto-ID des Ressourcenbesitzers imaws:SourceAccountBedingungsschlüssel.

- Konten in einer Organisation— Wenn das Sharing-Konto verwaltet wird vonAWS Organizations, dann kann im Resource Share die ID der Organisation angegeben werden, die mit allen Konten in der Organisation geteilt werden soll. Die Ressourcenfreigabe kann alternativ eine Organisationseinheit-ID (OU) angeben, die von allen Konten in dieser Organisationseinheit gemeinsam genutzt werden soll. Ein Sharing-Konto kann nur mit der eigenen Organisation oder mit OU-IDs innerhalb der eigenen Organisation geteilt werden. Geben Sie Konten in einer Organisation anhand des ARN der Organisation oder der Organisationseinheit an.
  - Alle Konten in einer Organisation— Es folgt ein Beispiel für einen ARN einer Organisation inAWS 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 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 RichtlinieAWS RAMwird an jede Ressource angehängt, die von der Share verwendet wird`"Principal": "*"`.

Weitere Informationen finden Sie unter Auswirkungen der Verwendung"Principal": "*"in einer ressourcenbasierten Politik.
Die Principals der anderen Konten, die die Aktie konsumieren, 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 Folgendes gewährenAllowZugriff auf die ARNs einzelner Ressourcen im Resource Share. 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 IAM-Richtliniensprache implementieren. Im Gegensatz zu identitätsbasierten Richtlinien, die Sie an den Prinzipal anfügen können, wie z. B. IAM-Gruppen oder -Gruppen, fügen Sie ressourcenbasierte Richtlinien an die Ressource an.AWS RAMerstellt in Ihrem Namen ressourcenbasierte Richtlinien auf der Grundlage der Informationen, die Sie für Ihren Resource Share angeben. Sie müssen angeben:PrincipalRichtlinienelement, das bestimmt, wer auf die Ressource zugreifen kann. Weitere Informationen finden Sie unterIdentitätsbasierte Richtlinien und ressourcenbasierte Richtlinienin derIAM User Guide.

Die ressourcenbasierten Richtlinien werden generiert vonAWS RAMwerden 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 Service Control Policies (SCPs) fürAWS Organizationsdas könnte gelten fürAWS-Konto. Ressourcenbasierte Richtlinien generiert vonAWS RAMunterliegen derselben Richtlinienbewertungslogik wie alle anderen IAM-Richtlinien. Vollständige Informationen zur Richtlinienbewertung und zur Bestimmung der daraus resultierenden Berechtigungen finden Sie unterAuswertungslogik für Richtlinienin derIAM User Guide.

AWS RAMbietet ein einfaches und sicheres Erlebnis beim Teilen von Ressourcen, indem easy-to-use ressourcenbasierte abstraktionsbasierte Richtlinien.

Für die Ressourcentypen, die ressourcenbasierte Richtlinien unterstützen,AWS RAMerstellt und verwaltet automatisch die ressourcenbasierten Richtlinien für Sie. Für eine bestimmte RessourceAWS RAMerstellt die ressourcenbasierte Richtlinie, indem die Informationen aus allen Ressourcenfreigaben kombiniert werden, zu denen diese Ressource gehört. Stellen Sie sich zum Beispiel einen Amazon vor SageMaker Pipeline, die Sie gemeinsam nutzenAWS RAMund

in zwei verschiedene Ressourcenfreigaben einbeziehen. Sie könnten eine Ressourcenfreigabe verwenden, um Ihrer gesamten Organisation schreibgeschützten Zugriff zu gewähren. Sie könnten dann die andere Ressourcenfreigabe verwenden, um nur zu gewähren SageMaker Ausführungsberechtigungen für ein einzelnes Konto.AWS RAMkombiniert diese beiden unterschiedlichen Berechtigungssätze automatisch zu einer einzigen Ressourcenrichtlinie mit mehreren Anweisungen. Anschließend fügt es die kombinierte ressourcenbasierte Richtlinie an die Pipeline-Ressource an. Sie können sich diese zugrunde liegende Ressourcenrichtlinie ansehen, indem SieGetResourcePolicyBetrieb.AWS-Servicesverwenden 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 Ihren Ressourcen zuordnen, indem Sie Folgendes aufrufen`PutResourcePolicy`, wir empfehlen Ihnen zu verwendenAWS RAMweil es folgende Vorteile bietet:

- Auffindbarkeit für Aktienverbraucher— Wenn Sie Ressourcen teilen, indem SieAWS RAM, können Benutzer alle Ressourcen, die mit ihnen geteilt wurden, direkt in der Konsole und in den API-Vorgängen des Dienstes, der die Ressourcen besitzt, sehen, als ob sich diese Ressourcen direkt im Konto des Benutzers befinden würden. Wenn Sie beispielsweise eine teilenAWS CodeBuildEin Projekt mit einem anderen Konto können Benutzer des Benutzerkontos das Projekt in der CodeBuild Konsole und in den Ergebnissen von CodeBuild API-Operationen wurden ausgeführt. 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 Inhaber von Anteilen— Wenn Sie Ressourcen gemeinsam nutzenAWS 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 teilen, indem SieAWS RAM, Sie können mehrere Ressourcen gemeinsam nutzen und sie als Einheit verwalten. Ressourcen, die nur mithilfe von ressourcenbasierten Richtlinien gemeinsam genutzt werden, erfordern individuelle Richtlinien, die an jede Ressource angehängt werden, die Sie gemeinsam nutzen.
- Einfachheit— MitAWS RAM, Sie müssen die JSON-basierte IAM-Richtliniensprache nicht verstehen können.AWS RAMbietet ready-to-use AWSverwaltete Berechtigungen, aus denen Sie wählen können, um sie an Ihre Ressourcenfreigaben anzuhängen.

Durch die Verwendung vonAWS RAM, können Sie sogar einige Ressourcentypen gemeinsam nutzen, die noch keine ressourcenbasierten Richtlinien unterstützen. Für solche RessourcentypenAWS RAMgeneriert automatisch eine ressourcenbasierte Richtlinie als Darstellung der tatsächlichen Berechtigungen. Benutzer können sich diese Darstellung ansehen, indem sie anrufenGetResourcePolicy. Dazu gehören folgende 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-Domänen

Beispiele fürAWS RAMgenerierte ressourcenbasierte Richtlinien

Wenn Sie eine EC2 Image Builder Builder-Image-Ressource mit einer Einzelperson teilenKonto,AWS RAMgeneriert eine Richtlinie, die wie das folgende Beispiel aussieht, und hängt sie an alle Bildressourcen an, die in der Ressourcenfreigabe enthalten sind.

```
{
    "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 gemeinsam mit einemIAM-Rolle oder -Benutzerin einem anderenAWS-Konto,AWS RAMgeneriert eine Richtlinie, die wie das folgende

Beispiel aussieht, und hängt sie an alle Bildressourcen an, die in der Ressourcenfreigabe enthalten sind.

```
{
  "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 RAMgeneriert eine Richtlinie, die wie das folgende Beispiel aussieht, und fügt sie allen Bildressourcen hinzu, die in der Ressourcenfreigabe enthalten sind.

> **Note**
>
> Diese Richtlinie verwendet`"Principal": "*"`und verwendet dann die`"Condition"`Element, um Berechtigungen auf Identitäten zu beschränken, die den angegebenen entsprechen`PrincipalOrgID`. Weitere Informationen finden Sie unter Auswirkungen der Verwendung"Principal": "*"in einer ressourcenbasierten Politik.

```
{
    "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 Politik

Wenn Sie einschließen`"Principal": "*"`In einer ressourcenbasierten Richtlinie gewährt die Richtlinie Zugriff auf alle IAM-Prinzipale in dem Konto, das die Ressource enthält, vorbehaltlich aller Einschränkungen, die durch eine`Condition`Element, falls es existiert. Explizit`Deny`Aussagen in allen Richtlinien, die für den aufrufenden Principal gelten, haben Vorrang vor den durch diese Richtlinie gewährten Berechtigungen. Jedoch einimplizit `Deny`(was das Fehlen einesnicht jugendfrei `Allow`) in allen geltenden Identitäts-, Berechtigungsgrenzen- oder Sitzungsrichtliniennichtresultiert in`Deny`an die Schulleiter, die im Rahmen einer solchen ressourcenbasierten Richtlinie Zugriff auf eine Aktion erhalten haben.

Wenn dieses Verhalten für Ihr Szenario nicht wünschenswert ist, können Sie dieses Verhalten einschränken, indem Sie einnicht jugendfrei `Deny`Erklärung zu einer Identitätsrichtlinie, einer Berechtigungsgrenze oder einer Sitzungsrichtlinie, 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 können, welche verwalteten Berechtigungen Sie für die einzelnen in der Ressourcenfreigabe enthaltenen Ressourcentypen verwenden können. Eine verwaltete Berechtigung listet den Satz von`actions`und`Bedingungen`dass Principals mit der gemeinsam genutzten Ressource arbeiten können`AWS RAM`.

Sie können nur eine verwaltete Berechtigung für jeden Ressourcentyp in einer Ressourcenfreigabe anhängen. 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:

AWSverwaltete Berechtigungen

AWSverwaltete Berechtigungen werden erstellt und verwaltet vonAWSund gewähren Berechtigungen für gängige Kundenszenarien.AWS RAMdefiniert mindestens einenAWSverwaltete Berechtigungen für jeden unterstützten Ressourcentyp. Einige Ressourcentypen unterstützen mehr als einenAWSverwaltete Berechtigung, wobei eine verwaltete Berechtigung alsAWSStandard. DerStandardAWSverwaltete Berechtigungist verknüpft, sofern Sie nichts anderes angeben.

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 könnenAWS 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 die bewährte Methode der Methode der geringsten Rechte anwenden, indem Sie nur die Berechtigungen gewähren können, die für die Ausführung von Aufgaben an gemeinsam genutzten Ressourcen erforderlich sind.

Sie definieren Ihre eigenen Berechtigungen für einen Ressourcentyp in einer gemeinsam genutzten Ressource mit der Option, Bedingungen hinzuzufügen, wieGlobale Kontexttastenundservicespezifische Schlüsselum die Bedingungen festzulegen, unter denen Principals Zugriff auf die Ressource haben. Diese Berechtigungen können in einer oder mehreren verwendet werdenAWS RAMAktien. Kundenverwaltete Berechtigungen sind regionsspezifisch.

AWS RAMverwendet verwaltete Berechtigungen als Eingabe für die Erstellung desressourcenbasierte Richtlinienfür 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 du oderAWSerstellt eine neue Version mit verwalteten Berechtigungen, 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.

AWSVersionen mit verwalteten Berechtigungen

> AWSverarbeitet alle Änderungen anAWSverwaltete 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 AktualisierungAWS verwalteter Berechtigungen auf eine neuere Version.

Teilen Sie Ihre AWS Ressourcen

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

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

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 RAMist ein regionaler Dienst. Die Prinzipale, für die Sie die gemeinsame Nutzung verwenden, können nur auf die Ressourcenfreigaben zugreifen, AWS-Regionen in der sie 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 wirdAWS 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.

Wenn Sie Ressourcen nicht mehr für Ihre gesamte Organisation oder Organisationseinheiten gemeinsam nutzen müssen, können Sie die gemeinsame Nutzung von Ressourcen deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Ressourcenfreigabe 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 OrganizationsBenutzerhandbuch 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-accessAWS CLIBefehl 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 aktivieren

1. Öffnen Sie die Seite „Einstellungen“ in der AWS RAM Konsole.

2. Wählen Sie Freigabe mit AWS Organizations aktivieren und dann Einstellungen speichern aus.

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 Sie eine gemeinsame Nutzung von Ressourcen

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.
   - AWSverwaltete Berechtigungen werden von erstelltAWS, 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 sie besitzen. Sie können eine Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- AWS RAMist ein regionaler Dienst. Wenn Sie eine Ressource mit Prinzipalen in anderen teilenAWS-Konten, müssen diese Prinzipale auf jede Ressource von derselben Seite aus zugreifenAWS-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 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 Politik.
  > 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 ARNs der einzelnen Ressourcen im Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

- Sie können nur die Organisation, der Ihr Konto angehört, und Organisationseinheiten dieser Organisation zu Ihren Ressourcenfreigaben hinzufügen. Sie können einer Ressourcenfreigabe

keine Organisationseinheiten 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 — Weiterleitungsregeln
  - 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 gibtAWS-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 habenAWS 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 IhreAWS 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 Eine vom Kunden verwaltete Berechtigung erstellen. 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 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 Politik.
> 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 ARNs der einzelnen Ressourcen im 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-), können Prinzipale AWS-Konten in allen Organisationseinheiten dieser Organisationseinheit und ihren untergeordneten Organisationseinheiten auf die Ressourcenfreigabe zugreifen.
- Wenn Sie eine Einzelperson auswählenAWS-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. Die verfügbaren Prinzipaltypen sowie ID- ARN ARN-Formate lauten wie folgt:
  - AWS-Konto— Um eine hinzuzufügenAWS-Konto, geben Sie die 12-stellige Konto-ID ein. Beispiele:

    ```
    123456789012
    ```

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

    ```
    o-abcd1234
    ```

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

    ```
    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
    ```

    Beispiele:

    ```
    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`*

  Beispiele:

  `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-userAWS CLIBefehl 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`

    Beispiele:

    `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 SieAWS 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 Eine vom Kunden verwaltete Berechtigung erstellen.

```
$ 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"
    }
}
```

Verwenden gemeinsam genutzterAWS Ressourcen

Um mit der Nutzung von Ressourcen zu beginnen, die mit Ihrem Konto geteilt wurdenAWS Resource Access Manager, führen Sie die folgenden Aufgaben aus.

Aufgaben

- Antworscht.
- Verwenden Sie die Ressourcen, die mit Ihnen geteilt werden

Antworscht.

Wenn Sie eine Einladung erhalten, um einer Ressourcenfreigaaabeeinladung beizutreten beizutreten, müssen Sie diese annehmen, um Zugriff auf die freigegebenen Ressourcen beizutreten.

Einladungen werden in den folgenden Szenarien nicht verwendet:

- Wenn Sie Teil einer Organisation in sindAWS Organizations und die Freigabe in Ihrer Organisation aktiviert ist, erhalten die Schulleiter in der Organisation automatisch Zugriff auf die freigegebenen Ressourcen ohne Einladungen gewährt.
- Wenn Sie die Ressource mitAWS-Konto demjenigen teilen, dem die Ressource gehört, erhalten die Prinzipale in diesem Konto automatisch Zugriff auf die gemeinsam genutzten Ressourcen, ohne dass Sie dazu eingeladen werden.

Console

So reagieren Sie auf Einladungen

1. Öffnen Sie in derAWS RAM Konsole die Seite Mit mir geteilt: Resource Shares.

   > **Note**
   >
   > Ein Ressourcenanteil ist nur in dem sichtbar,AWS-Region in dem er erstellt wurde. Wenn ein erwarteter Ressourcenanteil nicht in der Konsole angezeigt wird, müssen Sie möglicherweiseAWS-Region mithilfe des Dropdown-Steuerelements in der oberen rechten Ecke zu einem anderen wechseln.

2. Sehen Sie sich die Liste der Ressourcenfreigaben an, auf die Ihnen Zugriff gewährt wurde.

   In der Spalte Status wird Ihr aktueller Teilnahmestatus für den Ressourcenanteil angezeigt. Der`Pending` Status gibt an, dass Sie zu einer Ressourcenfreigabe hinzugefügt wurden, die Einladung jedoch noch nicht angenommen oder abgelehnt haben.
3. Um auf die Einladung zur Ressourcennutzung 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 im`PENDING` Bundesstaat eine Ressourcenfreigabe 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`ACCEPTED`. Die Ressourcen, die in diesem Ressourcenanteil enthalten sind, stehen nun den Schulleitern im akzeptierenden Konto zur Verfügung.

Verwenden Sie die Ressourcen, die mit Ihnen geteilt werden

Nachdem Sie die Einladung zur Teilnahme an einer Ressourcennutzung 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-Vorgängen jeder Ressource verfügbar. Wenn es sich bei der Ressource um eine regionale Ressource handelt, müssen SieAWS-Region in der Servicekonsole den richtigen Befehl oder den 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 anzuzeigenAWS RAM, müssen Sie dieAWS RAM Konsole öffnen, in derAWS-Region die Ressourcenfreigabe erstellt wurde.

Arbeiten mit gemeinsam genutztenAWS Ressourcen

Sie könnenAWS Resource Access Manager (AWS RAM) verwenden, umAWS Ressourcen, die Sie besitzen, zu teilen und aufAWS Ressourcen zuzugreifen, die mit Ihnen geteilt wurden.

Inhalt

Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen

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

Die Ressourcen sind entweder regional oder global. Sie können das vierte Feld im Amazon-Ressourcennamen (ARN) verwenden, um festzustellen, ob es sich bei einer Ressource um eine regionale oder eine globale Ressource handelt. Regionale Ressourcen zeigen dieAWS-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 teilen können, AWS RAM sind regional. Sie erstellen sie in einer bestimmten RegionAWS-Region, und dann existieren sie in dieser Region. Um diese Ressourcen zu sehen 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 erstellenAWS Management Console, wählen Sie die Instance aus, in der Sie AWS-Region die Instance erstellen möchten. Wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, um die Instanz zu erstellen, schließen Sie den `--region` Parameter ein. Die AWS SDKs verfügen jeweils über ihren eigenen äquivalenten Mechanismus zur Angabe der Region, die für die Operation verwendet wird.

Es gibt mehrere Gründe für die Verwendung regionaler Ressourcen. Ein guter Grund besteht darin, sicherzustellen, dass sich die Ressourcen und die Serviceendpunkte, die Sie für den Zugriff darauf verwenden, 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 eine andere Option angeben, können Sie die Ressourcen, die Sie in der vorherigen Region sehen konnten, nicht mehr sehen oder mit ihnen interagieren.

Wenn Sie sich den Amazon-Ressourcennamen (ARN) für eine regionale Ressource ansehen, 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, die dem folgenden Beispiel für eine VPC in der `us-east-1` Region ähneln.

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

Globale Ressourcen

Einige AWS Dienste unterstützen Ressourcen, auf die Sie global zugreifen können, sodass 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 keinen `--region` Parameter an, wenn Sie die Service AWS CLI - und AWS SDK-Operationen verwenden.

Globale Ressourcen unterstützen Fälle, in denen es wichtig 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. Der Zugriff auf einen einzigen globalen Endpunkt mit einer möglichen Erhöhung der Latenz wird als akzeptabel angesehen, um sicherzustellen, dass alle Änderungen für die Verbraucher 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, wie der folgende Beispiel-ARN für ein Cloud-WAN-Kernnetzwerk.

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

Ressourcenanteile und ihre Regionen

AWS RAMist ein regionaler Dienst, und ein Ressourcenanteil ist regional. Daher kann eine Ressourcenfreigabe Ressourcen aus derselben Ressourcenfreigabe 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 Ressourcenanteile mit globalen Ressourcen nur in der ausgewiesenen Heimatregion USA Ost (Nord-Virginia) erstellen`us-east-1`. Sie können die Ressourcenfreigabe zwar nur in dieser einzigen 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 des Dienstes angezeigt wird. Die Beschränkung auf die Heimatregion gilt nur für den Ressourcenanteil, 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 sie verwendet wird, `us-west-2` und die Ressourcenfreigabe dort erstellen. Sie können keine Ressourcenfreigabe erstellen, die regionale Ressourcen aus verschiedenen Ländern umfasstAWS-Regionen. Das bedeutet, dass Sie zwei verschiedene Ressourcenanteile erstellen müssen`eu-north-1`, um Ressourcen von beiden `us-west-2` gemeinsam nutzen zu können. Du kannst Ressourcen aus zwei verschiedenen Regionen nicht zu einem einzigen Ressourcenanteil kombinieren.

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

Obwohl die globale Ressource in einer AWS RAM Ressourcen-Freigabe nur in der angegebenen Heimatregion sichtbar ist, ist sie nach dem Teilen immer noch eine globale Ressource. Sie können im Shared AWS-Konten von jeder Region aus darauf zugreifen, von der aus Sie im Original darauf zugreifen konntenAWS-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 einbeziehen möchten, müssen Sie die angegebene Heimatregion verwenden, um die Aktie 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 Operationen AWS RAM AWS CLI und SDK nur mit Ressourcenfreigaben interagieren, die sich in der Region befinden, die Sie in Ihrem Vorgang angeben. Um Ressourcenanteile anzuzeigen oder zu ändern, die globale Ressourcen enthalten, 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, die die regionale Ressource enthält.
- 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), verwenden`us-east-1`.

- Sie können eine Ressourcenfreigabe sowohl mit regionalen als auch mit globalen Ressourcen nur in der angegebenen Heimatregion, USA Ost (Nord-Virginia), erstellen`us-east-1`.

Teilen SieAWS Ressourcen, die Ihnen gehören

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

Themen

Ressourcenanteile anzeigen, die Sie in erstellt habenAWS RAM

Sie können eine Liste der Ressourcenfreigaben anzeigen, die Sie erstellt haben. Sie können sehen, welche Ressourcen Sie teilen und mit welchen Schulleitern sie geteilt werden.

Console

Um deine Ressourcenanteile einzusehen

1. Öffnen Sie in derAWS RAM Konsole die Seite Von mir geteilt: Resource Shares.
2. Da es bestimmteAWS RAM Ressourcenfreigaben gibtAWS-Regionen, wählen Sie in der oberen rechten Ecke der Konsole die entsprechendeAWS-Region aus der Drop-down-Liste aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) einstellen. Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wenn für eine der verwalteten Berechtigungen, die von den Ressourcenanteilen in den Ergebnissen verwendet werden, eine neue Version der verwalteten Berechtigung gilt, die als

Standard festgelegt ist, wird auf der Seite ein Banner angezeigt, um Sie darauf aufmerksam zu machen. Sie können wählen, ob Sie alle Versionen verwalteter Berechtigungen gleichzeitig aktualisieren möchten, indem Sie oben auf der Seite die Option Alle überprüfen und aktualisieren wählen.

Alternativ wird für einzelne Ressourcenfreigaben mit einer oder mehreren neuen Versionen verwalteter Berechtigungen in der Spalte Status die Meldung Update verfügbar angezeigt. Wenn Sie diesen Link auswählen, werden die aktualisierten Versionen der verwalteten Berechtigungen überprüft und Sie können sie als Versionen für die relevanten Ressourcentypen in dieser einen Ressourcenfreigabe zuweisen.

4. (Optional) Wenden Sie einen Filter an, um bestimmte Ressourcenanteile zu finden. Sie können mehrere Filter anwenden, um die Suche zu verfeinern. Sie können ein Schlüsselwort eingeben, z. B. einen Teil des Namens einer Ressourcenfreigabe, um nur die Ressourcenanteile aufzulisten, die diesen Text im Namen enthalten. Wählen Sie das Textfeld aus, um eine Dropdown-Liste mit vorgeschlagenen Attributfeldern zu sehen. Nachdem Sie einen Wert ausgewählt haben, können Sie aus der Liste der verfügbaren Werte für dieses Feld wählen. Sie können weitere Attribute oder Schlüsselwörter hinzufügen, bis Sie die gewünschte Ressource gefunden haben.
5. Wählen Sie den Namen der Ressourcenfreigabe aus, die Sie überprüfen möchten. In der Konsole werden die folgenden Informationen über die gemeinsame Nutzung der Ressourcen angezeigt:

   - Zusammenfassung — Listet den Namen, die ID, den Eigentümer, den Amazon-Ressourcennamen (ARN), das Erstellungsdatum, ob die gemeinsame Nutzung mit externen Konten zulässig ist, und den aktuellen Status auf.
   - Verwaltete Berechtigungen — Listet die verwalteten Berechtigungen auf, die mit dieser Ressourcenfreigabe verknüpft sind. In der Ressourcenfreigabe kann maximal eine verwaltete Berechtigung pro Ressourcentyp enthalten sein. Jede verwaltete Berechtigung zeigt die Version dieser verwalteten Berechtigung an, die der Ressourcennutzung zugeordnet ist. Wenn es sich nicht um die Standardversion handelt, zeigt die Konsole einen Link zur Standardversion aktualisieren an. Wenn Sie diesen Link wählen, haben Sie die Möglichkeit, den Resource Share zu aktualisieren, um die Standardversion zu verwenden.
   - 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.

- Gemeinsame Prinzipale — Listet die Prinzipale auf, mit denen die Ressourcen gemeinsam genutzt werden.
- Schlagworte — Listet die Tag-Schlüssel-Wert-Paare auf, die der Ressourcenfreigabe selbst zugeordnet sind. Dies sind nicht die Tags, die den einzelnen Ressourcen zugeordnet sind, die in der Ressourcenfreigabe enthalten sind.

AWS CLI

Um deine Ressourcenanteile einzusehen

Sie können den get-resource-sharesBefehl mit dem auf`--resource-owner` gesetzten Parameter verwenden`SELF`, um Details der in Ihrem erstellten Ressourcenanteil anzuzeigenAWS-Konto.

Das folgende Beispiel zeigt die Ressourcenanteile, die in currentAWS-Region (`us-east-1`) für den Aufruf gemeinsam genutzt werdenAWS-Konto. Verwenden Sie den`--region` *<region-code>* Parameter, um die in einer anderen Region erstellten Ressourcenanteile abzurufen. Zum Einbeziehen von Ressourcenfreigaben, 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.
   - AWSverwaltete Berechtigungen werden von erstelltAWS, 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 sie besitzen. Sie können eine Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- AWS RAMist ein regionaler Dienst. Wenn Sie eine Ressource mit Prinzipalen in anderen teilenAWS-Konten, müssen diese Prinzipale auf jede Ressource von derselben Seite aus zugreifenAWS-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 Politik.
>
> 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 ARNs der einzelnen Ressourcen im Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

- Sie können nur die Organisation, der Ihr Konto angehört, und Organisationseinheiten dieser Organisation zu Ihren Ressourcenfreigaben hinzufügen. Sie können einer Ressourcenfreigabe keine Organisationseinheiten 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 — Weiterleitungsregeln
- 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 gibtAWS-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 habenAWS 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 IhreAWS 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 Eine vom Kunden verwaltete Berechtigung erstellen. 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 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 Politik.
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 ARNs der einzelnen Ressourcen im 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-), können Prinzipale AWS-Konten in allen Organisationseinheiten dieser Organisationseinheit und ihren untergeordneten Organisationseinheiten auf die Ressourcenfreigabe zugreifen.
- Wenn Sie eine Einzelperson auswählenAWS-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. Die verfügbaren Prinzipaltypen sowie ID- ARN ARN-Formate lauten wie folgt:

- AWS-Konto— Um eine hinzuzufügenAWS-Konto, geben Sie die 12-stellige Konto-ID ein. Beispiele:

  `123456789012`

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

  `o-abcd1234`

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

  `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`

  Beispiele:

  `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`

  Beispiele:

  `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-userAWS CLIBefehl 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

    Beispiele:

    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 SieAWS 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 Eine vom Kunden verwaltete Berechtigung erstellen.

```
$ 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 einen Ressourcenanteil inAWS RAM

Sie können eine RessourcenfreigabeAWS RAM jederzeit auf folgende Weise aktualisieren:

- Sie können einer von Ihnen erstellten Ressourcenfreigabe Principale, Ressourcen oder Tags hinzufügen.
- Für Ressourcentypen, die mehr als die standardmäßigeAWS verwaltete Berechtigung unterstützen, können Sie wählen, welche verwaltete Berechtigung für Ressourcen jedes Typs gilt.
- Wenn eine verwaltete Berechtigung, die an die Ressourcennutzung angehängt ist, eine neue Standardversion hat, können Sie die verwaltete Berechtigung aktualisieren, um die neue Version zu verwenden.
- Sie können den Zugriff auf gemeinsam genutzte Ressourcen widerrufen, indem Sie Prinzipale oder Ressourcen aus einer Ressourcenfreigabe entfernen. Wenn Sie den Zugriff widerrufen, haben die Prinzipale keinen Zugriff mehr auf die gemeinsam genutzten Ressourcen.

> **Note**
>
> Prinzipale, mit denen Sie Ressourcen teilen, können Ihren Ressourcenanteil verlassen, wenn der Share leer ist oder nur Ressourcentypen enthält, die das Verlassen einer Ressourcenbeteiligung unterstützen. Wenn die Ressourcenfreigabe Ressourcentypen enthält, die das Verlassen der Ressource nicht unterstützen, erscheint eine Meldung, in der die Schulleiter darüber informiert werden, dass sie den Eigentümer der Ressource kontaktieren müssen. In diesem Fall müssen Sie als Eigentümer des Resource Share die Principale aus Ihrem Resource Share entfernen. Eine Liste der Ressourcentypen, die diese Aktion nicht unterstützen, finden Sie unterVoraussetzungen für das Verlassen einer Ressourcenfreigabe.

Console

Um einer Ressourcenfreigabe

1. Navigiere in derAWS RAM Konsole zur Seite Von mir geteilt: Resource Shares.
2. DaAWS RAM Ressourcenfreigabe in der rechten oberen Ecke der Konsole verfügbar istAWS-Regionen, wählen Sie die entsprechendeAWS-Region aus der Drop-down-Liste in der rechten oberen Ecke der Konsole. Um Ressourcenfreigabe zu sehen, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia) setzen, (`us-east-1`). Weitere Informationen

zur freigabe globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.

3. Wählen Sie den Ressourcenanteil aus und klicken Sie dann auf Ändern.
4. Schritt 1: Geben Sie die Details zur Ressourcennutzung an, überprüfen Sie die Details zur Ressourcennutzung und aktualisieren Sie bei Bedarf eines der folgenden Elemente:

   a. (Optional) Sie ändern den Namen der Ressourcenfreigabe.

   b. (Optional) Um eine Ressource zur Ressourcenfreigabe 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 die Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzenAWS Management Console.

   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) Sie fügen einem Ressourcenfreigabe ein Tag hinzu, indem Sie Neuen Tag-Schlüssel und -Wert eingeben. Um mehr als ein Tag-Schlüssel- und Wertepaar hinzuzufügen, wählen Sie Neues Tag hinzufügen. Sie können bis zu 50 Tags hinzufügen.

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

5. Wählen Sie Next (Weiter).
6. (Optional) In Schritt 2: Ordnen Sie jedem Ressourcentyp eine verwaltete Berechtigung zu, können Sie wählen, ob SieAWS dem Ressourcentyp eine verwaltete Berechtigung zuordnen möchten, eine vorhandene 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“ wählen, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls zum Teilen entspricht. Weitere Informationen finden Sie unter Eine vom Kunden verwaltete Berechtigung erstellen. Nachdem Sie den Vorgang abgeschlossen haben 
   wählen Sie, und dann können Sie Ihre neue verwaltete Kundenberechtigung aus der Dropdown-Liste Verwaltete Berechtigungen auswählen.

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

7. Wenn die Version der verwalteten Berechtigung, die derzeit der Ressourcennutzung zugewiesen ist, nicht die aktuelle Standardversion ist, können Sie auf die Standardversion aktualisieren, indem Sie Auf Standardversion aktualisieren klicken.

> **Note**
>
> Bis Sie Ihre Änderungen am Resource Share nach dem letzten Schritt speichern, können Sie das Versionsupdate abbrechen, indem Sie Zurück zur vorherigen Version wählen. BeiAWS verwalteten Berechtigungen ist die Änderung jedoch nach dem Speichern der Ressourcenfreigabe endgültig und Sie können nicht mehr zur vorherigen Version zurückkehren.

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

   a. (Optional) Um zu ändern, wählen Sie eine der folgenden Optionen, indem Sie eine der folgenden Optionen auswählen:

      - Um Ressourcen mitAWS-Konten oder einzelnen IAM-Rollen oder Benutzern außerhalb Ihrer Organisation zu teilen, wählen Sie Freigabe für externe Prinzipale zulassen aus.
      - Um die gemeinsame Nutzung von Ressourcen nur auf Hauptpersonen in Ihrer Organisation zu beschränkenAWS Organizations, wählen Sie Nur gemeinsame Nutzung für Hauptpersonen in Ihrer Organisation zulassen aus.

   b. Gehen Sie für Principals wie folgt vor:

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

Important

Wenn Sie eine gemeinsame Nutzung mit einer Organisation oder Organisationseinheit durchführen und dieser Geltungsbereich das Konto umfasst, das die Ressourcenfreigabe besitzt, erhalten alle Hauptpersonen im gemeinsamen Konto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die dem Share zugeordnet sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie,AWS RAM die an jede Ressource in der Aktie gebunden ist, verwendet`"Principal": "*"`. Weitere Informationen finden Sie unter Auswirkungen der Verwendung"Principal": "*"in einer ressourcenbasierten Politik.

Die Principals der anderen Verbraucherkonten erhalten nicht sofort Zugriff auf die Ressourcen der Aktie. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Prinzipale anhängen. Diese Richtlinien müssen den`Allow` Zugriff auf die ARNs einzelner Ressourcen im Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung, die der Ressourcennutzung zugeordnet ist, angegebenen Berechtigungen nicht überschreiten.

Note

Der Schalter „Organisationsstruktur anzeigen“ wird nur angezeigt, wenn das Teilen mit aktiviertAWS Organizations ist und Sie als Principal im Verwaltungskonto der Organisation angemeldet sind.

Sie können diese Methode nicht verwenden, um eine Rolle oder einen BenutzerAWS-Konto außerhalb Ihrer Organisation oder einer IAM-Rolle oder eines Benutzers anzugeben. Stattdessen müssen Sie diese Hauptpersonen hinzufügen, indem Sie ihre Identifikatoren eingeben. Diese werden im Textfeld unter dem Schalter Organisationsstruktur anzeigen angezeigt. Siehe den nächsten Aufzählungspunkt.

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

  Wenn Sie eine Person auswählenAWS-Konto, kann nur dieses Konto auf die Ressourcenfreigabe zugreifen. Sie können eine der folgenden Optionen auswählen.

  - Ein andererAWS-Konto (außer dem Ressourcenbesitzer) — 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 die in den verwalteten Berechtigungen, die der Ressourcennutzung zugeordnet sind, definierten Berechtigungen nicht überschreiten.
  - DiesAWS-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, Organisationseinheiten oder Ihre Organisation hinzufügen, 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 Auswahl aufheben.

10. Wählen Sie Next (Weiter).
11. Überprüfen Sie in Schritt 4: Überprüfen und Aktualisieren die Konfigurationsdetails für Ihren Resource Share.
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 Add (Ressourcenfreigabe), wenn Sie mit den Änderungen fertig sind.

AWS CLI

Um einer Ressourcenfreigabe

Sie können die folgendenAWS CLI -Befehle verwenden, um eine Ressourcenfreigabe zu ändern:

- Verwenden Sie den Befehl, um eine Ressourcenfreigabe umzubenennen oder zu ändern, ob externe Prinzipale zulässig sind update-resource-share. Das folgende Beispiel benennt die angegebene Ressourcenfreigabe um und legt sie so fest, dass nur Hauptpersonen aus ihrer Organisation zugelassen sind. Sie müssen den Dienstendpunkt für den verwendenAWS-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 Resource Share eine Ressource hinzuzufügen associate-resource-share. Im folgenden Beispiel wird der angegebenen Ressourcenfreigabe ein Subnetz hinzugefügt.

```
$ 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 und, um eine verwaltete Berechtigung für einen Ressourcentyp in einer Ressourcenfreigabe hinzuzufügen oder [list-permissions](#)zu ersetzen [associate-resource-share-permission](#). In einer Ressourcenfreigabe können Sie pro Ressourcentyp nur eine verwaltete Berechtigung zuweisen. Wenn Sie versuchen, einem Ressourcentyp, der bereits über eine verwaltete Berechtigung verfügt, eine verwaltete Berechtigung hinzuzufügen, müssen Sie die`--replace` Option einschließen, andernfalls schlägt der Befehl mit einer Fehlermeldung fehl.

  Der folgende Beispielbefehl listet die ARNs für die verwalteten Berechtigungen auf, die für ein Amazon Elastic Compute Cloud (Amazon EC2) -Subnetz verfügbar sind, und verwendet dann einen dieser ARNs, um die aktuell zugewieseneAWS 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, um eine Ressource aus einer Resource Share zu entfernen disassociate-resource-share. Das folgende Beispiel entfernt das Amazon EC2-Subnetz mit dem angegebenen ARN aus der angegebenen Ressourcenfreigabe.

```
$ 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 hinzu`project=lima`, indem Sie die Ressourcenfreigabe verwenden.

```
$ 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.

Anzeige Ihrer geteilten Ressourcen inAWS RAM

Sie können die Liste der einzelnen Ressourcen, die Sie freigegeben haben, innerhalb aller Ressourcenfreigaben anzeigen. Anhand der Liste können Sie ermitteln, welche Ressourcen Sie gerade gemeinsam nutzen, in wie vielen Ressourcenfreigaben sie enthalten sind und wie viele Prinzipale Zugriff auf sie haben.

Console

Um die Ressourcen anzuzeigen, die Sie gerade teilen

1. Öffnen Sie in derAWS RAM Konsole die Seite Von mir geteilt: Geteilte Ressourcen.
2. Da es bestimmteAWS RAM Ressourcenfreigaben gibtAWS-Regionen, wählen Sie in der oberen rechten Ecke der Konsole die entsprechendeAWS-Region aus der Drop-down-Liste aus. Wenn Sie Ressourcenfreigaben anzeigen möchten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) einstellen. Weitere Informationen zum Freigeben von globalen 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 ihrer nativen Servicekonsole anzuzeigen.
   - Ressourcentyp — Der Ressourcentyp.
   - Datum der letzten Freigabe — Das Datum, an dem die Ressource zuletzt geteilt wurde.
   - Ressourcenanteile — Die Anzahl der Ressourcenanteile, die die Ressource enthalten. Um die Liste der Ressourcenanteile zu sehen, wählen Sie die Nummer aus.

- Principals — Die Anzahl der Principale, die auf die Ressource zugreifen können. Wählen Sie den Wert, um die Prinzipale anzuzeigen.

AWS CLI

Um die Ressourcen anzuzeigen, die Sie gerade teilen

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

Das folgende Beispiel zeigt die Ressourcen, die in den Ressourcenanteilen in derAWS-Region (`us-east-1`) für den Aufruf enthalten sindAWS-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"
        }
    ]
}
```

Anzeige der Auftraggeber, mit denen Sie Ressourcen teilen, inAWS RAM

Sie können die Prinzipale, für die Sie Ihre Ressourcen freigeben, innerhalb aller Ressourcenfreigaben anzeigen. Diese Liste der Prinzipale hilft Ihnen dabei, zu bestimmen, wer Zugriff auf Ihre freigegebenen Ressourcen hat.

Console

Um die Prinzipale zu sehen, mit denen Sie Ressourcen teilen

1. Navigiere in derAWS RAM Konsole zur Seite Von mir geteilt: Principals.
2. DaAWS RAM Ressourcenfreigaben in der rechten oberen Ecke der Konsole auswählen Sie die entsprechendeAWS-Region aus der Drop-down-Liste in der rechten oberen Ecke der Konsole auswählen.AWS-Regionen Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzen. Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wenden Sie einen Filter an, um bestimmte Prinzipien zu finden. Sie können mehrere Filter anwenden, um die Suche zu verfeinern. Wählen Sie das Textfeld aus, um eine Dropdown-Liste mit vorgeschlagenen Attributfeldern zu sehen. Nachdem Sie einen Wert ausgewählt haben, können Sie aus der Liste der verfügbaren Werte für dieses Feld wählen. Sie können weitere Attribute oder Schlüsselwörter hinzufügen, bis Sie die gewünschte Ressource gefunden haben.
4. Für jeden Principal in der Liste zeigt die Konsole die folgenden Informationen an:

   - Principal ID — Die ID des Principals. Wählen Sie die ID, um einen neuen Browser-Tab zu öffnen und den Principal in seiner nativen Konsole anzuzeigen.
   - Ressourcenanteile — Die Anzahl der Ressourcenanteile, die Sie mit dem angegebenen Principal geteilt haben. Wählen Sie die Nummer aus, um die Liste der Ressourcenfreigaben anzuzeigen.
   - Ressourcen — Die Anzahl der Ressourcen, die Sie mit dem Schulleiter geteilt haben. Wählen Sie die Nummer aus, um die Liste der freigegebenen Ressourcen anzuzeigen.

AWS CLI

Um die Prinzipale zu sehen, mit denen Sie Ressourcen teilen

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

Im folgenden Beispiel sind die Principale aufgeführt, die Zugriff auf Shares haben, die in der Standardregion für das aufrufende Konto erstellt wurden. In diesem Beispiel sind die Hauptpersonen die Organisation des aufrufenden Kontos und eine separate OrganisationAWS-Konto, die Teil von zwei verschiedenen Ressourcenanteilen ist. Sie müssen den Dienstendpunkt für den verwendenAWS-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 Ressourcenbeteiligung inAWS RAM

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

> **Um eineAWS Ressource zu löschen**
>
> Wenn Sie eineAWS Ressource löschen müssen, die Sie in eine Ressourcenfreigabe aufgenommen haben,AWS empfiehlt, zunächst sicherzustellen, dass Sie die Ressource entweder aus jeder Ressourcenfreigabe entfernen, die sie enthält, oder die Ressourcenfreigabe löschen.

Die gelöschte Ressourcenfreigabe bleibt nach dem Löschen für einen kurzen Zeitraum in derAWS RAM Konsole sichtbar, ihr Status ändert sich jedoch zu`Deleted`.

Console

Einen Ressourcenfreigabe

1. Öffnen Sie in derAWS RAM Konsole die Seite Von mir geteilt: Resource Shares.
2. DaAWS RAM Ressourcenfreigabe in der Konsole in der rechten oberen Ecke der Konsole die entsprechendeAWS-Region aus der Drop-down-Liste in der oberen rechten Ecke der Konsole auswählen.AWS-Regionen Zum Anzeigen von Ressourcenfreigabe, die globale Ressourcen enthalten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzen. Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. Wählen Sie den Ressourcenfreigabe aus, den Sie löschen möchten.

   > **Warning**
   >
   > Stellen Sie sicher, dass Sie den richtigen Ressourcenfreigabe auswählen. Eine Ressourcenfreigabe kann nicht mehr wiederhergestellt werden.

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

AWS CLI

Einen 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 zum Abrufen des Amazon-Ressourcennamen (ARN) des Ressourcenfreigabe, den Sie löschen möchten. Dann wird es verwendet delete-resource-share, um den angegebenen Ressourcenanteil zu löschen.

```
$  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
}
```

Zugriff auf für Sie freigegebene AWS Ressourcen

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

Inhalt

Annehmen und Ablehnen von Einladungen zur gemeinsamen Nutzung von Ressourcen

Um auf freigegebene Ressourcen zuzugreifen, muss der Eigentümer der Ressourcenfreigabe Sie als Prinzipal hinzufügen. Der Eigentümer kann der Ressourcenfreigabe eine der folgenden Optionen als Prinzipal 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 Ihren spezifischen IAM-Benutzer

Wenn Sie der Ressourcenfreigabe über ein hinzugefügt werden AWS-Konto , das Mitglied einer Organisation in ist AWS Organizations, und die Freigabe innerhalb der Organisation aktiviert ist, erhalten Sie automatisch Zugriff auf die freigegebenen Ressourcen, ohne eine Einladung annehmen zu müssen. Service-Prinzipale erhalten auch automatischen Zugriff auf gemeinsam genutzte Ressourcen, ohne eine Einladung anzunehmen. Wenn das Konto, über das Sie Zugriff erhalten, später aus der Organisation entfernt wird, verlieren alle Prinzipale in diesem Konto automatisch den Zugriff auf die Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.

Wenn Sie einer Ressourcenfreigabe von einer der folgenden Optionen hinzugefügt werden, erhalten Sie eine Einladung zur Teilnahme an der Ressourcenfreigabe:

- Ein Konto außerhalb Ihrer Organisation in AWS Organizations
- Ein Konto in Ihrer Organisation, wenn die Freigabe für nicht aktiviert AWS Organizations ist

Wenn Sie eine Einladung erhalten, einer Ressourcenfreigabe beizutreten, müssen Sie sie akzeptieren, um auf ihre freigegebenen Ressourcen zuzugreifen. Wenn Sie die Einladung ablehnen, können Sie nicht auf die freigegebenen Ressourcen zugreifen.

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

> **Important**
>
> Für freigegebene Ressourcentypen, die nicht auf der folgenden Liste aufgeführt sind, haben Sie 12 Stunden Zeit, um die Einladung zur Teilnahme an der Ressourcenfreigabe anzunehmen. Nach 12 Stunden läuft die Einladung ab und der Endbenutzer-Prinzipal in der Ressourcenfreigabe wird getrennt. 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 – Lokale Gateway-Routing-Tabellen, Outposts und Standorte
- Amazon Route 53 – Weiterleitungsregeln
- Amazon VPC – Kundeneigene IPv4-Adressen, Präfixlisten, Subnetze, Traffic Mirror-Ziele, Transit-Gateways, Transit-Gateway-Multicast-Domänen

Console

So antworten Sie auf eine Einladung zu einer Ressourcenfreigabe

1. Navigieren Sie zur Seite Mit mir geteilt: Ressourcenfreigaben in der - AWS RAM Konsole.
2. Da AWS RAM Ressourcenfreigaben in bestimmten vorhanden sind AWS-Regionen, wählen Sie die entsprechende AWS-Region aus der Dropdown-Liste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie AWS-Region auf USA Ost (Nord-Virginia), () festlegen`us-east-1`. Weitere Informationen zum Teilen globaler Ressourcen finden Sie unter Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.

3. Überprüfen Sie die Liste der Ressourcenfreigaben, denen Sie hinzugefügt wurden.

   Die Spalte Status gibt Ihren aktuellen Teilnahmestatus für die Ressourcenfreigabe an. Der `Pending` Status gibt an, dass Sie zu einer Ressourcenfreigabe hinzugefügt wurden, die Einladung aber noch nicht angenommen oder abgelehnt haben.
4. Um auf die Einladung zur gemeinsamen Nutzung von Ressourcen zu antworten, wählen Sie die ID der Ressourcenfreigabe aus und wählen Sie Ressourcenfreigabe akzeptieren aus, um die Einladung anzunehmen, oder Ressourcenfreigabe 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

So antworten Sie auf eine Einladung zu einer Ressourcenfreigabe

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. Das folgende Beispiel beginnt mit dem -get-resource-share-invitationsBefehl, um eine Liste aller Einladungen abzurufen, die dem des Benutzers zur Verfügung stehen AWS-Konto. Mit dem AWS CLI `query` Parameter können Sie die Ausgabe auf die Einladungen beschränken, deren Einstellung auf `status` festgelegt ist`PENDING`. Dieses Beispiel zeigt, dass eine Einladung vom Konto `111111111111` derzeit `PENDING` für das aktuelle Konto `123456789012` in der angegebenen gilt 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, die Sie im nächsten Befehl verwenden möchten, um die Einladung 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"
    }
}
```

   Beachten Sie bei Erfolg, dass sich die Antwort von `PENDING` in geändert `status` hat`ACCEPTED`.

Wenn Sie stattdessen die Einladung ablehnen möchten, führen Sie den reject-resource-share-invitation Befehl mit den gleichen 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 Ressourcenanteile anzeigen

Sie können die Ressourcenanteile anzeigen, auf die Sie Zugriff haben. Sie können sehen, welche Schulleiter Ressourcen mit Ihnen teilen und welche Ressourcen sie teilen.

Console

Um die Ressourcenanteile einzusehen

1. Navigiere in derAWS RAM Konsole zur Seite Mit mir geteilt: Resource Shares.
2. DaAWS RAM es in der oberen rechten Ecke der Konsole die entsprechendeAWS-Region aus der rechten oberen Ecke der Konsole auswählen.AWS-Regionen Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzen. Weitere Informationen zur gemeinsamen Nutzung von globalen Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen.
3. (Optional) Wenden Sie einen Filter an, um bestimmte Ressourcenanteile zu finden. Sie können mehrere Filter anwenden, um die Suche zu verfeinern. Sie können ein Schlüsselwort eingeben, z. B. einen Teil des Namens einer Ressourcenfreigabe, um nur die Ressourcenanteile aufzulisten, die diesen Text im Namen enthalten. Wählen Sie das Textfeld aus, um eine Dropdown-Liste mit vorgeschlagenen Attributfeldern zu sehen. Nachdem Sie einen Wert ausgewählt haben, können Sie aus der Liste der verfügbaren Werte für dieses

Feld wählen. Sie können weitere Attribute oder Schlüsselwörter hinzufügen, bis Sie die gewünschte Ressource gefunden haben.

4. DieAWS RAM Konsole zeigt die folgenden Informationen an:

   - Name — Der Name der Ressourcenfreigabe.
   - ID — Die ID der gemeinsam genutzten Ressource. Wählen Sie die ID aus, um die Detailseite der Ressourcenfreigabe aufzurufen.
   - Besitzer — Die ID des BenutzersAWS-Konto, der den Resource Share erstellt hat.
   - Status – Der aktuelle Status der Ressourcenfreigabe. Mögliche Werte sind:
     - `Active`— Die Ressourcenfreigabe ist aktiv und kann verwendet werden.
     - `Deleted`— Die Ressourcenfreigabe wird gelöscht und steht nicht mehr zur Verfügung.
     - `Pending`— Eine Einladung zur Annahme der Ressourcenfreigabe wartet auf eine Antwort.

AWS CLI

Um die Ressourcenanteile einzusehen

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

Das folgende Beispiel zeigt die Liste der Ressourcenanteile, die im angegebenen KontoAWS-Region mit dem aufrufenden Konto von anderen geteilt wurdenAWS-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 Principals die Ressourcen mit Ihnen geteilt haben und welche Ressourcenanteile die Ressourcen beinhalten.

Console

Um Ressourcen anzusehen, die mit Ihnen geteilt wurden

1. Navigiere in derAWS RAM Konsole zur Seite Mit mir geteilt: Geteilte Ressourcen.
2. DaAWS RAM es in der rechten oberen Ecke der Konsole die entsprechendeAWS-Region aus der oberen Ecke der Konsole auswählen.AWS-Regionen Ihre -Konto-Ressource finden Sie, indemAWS-Region Sie die auf () setzen.`us-east-1` Weitere Informationen zum Freigeben von globalen 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:

   - Resource 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.
- Ressourcenanteile — Die Anzahl der Ressourcenanteile, in denen die Ressource enthalten ist. Wählen Sie den Wert, um die Ressourcenanteile anzuzeigen.
- Besitzer-ID — Die ID des Principals, dem die Ressource gehört.

AWS CLI

Um Ressourcen anzusehen, die mit Ihnen geteilt wurden

Sie können den Befehl list-resources verwenden, um Ressourcen anzuzeigen, die für Sie freigegeben wurden.

Der folgende Beispielbefehl zeigt Details zu der Ressource an, auf die über eine Ressourcenfreigabe in der angegebenenAWS-Region von einer anderen Ressource zugegriffen werden kannAWS-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 dir geteilt wurden

Sie können eine Liste aller der Prinzipale anzeigen, die Ressourcen für Sie freigeben. Sie können sehen, welche Ressourcen und Ressourcenfreigaben sie für Sie freigeben.

Console

Um die Prinzipale anzuzeigen, die Ressourcen für Sie freigeben

1. Öffnen Sie die AWS RAM-Konsole unter https://console.aws.amazon.com/ram.
2. DaAWS RAM es in der oberen Ecke der Ecke der oberen Ecke der Ecke der Konsole die entsprechendeAWS-Region ausAWS-Regionen, wählen Sie die entsprechende aus der oberen Ecke der Ecke der Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzen. Weitere Informationen zum Teilen 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 bestimmte Prinzipale zu finden. Sie können mehrere Filter anwenden, um die Suche zu verfeinern.
5. Die Konsole zeigt die folgenden Informationen an:
   - Principal ID — Die ID des Principals, der die Daten mit Ihnen teilt.
   - Ressourcenanteile — Die Anzahl der Ressourcenanteile, zu denen der Principal Sie hinzugefügt hat. Wählen Sie die Nummer aus, 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 Prinzipale anzuzeigen, die Ressourcen für Sie freigeben

Sie können den Befehl list-principals verwenden, um die Liste der Prinzipale abzurufen, die Ressourcen mit Ihrem teilenAWS-Konto.

Der folgende Beispielbefehl zeigt Details zu dem anAWS-Konto, der eine Ressourcennutzung mit dem Konto geteilt hat, das zum Aufrufen des Vorgangs in der angegebenen Datei verwendet wurdeAWS-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 gibtAWS-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 dazuAWS-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 weiterleitenAWS-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"
        }
    ]
}
```

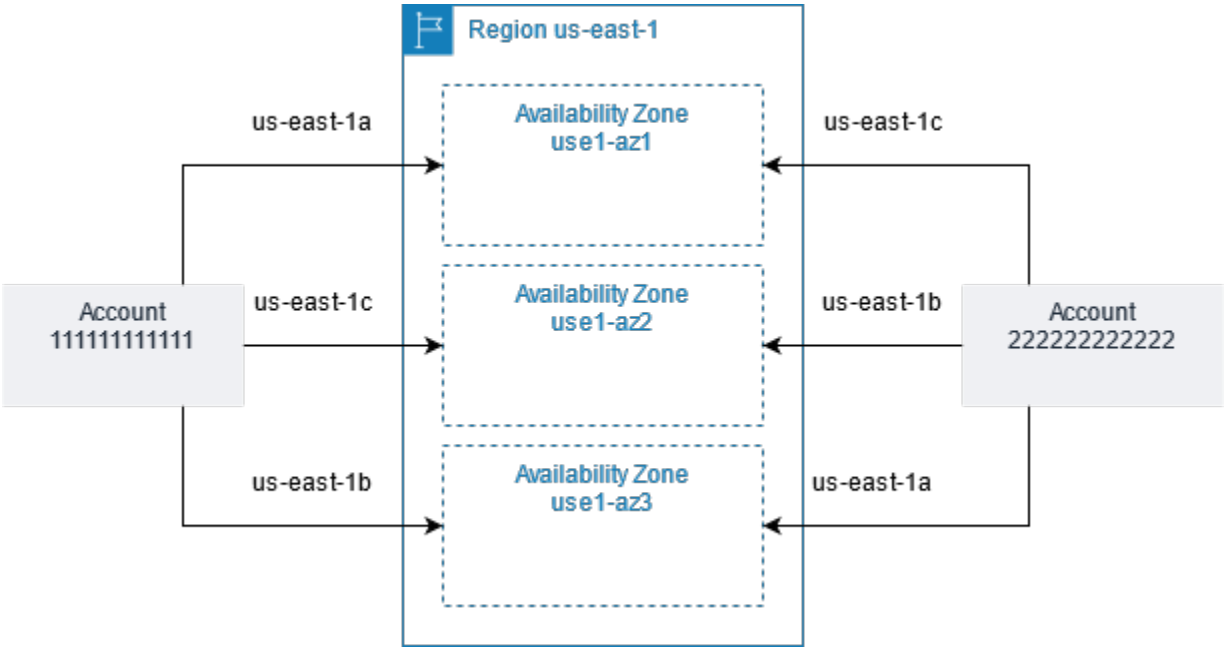
2. Anschließend können Sie den Befehl ausführen, um diese Ressourcenfreigabe zu verlassen. Beachten Sie, dass Sie auch Ihre Konto-ID als Principal angeben müssen`123456789012`, um die Verbindung zu der angegebenen Ressourcenfreigabe zu trennen, die von den Konten `111111111111` gemeinsam genutzt wird.

```
$ 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 IhreAWS Ressourcen

AWSordnet die physischen Availability Zones nach dem Zufallsprinzip den jeweiligen Availability Zonennamen zuAWS-Konto. Dieser Ansatz hilft, Ressourcen auf die Availability Zones in einer Region zu verteilenAWS-Region, anstatt dass Ressourcen wahrscheinlich in der Availability Zone „a“ für jede Region konzentriert werden. Daher entspricht die Availability Zone`us-east-1a` für IhrAWS Konto möglicherweise nicht demselben physischen Standort wie`us-east-1a` für ein anderesAWS Konto. Weitere Informationen finden Sie unter Regionen und Availability Zones im Amazon EC2 EC2-Benutzerhandbuch.

Die folgende Abbildung zeigt, dass die AZ-IDs für jedes Konto identisch sind, obwohl die Availability Zone-Namen für jedes Konto unterschiedlich zugeordnet werden können.



Für einige Ressourcen müssen Sie nicht nur die Availability ZoneAWS-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 SieAWS RAM eine solche Ressource jedoch mit anderen teilenAWS-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, können Sie mit diesen Ressourcen auch anhand der AZ-ID den tatsächlichen Standort Ihrer Ressourcen im Verhältnis zu Ihren Konten ermitteln. Eine AZ-ID ist eine eindeutige, konsistente Kennung für eine Availability Zone innerhalb aller Availability ZonesAWS-Konten. `use1-az1`Ist beispielsweise eine AZ-ID für eine Availability Zone in der`us-east-1` -Region und steht für den gleichen physischen Standort in jedemAWS Konto.

Sie können AZ-IDs verwenden, 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 der Amazon VPC-Konsole abgefragt werdenAWS CLI.

Console

So zeigen Sie die AZ-IDs für die Availability Zones in Ihrem Konto an

1. Navigieren Sie in der AWS RAMKonsole zurAWS RAM Konsolenseite.
2. Die aktuellen AZ-IDs können SieAWS-Region unter Ihrer AZ-ID einsehen.

AWS CLI

So zeigen Sie die AZ-IDs für die Availability Zones in Ihrem Konto an

Der folgende Beispielbefehl zeigt die AZ-IDs für die Availability Zones in der Region us-west-2 und wie sie für den Anruf zugeordnet werdenAWS-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) 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 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
Mesh `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
Graphische QL-API `appsync:APIs`	Verwalten Sie AWS AppSync GraphQL-APIs zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere Konten AWS AppSync APIs gemeinsam nutzen, um eine einheitliche AWS AppSync zusammengeführte API zu erstellen, die auf Daten aus mehreren Subschema-APIs über verschiedene Konten in derselben Region zugreifen kann. Weitere Informationen finden Sie unter Zusammengeführte APIs im AWS AppSync Entwicklerhandbuch.	 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
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 einen gemeinsam genutzten, zentral verwalteten DB-Cluster AWS-Konten klonen. Weitere Informationen finden Sie unter Kontoübergreifendes Klonen mit AWS RAM und Amazon Aurora im Amazon Aurora Aurora-Benutzerhandbuch.	N	Ja Kann mit jedem geteilt werden. AWS-Konto	N	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 (CA) `acm-pca:CertificateAuthority`	Erstellen und verwalten Sie private Zertifizierungsstellen (CAs) für die interne Public Key-Infrastruktur (PKI) Ihrer Organisation und teilen Sie diese Zertifizierungsstellen 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

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 Domäne `datazone:Domain`	Erstellen und verwalten Sie Domains zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Dadurch 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 teilen AWS-Konto.	 N	 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
Projekt `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
Berichtsgruppe `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.		

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. **Important** Wenn Sie nicht alle Voraussetzungen für die gemeinsam	 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
	e Nutzung einer Kapazitätsreservierung erfüllen, kann der Vorgang zur gemeinsamen 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				

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
	gemeinsame 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				

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 Beispiel: 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
Komponenten `imagebuilder:Component`	Erstellen und verwalten Sie Komponenten zentral und teilen Sie sie mit anderen Personen 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 `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.				
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 `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

Amazon FSx für OpenZFS

Sie können die folgenden Ressourcen von Amazon FSx für OpenZFS 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
FSx-Volumen `fsx:Volume`	Erstellen und verwalten Sie FSx for 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 unter gemeinsam genutzten Volumes über FSx-APIs `CreateVolume` oder durchführen. `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
Datenkataloge `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
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
Tabellen `glue:Table`	Erstellen und verwalten Sie Datenkatalogtabellen zentral und teilen Sie sie mit AWS-Konten oder 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 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.	 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
Marketplace-Katalogeinheit `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.	 Nein	 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

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
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 zur Netzwerküberwachung, zum Schutz und zur Filterung gemeinsam nutzen. Weitere Informationen finden Sie im AWS Network Firewall Entwicklerhandbuch unter Gemeinsame Nutzung von Firewallrichtlinien und Regelgruppen.	 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
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Sie können statusfreie und statusbehaftete Regelgruppen zentral erstellen und verwalten und sie mit anderen AWS-Konten oder Ihrer Organisation teilen. 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 Gemeinsame Nutzung von Firewallrichtlinien und Regelgruppen.	 Ja	 Ja
			
			Kann mit jedem geteilt werden AWS-Konto.
				 Nein	 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-Tabelle für das lokale Gateway `ec2:LocalGatewayRouteTable`	Erstellen und verwalten Sie VPC-Verknüpfungen zu einem lokalen Gateway zentral und teilen Sie sie mit anderen Personen AWS-Konten in Ihrer Organisation. Auf	 N	 N Kann nur mit der eigenen AWS-Konten	 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
	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		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
Standorte `outposts:Site`	Erstellen und verwalten Sie Outpost-Websites und teilen Sie sie mit anderen AWS-Konten in Ihrer 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 in Outposts

Sie können die folgende Amazon S3 on Outposts-Ressource 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 Ressourcen Explorer

Sie können die folgenden AWS Ressourcen 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 `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 Ressourcen Explorer Benutzerhandbuch unter Teilen von Resource Explorer-Ansichten.	 N	 N Kann nur innerhalb AWS-Konten der eigenen Organisation geteilt werden.	 N	 Nein

AWS Resource Groups

Sie können die folgenden AWS Resource Groups 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 DNS-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-Konten im Amazon Route 53-Entwicklerhandbuch.	 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
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 VPCs anwenden. 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 Virtual Private 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
Logs 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 Ursprung in ihren VPCs 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 Route 53 Application Recovery-Controller

Sie können die folgenden Amazon Route 53 Application Recovery Controller-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 ARC-Cluster `route53-recovery-control:Cluster`	Erstellen und verwalten Sie Route 53 53-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 Route 53 Application Recovery Controller Developer Guide.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 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
Zugangszuschüsse `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

Sie können die folgenden SageMaker 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
SageMaker Katalog `sagemaker:SagemakerCatalog`	Aus Gründen der Auffindbarkeit — ermöglicht es Kontoinhabern, anderen Konten für alle Featuregruppen-Ressourcen im Katalog Auffindbarkeitsberechtigungen zu gewähren. SageMaker Sobald der Zugriff gewährt wurde, können Benutzer dieser Konten die Feature-Gruppen, die für sie freigegeben wurden, im Katalog einsehen. Weitere Informationen finden Sie unter Auffindbarkeit und Zugriff auf kontoübergreifende Funktionsgruppen im Amazon SageMaker Developer Guide. **Note** Auffindbarkeit und Zugriff	N	Ja Kann mit jedem AWS-Konto teilen.	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
	sind separate Berechtigungen in. 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 Feature-Gruppe `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 Auffindbarkeit und Zugriff auf kontoübergreifende Funktionsgruppen im Amazon SageMaker Developer Guide. **Note** Auffindbarkeit und Zugriff sind separate	 Ja	 Ja Kann mit jedem AWS-Konto teilen.	 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
	Berechtigungen in. 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
Lineage-Gruppe `sagemaker:LineageGroup`	SageMaker Mit Amazon können Sie Abstammungsgruppen Ihrer Pipeline-Metadaten erstellen, um ein tieferes Verständnis der Geschichte und der 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 im Amazon SageMaker Developer Guide unter Accountübergreifendes Abstammungs-Tracking.	 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 Modellkarten `sagemaker:ModelCard`	Amazon SageMaker erstellt Model Cards, 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 maschinellen Lernvorgänge 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 Model Cards im	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 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 Developer Guide.				

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 Pipeline `sagemaker:Pipeline`	Mit Amazon SageMaker 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 maschinellen Lernvorgänge 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 Account-übergreifender Support für SageMaker Pipelines im Amazon SageMaker 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
Anwendung `servicecatalog:Application`	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
Attribut-Gruppe `servicecatalog:AttributeGroup`	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
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. 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
Reaktionspläne `ssm-incidents:ResponsePlan`	Erstellen und verwalten Sie Reaktionspläne zentral und teilen Sie sie mit anderen AWS-	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
	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.		Kann mit jedem geteilt werden AWS-Konto.		

AWS Systems Manager Parameter speichern

Sie können die folgenden AWS Systems Manager Parameter Store-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
Parameter `ssm:Parameter`	Erstellen Sie einen Parameter und verwenden Sie ihn, um Konfigurationsdaten zu speichern, auf die Sie in Ihren Skripten, Befehlen, SSM-Dokumenten sowie Konfiguration 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
Kundeneigene IPv4-Adressen `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
Pools von IP Address Manager (IPAM) `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 CIDRs aus dem Pool AWS Ressourcen wie VPCs in ihren jeweiligen Konten zuweisen. 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
Erkennung von Ressourcen im IP Address Manager (IPAM) `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 Ressourcenentdeckungen im Amazon VPC IPAM-Benutzerhandbuch.	 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
Subnetze `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
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 Benutzer den Datenverkehr 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 Gruppe `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 teilen 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
Amazon VPC Lattice-Dienst `vpc-lattice:Service`	Erstellen und verwalten Sie Amazon VPC Lattice-Services 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
Amazon VPC Lattice-Servicenetzwerk `vpc-lattice:ServiceNetwork`	Erstellen und verwalten Sie Amazon VPC Lattice-Servicenetzwerke zentral und teilen Sie sie mit Einzelpersonen AWS-	 N	 Ja Kann mit jedem geteilt	 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
	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.		werden. AWS-Konto		

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
Cloud-WAN-Kernnetzwerk `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

Verwaltung von Berechtigungen inAWS RAM

InAWS 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 Ressourcenfreigabe reagieren kann. Wenn Sie eine Ressourcenfreigabe erstellen, müssen Sie angeben, welche verwaltete Berechtigung für jeden Ressourcentyp verwendet werden soll, der in der Ressourcenfreigabe enthalten ist. Die Richtlinienvorlage in der verwalteten Berechtigung enthält alles, was für eine ressourcenbasierte Richtlinie benötigt wird, außer dem Principal und der Ressource. Der Amazon-Ressourcenname (ARN) der Ressourcenname (ARN) der Ressourcenname (ARN) der Ressourcenname (ARN) der Ressourcenname (ARN) der Ressourcenname (ARN) der Ressourcen. AWS RAMerstellt dann die ressourcenbasierte Richtlinie, die allen Ressourcen in diesem Ressourcenanteil zugewiesen wird.

Jede verwaltete Berechtigung kann über eine oder mehrere Versionen verfügen. Eine Version wird als Standardversion für diese verwaltete Berechtigung festgelegt. AWSAktualisiert gelegentlich eineAWS 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 an eine Ressourcenfreigabe angehängt sind, werden nicht automatisch aktualisiert. DieAWS 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 Ihnen, so bald wie möglich auf die neue Version derAWS verwalteten Berechtigung zu aktualisieren. Mit diesen Updates wird in der Regel Unterstützung für neue oder aktualisierte Ressourcen hinzugefügt, mitAWS-Services denen zusätzliche Ressourcentypen gemeinsam genutzt werden könnenAWS 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 zu sehen, verwenden Sie die Bibliothek für verwaltete Berechtigungen in derAWS RAM Konsole.

Console

Einzelheiten zu den verwalteten Berechtigungen finden Sie unterAWS RAM

1. Navigieren Sie in derAWS RAM Konsole zur Seite Bibliothek für verwaltete Berechtigungen.
2. Da es bestimmteAWS RAM Ressourcenfreigaben gibtAWS-Regionen, wählen Sie die entsprechendeAWS-Region aus der Dropdownliste oben rechts in der Konsole aus. Zum Anzeigen von Ressourcenanteilen, die globale Ressourcen enthalten, müssen Sie dieAWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) setzen. Weitere Informationen über das Teilen globaler Ressourcen finden Sie unterGemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen. Zwar haben alle Regionen dieselben verfügbarenAWS verwalteten Berechtigungen, dies wirkt sich jedoch auf die Anzahl der zugehörigen Ressourcenanteile 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. Über das Suchfeld können Sie die Liste der verwalteten

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

4. (Optional) Zum Ändern der Anzeigeeinstellungen wählen Sie das Zahnradsymbol rechts oben im Bereich Verwaltete Berechtigungen aus. Sie können die folgenden Einstellungen ändern:

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

   Wenn Sie mit dem Festlegen der Anzeigeeinstellungen fertig sind, wählen Sie Bestätigen.

5. Für jede verwaltete Berechtigung zeigt die Liste die folgenden Informationen an:

   - Name der verwalteten Berechtigung — Der Name der verwalteten Berechtigung.
   - Ressourcentyp — Der Ressourcentyp, der der verwalteten Berechtigung zugeordnet ist.
   - Verwalteter Berechtigungstyp — Ob es sich bei der verwalteten Berechtigung um eineAWS verwaltete Berechtigung oder um eine vom Kunden verwaltete Berechtigung handelt.
   - Verknüpfte Freigaben — Die Anzahl der Ressourcenfreigaben, die der verwalteten Berechtigung zugeordnet sind. Wenn eine Zahl angezeigt wird, können Sie die Zahl auswählen, um eine Tabelle der Ressourcenanteile 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 an diese Ressourcenfreigabe angehängt ist.
     - Besitzer — DieAWS-Konto Nummer des Resource Share-Besitzers.
     - Externe Auftraggeber zulassen — Ob diese Ressourcennutzung die gemeinsame Nutzung mit Prinzipalen außerhalb der Organisation ermöglichtAWS Organizations.
     - Status — Der aktuelle Status der Verknüpfung 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 anhängbar — 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. Es bleibt zwei Stunden lang sichtbar, bevor es aus der Bibliothek für verwaltete Berechtigungen verschwindet.

Sie können den Namen der verwalteten Berechtigung wählen, um weitere Informationen zu dieser verwalteten Berechtigung anzuzeigen. Die Detailseite für eine verwaltete Berechtigung zeigt die folgenden Informationen an:

- Ressourcentyp — DerAWS Ressourcentyp, für den diese verwaltete Berechtigung gilt.
- Anzahl der Versionen — Sie können bis zu fünf Versionen einer vom Kunden verwalteten Berechtigungen 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, wird eine Aufforderung angezeigt, die Ressourcenfreigabe auf die Standardversion zu aktualisieren.
- ARN — Der Amazon-Ressourcenname (ARN) der verwalteten Berechtigung. Die ARNs fürAWS verwaltete 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 auf den Tabs unter dieser Dropdown-Liste 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 gegebenenfalls der Bedingungen, die diese Version der verwalteten Berechtigung den Prinzipalen für den zugehörigen Ressourcentyp ermöglicht.
- Verknüpfte Ressourcenfreigaben — Die Liste der Ressourcenfreigaben, die diese Version der verwalteten Berechtigung verwenden.

AWS CLI

Einzelheiten zu den verwalteten Berechtigungen finden Sie unterAWS RAM

Sie können den list-permissionsBefehl verwenden, um eine Liste der verwalteten Berechtigungen abzurufen, die für Ressourcenfreigaben in der aktuellen VersionAWS-Region für das aufrufende Konto 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 außerdem an, dass wir nur das ARN-Feld in den Ergebnissen sehen möchten, und zwar im Klartextformat anstelle des Standard-JSON-Formats.

```
$ 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"
    }
}
```

Vom Kunden verwaltete Berechtigungen erstellen und verwenden inAWS RAM

AWS Resource Access Manager(AWS RAM) stellt mindestens eineAWS verwaltete Berechtigung für jeden Ressourcentyp bereit, den Sie teilen können. Diese verwalteten Berechtigungen bieten jedoch möglicherweise nicht die geringsten Zugriffsrechte für Ihren Anwendungsfall zum Teilen. Wenn eine

der bereitgestelltenAWS 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 könnenAWS 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 vom Kunden verwaltete Berechtigungen für Ihre Entwickler erstellen, um IP-Adressen zuzuweisen, aber nicht den IP-Adressbereich einsehen, den andere Entwicklerkonten zugewiesen haben. Sie können das bewährte Verfahren anwenden, d. h. es werden nur die Berechtigungen erteilt, die zum Durchführen von Aufgaben auf gemeinsam genutzten Ressourcen erforderlich sind.

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

Themen

Eine vom Kunden verwaltete Berechtigung erstellen

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

Console

So erstellen Sie eine vom verwalteten Richtlinie für Kunden verwalteten Richtlinie

1. Führen Sie eine der folgenden Aktionen aus:

   - Navigieren Sie zur Bibliothek für verwaltete Berechtigungen und wählen Sie Vom Kunden verwaltete Berechtigung erstellen aus.

- Rufen Sie in der Konsole direkt die Seite „Benutzerverwaltete Berechtigungen erstellen“ auf.

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 für diesen Ressourcentyp ausgeführt werden dürfen.

   - Sie können Verwaltete Berechtigung importieren wählen, um Aktionen aus einer vorhandenen verwalteten Berechtigung zu verwenden.
   - Aktivieren oder deaktivieren Sie Informationen zur Zugriffsebene, um Ihre Anforderungen im visuellen Editor zu erfüllen.
   - Fügen Sie Bedingungen mit dem JSON-Editor hinzu oder ändern Sie sie.
5. (Optional) Um der verwalteten Berechtigung Stichwörter zuzuordnen, geben Sie für Tags einen Tag-Schlüssel und einen Wert ein. Füge weitere Tags hinzu, indem du Neues Tag hinzufügen wählst. Wiederholen Sie diesen Schritt nach Bedarf.
6. Wählen Sie danach Create Kundenverwalteten Richtlinie aus.

AWS CLI

So erstellen Sie eine vom verwalteten Richtlinie für Kunden verwalteten Richtlinie

- Führen Sie den Befehl create-permission aus und geben Sie einen Namen, den Ressourcentyp, für den die vom Kunden verwaltete Berechtigung gilt, und den Text 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 Erstellen Sie eine vom Kunden verwalteten Richtlinie, d. h. es werden keine Kunden verwalteten Richtlinie

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 Ressourcenanteile aus, sondern nur auf die zukünftigen Ressourcenfreigaben, für die diese vom Kunden verwaltete Berechtigung verwendet wird.

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

Console

So erstellen Sie eine vom verwalteten Richtlinie, sodass Sie eine vom Kunden verwalteten Richtlinie für das Erteilen

1. Navigieren Sie zur Bibliothek für verwaltete 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 verwalteter Berechtigungen die Option Version erstellen aus.
4. Für die Richtlinienvorlage können Sie Aktionen und Bedingungen mit dem visuellen Editor oder JSON-Editor hinzufügen oder entfernen.

   Sie haben auch die Möglichkeit, verwaltete Berechtigung importieren zu wählen, um eine vorhandene Richtlinienvorlage zu verwenden.

5. Wählen Sie danach Create Version unten auf der Seite aus.

AWS CLI

So erstellen Sie eine vom verwalteten Richtlinie, sodass Sie eine vom Kunden verwalteten Richtlinie für das Erteilen

1. Suchen Sie den Amazon-Ressourcenname (ARN) der verwalteten Richtlinie, 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 für verwaltete 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. Verwenden Sie auf der Seite mit den Details der vom Kunden verwalteten Berechtigungen im Abschnitt Versionen verwalteter Berechtigungen die Dropdownliste, um die Version auszuwählen, die Sie als neue Standardversion festlegen möchten.
4. Wählen Sie Als Standardversion festlegen.
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.

   Der folgende Beispielbefehl ruft die aktuellen Versionen für die angegebene verwalteten Berechtigung ab.

```
$ 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
```

   Wenn dieser Befehl erfolgreich ausgeführt wird, wird keine Ausgabe zurückgegeben. Sie können den list-permission-versionsVorgang erneut ausführen und überprüfen, ob das`defaultVersion` Feld der ausgewählten Version jetzt auf gesetzt ist`true`.

Eine vom Kunden verwaltete Berechtigungsversion löschen

Sie können bis zu fünf Versionen jeder Kunden verwalteten Richtlinie für das Erteilen von Kunden verwalteten Richtlinie. Wenn eine Version nicht mehr benötigt wird, können Sie sie löschen. Die Standardversion einer vom Kunden verwalteten Richtlinie, d. h. es kann nicht gelöscht werden. Gelöschte Versionen bleiben bis zu zwei Stunden mit dem Status „Gelöscht“ in der Konsole sichtbar, bevor sie vollständig entfernt werden.

Console

So löschen Sie eine vom Kunden verwaltete Berechtigungsversion

1. Navigieren Sie zur Bibliothek für verwaltete 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. Vergewissern Sie sich, dass Sie löschen möchten, dass Sie löschen möchten, indem Sie die Standardversion, die Sie löschen möchten, indem Sie OK auswählen.
4. Wählen Sie im Abschnitt Versionen der Seite die Registerkarte Verknüpfte Ressourcenfreigaben aus, um zu sehen, ob Shares diese Version verwenden.

   Wenn Freigaben zugeordnet sind, müssen Sie die Version der 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.

6. Bestätigen Sie im Bestätigungsdialogfeld, dass Sie diese Version Ihrer Kunden verwalteten Richtlinie (Kunden verwalteten Richtlinie, d. h. es werden keine Kunden verwalteten Richtlinie, d. h. es werden Kunden verwalteten Richtlinie für Kunden verwalteten Richtlinie

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

AWS CLI

So löschen Sie eine vom verwalteten Richtlinie, d. h. es werden keine vom Kunden verwalteten Richtlinie

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
```

   Wenn dieser Befehl erfolgreich ausgeführt wird, wird keine Ausgabe zurückgegeben. Sie können list-permission-versionses erneut ausführen und überprüfen, ob die Version nicht mehr in der Ausgabe enthalten ist.

Eine vom Kunden verwaltete Berechtigung löschen

Wenn eine vom Kunden verwaltete Berechtigung nicht mehr benötigt wird und nicht verwendet wird, können Sie sie löschen. Sie können keine vom verwalteten Richtlinie, die mit einer vom Kunden verwalteten Richtlinie, die mit einer vom Kunden verwalteten Richtlinie für das Erteilen von Ressourcen verwalteten Die gelöschte, vom Kunden verwaltete Berechtigung verschwindet nach zwei Stunden. Bis dahin bleibt es in der Bibliothek für verwaltete Berechtigungen mit dem Status „Gelöscht“ sichtbar.

Console

Um eine vom Kunden verwaltete Berechtigung zu löschen

1. Navigieren Sie zur Bibliothek für verwaltete 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 0 verknüpfte Freigaben aus der Liste der verwalteten Berechtigungen 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 oben rechts auf der Seite „Vom Kunden verwalteten Richtlinie“ verwalteten Richtlinie 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. Finden 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 Berechtigung zum Löschen erhalten haben, geben Sie ihn als Parameter für die Löschberechtigung an.

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

AktualisierungAWS verwalteter Berechtigungen auf eine neuere Version

AWSAktualisiert gelegentlich dieAWS verwalteten Berechtigungen, die für das Anhängen an eine Ressourcenfreigabe für einen bestimmten Ressourcentyp verfügbar sind. WennAWS dies der Fall ist, wird eine neue Version derAWS verwalteten Berechtigung erstellt. Ressourcenfreigaben, die den angegebenen Ressourcentyp enthalten, werden nicht automatisch aktualisiert, um die neueste Version der verwalteten Berechtigung zu verwenden. Sie müssen die verwaltete Berechtigung für jede Ressourcenfreigabe explizit aktualisieren. Dieser zusätzliche Schritt ist erforderlich, damit Sie die Änderungen bewerten können, bevor Sie sie auf Ihre Ressourcenanteile anwenden.

Console

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

Darüber hinaus können einzelne Berechtigungen neben der aktuellen Versionsnummer die Schaltfläche Auf Standardversion aktualisieren anzeigen, wenn diese Version nicht die Standardversion ist.

Wenn Sie auf diese Schaltfläche klicken, wird der Assistent zum Aktualisieren der Ressourcennutzung gestartet. In Schritt 2 des Assistenten können Sie die Version aller nicht standardmäßigen Berechtigungen aktualisieren, um deren Standardversionen zu verwenden.

Die Änderungen werden erst gespeichert, wenn Sie den Assistenten abgeschlossen haben, indem Sie auf der letzten Seite des Assistenten die Option Senden wählen.

> **Note**
>
> Sie können nur die Standardversion anhängen und Sie können nicht zu einer anderen Version zurückkehren.
> Bei vom Kunden verwalteten Berechtigungen können Sie, nachdem Sie die Berechtigungen auf die Standardversion aktualisiert haben, keine weitere Version auf eine Ressourcenfreigabe anwenden, es sei denn, Sie haben diese andere Version zuerst als Standard festgelegt. Wenn Sie beispielsweise eine Berechtigung auf die Standardversion aktualisiert haben und dann einen Fehler gefunden haben, den Sie rückgängig machen möchten, können Sie die vorherige Version als Standardversion festlegen. Alternativ können Sie eine andere neue Version erstellen und diese dann als Standard festlegen. Nachdem Sie eine dieser Optionen ausgeführt haben, würden Sie Ihre Resource Shares aktualisieren, um die aktuelle Standardversion zu verwenden.

AWS CLI

Um die Version einerAWS 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 standardmäßigeAWS verwaltete Berechtigung für Amazon EC2-Kapazitätsreservierungen verwendet.

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

   Die Ausgabe enthält den ARN jeder Ressource, die mit mindestens einer Ressource geteilt wird, deren Zugriff durch diese verwaltete Berechtigung gesteuert wird.

2. Führen Sie für jede im vorherigen Befehl angegebene Ressourcennutzung den Befehl aus associate-resource-share-permission. Geben Sie den an,`--resource-share-arn` um die zu aktualisierende Ressourcenfreigabe anzugeben, den,`--permission-arn` um anzugeben, welcheAWS verwaltete Berechtigung Sie aktualisieren, und den`--replace` Parameter, um anzugeben, dass Sie die Freigabe aktualisieren möchten, um die neueste Version dieser verwalteten Berechtigung zu verwenden. 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 inAWS RAM

Vom Kunden verwaltete Berechtigungen sind nur in dem verfügbarAWS-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 Anweisungen werden nicht unterstützt. In vom Kunden verwalteten Berechtigungen können Sie nur einzelne, nicht negierende Operatoren verwenden.

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

- Schulleiter in der Organisation in Bezug auf:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Prinzipal für eine bestimmte Dienstleistung im Zusammenhang mit:
  - `aws:SourceArn`
  - `aws:SourceAccount`
- System-Tags:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

So funktionieren verwaltete Berechtigungen

Einen kurzen Überblick erhalten Sie im folgenden Video, in dem gezeigt wird, wie Sie mithilfe verwalteter Berechtigungen die bewährte Methode des Zugriffs mit geringsten Rechten auf IhreAWS Ressourcen anwenden können.

In diesem Video wird gezeigt, wie Sie vom Kunden verwaltete Berechtigungen erstellen und verknüpfen, die bewährten Methoden der geringsten Rechte befolgen. Weitere Informationen finden Sie unter ???.

Wenn Sie eine Ressourcenfreigabe erstellen, ordnen Sie jedem Ressourcentyp, den Sie teilen möchten, eineAWS verwaltete Berechtigung zu. Wenn die verwaltete Berechtigung mehr als eine Version hat, verwendet die neue Resource Share immer die Version, die als Standard festgelegt ist.

Nachdem Sie die Ressourcenfreigabe erstellt haben,AWS RAM verwendet die verwaltete Berechtigung, um eine ressourcenbasierte Richtlinie zu generieren, die an jede gemeinsam genutzte Ressource angehängt wird.

Die Richtlinienvorlage in einer verwalteten Berechtigung legt Folgendes fest:

Auswirkung

> Gibt an, ob`Allow` oder ob`Deny` der Prinzipal berechtigt ist, einen Vorgang an einer gemeinsam genutzten Ressource auszuführen. Bei einer verwalteten Berechtigung ist die Wirkung immer`Allow`. Weitere Informationen finden Sie unter Effekt im IAM-Benutzerhandbuch.

Action

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

Bedingung

Wann und wie ein Principal mit einer Ressource in einem Resource Share interagieren kann. Bedingungen sorgen für eine zusätzliche Sicherheitsebene für Ihre gemeinsam genutzten Ressourcen. Verwenden Sie sie, um den Zugriff für sensible Aktionen auf Ihre gemeinsam genutzten Ressourcen zu beschränken. Sie können beispielsweise Bedingungen angeben, nach denen die Aktionen aus einem bestimmten Unternehmens-IP-Adressbereich stammen müssen oder dass die Aktionen von Benutzern ausgeführt werden müssen, die mit der Multi-Faktor-Authentifizierung authentifiziert wurden. Weitere Informationen zu Bedingungen finden Sie unter AWSGlobale Bedingungskontextschlüssel Principal -Schlüssel. Weitere Informationen zu dienstspezifischen Bedingungen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel fürAWS Dienste in der Service Authorization-Referenz.

> **Note**
>
> Bedingungen sind für vom Kunden verwaltete Berechtigungen und unterstützte Ressourcentypen fürAWS 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 inAWS RAM.

Arten von verwalteten Berechtigungen

Wenn Sie eine Ressourcenfreigabe erstellen, wählen Sie eine verwaltete Berechtigung, um sie jedem Ressourcentyp zuzuordnen, den Sie in die Ressourcenfreigabe aufnehmen. AWSverwaltete Berechtigungen werden vomAWS ressourceneigenen Dienst definiert und von verwaltetAWS RAM. Sie erstellen und verwalten Ihre eigenen, vom Kunden verwalteten Berechtigungen.

- AWSverwaltete Berechtigung — Für jedenAWS RAM unterstützten Ressourcentyp ist eine verwaltete Standardberechtigung verfügbar. Die verwaltete Standardberechtigung wird für einen Ressourcentyp verwendet, 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. Mit der standardmäßigen verwalteten Berechtigung können Prinzipale bestimmte Aktionen ausführen, die vom Dienst für den Ressourcentyp definiert sind. Für den Amazon`ec2:Subnet` VPC-Ressourcentyp ermöglicht die verwaltete Standardberechtigung den Prinzipalen beispielsweise, die folgenden Aktionen auszuführen:

- `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 standardmäßige verwaltete Berechtigung ist von der Standardversion einer verwalteten Berechtigung getrennt. Bei allen verwalteten Berechtigungen, ob Standardberechtigungen oder eine der zusätzlichen verwalteten Berechtigungen, die von einigen Ressourcentypen unterstützt werden, handelt es sich um separate, vollständige Berechtigungen mit unterschiedlichen Auswirkungen und Aktionen, die unterschiedliche Freigabeszenarien unterstützen, z. B. Lese-/Schreib- oder Nur-Lesezugriff. Jede verwaltete Berechtigung, unabhängig davon, AWS ob sie 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 Vollzugriffsberechtigung (`Read` und `Write`) als auch eine verwaltete Leseberechtigung unterstützt, können Sie eine Ressourcenfreigabe für den Administrator mit der verwalteten Vollzugriffsberechtigung erstellen. Sie können dann eine separate Ressourcennutzung für andere Entwickler erstellen, indem Sie die verwaltete Leseberechtigung verwenden, um der Praxis zu folgen, bei der die geringsten Rechte vergeben werden.

> **Note**
>
> AlleAWS Dienste, die damit arbeiten,AWS RAM unterstützen mindestens eine verwaltete Standardberechtigung. Sie können die jeweils verfügbaren BerechtigungenAWS-Service auf der Seite Bibliothek für verwaltete Berechtigungen einsehen. Auf dieser Seite finden Sie Informationen zu jeder verfügbaren verwalteten Berechtigung, 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 RessourcenfreigabeAWS RAM automatisch die Standardberechtigung angewendet, die für den ausgewählten Ressourcentyp definiert ist. Falls unterstützt, haben Sie auch die Möglichkeit, auf der Seite Verwaltete Berechtigungen zuordnen die Option Kundenverwaltete Berechtigung 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 gemeinsam genutzten Ressourcen ausgeführt werden könnenAWS 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 vom Kunden verwaltete Berechtigungen für Ihre Entwickler erstellen, um IP-Adressen zuzuweisen, aber nicht den IP-Adressbereich einsehen, den andere Entwicklerkonten zugewiesen haben. Sie können die bewährten Methoden der geringsten Rechte befolgen, d. h. es werden nur die Berechtigungen erteilt, die zum Durchführen von Aufgaben auf freigabe erforderlich sind.

Sicherheit in AWS RAM

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, 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 – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. 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 geteilten Verantwortung bei der Verwendung von AWS RAM einsetzen können. Die folgenden Themen veranschaulichen, wie Sie AWS RAM zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre AWS RAM-Ressourcen zu überwachen und zu schützen.

Themen

Datenschutz in AWS RAM

Das Modell der geteilten Verantwortung von AWS gilt für den Datenschutz in AWS Resource Access Manager. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. 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, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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 auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 unter Verwendung der Konsole, der API, AWS CLI oder AWS SDKs mit AWS RAM oder anderen AWS-Services arbeiten. 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.

Identity and Access Management für AWS RAM

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem ein Administrator den Zugriff auf AWS-Ressourcen sicher steuern kann. Administratoren in IAM kontrollieren, wer authentifiziert (angemeldet) und autorisiert (mit Berechtigungen) zur Nutzung AWS von Ressourcen autorisiert werden kann. Durch die Verwendung von IAM erstellen Sie Prinzipien wie Rollen, Benutzer und Gruppen in Ihrem. AWS-Konto Sie kontrollieren die Berechtigungen, die diese Schulleiter haben, um Aufgaben mithilfe von AWS Ressourcen auszuführen. 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.

Themen

Funktionsweise von AWS RAM mit IAM

IAM-Personen besitzen keine Berechtigungen zum Erstellen oder Ändern vonAWS RAM -Ressourcen. Um IAM-Mitarbeitern zu erlauben, Ressourcen zu erstellen oder zu ändern und Aufgaben durchzuführen, führen Sie einen folgenden Format. Diese Aktionen gewähren die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren.

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 Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer 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 RAMbietet mehrereAWS verwaltete Richtlinien, die Sie verwenden können, um den Bedürfnissen vieler Benutzer gerecht zu werden. Weitere Informationen dazu finden Sie unter AWS Von verwaltete Richtlinien für AWS RAM.

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

Die folgenden Abschnitte enthalten dieAWS RAM spezifischen Details für die Erstellung einer IAM-Berechtigungsrichtlinie.

Inhalt

Richtlinienstruktur

Eine IAM-Berechtigungsrichtlinie ist ein JSON-Dokument, das die folgenden Anweisungen enthält: Effect, Action, Resource und Condition. Eine IAM-Richtlinie hat in folgenden Format.

```
{
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
```

```
        "Condition":{
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

Auswirkung

Die Erklärung „Wirkung“ gibt an, ob die Richtlinie einem Principal die Erlaubnis zur Ausführung einer Aktion erlaubt oder verweigert. Zu den möglichen Werten gehören:`Allow` und`Deny`.

Action

Die Action-Anweisung gibt dieAWS RAM API-Aktionen an, für die die Richtlinie die Erlaubnis zulässt oder verweigert. Eine vollständige Liste der zulässigen Aktionen finden Sie unter Actions defined byAWS Resource Access Manager im IAM-Benutzerhandbuch.

Ressource

Die Ressourcenerklärung gibt dieAWS RAM Ressourcen an, die von der Richtlinie betroffen sind. Um eine Ressource in der Anweisung anzugeben, müssen Sie deren eindeutigen Amazon Resource Name (ARN) verwenden. Eine vollständige Liste der zulässigen Ressourcen finden Sie unter Resources defined byAWS Resource Access Manager im IAM-Benutzerhandbuch.

Bedingung

Zustandsangaben sind optional. Sie können verwendet werden, um die Bedingungen zu verfeinern, unter denen die Richtlinie angewendet wird. AWS RAMunterstützt folgende:::

- `aws:RequestTag/${TagKey}`— Testet, ob die Serviceanfrage ein Tag enthält, wobei der angegebene Tag-Schlüssel existiert und den angegebenen Wert hat.
- `aws:ResourceTag/${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.

  Die folgende Beispielbedingung 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-Format an, die zum Erstellen oder Markieren einer Ressourcenfreigabe verwendet werden müssen.
- `ram:AllowsExternalPrincipals`— Testet, ob der Ressourcenanteil in der Serviceanfrage die gemeinsame Nutzung mit externen Prinzipalen ermöglicht. Ein externer Schulleiter ist einAWS-Konto Außenstehender Ihrer Organisation inAWS Organizations. Wenn dies zutrifft`False`, können Sie diesen Ressourcenanteil 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 Ressourcentypzeichenfolge 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 sich die Serviceanfrage bezieht, mit einer Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.
- `ram:ShareOwnerAccountId`— Testet, ob die Konto-ID-Nummer der Ressourcenfreigabe, auf die die Serviceanfrage reagiert, mit einer Zeichenfolge übereinstimmt, die Sie in der Richtlinie angeben.

AWS Von verwaltete Richtlinien für AWS RAM

AWS Resource Access Managerbietet derzeit mehrereAWS RAMverwaltete Richtlinien, die in diesem Thema beschrieben werden.

Von AWS verwaltete Richtlinien

- AWS verwaltete Richtlinie: AWSResourceAccessManagerReadOnlyAccess
- AWS verwaltete Richtlinie: AWSResourceAccessManagerFullAccess
- AWS verwaltete Richtlinie: AWSResourceAccessManagerResourceShareParticipantAccess
- AWS verwaltete Richtlinie: AWSResourceAccessManagerServiceRolePolicy
- AWS RAM-Aktualisierungen für AWS verwaltete Richtlinien

In der vorherigen Liste können Sie die ersten drei Richtlinien an Ihre IAM-Rollen, -Gruppen und -Benutzer anhängen, um Berechtigungen zu gewähren. Die letzte Richtlinie in der Liste ist reserviert fürAWS RAMdie dienstleistungsgebundene Rolle des Dienstes.

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWSaktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

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

AWS verwaltete Richtlinie: AWSResourceAccessManagerReadOnlyAccess

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

Diese Richtlinie gewährt schreibgeschützte Berechtigungen für die Resource Shares, die Ihrem gehörenAWS-Konto.

Dies geschieht, indem es die Erlaubnis erteilt, eines der`Get*`oder`List*`operationen. Es bietet keine Möglichkeit, einen Ressourcenanteil zu ändern.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ram`— Ermöglicht es Principals, Details zu den Ressourcenanteilen einzusehen, die dem Konto gehören.

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

AWS verwaltete Richtlinie: AWSResourceAccessManagerFullAccess

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

Diese Richtlinie bietet vollen Administratorzugriff, um die Resource Shares einzusehen oder zu ändern, die sich im Besitz IhresAWS-Konto.

Dies geschieht, indem es die Erlaubnis erteilt, beliebige auszuführen`ram`operationen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ram`— Ermöglicht es Schulleitern, alle Informationen über die Ressourcenanteile einzusehen oder zu ändern, die sich im Besitz derAWS-Konto.

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

AWS verwaltete Richtlinie: AWSResourceAccessManagerResourceShareParticipantAccess

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

Diese Richtlinie gibt Schulleitern die Möglichkeit, gemeinsam genutzte Ressourcen zu akzeptieren oder abzulehnen.AWS-Konto, und um Details zu diesen Ressourcenanteilen einzusehen. Es bietet keine Möglichkeit, diese Ressourcenanteile zu ändern.

Es tut dies, indem es die Erlaubnis erteilt, einige zu betreiben`ram`operationen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ram`— Ermöglicht es Schulleitern, Einladungen zur gemeinsamen Nutzung von Ressourcen anzunehmen oder abzulehnen und Details zu den Ressourcenfreigaben einzusehen, die mit dem Konto geteilt wurden.

```
{
    "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: AWSResourceAccessManagerServiceRolePolicy

DerAWSverwaltete Richtlinie`AWSResourceAccessManagerServiceRolePolicy`kann nur mit der serviceverknüpften Rolle verwendet werden fürAWS RAM. Sie können diese Richtlinie nicht anhängen, trennen, ändern oder löschen.

Diese Richtlinie bietetAWS RAMmit schreibgeschütztem Zugriff auf die Struktur Ihrer Organisation. Wenn Sie die Integration aktivieren zwischenAWS RAMundAWS Organizations,AWS RAMerstellt automatisch eine dienstverknüpfte Rolle mit dem NamenAWSServiceRoleForResourceAccessManagerdass der Dienst davon ausgeht, wenn er nach Informationen über Ihre Organisation und deren Konten suchen muss, z. B. wenn Sie die Struktur der Organisation in derAWS RAMKonsole.

Dies geschieht, indem es eine schreibgeschützte Berechtigung zum Ausführen von gewährt`organizations:Describe`und`organizations:List`Operationen, die Einzelheiten zur Struktur und den Konten der Organisation enthalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations`— Ermöglicht es Schulleitern, Informationen über die Struktur der Organisation einzusehen, einschließlich der Organisationseinheiten, undAWS-Kontensie enthalten.

```
{
    "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 für AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für AWS RAM, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS RAM-Dokumentverlauf.

Änderung	Beschreibung	Datum
AWS Resource Access Manager hat die Änderungs verfolgung gestartet	AWS RAMdokumentierte die bestehenden verwaltet en Richtlinien und begann, Änderungen zu verfolgen.	16. September 2021

Verwenden von serviceverknüpften Rollen für AWS RAM

AWS Resource Access Manager verwendet serviceverknüpfte Rollen vonAWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit dem AWS RAM Service verknüpft ist. Serviceverknüpfte Rollen werden von vordefiniert AWS und schließen alle Berechtigungen ein, die zum Aufrufen anderer -AWSServices in Ihrem Namen AWS RAM benötigt.

Eine serviceverknüpfte Rolle vereinfacht die Konfiguration von , AWS RAM da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS RAM definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, AWS RAM kann nur seine serviceverknüpften 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.

Berechtigungen von serviceverknüpften Rollen für AWS RAM

AWS RAM verwendet die serviceverknüpfte Rolle namens , `AWSServiceRoleForResourceAccessManager` wenn Sie die Freigabe mit aktivierenAWS Organizations. Diese Rolle gewährt dem AWS RAM Service Berechtigungen zum Anzeigen von Organisationsdetails, z. B. der Liste der Mitgliedskonten und der Organisationseinheiten, in denen sich jedes Konto befindet.

Diese serviceverknüpfte Rolle vertraut dem folgenden Service, die Rolle zu übernehmen:

- `ram.amazonaws.com`

Die Rollenberechtigungsrichtlinie namens AWSResourceAccessManagerServiceRolePolicy ist an diese serviceverknüpfte Rolle angehängt und ermöglicht AWS RAM die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- Aktionen: Schreibgeschützte Aktionen, die Details zur Struktur Ihrer Organisation abrufen. Eine vollständige Liste der Aktionen finden Sie in der IAM-Konsole: AWSResourceAccessManagerServiceRolePolicy.

Damit ein Prinzipal die AWS RAM Freigabe innerhalb Ihrer Organisation aktivieren kann, muss dieser Prinzipal (eine IAM-Entität wie ein Benutzer, eine Gruppe oder eine Rolle) über die Berechtigung zum Erstellen einer serviceverknüpften Rolle verfügen. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS RAM

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die AWS RAM Freigabe innerhalb Ihrer Organisation in der aktivieren AWS Management Consoleoder die EnableSharingWithAwsOrganization in Ihrem Konto mithilfe der AWS CLI oder einer AWS API ausführen, AWS RAM erstellt die serviceverknüpfte Rolle für Sie.

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

Wenn Sie diese serviceverknüpfte Rolle löschen, hat AWS RAM keine Berechtigungen mehr zum Anzeigen der Details der Struktur Ihrer Organisation.

Bearbeiten einer serviceverknüpften Rolle für AWS RAM

AWS RAM erlaubt es Ihnen nicht, die AWSResourceAccessManagerServiceRolePolicy serviceverknüpfte 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, AWS CLI- oder AWS-API, um die `AWSResourceAccessManagerServiceRolePolicy` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte AWS RAM-Rollen

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

Beispiel-IAM-Richtlinien für AWS RAM

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

Beispiele für IAM-Richtlinien

- Beispiel 1: Erlaube 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: Erlaube die gemeinsame Nutzung bestimmter Ressourcen

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

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

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

```
{
    "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, Ressourcenanteilen nur bestimmte Ressourcentypen zuzuordnen.

Die folgende Richtlinie beschränkt Prinzipale beispielsweise darauf, nur Resolver-Regeln gemeinsam zu nutzen.

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

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

Sie können eine IAM-Richtlinie verwenden, um zu verhindern, dass Schulleiter Ressourcen mit Personen teilenAWS-Konten, die sich außerhalb der Organisation befinden. AWS

Die folgende IAM-Richtlinie verhindert beispielsweise, dass Principals externe Ressourcen AWS-Konten zu Ressourcenfreigaben hinzufügen.

```
{
    "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 Service-Kontrollrichtlinien (Service Control Policies, SCPs). SCPs sind Richtlinien, die Sie an Elemente in einer Organisation anfügen, 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 aller Konten Ihrer Organisation. Sie können Ihnen dabei helfen, sicherzustellen, dass Sie die Richtlinien Ihrer Organisation zur Zugangskontrolle einhalten. AWS-Konten Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations-Benutzerhandbuch.

Voraussetzungen

Um SCPs zu verwenden, müssen Sie Folgendes ausführen:

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

Beispiel für Service-Kontrollrichtlinien

Inhalt

- Beispiel 2: Verhindern Sie, dass Benutzer Einladungen zur gemeinsamen Nutzung von Ressourcen von externen Konten außerhalb Ihrer Organisation annehmen
- Beispiel 3: Erlauben Sie bestimmten Konten, bestimmte Ressourcentypen gemeinsam zu nutzen
- Beispiel 4: Verhindern Sie die gemeinsame Nutzung mit der gesamten Organisation oder mit Organisationseinheiten
- Beispiel 5: Erlauben Sie die gemeinsame Nutzung nur mit bestimmten Prinzipalen

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.

```
{
    "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.

```
{
    "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.

```
{
    "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.

```
{
    "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: Erlauben Sie die gemeinsame Nutzung nur mit bestimmten Prinzipalen

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`

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

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

Deaktivieren der Ressourcenfreigabe mit AWS Organizations

Wenn Sie zuvor die Freigabe für aktiviert haben AWS Organizations und keine Ressourcen mehr für Ihre gesamte Organisation oder Organisationseinheiten (OUs) freigeben müssen, können Sie die Freigabe deaktivieren. Wenn Sie die Freigabe mit deaktivierenAWS Organizations, werden alle Organisationen oder OUs aus den von Ihnen erstellten Ressourcenfreigaben entfernt und sie verlieren den Zugriff auf die freigegebenen Ressourcen. Externe Konten (Konten, die der Ressourcenfreigabe per Einladung hinzugefügt wurden) sind nicht betroffen und werden weiterhin mit der Ressourcenfreigabe verknüpft.

So deaktivieren Sie die Freigabe mit AWS Organizations

1. Deaktivieren Sie den vertrauenswürdigen Zugriff auf AWS Organizations mithilfe 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 deaktivierenAWS Organizations, werden Prinzipale innerhalb Ihrer Organisation aus allen Ressourcenfreigaben entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

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

Protokollieren und Überwachen in AWS RAM

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Performance von AWS RAM und Ihren AWS-Lösungen. Erfassen Sie Überwachungsdaten aller Bestandteile Ihrer AWS-Lösung, damit Sie Ausfälle an mehreren Punkten leichter debuggen können. AWS bietet mehrere Tools für die Überwachung Ihrer AWS RAM-Ressourcen und die Reaktion auf potenzielle Vorfälle:

CloudWatch Amazon-Ereignisse

Stellt einen near-real-time Strom von Systemereignissen bereit, die Änderungen inAWS -Ressourcen beschreiben. CloudWatch Events ermöglicht automatisierte, ereignisgesteuerte Datenverarbeitung, denn Sie können Regeln schreiben, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderenAWS -Services auslösen, wenn diese Ereignisse auftreten. Weitere Informationen finden Sie unter ÜberwachungAWS RAM mithilfe von CloudWatch Ereignissen.

AWS CloudTrail

Erfasst API-Aufrufe und zugehörige Ereignisse, die von oder in Ihrem Namen erfolgten,AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie unter Protokollierung von AWS RAM-API-Aufrufen mit AWS CloudTrail.

ÜberwachungAWS RAM mithilfe von CloudWatch Ereignissen

Mit Amazon CloudWatch Events können Sie automatische Benachrichtigungen für bestimmte Ereignisse in einrichtenAWS RAM. Ereignisse vonAWS RAM werden nahezu in Echtzeit an CloudWatch Events übermittelt. Sie können CloudWatch Ereignisse konfigurieren, um Ereignisse zu überwachen und Ziele als Reaktion auf Ereignisse aufzurufen, die auf Änderungen Ihrer Ressourcenanteile hinweisen. Änderungen an einer Ressourcenfreigabe lösen Ereignisse sowohl für den Eigentümer der Ressourcennutzung als auch für die Prinzipale aus, denen Zugriff auf die Ressourcennutzung gewährt wurde.

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

> **Note**
>
> Seien Sie vorsichtig, wenn Sie Code schreiben, der von diesen Ereignissen abhängt. Diese Ereignisse können nicht garantiert, sondern werden auf bestmögliche Weise ausgegeben. Tritt beimAWS RAM Versuch, ein Ereignis auszulösen, ein Fehler auf, 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 Amazon CloudWatch Events-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 die Ausführung der asynchronen Aufgaben, die mit der gemeinsamen Nutzung von Ressourcen verbunden sind, unbemerkt fehlschlagen. 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 als erwarteten Kosten führen.

Um auf Fehler bei der Ressourcennutzung zu achten, richten Sie eine Amazon CloudWatch Events-Regel ein, die Sie benachrichtigt, wenn eineAWS RAM Ressourcennutzung ausfällt. Das

folgende Tutorial verwendet ein Amazon Simple Notification Service (SNS) -Thema verwendet ein Amazon Simple Notification Service (SNS) -Thema verwendet, um alle Themenabonnenten zu benachrichtigen, wenn ein Fehler bei der gemeinsamen Nutzung von Ressourcen EventBridge nicht erfüllt. 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 Regelliste Regel erstellen aus.
3. Geben Sie einen Namen und eine optionale Beschreibung für Ihre Regel ein und wählen Sie dann Weiter.
4. Scrollen Sie nach unten zum Feld Ereignismuster und wählen Sie Benutzerdefinierte Muster (JSON-Editor).
5. Kopieren Sie das folgende Ereignismuster und fügen Sie ein bereits ein.

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

6. Wählen Sie Next (Weiter).
7. Wählen Sie für Ziel 1 unter Zieltyp AWS-Service.
8. Wählen Sie unter Ziel auswählen die Option SNS-Thema aus.
9. Unter Thema wählen Sie das SNS-Thema aus, für das Sie die Benachrichtigung veröffentlichen möchten Dieses Thema muss bereits bereits bereits bereits
10. Wählen Sie Weiter und dann erneut Weiter, um Ihre Konfiguration zu überprüfen.
11. Wenn Sie mit Ihren Optionen zufrieden sind, klicken Sie Regel erstellen möchten.

12. Stellen Sie auf der Regelseite sicher, dass Ihre neue Regel als Aktiviert markiert ist. Falls erforderlich, wählen Sie das Optionsfeld neben Ihrem Regelnamen und dann aktivieren Sie dann aktivieren möchten.

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

Sie können auch überprüfen, ob Reservierungen für gemeinsam genutzte 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.

Protokollierung von AWS RAM-API-Aufrufen mit AWS CloudTrail

AWS RAMist in integriertAWS CloudTrail, einen Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS -Service durchgeführten Aktionen bereitstelltAWS RAM. CloudTrail erfasst alle API-Aufrufe fürAWS RAM als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS RAM-Konsole und Code-Aufrufe der AWS RAM-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 Bucket, einschließlich Ereignissen für, aktivierenAWS RAM. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail Konsole trotzdem in Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die an AWS RAM gestellte Anforderung, die anfordernde IP-Adresse, den Anforderer, den Zeitpunkt der Anforderung und weitere Angaben bestimmen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrailBenutzerhandbuch.

AWS RAMInformationen in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres für Sie aktiviert. Die inAWS RAM auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderenAWS -Serviceereignissen in Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS RAM, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von -Protokolldateien in einem Amazon S3 Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser 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 andereAWS -Services konfigurieren, um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Erstellen eines Trails für AWS-Konto
- AWS-ServiceIntegrationen mit CloudTrail Protokollen
- Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail -Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail -Protokolldateien aus mehreren Konten

AlleAWS RAM Aktionen werden von der AWS RAMAPI-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-KontoAnmeldeinformationen
- Temporäre Sicherheits-Anmeldeinformationen von einer AWS Identity and Access Management (IAM)-Rolle oder einem Verbundbenutzer.
- Langfristige Sicherheits-Anmeldeinformation eines IAM-Benutzers.
- Ein anderer AWS-Service.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS RAM-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

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"
}
```


Ausfallsicherheit in AWS RAM

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz 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 über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Sicherheit der Infrastruktur in AWS RAM

Als verwalteter Dienst AWS Resource Access Manager ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf AWS RAM zuzugreifen. 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 Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Beheben von Problemen mit AWS RAM

Verwenden Sie die Informationen in diesem Abschnitt des Handbuchs, um häufige Probleme bei der Arbeit mit AWS Resource Access Manager () zu diagnostizieren und zu behebenAWS RAM.

Themen

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

Szenario

Sie erhalten die Fehlermeldung „Ihre Konto-ID ist in einer AWS Organisation nicht vorhanden “, wenn Sie versuchen, eine Ressource für Konten oder Organisationseinheiten (OUs) in Ihrer Organisation freizugeben.

Ursache

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

Lösung

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

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie zur Seite Services in der AWS OrganizationsKonsole .
3. Wählen Sie RAM aus.
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie zur Seite Einstellungen in der AWS RAMKonsole .
6. Aktivieren Sie das Kontrollkästchen Freigabe mit aktivieren AWS Organizationsund wählen Sie dann Einstellungen speichern aus.

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

Sie sollten jetzt verwenden könnenAWS RAM, um Ihre Ressourcen mit Konten und OUs in der Organisation gemeinsam zu nutzen.

Fehler: "AccessDeniedException"

Szenario

Sie erhalten eine Ausnahme aufgrund einer Zugriffsverweigerung, wenn Sie versuchen, eine Ressource freizugeben oder eine Ressourcenfreigabe anzuzeigen.

Ursache

Sie können diesen Fehler erhalten, wenn Sie versuchen, eine Ressourcenfreigabe zu erstellen, wenn Sie nicht über die erforderlichen Berechtigungen verfügen. Dies kann durch unzureichende Berechtigungen in Richtlinien verursacht werden, die Ihrem AWS Identity and Access Management (IAM)-Prinzipal zugeordnet sind. Dies kann auch aufgrund von Einschränkungen durch eine -AWS OrganizationsService-Kontrollrichtlinie (SCP) passieren, die sich auf Ihr auswirktAWS-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 Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer 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 Anforderung stellt. Darüber hinaus dürfen die Berechtigungen nicht von den SCPs Ihrer Organisation blockiert werden.

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 Berechtigungen an eine Ressourcenfreigabe anzufügen, benötigen Sie die folgende Berechtigung:

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

  Dies ist ein Platzhalter. Sie müssen sie durch die „PutPolicy“-Berechtigung (oder gleichwertig) für den Service ersetzen, der Eigentümer der Ressource ist, die Sie freigeben möchten.

Wenn Sie beispielsweise eine Route-53-Resolverregel freigeben, wäre die erforderliche Berechtigung: `route53resolver:PutResolverRulePolicy`. Wenn Sie die Erstellung einer Ressourcenfreigabe zulassen möchten, die mehrere Ressourcentypen enthält, müssen Sie die entsprechende Berechtigung für jeden Ressourcentyp angeben, den Sie zulassen möchten.

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

```
{
    "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 ou-*xxxx* konnte nicht gefunden werden“
- „CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx* konnte nicht gefunden werden.“

Ursache

Diese Fehler können auftreten, wenn Sie die Integration zwischen AWS RAM und aktivieren, AWS Organizations indem Sie entweder die Organizations-Konsole oder die Organizations-

EnableAWSServiceAccess -API verwenden, anstatt die AWS RAMKonsole zu verwenden. Wenn Sie die Integration über die Organizations-Konsole oder API aktivieren, erstellt der Service 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 zugreifen.

Lösung

Um das Problem zu beheben, deaktivieren Sie die Integration zwischen AWS RAM und AWS Organizations. Aktivieren Sie sie dann erneut, indem Sie die AWS RAM EnableSharingWithAwsOrganization -API-Operation aufrufen oder die verwenden, AWS Management Console um die folgenden Schritte auszuführen.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie zur Seite Services in der AWS OrganizationsKonsole .
3. Wählen Sie RAM .
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie zur Seite Einstellungen in der AWS RAMKonsole .
6. Aktivieren Sie das Kontrollkästchen Freigabe mit aktivieren AWS Organizationsund wählen Sie dann Einstellungen speichern aus.

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

Sie sollten jetzt verwenden könnenAWS RAM, um Ihre Ressourcen mit Konten und OUs in der Organisation gemeinsam zu nutzen.

Fehler beim Versuch, für Konten außerhalb meiner Organisation freizugeben

Szenario

Sie erhalten einen der folgenden Fehler, wenn Sie versuchen, Ressourcen für Konten außerhalb Ihrer Organisation freizugeben:

- „Sie können die Ressource nicht außerhalb Ihrer Organisation freigeben.“
- „Die Ressource, die Sie freigeben möchten, kann nur innerhalb Ihrer AWS Organisation freigegeben werden.“
- „InvalidParameterException: Principal Account-ID befindet sich nicht in Ihrer AWS Organisation. Sie haben keine Berechtigung zum Hinzufügen AWS-Konten von außerhalb einer Ressourcenfreigabe.“
- „OperationNotPermittedException: Die Ressource, die Sie freigeben möchten, kann nur innerhalb Ihrer AWS Organisation freigegeben werden.“

Mögliche Ursachen und Lösungen

Einige Ressourcentypen können nur für Konten in derselben Organisation freigegeben werden

Einige Ressourcentypen können nicht mit einem Konto geteilt werden, das kein Mitglied dieser Organisation ist. Ein Beispiel für einen Ressourcentyp mit dieser Einschränkung sind Virtual Private Connections (VPCs), die Teil von Amazon Elastic Compute Cloud (Amazon EC2) sind.

Informationen dazu, ob Sie einen bestimmten Ressourcentyp für Konten und Prinzipale außerhalb Ihrer Organisation freigeben können, finden Sie unter Freigebbare AWS Ressourcen.

Die serviceverknüpfte Rolle wurde nicht erfolgreich erstellt

Dieses Problem kann auftreten, wenn die serviceverknüpfte Rolle nicht erfolgreich erstellt `AWSServiceRoleForResourceAccessManager` wurde, wenn Sie die Integration zwischen AWS RAM und aktiviert habenAWS Organizations.

Wenn Sie beim Versuch, eine Ressource für ein Konto freizugeben, das Teil Ihrer Organisation ist, einen dieser Fehler erhalten, führen Sie die folgenden Schritte aus, um die serviceverknüpfte Rolle zu löschen und neu zu erstellen.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie zur Seite Services in der AWS OrganizationsKonsole .
3. Wählen Sie RAM .
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie zur Seite Einstellungen in der AWS RAMKonsole .
6. Aktivieren Sie das Kontrollkästchen Freigabe mit aktivieren AWS Organizationsund wählen Sie dann Einstellungen speichern aus.

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

Geteilte Ressourcen im Zielkonto können nicht angezeigt werden

Szenario

Benutzer können die Ressourcen, von denen sie glauben, dass sie für sie freigegeben sind, nicht von anderen aus sehenAWS-Konten.

Mögliche Ursachen und Lösungen

Die Freigabe mit AWS Organizations wurde mithilfe von Organizations anstelle von aktiviert AWS RAM

Wenn mithilfe von Organizations anstelle von aktiviert AWS Organizations wurdeAWS RAM, schlägt die Freigabe innerhalb der Organisation fehl. Um zu überprüfen, ob dies die Ursache des Problems ist, navigieren Sie zur Seite Einstellungen in der -AWS RAMKonsole und überprüfen Sie, ob das Kontrollkästchen Freigabe mit aktivieren AWS Organizations aktiviert ist.

- Wenn das Kontrollkästchen aktiviert ist, ist dies nicht die Ursache.
- Wenn das Kontrollkästchen nicht aktiviert ist, kann dies die Ursache sein. Aktivieren Sie das Kontrollkästchen noch nicht. Führen Sie die folgenden Schritte aus, um die Situation zu korrigieren.

1. Melden Sie sich mit einer IAM-Rolle oder einem Benutzer mit Administratorberechtigungen bei Ihrem Verwaltungskonto Ihrer Organisation an.
2. Navigieren Sie zur Seite Services in der AWS Organizations Konsole .
3. Wählen Sie RAM .
4. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
5. Navigieren Sie zur Seite Einstellungen in der AWS RAMKonsole .
6. Aktivieren Sie das Kontrollkästchen Freigabe mit aktivieren AWS Organizationsund wählen Sie dann Einstellungen speichern aus.

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

Möglicherweise müssen Sie die Freigabe aktualisieren und die Konten oder Organisationseinheiten innerhalb der Organisation angeben, für die die Freigabe erfolgen soll.

Die Ressourcenfreigabe gibt dieses Konto nicht als Prinzipal an

Zeigen Sie in der AWS-Konto , die die Ressourcenfreigabe erstellt hat, die Ressourcenfreigabe in der AWS RAM Konsole an. Stellen Sie sicher, dass das Konto, das nicht auf die Ressourcen zugreifen kann, als Prinzipal aufgeführt ist. Ist dies nicht der Fall, aktualisieren Sie die Freigabe, um das Konto als Prinzipal hinzuzufügen.

Die Rolle oder der Benutzer im Konto verfügt nicht über die erforderlichen Mindestberechtigungen

Wenn Sie eine Ressource in Konto A für ein anderes Konto B freigeben, 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 Berechtigung erteilen. Die folgende Richtlinie zeigt beispielsweise, wie Sie Rollen und Benutzern in Konto B schreibgeschützten Zugriff für eine Ressource aus Konto A gewähren können. Die Richtlinie gibt die Ressource anhand ihres Amazon-Ressourcennamens (ARN) an.

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

Die Ressource befindet sich in einer anderen AWS-Region als der aktuellen Konsoleneinstellung

AWS RAM ist ein regionaler Service. Ressourcen sind in einer bestimmten vorhandenAWS-Region, und um sie anzuzeigen, AWS Management Console muss so konfiguriert sein, dass die Ressourcen in dieser Region angezeigt werden.

Die AWS-Region, auf die die Konsole derzeit zugreift, wird in der oberen rechten Ecke der Konsole angezeigt. Um ihn zu ändern, wählen Sie den aktuellen Regionsnamen aus und wählen Sie im Dropdown-Menü 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 freigeben können, ResourceShareLimitExceededExceptionwenn Sie versuchen, Ressourcen freizugeben.

Ursache

Diese Fehler treten auf, wenn Sie die maximale Anzahl von Ressourcen erreichen, die Sie entweder über den -AWS RAMService oder die freigeben könnenAWS-Service, die die Ressource erstellt hat, die Sie freigeben möchten. Dieses Kontingent (früher als Limit bezeichnet) kann sich sowohl auf das Freigabekonto als auch auf das Konto auswirken, für das Sie die Ressource freigeben.

Lösung

1. Um Ihre Kontingente anzuzeigen, navigieren Sie in der AWS-Konto , in der Sie den Fehler sehen, je nach Art des Kontingents, das Sie erreichen, zu einer der folgenden Seiten:
   - Die AWS RAM Seite in der Service Quotas-Konsole
   - Die Seite für die 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 anfordern aus.
4. Geben Sie einen neuen Wert für das Kontingent ein und wählen Sie dann Anfordern aus.
5. Die Anforderung wird auf der Seite Verlauf der Kontingentanforderung angezeigt, auf der Sie den Status der Anforderung überprüfen können, bis sie abgeschlossen ist.

Das andere Konto in meiner Organisation erhält nie eine Einladung

Szenario

Wenn Sie Ressourcen für ein anderes Konto in derselben von verwalteten Organisation freigebenAWS Organizations, erhalten diese keine Einladungen.

Ursache

Dies ist ein erwartetes Verhalten, wenn Ihr Konto die Freigabe innerhalb der AWS Organisation aktiviert hat.

Wenn diese Option aktiviert ist und Sie mit einem anderen Konto in Ihrer Organisation teilen, werden keine Einladungen gesendet und es ist keine Annahme erforderlich. Alle Organisationskonten, auf die Sie als Prinzipale in der Ressourcenfreigabe verweisen, können sofort mit dem Zugriff auf die Ressourcen in der Freigabe beginnen.

Wenn Ihr Konto die Freigabe innerhalb der AWS Organisation nicht aktiviert hat, werden sie als eigenständige Konten behandelt, wenn Sie sie mit anderen Konten teilen, auch wenn sie sich in derselben AWS Organisation befinden. Einladungen werden gesendet und müssen akzeptiert werden, bevor Benutzer auf die Ressourcen in den Freigaben zugreifen können.

Sie können ein VPC-Subnetz nicht freigeben

Szenario

Wenn Sie versuchen, zu verwendenAWS RAM, um ein VPC-Subnetz für ein anderes Konto freizugeben, ist der Freigabevorgang erfolgreich. Das verbrauchende Konto zeigt jedoch `LIMIT EXCEEDED` für diese Ressource in der -AWS RAMKonsole an.

Ursache

Einige einzelne Ressourcentypen haben servicespezifische Einschränkungen, die von den Einschränkungen abweichen, die von durchgesetzt werdenAWS RAM. Einige dieser Einschränkungen können die Freigabe effektiv verhindern, auch wenn Sie eine der Einschränkungen in nicht erreicht habenAWS RAM. Limits sind ein Beispiel für diese Einschränkungen. Amazon Virtual Private Cloud (Amazon VPC) begrenzt die Anzahl der Subnetze, die Sie für ein anderes einzelnes Konto freigeben können. Wenn Sie versuchen, ein Subnetz für ein verbrauchendes Konto freizugeben, das bereits die maximale Anzahl von Subnetzen enthält, werden diese verbrauchenden Konten `LIMIT EXCEEDED` in der Konsole für diese Ressource angezeigt. Weitere Informationen zu diesem Limit finden Sie unter Amazon-VPC-Kontingente – VPC-Freigabe im Amazon-Amazon Virtual Private Cloud-Benutzerhandbuch.

Um dies zu beheben, suchen Sie zunächst nach anderen Ressourcenfreigaben, die die angegebene Ressource möglicherweise für das betroffene Konto freigeben, und entfernen Sie die Freigaben, die Sie möglicherweise nicht mehr benötigen. Sie können auch eine Erhöhung für ein Limit beantragen, das die Anpassung unterstützt. Verwenden Sie die Service Quotas-Konsole, um eine Erhöhung des Limits anzufordern.

> **Note**
>
> AWS RAM erkennt Limiterhöhungsänderungen nicht automatisch. Sie müssen die Ressource oder den Prinzipal erneut mit der Ressourcenfreigabe verknüpfen, damit RAM die Änderung erkennt.

Service-Kontingente 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 AWS 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-Bucket oder eine Amazon EC2-Instance. Jede Ressource, auf die in einem Ressourcenanteil verwiesen wird, wird als eine Ressource auf dieses Kontingent angerechnet. Wenn Sie dieselbe Ressource in drei verschiedenen Ressourcenanteilen teilen, erhöht sich Ihre Anzahl für dieses Kontingent um drei.
> - Resource Share — Ein AWS RAM erstellter Container, mit dem Sie Ressourcen gemeinsam nutzen können. Jeder Ressourcenanteil, unabhängig davon, wie viele Ressourcen er enthält, wird auf Ihr Kontingent angerechnet.
> - Gemeinsamer Principal — Eine Kennung, die Sie einer Ressourcenfreigabe zugeordnet haben. Dies kann eine AWS Identity and Access Management (IAM-) Rolle oder ein Benutzer, ein AWS-Konto Identifier, eine Organisationseinheit oder eine gesamte Organisation sein. Jeder gemeinsam genutzte Principal, auf den Sie in einer Ressourcenfreigabe verweisen, erhöht Ihre Quotennutzung um einen. Wenn Sie mit einer gesamten Organisation teilen, indem Sie deren ID referenzieren, wird diese ID nur als eine Nummer auf dieses Kontingent angerechnet.
> - Vom Kunden verwaltete Berechtigungen — Verwaltete Berechtigungen, die Sie für bestimmte Anwendungsfälle erstellen, indem Sie den Zugriff mit den geringsten Rechten verwenden, um zu verwalten, wie Ihre gemeinsam genutzten Ressourcen genutzt werden.

Ressource	Standardlimit
Maximale Anzahl von Ressourcenanteilen pro AWS-Region	25,000

Ressource	Standardlimit
Maximale Anzahl von Ressourcenzuordnungen pro Ressourcenanteil	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 verwaltete Berechtigung	5
Maximale Anzahl von Ressourcenzuordnungen für alle Ressourcenanteile in einem AWS-Region **Note** Jede Ressource, die in einem Ressourcenanteil enthalten ist, wird auf dieses Limit angerechnet. Wenn eine Ressource in 10 verschiedenen Ressourcenanteilen enthalten ist, werden 10 auf das Limit angerechnet.	25,000

Ressource	Standardlimit
Maximale Anzahl von Hauptverbänden für alle Ressourcenanteile in einem AWS-Region **Note** Jeder in einem Ressourcenanteil enthaltene Kapitalbetrag wird auf diese Obergrenze angerechnet. Wenn ein Principal in 10 verschiedenen Ressourcenanteilen enthalten ist, werden 10 auf das Limit 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 sindAWS Organizations. • Es gibt kein Kontingent, das begrenzt, wie viele ausstehende Einladungen ein Empfängerkonto haben kann. • Einladungen werden nicht verwendet, wenn sie zwischen Konten geteilt werden, die Teil desselben Kontos sind AWS Organizat ions und Sie die gemeinsame Nutzung von Ressourcen innerhalb von aktiviert haben. AWS Organizations	250

Verwendung von AWS RAM mit einem AWS SDK

AWS-Software Development Kits (SDKs) sind für viele gängige Programmiersprachen erhältlich. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die Entwicklern helfen, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Code-Beispiele
AWS SDK for C++	Codebeispiele für AWS SDK for C++
AWS SDK for Go	Codebeispiele für AWS SDK for Go
AWS SDK for Java	Codebeispiele für AWS SDK for Java
AWS SDK for JavaScript	Codebeispiele für AWS SDK for JavaScript
AWS SDK for .NET	Codebeispiele für AWS SDK for .NET
AWS SDK for PHP	Codebeispiele für AWS SDK for PHP
AWS SDK for Python (Boto3)	Codebeispiele für AWS SDK for Python (Boto3)
AWS SDK for Ruby	Codebeispiele für AWS SDK for Ruby

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 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.	8. November 2023
Unterstützung für das Teilen von AWS Ressourcen	Sie können jetzt AWS Ressourcen Explorer	14. November 2023

Explorer Ansichten wurde hinzugefügt.	Ansichten mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	
Unterstützung für die gemeinsame Nutzung von Amazon Route 53 Application Recovery Controller-Ressourcen hinzugefügt.	Sie können jetzt Amazon Route 53 Application Recovery Controller-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 wurde 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 Feature Store-Funktionsgruppen und SageMaker Catalog als gemeinsam nutzbare Ressourcen hinzugefügt.	Sie können jetzt Amazon SageMaker Feature Store-Funktionsgruppen und SageMaker 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-APIs jetzt 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 Ressourcenzugriffskontrollen für unterstützte Ressourcentypen erstellen und verwalten.	19. April 2023
Unterstützung für Amazon VPC Lattice Service und gemeinsam nutzbare Service-Netzwerkressourcen hinzugefügt.	Sie können jetzt Amazon VPC Lattice Service- und Service-Netzwerkressourcen mit anderen teilen. AWS-Konten	31. März 2023
Unterstützung für AWS Marketplace Katalogentitäten 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.	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	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 über AWS RAM hinzugefügt.	Es wurden Übersichtsvideos hinzugefügt, die das Teilen einer Ressource mit anderen beschreiben AWS RAM und erläutern. AWS-Konten	2p. August 2022
Unterstützung für SageMaker Amazon-Pipelines hinzugefügt.	Sie können SageMaker Pipelines jetzt mit anderen teilen. AWS-Konten	02.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 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 SageMaker Amazon-Ressourcen	Sie können es verwenden AWS RAM , um SageMaker 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 AWS RAM jetzt Amazon Route 53 Resolver DNS-Firewall-Regelgruppen mit anderen AWS-Konten 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 das Teilen 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 wurde 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 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 wurde hinzugefügt.	Sie können AWS RAM jetzt AWS Glue-Datenkataloge, Datenbanken und Tabellen mit anderen AWS-Konten 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 IPv4-Adressen 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 die gemeinsame Nutzung von Meshes hinzugefügt AWS App Mesh	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 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 wurde hinzugefügt	Sie können es jetzt verwenden , AWS RAM um Amazon EC2 Dedicated Hosts, AWS Resource Groups Ressourcengruppen und Amazon EC2 Image Builder Builder-Komponenten, Images und Image-Rezepte mit anderen zu teilen. AWS-Konten	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-Konten.	29. Juli 2019
Unterstützung für die gemeinsame Nutzung von Aurora-DB-Clustern hinzugefügt	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 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 AWS License Manager Manager-Lizenzkonfigurationen jetzt mit anderen teilen AWS-Konten. AWS RAM	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.