



User Guide

AWS Resource Access Manager



AWS Resource Access Manager: User Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS RAM?	1
Videoübersichten	1
Vorteile von AWS RAM	2
Wie steht es mit kontenübergreifenden Zugriffen mit ressourcenbasierten Richtlinien?	2
Funktionsweise der Ressourcenfreigabe	3
Teilen Sie Ihre Ressourcen	4
Verwenden gemeinsam genutzter Ressourcen	5
Zugriff auf AWS RAM	5
Preise für AWS RAM	6
Konformität und internationale Standards	7
PCI-DSS	7
FedRAMP	7
SOC und ISO	7
Erste Schritte	8
Begriffe und Konzepte	8
Ressourcenfreigabe	8
Konto teilen	9
Prinzipale werden konsumiert	10
Ressourcenbasierte Richtlinie	12
Verwaltete Berechtigungen	16
Version mit verwalteten Berechtigungen	18
Teilen Sie Ihre Ressourcen	18
Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb AWS Organizations	19
Erstellen einer Ressourcen-Freigabe	21
Verwenden gemeinsam genutzter Ressourcen	31
Antworscht.	31
Verwenden Sie die Ressourcen, die mit Ihnen geteilt werden	33
Arbeiten mit freigegebenen	35
Regionale und globale Ressourcen	35
Was sind die Unterschiede zwischen regionalen und globalen Ressourcen?	36
Ressourcenanteile und ihre Regionen	37
Ressourcen, die Ihnen gehören	39
Von Ihnen erstellte Ressourcenanteile anzeigen	39
Eine Ressourcenfreigabe erstellen	42

Eine Ressourcenfreigabe aktualisieren	52
Ihre geteilten Ressourcen anzeigen	60
Prinzipale, mit denen Sie teilen, anzeigen	62
Löschen	63
Für Sie freigegebene Ressourcen	65
Annehmen und Ablehnen von Einladungen	66
Für Sie geteilte Ressourcenanteile anzeigen	70
Mit Ihnen geteilte Ressourcen anzeigen	72
Principals anzeigen, die mit dir geteilt wurden	73
Eine gemeinsame Nutzung einer Ressource verlassen	75
IDs der Availability Zone	78
Gemeinsam nutzbare Ressourcen	82
APIAmazon-Gateway	84
AWS App Mesh	85
AWS AppSync GraphQL API	86
Amazon Aurora	87
AWS Backup	87
Amazon Bedrock	88
AWS Billing Service anzeigen	89
AWS Private Certificate Authority	90
Amazon DataZone	92
AWS CloudHSM	92
AWS CodeBuild	93
Amazon EC2	95
EC2Image Builder	100
AWS Endbenutzer-Messaging SMS	104
Amazon FSx für Open ZFS	108
AWS Glue	110
AWS License Manager	113
AWS Marketplace	114
AWS Migration Hub Refactor Spaces	114
AWS Network Firewall	116
AWS Outposts	117
Amazon S3 in Outposts	120
AWS Ressourcen Explorer	121
AWS Resource Groups	122

Amazon Route 53	123
Amazon Application Recovery Controller (ARC)	128
Amazon Simple Storage Service	129
Amazon SageMaker KI	130
AWS Service Catalog AppRegistry	138
AWS Systems Manager Incident Manager	140
AWS Systems Manager Parameter speichern	142
Amazon VPC	144
VPCAmazon-Gitter	156
AWS Wolke WAN	158
Verwaltung von Berechtigungen inAWS RAM	160
Verwaltete Berechtigungen anzeigen	161
Vom Kunden verwaltete Berechtigungen erstellen und verwenden	166
Eine vom Kunden verwaltete Berechtigung erstellen	167
Erstellen Erstellen Sie eine vom Kunden verwalteten Richtlinie, d. h. es werden keine Kunden verwalteten Richtlinie	169
Wählen Sie eine andere Version als Standard für eine vom Kunden verwaltete Berechtigung	171
Eine vom Kunden verwaltete Berechtigungsversion löschen	173
Eine vom Kunden verwaltete Berechtigung löschen	174
Aktualisierung der Versionen verwalteter Berechtigungen	176
Überlegungen zu vom Kunden verwalteten Berechtigungen	178
So funktionieren verwaltete Berechtigungen	179
Arten von verwalteten Berechtigungen	181
Sicherheit	183
Datenschutz	184
Identity and Access Management	185
Wie AWS RAM funktioniert mit IAM	185
Von AWS verwaltete Richtlinien	189
Verwenden von serviceverknüpften Rollen	194
IAM-Beispielrichtlinien	196
Beispiel SCPs	198
Deaktivieren der Freigabe für Organizations	202
Protokollierung und Überwachung	203
Überwachung mit EventBridge	204
Protokollierung von AWS RAM-API-Aufrufen mit AWS CloudTrail	206

Ausfallsicherheit	208
Sicherheit der Infrastruktur	209
AWS PrivateLink	209
Überlegungen	210
Erstellen eines Schnittstellenendpunkts	210
Erstellen einer Endpunktrichtlinie	210
Fehlerbehebung	212
Fehler: Konto-ID existiert nicht	212
Szenario	212
Ursache	212
Lösung	212
Fehler: Ausnahme „Zugriff verweigert“	213
Szenario	213
Ursache	213
Lösung	214
Fehler: Unbekannte Ressourcenausnahme	215
Szenario	215
Ursache	216
Lösung	216
Fehler: Teilen außerhalb einer Organisation ist nicht erlaubt	217
Szenario	217
Mögliche Ursachen und Lösungen	217
Fehler: Geteilte Ressourcen können nicht angezeigt werden	218
Szenario	218
Mögliche Ursachen und Lösungen	218
Fehler: Ausnahme: Limit überschritten	220
Szenario	220
Ursache	221
Lösung	221
Keine Einladungen erhalten	221
Szenario	221
Ursache	221
Sie können kein teilen VPC	222
Szenario	222
Ursache	222
Servicekontingente	223

Verwenden der AWS-SDKs	226
Dokumentverlauf	227
.....	ccxxxix

Was ist AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) hilft Ihnen dabei, Ihre Ressourcen sicher zwischen AWS-Konten, innerhalb Ihrer Organisation oder Organisationseinheiten (OUs) sowie mit AWS Identity and Access Management (IAM-) Rollen und Benutzern für unterstützte Ressourcentypen zu teilen. Wenn Sie mehrere haben AWS-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 wird AWS Organizations, können Sie Ressourcen mit allen anderen Konten in der Organisation oder nur mit den Konten teilen, die zu einer oder mehreren bestimmten Organisationseinheiten (OUs) gehören. Sie können Inhalte auch mit einer bestimmten AWS-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](#)
- [Vorteile von AWS RAM](#)
- [Funktionsweise der Ressourcenfreigabe](#)
- [Zugriff auf AWS RAM](#)
- [Preise für AWS RAM](#)
- [Konformität und internationale Standards](#)

Videoübersichten

Das folgende Video stellt eine kurze Einführung AWS RAM und beschreibt, wie ein Ressourcenfreigabe erstellt wird. Weitere Informationen finden Sie unter [???](#).

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

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 einer AWS RAM Ressourcennutzung durch einen einzigen Satz von Richtlinien und Berechtigungen verwaltet. AWS RAM bietet ein einheitliches Erlebnis für die gemeinsame Nutzung verschiedener Arten von AWS Ressourcen.
- Sorgt für Transparenz und Überprüfbarkeit — Durch die Integration von AWS RAM Amazon CloudWatch und können Sie sich die Nutzungsdetails Ihrer gemeinsam genutzten Ressourcen anzeigen lassen AWS CloudTrail. AWS RAM bietet einen umfassenden Überblick über gemeinsam genutzte Ressourcen und Konten.

Wie steht es mit kontenübergreifenden Zugriffen mit ressourcenbasierten Richtlinien?

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

- Sie können die Daten für eine [Organisation oder eine Organisationseinheit \(OE\)](#) freigeben, ohne jede einzelne der AWS-Konto IDs aufzählen zu müssen.

- Benutzer können die für sie freigegebenen Ressourcen direkt in der ursprünglichen AWS-Service Konsole und in den API-Vorgängen sehen, als ob sich diese Ressourcen direkt im Konto des Benutzers befinden würden. Wenn Sie AWS RAM beispielsweise ein Amazon VPC-Subnetz mit einem anderen Konto teilen, können Benutzer dieses Kontos das Subnetz in der Amazon VPC-Konsole und in den Ergebnissen der Amazon VPC-API-Operationen sehen, die in diesem Konto ausgeführt wurden. Ressourcen, die durch das Anhängen einer ressourcenbasierten Richtlinie gemeinsam genutzt werden, sind auf diese Weise nicht sichtbar. Stattdessen müssen Sie die Ressource anhand ihres Amazon-Ressourcennamens (ARN) ermitteln und explizit darauf verweisen.
- Die Besitzer einer Ressource können sehen, welche Principals Zugriff auf jede einzelne Ressource haben, die sie gemeinsam genutzt haben.
- Wenn Sie Ressourcen mit einem Konto teilen, das nicht zu Ihrer Organisation gehört, wird ein AWS 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 vollständig AWS 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-policy](#) Befehl AWS Command Line Interface (AWS CLI).

Funktionsweise der Ressourcenfreigabe

Wenn Sie eine Ressource im Eigentümerkonto mit einer anderen Ressource AWS-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 dem AWS-Konto 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 der AWS 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 Einzelpersonen AWS-Konten, die Konten einer Organisation oder einer Organisationseinheit (OU) in AWS Organizations oder einzelne Rollen oder Benutzer AWS 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 unter [Gemeinsam 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 zugewiesene AWS 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 wie AWS-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 zugreifen AWS-Region, den die Servicekonsole und die Tools der Ressource unterstützen. Sie können die Ressourcenfreigabe und die zugehörigen globalen Ressourcen in der AWS RAM Konsole und den Tools nur in der dafür vorgesehenen Heimatregion USA Ost (Nord-Virginia) anzeigen und verwalten us-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 Console](#)und 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 RAM unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstleister und wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert.

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

FedRAMP

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

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

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

Weitere Informationen zur FedRAMP-Konformität finden Sie unter [FedRAMP](#).

SOC und ISO

AWS RAM kann für Workloads verwendet werden, die 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 den AWS 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

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

Wenn Sie das Teilen innerhalb von nicht aktivieren AWS 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-Konten in Ihrer Organisation. Für [unterstützte Ressourcenfreigabe](#), Sie können Ressourcen auch mit einzelnen Personen teilen AWS 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 für AWS RAM](#)
- [Teilen Sie Ihre AWS Ressourcen](#)
- [Verwenden gemeinsam genutzter AWS Ressourcen](#)

Begriffe und Konzepte für AWS RAM

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

Ressourcenfreigabe

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

- Eine Liste mit einer oder mehreren AWS Ressourcen, die gemeinsam genutzt werden sollen.
- Eine Liste mit einem oder mehreren [Prinzipalen](#), denen Zugriff auf die Ressourcen gewährt wird.

- Eine [verwaltete Berechtigung](#) für jeden Ressourcentyp, den Sie in die Freigabe aufnehmen. Jede verwaltete Berechtigung gilt für alle Ressourcen dieses Typs in dieser Ressourcenfreigabe.

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

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

Konto teilen

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

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

Prinzipale werden konsumiert

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

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

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

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

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

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

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

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

- `service-id.amazonaws.com`

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

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

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

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

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

Important

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

Informationen finden Sie unter [Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten 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 einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

Ressourcenbasierte Richtlinie

Bei ressourcenbasierten Richtlinien handelt es sich um JSON Textdokumente, in denen die IAM Richtlinienprache implementiert wird. Im Gegensatz zu identitätsbasierten Richtlinien, die Sie dem Prinzipal zuordnen, z. B. einer IAM Rolle oder einem Benutzer, fügen Sie der Ressource ressourcenbasierte Richtlinien hinzu. AWS RAM erstellt in Ihrem Namen ressourcenbasierte Richtlinien auf der Grundlage der Informationen, die Sie für Ihren Resource Share angeben. Sie müssen ein `Principal` Richtlinienelement angeben, das festlegt, wer auf die Ressource zugreifen kann. Weitere Informationen finden Sie im [Benutzerhandbuch unter Identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien](#). IAM

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

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

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

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

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

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

Mithilfe AWS RAM von können Sie sogar einige Ressourcentypen gemeinsam nutzen, die noch keine ressourcenbasierten Richtlinien unterstützen. Generiert für solche Ressourcentypen AWS RAM automatisch eine ressourcenbasierte Richtlinie als Darstellung der tatsächlichen Berechtigungen. Benutzer können sich diese Darstellung ansehen, indem sie aufrufen [GetResourcePolicy](#). Dazu gehören die folgenden Ressourcentypen:

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

Beispiele für generierte ressourcenbasierte Richtlinien AWS RAM

Wenn Sie eine EC2 Image Builder Builder-Bildressource mit einem einzelnen Konto gemeinsam nutzen, AWS RAM generiert es eine Richtlinie, die wie im folgenden Beispiel aussieht, und fügt sie allen Bildressourcen hinzu, 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-Bildressource mit einer IAMRolle oder einem Benutzer in einem anderen teilen AWS-Konto, AWS RAM generiert es eine Richtlinie, die wie im folgenden

Beispiel aussieht, und fügt sie allen Bildressourcen hinzu, 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 RAM generiert sie eine Richtlinie, die wie im folgenden Beispiel aussieht, und fügt sie allen Bildressourcen hinzu, die in der Ressourcenfreigabe enthalten sind.

Note

Diese Richtlinie verwendet das "Condition" Element "Principal": "*" und verwendet es dann, um Berechtigungen auf Identitäten zu beschränken, die den angegebenen entsprechen. `PrincipalOrgID` Weitere Informationen finden Sie unter [Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten 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 "Principal": "*" in eine ressourcenbasierte Richtlinie einbeziehen, gewährt die Richtlinie Zugriff auf alle IAM Prinzipale in dem Konto, das die Ressource enthält, vorbehaltlich aller Einschränkungen, die durch ein Condition Element, sofern vorhanden, auferlegt werden. Explizite Deny Aussagen in allen Richtlinien, die für den aufrufenden Prinzipal gelten, haben Vorrang vor den durch diese Richtlinie gewährten Berechtigungen. Eine implizite Deny (d. h. das Fehlen einer expliziten Angabe Allow) in allen geltenden Identitäts-, Berechtigungsgrenzen- oder Sitzungsrichtlinien führt jedoch nicht dazu, dass den Prinzipalen durch eine Deny solche ressourcenbasierte Richtlinie Zugriff auf eine Aktion gewährt wird.

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

Verwaltete Berechtigungen

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

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

AWS verwaltete Berechtigungen

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

Vom Kunden verwaltete Berechtigungen

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

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

AWS RAM verwendet verwaltete Berechtigungen als Eingabe für die Erstellung der [ressourcenbasierten Richtlinien](#) für die Ressourcen, die Sie gemeinsam nutzen.

Version mit verwalteten Berechtigungen

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

AWS Versionen mit verwalteten Berechtigungen

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

Versionen mit vom Kunden verwalteten Berechtigungen

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

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

Teilen Sie Ihre AWS Ressourcen

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

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

Hinweise

- Die gemeinsame Nutzung einer Ressource mit Prinzipalen außerhalb des AWS-Konto Eigentümers der Ressource hat keine Auswirkung auf die Berechtigungen oder Kontingente, die für die Ressource innerhalb des Kontos gelten, mit dem sie erstellt wurde.
- AWS RAM ist ein regionaler Dienst. Die Prinzipale, 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 wird AWS Organizations, können Sie dies nutzen, um Ressourcen einfacher gemeinsam zu nutzen. Mit oder ohne Organizations kann ein Benutzer Inhalte mit einzelnen Konten teilen. Wenn sich Ihr Konto jedoch in einer Organisation befindet, können Sie Inhalte für einzelne Konten oder für alle Konten in der Organisation oder in einer Organisationseinheit freigeben, ohne jedes Konto aufzählen zu müssen.

Um Ressourcen innerhalb einer Organisation gemeinsam zu nutzen, müssen Sie zuerst die AWS RAM Konsole verwenden oder AWS Command Line Interface (AWS CLI), um das Teilen mit zu aktivieren. AWS Organizations Wenn Sie Ressourcen in Ihrer Organisation gemeinsam nutzen, sendet AWS RAM keine Einladungen an Schulleiter. Principals in Ihrer Organisation erhalten Zugriff auf gemeinsam genutzte Ressourcen, ohne Einladungen austauschen zu müssen.

Wenn Sie die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation aktivieren, AWS RAM wird eine dienstbezogene Rolle mit dem Namen erstellt.

AWSServiceRoleForResourceAccessManager Diese Rolle kann nur vom AWS RAM Dienst übernommen werden und erteilt die AWS RAM Berechtigung, mithilfe der AWS verwalteten Richtlinie `AWSResourceAccessManagerServiceRolePolicy` Informationen über die Organisation abzurufen, der er angehört.

Wenn Sie Ressourcen nicht mehr mit Ihrer gesamten Organisation gemeinsam nutzen müssen oder OUs 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 Organizations Benutzerhandbuch unter [Alle Funktionen in Ihrer Organisation aktivieren](#).

Important

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

Console

Um die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation zu aktivieren

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

AWS CLI

Um die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation zu aktivieren

Verwenden Sie den Befehl [enable-sharing-with-aws-organization](#).

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

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

Erstellen einer Ressourcen-Freigabe

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

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

Note

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

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

Überlegungen

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

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

Important

Wenn Sie Daten mit einer Organisation oder einer Organisationseinheit teilen und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im 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 Freigabe. Die Administratoren der anderen Konten müssen zunächst identitätsbasierte Berechtigungsrichtlinien an die entsprechenden Principals anhängen. Diese Richtlinien müssen Allow Zugriff auf die einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

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

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

Note

Nicht alle Ressourcentypen können mit IAM Rollen und Benutzern gemeinsam genutzt werden. Informationen zu Ressourcen, die Sie mit diesen Prinzipalen gemeinsam nutzen können, finden Sie unter [Gemeinsam nutzbare Ressourcen AWS](#).

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

Important

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

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

Console

Um eine Ressourcenfreigabe zu erstellen

1. Öffnen Sie die [AWS RAM -Konsole](#).

2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben anzuzeigen, die globale Ressourcen enthalten, müssen Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), (us-east-1) setzen. Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unter [Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen](#). Wenn Sie globale Ressourcen in die gemeinsame Nutzung von Ressourcen einbeziehen möchten, müssen Sie die angegebene Heimatregion, USA Ost (Nord-Virginia), auswählen us-east-1.
3. Wenn Sie noch keine Erfahrung damit haben AWS RAM, wählen Sie auf der Startseite die Option Ressourcenfreigabe erstellen aus. Wählen Sie andernfalls auf der Seite [Von mir geteilt: Gemeinsam genutzte Ressourcen die Option Ressourcenfreigabe](#) erstellen aus.
4. Gehen Sie in Schritt 1: Angaben zur Ressourcenfreigabe angeben wie folgt vor:
 - a. Geben Sie unter Name einen beschreibenden Namen für die Ressourcenfreigabe ein.
 - b. Wählen Sie unter Ressourcen wie folgt die Ressourcen aus, die der Ressourcenfreigabe hinzugefügt werden sollen:
 - Wählen Sie unter Ressourcentyp auswählen den Ressourcentyp aus, den Sie gemeinsam nutzen möchten. Dadurch wird die Liste der gemeinsam nutzbaren Ressourcen auf die Ressourcen des ausgewählten Typs gefiltert.
 - Aktivieren Sie in der resultierenden Ressourcenliste die Kontrollkästchen neben den einzelnen Ressourcen, die Sie gemeinsam nutzen möchten. Die ausgewählten Ressourcen werden unter Ausgewählte Ressourcen verschoben.

Wenn Sie Ressourcen gemeinsam nutzen, die einer bestimmten Availability Zone zugeordnet sind, können Sie mithilfe der Availability Zone ID (AZ ID) den relativen Standort dieser Ressourcen zwischen Konten ermitteln. Weitere Informationen finden Sie unter [Availability Zone-IDs für Ihre AWS Ressourcen](#).
 - c. (Optional) Um der Ressourcenfreigabe [Tags](#) hinzuzufügen, geben Sie unter Tags einen Tag-Schlüssel und einen Tag-Wert ein. Fügen Sie weitere hinzu, indem Sie Neues Tag hinzufügen wählen. Wiederholen Sie diesen Schritt nach Bedarf. Diese Tags gelten nur für die Ressourcenfreigabe selbst, nicht für die Ressourcen in der Ressourcenfreigabe.
5. Wählen Sie Weiter.
6. In Schritt 2: Ordnen Sie jedem Ressourcentyp eine verwaltete Berechtigung zu, können Sie wählen, ob Sie dem Ressourcentyp eine verwaltete Berechtigung zuordnen, eine bestehende

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

Wählen Sie Vom Kunden verwaltete Berechtigung erstellen aus, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls zum Teilen entspricht. Weitere Informationen finden Sie unter [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.
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. VPC Amazon-Subnetze. Sie können einige [unterstützte Ressourcentypen](#) auch mit IAM Rollen und Benutzern teilen.

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

- b. Gehen Sie für Principals wie folgt vor:

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

 **Important**

Wenn Sie Inhalte für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im Freigabekonto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet.

"Principal": "*" Weitere Informationen finden Sie unter [Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten 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 einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

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

 Note

Die Option „Organisationsstruktur anzeigen“ wird nur angezeigt, wenn „Teilen mit“ aktiviert AWS Organizations ist und Sie beim Verwaltungskonto der Organisation angemeldet sind.

Sie können diese Methode nicht verwenden, um eine Person AWS-Konto außerhalb Ihrer Organisation, eine IAM Rolle oder einen Benutzer anzugeben. Stattdessen müssen Sie die Option Organisationsstruktur anzeigen deaktivieren und in der Dropdownliste und im Textfeld die ID oder eingebenARN.

- Um einen Principal anhand der ID oderARN, einschließlich Principals außerhalb der Organisation, anzugeben, wählen Sie für jeden Prinzipal den Prinzipaltyp aus. Geben Sie als Nächstes die ID (für eine AWS-Konto Organisation oder Organisationseinheit) oder ARN (für eine IAM Rolle oder einen Benutzer) ein, und klicken Sie dann auf Hinzufügen. Die verfügbaren Haupttypen, IDs und ARN Formate lauten wie folgt:

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

123456789012

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

o-abcd1234

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

ou-abcd-1234efgh

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

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

Beispielsweise:

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

 Note

Rufen Sie die [Liste der Rollen in der IAM Konsole auf](#), verwenden Sie den [AWS CLI Befehl `get-role` oder die `GetRole` API Aktion](#), um die eindeutige [ARN Rolle](#) abzurufen. IAM

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

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

Beispielsweise:

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

 Note

Um den eindeutigen Namen ARN für einen IAM Benutzer zu erhalten, [rufen Sie die Benutzerliste in der IAM Konsole auf](#) und verwenden Sie den [`get-user` AWS CLI Befehl oder `GetUser` API Aktion](#).

- Service Principal — Um einen Service Principal hinzuzufügen, wählen Sie Service Principal aus der Dropdown-Principaltyp auswählen aus. Geben Sie den Namen des AWS Dienstprinzips ein. Verwenden Sie die folgende Syntax:

- *service-id*.amazonaws.com

Beispielsweise:

```
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.

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

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

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

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

AWS CLI

Um eine gemeinsame Nutzung einer Ressource zu erstellen

Verwenden der [create-resource-share](#) Befehl. Der folgende Befehl erstellt eine Ressourcenfreigabe, die von allen Mitarbeitern 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 die ARN für den 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-type LicenseConfiguration
```

```
--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 genutzter AWS Ressourcen

Um mit der Nutzung von Ressourcen zu beginnen, die mit Ihrem Konto geteilt wurden AWS 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 Ressourcenfreigabeabebienladung 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 sind AWS 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 mit AWS-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 der AWS 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 möglicherweise AWS-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 geändertstatus wurdeACCEPTED. 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 genutzten AWS Ressourcen

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

Inhalt

- [Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen](#)
 - [Was sind die Unterschiede zwischen regionalen und globalen Ressourcen?](#)
 - [Ressourcenanteile und ihre Regionen](#)
- [Teilen Sie AWS Ressourcen, die Ihnen gehören](#)
 - [Ressourcenanteile anzeigen, die Sie in erstellt haben AWS RAM](#)
 - [Einen Ressourcenanteil erstellen in AWS RAM](#)
 - [Aktualisieren Sie eine Ressourcenfreigabe in AWS RAM](#)
 - [Anzeige Ihrer geteilten Ressourcen in AWS RAM](#)
 - [Anzeige der Auftraggeber, mit denen Sie Ressourcen teilen, in AWS RAM](#)
 - [Löschen einer Ressourcenbeteiligung in AWS RAM](#)
- [Zugriff auf für Sie freigegebene AWS Ressourcen](#)
 - [Annehmen und Ablehnen von Einladungen zur gemeinsamen Nutzung von Ressourcen](#)
 - [Für Sie geteilte Ressourcenanteile anzeigen](#)
 - [Mit Ihnen geteilte Ressourcen anzeigen](#)
 - [Principals anzeigen, die mit dir geteilt wurden](#)
 - [Einen Ressourcenanteil hinterlassen](#)
 - [Voraussetzungen für das Verlassen einer Ressourcenfreigabe](#)
 - [Wie verlasse ich eine Ressourcenfreigabe](#)
- [Availability Zone-IDs für Ihre AWS Ressourcen](#)

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 die AWS-Region. Wenn es leer ist, ist die Ressource global.

Was sind die Unterschiede zwischen regionalen und globalen Ressourcen?

Regionale Ressourcen

Die meisten Ressourcen, mit denen Sie teilen können, AWS RAM sind regional. Sie erstellen sie in einer bestimmten Region AWS-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 erstellen AWS 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 RAM ist 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 umfasst AWS-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 konnten AWS-Konto.

Überlegungen

- Um eine Ressourcenfreigabe in der AWS RAM Konsole zu erstellen, müssen Sie die Region verwenden, die die Ressourcen enthält, die Sie teilen möchten. Wenn Sie eine globale Ressource 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 - east-1.

Teilen Sie AWS Ressourcen, die Ihnen gehören

Sie können AWS Resource Access Manager (AWS RAM) verwenden, um die von Ihnen angegebenen Ressourcen mit den von Ihnen angegebenen Prinzipalen 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 haben AWS RAM](#)
- [Einen Ressourcenanteil erstellen in AWS RAM](#)
- [Aktualisieren Sie eine Ressourcenfreigabe in AWS RAM](#)
- [Anzeige Ihrer geteilten Ressourcen in AWS RAM](#)
- [Anzeige der Auftraggeber, mit denen Sie Ressourcen teilen, in AWS RAM](#)
- [Löschen einer Ressourcenbeteiligung in AWS RAM](#)

Ressourcenanteile anzeigen, die Sie in erstellt haben AWS 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 der AWS RAM Konsole die Seite [Von mir geteilt: Resource Shares](#).
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie in der oberen rechten Ecke der Konsole die entsprechende AWS-Region aus der Drop-down-Liste aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie die AWS-Region auf USA Ost (Nord-Virginia), (us-east-1) einstellen. Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unter [Gemeinsame 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-shares](#) Befehl mit dem auf `--resource-owner SELF` gesetzten Parameter verwenden, um Details der in Ihrem erstellten Ressourcenanteil anzuzeigen AWS-Konto.

Das folgende Beispiel zeigt die Ressourcenanteile, die in current AWS-Region (`us-east-1`) für den Aufruf gemeinsam genutzt werden AWS-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.
 - AWS verwaltete Berechtigungen werden von erstellt AWS , um Standardanwendungsfälle abzudecken.
 - Mit vom Kunden verwalteten Berechtigungen können Sie Ihre eigenen verwalteten Berechtigungen an Ihre Sicherheits- und Geschäftsanforderungen anpassen.

Note

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

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

Überlegungen

- Wenn Sie später eine AWS Ressource löschen müssen, die Sie in eine Freigabe aufgenommen haben, empfehlen wir, die Ressource zunächst entweder aus einer Ressourcenfreigabe zu entfernen, die sie enthält, oder die Ressourcenfreigabe zu löschen.

- Die Ressourcentypen, die Sie in eine Ressourcenfreigabe aufnehmen können, sind unter [aufgeführt](#) [Gemeinsam nutzbare Ressourcen AWS](#).
- Sie können eine Ressource nur gemeinsam nutzen, wenn Sie [Eigentümer dieser](#) Ressource sind. Sie können eine Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- AWS RAM ist ein regionaler Dienst. Wenn Sie eine Ressource mit Prinzipalen in anderen teilen AWS-Konten, müssen diese Prinzipale auf jede Ressource von derselben Seite aus zugreifen AWS-Region, in der sie erstellt wurde. Auf unterstützte globale Ressourcen können Sie von allen AWS-Region Ressourcen aus zugreifen, die von der Servicekonsole und den Tools der jeweiligen Ressource unterstützt werden. Sie können solche gemeinsam genutzten Ressourcen und ihre globalen Ressourcen in der AWS RAM Konsole und in den Tools nur in der angegebenen Heimatregion, USA Ost (Nord-Virginia), einsehen -east-1. Weitere Informationen zu AWS RAM und globalen Ressourcen finden Sie unter [Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen](#).
- Wenn das Konto, von dem aus Sie Inhalte teilen, Teil einer Organisation ist AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten alle Prinzipale in der Organisation, für die Sie Inhalte freigeben, automatisch Zugriff auf die Ressourcenfreigaben, ohne dass Einladungen erforderlich sind. Ein Hauptbenutzer in einem Konto, mit dem Sie Inhalte außerhalb des Unternehmenskontextes teilen, erhält eine Einladung zur Teilnahme an der Resource Share und erhält erst dann Zugriff auf die gemeinsam genutzten Ressourcen, wenn sie die Einladung annehmen.
- Wenn Sie die Ressource mit einem Dienstprinzipal teilen, können Sie der Ressourcenfreigabe keine anderen Prinzipale zuordnen.
- Wenn die gemeinsame Nutzung zwischen Konten oder Prinzipalen erfolgt, die Teil einer Organisation sind, wirken sich alle Änderungen an der Organisationsmitgliedschaft dynamisch auf den Zugriff auf die gemeinsam genutzte Ressource aus.
 - Wenn Sie der Organisation oder Organisationseinheit ein Konto hinzufügen, das Zugriff auf eine Ressourcenfreigabe hat, erhält dieses neue Mitgliedskonto automatisch Zugriff auf die Ressourcenfreigabe. AWS-Konto Der Administrator des Kontos, für das Sie eine gemeinsame Nutzung vorgenommen haben, kann dann einzelnen Prinzipalen in diesem Konto Zugriff auf die Ressourcen in dieser Freigabe gewähren.
 - Wenn Sie ein Konto aus der Organisation oder einer Organisationseinheit entfernen, die Zugriff auf eine Ressourcenfreigabe hat, verlieren alle Prinzipale in diesem Konto automatisch den Zugriff auf Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.
 - Wenn Sie es direkt mit einem Mitgliedskonto oder mit IAM Rollen oder Benutzern im Mitgliedskonto geteilt haben und dieses Konto dann aus der Organisation entfernen,

verlieren alle Prinzipale in diesem Konto den Zugriff auf die Ressourcen, auf die über diese Ressourcenfreigabe zugegriffen wurde.

Important

Wenn Sie Daten mit einer Organisation oder einer Organisationseinheit teilen und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im 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 einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

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

Note

Nicht alle Ressourcentypen können mit IAM Rollen und Benutzern gemeinsam genutzt werden. Informationen zu Ressourcen, die Sie mit diesen Prinzipalen gemeinsam nutzen können, finden Sie unter [Gemeinsam nutzbare Ressourcen AWS](#).

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

Important

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

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

Console

Um eine Ressourcenfreigabe zu erstellen

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

- a. Geben Sie unter Name einen beschreibenden Namen für die Ressourcenfreigabe ein.
- b. Wählen Sie unter Ressourcen wie folgt die Ressourcen aus, die der Ressourcenfreigabe hinzugefügt werden sollen:
 - Wählen Sie unter Ressourcentyp auswählen den Ressourcentyp aus, den Sie gemeinsam nutzen möchten. Dadurch wird die Liste der gemeinsam nutzbaren Ressourcen auf die Ressourcen des ausgewählten Typs gefiltert.
 - Aktivieren Sie in der resultierenden Ressourcenliste die Kontrollkästchen neben den einzelnen Ressourcen, die Sie gemeinsam nutzen möchten. Die ausgewählten Ressourcen werden unter Ausgewählte Ressourcen verschoben.

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

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

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

Wählen Sie Vom Kunden verwaltete Berechtigung erstellen aus, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls zum Teilen entspricht. Weitere Informationen finden Sie unter [Eine vom Kunden verwaltete Berechtigung erstellen](#). Wählen Sie



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

 Note

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

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

7. Wählen Sie Weiter.
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. VPC Amazon-Subnetze. Sie können einige [unterstützte Ressourcentypen](#) auch für IAM Rollen und Benutzer freigeben.

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

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

 Important

Wenn Sie Inhalte für eine Organisation oder eine Organisationseinheit freigeben und dieser Bereich auch das Konto umfasst, dem die Ressourcenfreigabe gehört, erhalten alle Prinzipale im Freigabekonto automatisch Zugriff auf die Ressourcen in der Freigabe. Der gewährte Zugriff wird durch die verwalteten Berechtigungen definiert, die mit der Freigabe

verknüpft sind. Dies liegt daran, dass die ressourcenbasierte Richtlinie, die AWS RAM jeder Ressource in der Freigabe zugewiesen ist, verwendet.

"Principal": "*" Weitere Informationen finden Sie unter [Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten 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 einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

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

Note

Die Option „Organisationsstruktur anzeigen“ wird nur angezeigt, wenn „Teilen mit“ aktiviert AWS Organizations ist und Sie beim Verwaltungskonto der Organisation angemeldet sind.

Sie können diese Methode nicht verwenden, um eine Person AWS-Konto außerhalb Ihrer Organisation, eine IAM Rolle oder einen Benutzer anzugeben. Stattdessen müssen Sie die Option Organisationsstruktur anzeigen deaktivieren und in der Dropdownliste und im Textfeld die ID oder eingebenARN.

- Um einen Principal anhand der ID oderARN, einschließlich Principals außerhalb der Organisation, anzugeben, wählen Sie für jeden Prinzipal den Prinzipaltyp aus. Geben

Sie als Nächstes die ID (für eine AWS-Konto Organisation oder Organisationseinheit) oder ARN (für eine IAM Rolle oder einen Benutzer) ein, und klicken Sie dann auf Hinzufügen. Die verfügbaren Haupttypen, IDs und ARN Formate lauten wie folgt:

- **AWS-Konto**— Um eine hinzuzufügen AWS-Konto, geben Sie die 12-stellige Konto-ID ein. Beispielsweise:

```
123456789012
```

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

```
o-abcd1234
```

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

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

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

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

Beispielsweise:

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

 Note

Rufen Sie die [Liste der Rollen in der IAM Konsole auf, verwenden Sie den AWS CLI Befehl get-role oder die GetRole API Aktion, um die eindeutige ARN Rolle](#) abzurufen. IAM

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

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

Beispielsweise:

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

 Note

Um den eindeutigen Namen ARN für einen IAM Benutzer zu erhalten, [rufen Sie die Benutzerliste in der IAM Konsole auf](#) und verwenden Sie den [get-user](#) AWS CLI Befehl oder [GetUser](#)APIAktion.

- Service Principal — Um einen Service Principal hinzuzufügen, wählen Sie Service Principal aus der Dropbox Principtyp auswählen aus. Geben Sie den Namen des AWS Dienstprinzips ein. Verwenden Sie die folgende Syntax:

- `service-id.amazonaws.com`

Beispielsweise:

```
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.

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 der [create-resource-share](#) Befehl. Der folgende Befehl erstellt eine Ressourcenfreigabe, die von allen Mitarbeitern 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 die ARN für den 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 eine Ressourcenfreigabe in AWS RAM

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

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

Note

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

Console

So aktualisieren Sie eine Ressourcenfreigabe

1. Navigieren Sie in der AWS RAM Konsole zur Seite [Von mir geteilt: Ressourcenfreigaben](#).
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt AWS-Regionen, wählen Sie die entsprechende Option AWS-Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus. Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen

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

3. Wählen Sie die gemeinsam genutzte Ressource aus und klicken Sie dann auf Ändern.
4. Schritt 1: Geben Sie Details zur Ressourcenfreigabe an, überprüfen Sie die Details zur Ressourcenfreigabe und aktualisieren Sie bei Bedarf die folgenden Angaben:
 - a. (Optional) Um den Namen der Ressourcenfreigabe zu ändern, bearbeiten Sie Name.
 - b. (Optional) Um der Ressourcenfreigabe eine Ressource hinzuzufügen, wählen Sie unter Ressourcen den Ressourcentyp aus und aktivieren Sie dann das Kontrollkästchen neben der Ressource, um sie der Ressourcenfreigabe hinzuzufügen. Globale Ressourcen werden nur angezeigt, wenn Sie in der die Region auf USA Ost (Nord-Virginia), (us-east-1) setzen AWS 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) Um der Ressourcenfreigabe ein Tag hinzuzufügen, geben Sie unter Tags einen Tag-Schlüssel und einen Tag-Wert in die leeren Textfelder ein. Um mehr als ein Tag-Schlüssel-Wert-Paar hinzuzufügen, wählen Sie Neues Tag hinzufügen aus. Sie können bis zu 50 Tags hinzufügen.
 - e. Um ein Tag aus der Resource Share zu entfernen, suchen Sie unter Tags das Tag und wählen Sie neben dem Tag die Option Entfernen aus.
5. Wählen Sie Weiter.
6. (Optional) In Schritt 2: Ordnen Sie jedem Ressourcentyp eine verwaltete Berechtigung zu, können Sie wählen, ob Sie AWS dem Ressourcentyp eine verwaltete Berechtigung zuordnen, eine bestehende vom Kunden verwaltete Berechtigung auswählen oder Ihre eigene vom Kunden verwaltete Berechtigung erstellen möchten. Weitere Informationen finden Sie unter [Arten von verwalteten Berechtigungen](#).

Sie können auch vom Kunden verwaltete Berechtigung erstellen auswählen, um eine vom Kunden verwaltete Berechtigung zu erstellen, die den Anforderungen Ihres Anwendungsfalls für das Teilen entspricht. Weitere Informationen finden Sie unter [Eine vom Kunden verwaltete Berechtigung erstellen](#). Nachdem Sie den Vorgang abgeschlossen

haben 

wählen Sie und dann können Sie Ihre neue vom Kunden verwaltete Berechtigung aus der Dropdownliste Verwaltete Berechtigungen auswählen.

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

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

 Note

Bis Sie Ihre Änderungen an der Ressourcenfreigabe nach dem letzten Schritt gespeichert haben, können Sie das Versionsupdate abbrechen, indem Sie Auf vorherige Version zurücksetzen klicken. Bei AWS verwalteten Berechtigungen ist die Änderung nach dem Speichern der Ressourcenfreigabe jedoch endgültig und Sie können nicht mehr zur vorherigen Version zurückkehren.

8. Wählen Sie Weiter.
9. Schritt 3: Wählen Sie die Principals aus, die Zugriff haben, überprüfen Sie die ausgewählten Principals und aktualisieren Sie bei Bedarf eines der folgenden Elemente:
 - a. (Optional) Um zu ändern, ob die gemeinsame Nutzung für Prinzipale innerhalb oder außerhalb Ihrer Organisation aktiviert ist, wählen Sie eine der folgenden Optionen:
 - Um Ressourcen mit AWS-Konten oder einzelnen IAM Rollen oder Benutzern außerhalb Ihrer Organisation gemeinsam zu nutzen, wählen Sie Teilen mit externen Prinzipalen zulassen aus.
 - Um die gemeinsame Nutzung von Ressourcen auf Prinzipale in Ihrer Organisation zu beschränken AWS Organizations, wählen Sie Nur gemeinsame Nutzung mit Prinzipalen in Ihrer Organisation zulassen aus.
 - b. Gehen Sie für Principals wie folgt vor:
 - (Optional) Um eine Organisation, eine Organisationseinheit (OU) oder ein Mitglied AWS-Konto innerhalb Ihrer Organisation hinzuzufügen, aktivieren Sie die Option Organisationsstruktur anzeigen, um eine Strukturansicht Ihrer Organisation

anzuzeigen. Aktivieren Sie dann das Kontrollkästchen neben jedem Prinzipal, den Sie hinzufügen möchten.

 **Important**

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

"Principal": "*" Weitere Informationen finden Sie unter [Auswirkungen der Verwendung "Principal": "*" in einer ressourcenbasierten 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 einzelnen Ressourcen im ARNs Resource Share gewähren. Die Berechtigungen in diesen Richtlinien dürfen die in der verwalteten Berechtigung für die Ressourcenfreigabe angegebenen Berechtigungen nicht überschreiten.

 **Note**

Die Option Organisationsstruktur anzeigen wird nur angezeigt, wenn das Teilen mit aktiviert AWS Organizations ist und Sie als Hauptbenutzer im Verwaltungskonto der Organisation angemeldet sind.

Sie können diese Methode nicht verwenden, um eine Person AWS-Konto außerhalb Ihrer Organisation, eine IAM Rolle oder einen Benutzer anzugeben. Stattdessen müssen Sie diese Hauptbenutzer hinzufügen, indem Sie ihre Kennungen eingeben, die im Textfeld unter dem Schalter Organisationsstruktur anzeigen angezeigt werden. Siehe den nächsten Aufzählungspunkt.

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

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

- Andere AWS-Konto (nicht der Besitzer der Ressource) — Macht die Ressource für das andere Konto verfügbar. Der Administrator dieses Kontos muss den Vorgang abschließen, indem er einzelnen Rollen und Benutzern mithilfe identitätsbasierter Berechtigungsrichtlinien Zugriff auf die gemeinsam genutzte Ressource gewährt. Diese Berechtigungen dürfen nicht höher sein als diejenigen, die in den verwalteten Berechtigungen definiert sind, die der Ressourcenfreigabe zugeordnet sind.
- Dieser AWS-Konto (Ressourcenbesitzer) — Alle Rollen und Benutzer im Konto, dem die Ressource gehört, erhalten automatisch den Zugriff, der durch die verwalteten Berechtigungen definiert ist, die der Ressourcenfreigabe zugeordnet sind.
- Der Zusatz wird sofort in der Liste Ausgewählte Hauptbenutzer angezeigt.

Sie können dann weitere Konten oder Ihre Organisation hinzufügen OUs, indem Sie diesen Schritt wiederholen.

- (Optional) Um einen Hauptbenutzer zu entfernen, suchen Sie ihn unter Ausgewählte Hauptbenutzer, aktivieren Sie das entsprechende Kontrollkästchen und wählen Sie dann Abwählen aus.

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

Wenn verwaltete Berechtigungen immer noch andere Versionen als die Standardversion verwenden, haben Sie eine weitere Möglichkeit, dies zu beheben, indem Sie Auf Standardversion aktualisieren klicken.

13. Wählen Sie „Ressourcenfreigabe aktualisieren“, wenn Sie mit den Änderungen fertig sind.

AWS CLI

Um eine Ressourcenfreigabe zu aktualisieren

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

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

```
$ aws ram update-resource-share \
  --region us-east-1 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
  --name "my-renamed-resource-share" \
  --no-allow-external-principals
{
  "resourceShare": {
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
    "name": "my-renamed-resource-share",
    "owningAccountId": "123456789012",
    "allowExternalPrincipals": false,
    "status": "ACTIVE",
    "creationTime": 1565295733.282,
    "lastUpdatedTime": 1565303080.023
  }
}
```

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

```
$ aws ram associate-resource-share \
  --region us-east-1 \
  --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
```

```

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

```

- Verwenden Sie die folgenden Befehle, um eine verwaltete Berechtigung für einen Ressourcentyp in einer Ressourcenfreigabe hinzuzufügen oder zu ersetzen [list-permissions](#) und [associate-resource-share-permission](#). Sie können pro Ressourcentyp in einer Ressourcenfreigabe 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 angeben, da sonst der Befehl mit einem Fehler fehlschlägt.

Der folgende Beispielbefehl listet die vier verwalteten Berechtigungen auf, die ARNs für ein Amazon Elastic Compute Cloud (AmazonEC2) -Subnetz verfügbar sind, und verwendet dann eine davon, ARNs um die aktuell zugewiesene AWS verwaltete Berechtigung für diesen Ressourcentyp in der angegebenen Ressourcenfreigabe zu ersetzen.

```

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

```

```

--resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
--permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
  "returnValue": true
}

```

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

```

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

```

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

```

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

```

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

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

Die Tagging-Befehle erzeugen bei Erfolg keine Ausgabe.

Anzeige Ihrer geteilten Ressourcen in AWS 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 der AWS RAM Konsole die Seite [Von mir geteilt: Geteilte Ressourcen](#).
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt, wählen Sie in der oberen rechten Ecke der Konsole die entsprechende AWS-Region aus der Drop-down-Liste aus. Wenn Sie Ressourcenfreigaben anzeigen möchten, müssen Sie die AWS-Region auf USA Ost (Nord-Virginia), (`us-east-1`) einstellen. Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unter [Gemeinsame 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 `SELF` verwenden, um Details der Ressourcen anzuzeigen, die Sie derzeit gemeinsam nutzen.

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

```
$ aws ram list-resources \
  --region us-east-1 \
  --resource-owner SELF
{
  "resources": [
    {
      "arn": "arn:aws:license-manager:us-east-1:123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
      "type": "license-manager:LicenseConfiguration",
      "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
      "creationTime": "2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
    },
    {
      "arn": "arn:aws:license-manager:us-east-1:123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
      "type": "license-manager:LicenseConfiguration",
      "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
      "creationTime": "2021-07-22T11:48:11.104000-07:00",
      "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
    }
  ]
}
```

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 unter[Gemeinsame 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 eine AWS Ressource zu löschen

Wenn Sie eine AWS 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 der AWS RAM Konsole sichtbar, ihr Status ändert sich jedoch zu Deleted.

Console

Einen Ressourcenfreigabe

1. Öffnen Sie in der AWS RAM Konsole die Seite [Von mir geteilt: Resource Shares](#).
2. Da AWS RAM Ressourcenfreigabe in der Konsole in der rechten oberen Ecke der Konsole die entsprechende AWS-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 die AWS-Region auf USA Ost (Nord-Virginia), (us-east-1) setzen. Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unter [Gemeinsame 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-share](#) Befehl verwenden, um eine Ressourcenfreigabe zu löschen, die Sie nicht mehr benötigen.

Im folgenden Beispiel wird zunächst der [get-resource-shares](#) Befehl 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](#)
- [Für Sie geteilte Ressourcenanteile anzeigen](#)
- [Mit Ihnen geteilte Ressourcen anzeigen](#)
- [Principals anzeigen, die mit dir geteilt wurden](#)
- [Einen Ressourcenanteil hinterlassen](#)

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](#).

- 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.

- 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](#)

- Das folgende Beispiel beginnt mit dem [-get-resource-share-invitations](#)Befehl, 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-
fbf6-4336-8377-06c559dfec49",
```

```

        "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-fbf6-4336-8377-06c559dfec49
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfec49",
    "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 hatACCEPTED.

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 der AWS RAM Konsole zur Seite [Mit mir geteilt: Resource Shares](#).
2. Da AWS RAM es in der oberen rechten Ecke der Konsole die entsprechende AWS-Region aus der rechten oberen Ecke der Konsole auswählen. AWS-Regionen Um Ressourcenfreigaben zu sehen, die globale Ressourcen enthalten, müssen Sie die AWS-Region auf USA Ost (Nord-Virginia), (us-east-1) setzen. Weitere Informationen zur gemeinsamen Nutzung von globalen Ressourcen finden Sie unter [Gemeinsame 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. Die AWS 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 Benutzers AWS-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-shares](#) Befehl mit dem `--resource-owner` Parameter, der auf gesetzt ist `OTHER-ACCOUNTS`.

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

```
$ aws ram get-resource-shares \
  --region us-east-1 \
  --resource-owner OTHER-ACCOUNTS
{
  "resourceShares": [
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
      "name": "Prod Env Shared Licenses",
      "owningAccountId": "111111111111",
      "allowExternalPrincipals": true,
      "status": "ACTIVE",
      "creationTime": "2021-09-21T08:50:41.308000-07:00",
      "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
      "featureSet": "STANDARD"
    }
  ]
}
```

```
    },
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
      "name": "Prod Env Shared Subnets",
      "owningAccountId": "222222222222",
      "allowExternalPrincipals": true,
      "status": "ACTIVE",
      "creationTime": "2021-09-21T08:56:24.737000-07:00",
      "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
      "featureSet": "STANDARD"
    }
  ]
}
```

Mit Ihnen geteilte Ressourcen anzeigen

Sie können die freigegebenen Ressourcen anzeigen, auf die Sie Zugriff haben. Sie können sehen, welche 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 der AWS RAM Konsole zur Seite [Mit mir geteilt: Geteilte Ressourcen](#).
2. Da AWS RAM es in der rechten oberen Ecke der Konsole die entsprechende AWS-Region aus der oberen Ecke der Konsole auswählen. AWS-Regionen Ihre -Konto-Ressource finden Sie, indem AWS-Region Sie die auf () setzen. us-east-1 Weitere Informationen zum Freigeben von globalen Ressourcen finden Sie unter [Gemeinsame 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 angegebenen AWS-Region von einer anderen Ressource zugegriffen werden kann AWS-Konto.

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

Principals anzeigen, die mit 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 unter [Gemeinsame 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 \  
  --output text
```

```

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

```

Einen Ressourcenanteil hinterlassen

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

Voraussetzungen für das Verlassen einer Ressourcenfreigabe

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

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

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

Service	Ressourcentyp
	ec2:DedicatedHost
AWS License Manager	license-manager:LicenseConfiguration
AWS Outposts	ec2:LocalGatewayRouteTable outposts:Outpost outposts:Site
Amazon Route 53	route53resolver:ResolverRule
Amazon VPC	ec2:CoipPool ec2:PrefixList ec2:Subnet ec2:TrafficMirrorTarget ec2:TransitGateway ec2:TransitGatewayMulticastDomain

Wie verlasse ich eine Ressourcenfreigabe

Console

Um eine gemeinsame Nutzung einer Ressource zu verlassen

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

Sie den Wert AWS-Region auf USA Ost (Nord-Virginia), () setzen. us-east-1 Weitere Informationen zur gemeinsamen Nutzung globaler Ressourcen finden Sie unter [Gemeinsame 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

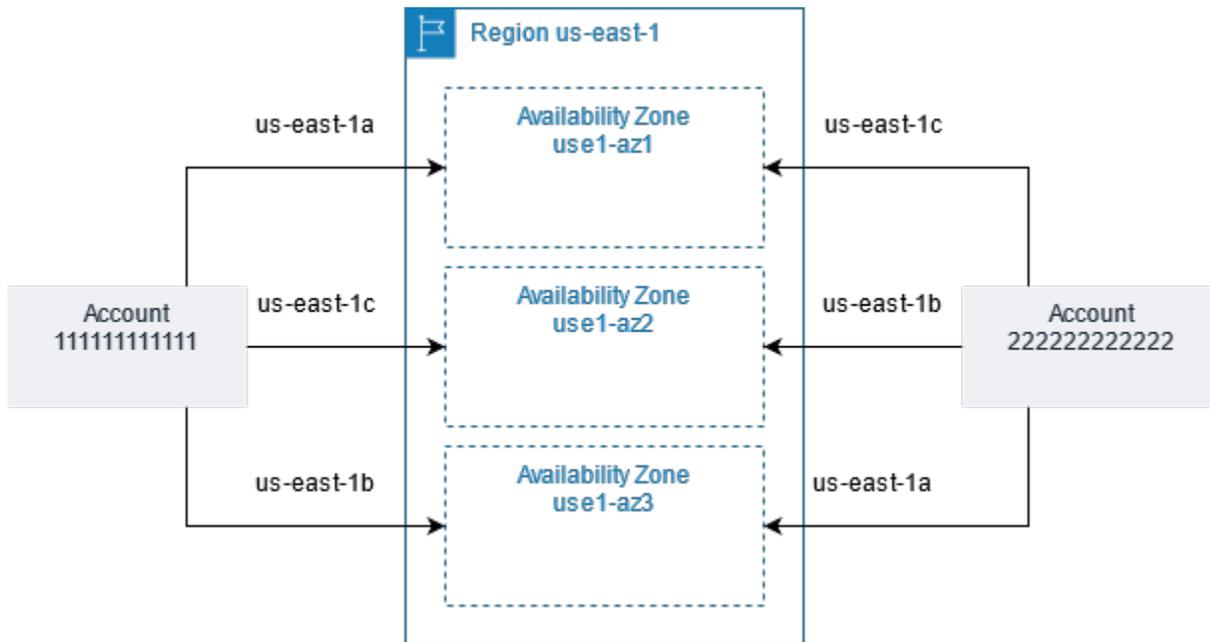
Um eine Ressourcenfreigabe zu verlassen

Sie können den [disassociate-resource-share](#) Befehl verwenden, um eine Ressourcenfreigabe zu verlassen.

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

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

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

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 RAM Konsole](#) zur AWS RAM Konsolenseite.
2. Die aktuellen AZ-IDs können Sie AWS-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 werden AWS-Konto.

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

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

Gemeinsam nutzbare Ressourcen AWS

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

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

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

	 <p>— Sie können Ressourcen dieses Typs nur mit Konten teilen, die Mitglieder derselben Organisation sind.</p>	Nein
<p>Kann vom Kunden verwaltete Berechtigungen verwenden</p>	<p>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.</p>  <p>— Ressourcen dieses Typs unterstützen die Verwendung von vom Kunden verwalteten Berechtigungen.</p>  <p>— Ressourcen dieses Typs unterstützen die Verwendung von vom Kunden verwalteten Berechtigungen nicht.</p>	Ja
<p>Kann mit Service Principals geteilt werden</p>	 <p>— Sie können Ressourcen dieses Typs mit AWS-Services teilen.</p>  <p>— Sie können Ressourcen dieses Typs nicht mit anderen teilen AWS-Services.</p>	Ja Nein

APIAmazon-Gateway

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

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

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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Mesh apppmesh: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.	 N	 Nein

AWS AppSync GraphQL API

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

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
GraphQL API appsync:Apis	Verwalte AWS AppSync GraphQL APIs zentral und teile sie mit anderen AWS-Konten oder deiner Organisation. Auf diese Weise können mehrere Konten gemeinsam AWS AppSync APIs genutzt werden, um ein einheitliches AWS AppSync Merged zu erstellenAPI, das auf Daten aus mehreren Subschemas APIs über verschiedene Konten in derselben Region zugreifen kann. Weitere Informationen finden Sie unter Zusammengeführt APIs im AWS AppSync Entwicklungshandbuch.	 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 seiner 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 AWS-Konten Benutzer einen gemeinsam genutzten, zentral verwalteten DB-Cluster 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 Backup

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

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

Amazon Bedrock

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

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

AWS Billing Service anzeigen

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

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Ansicht „Abrechnung“ billing:billingview	Erstellen und verwalten Sie benutzerdefinierte Abrechnungsansichten zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Inhaber von Anwendungen und Geschäftsbereichen von einem Mitgliedskonto aus auf AWS Ausgaben auf Geschäftseinheitsebene zugreifen. Weitere Informationen finden Sie im AWS Cost Management Benutzerhandbuch unter Steuern des Datenzugriffs für das Kostenmanagement mit Billing View .	 N	 N Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.	 Ja	 Nein

AWS Private Certificate Authority

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 Ihrer Organisation (PKI) und teilen Sie diese CAs mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können AWS Certificate Manager Benutzer mit 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.	 N	 Ja

Amazon DataZone

Sie können die folgenden DataZone Ressourcen mit anderen teilen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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. Auf diese Weise können mehrere Konten DataZone Amazon-Domains erstellen. Weitere Informationen finden Sie unter Was ist Amazon DataZone im DataZone Amazon-Benutzerhandbuch.	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

AWS CloudHSM

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

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

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 seiner 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 <u>Arbeiten mit gemeinsam genutzten Projekten</u> .	 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>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.</p>		AWS-Konto.		

Amazon EC2

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Kapazität sreservierungen</p> <p>ec2:CapacityReservation</p>	<p>Sie können Kapazität sreservierungen zentral erstellen und verwalten und die reservierte Kapazität gemeinsam mit anderen Personen AWS-Konten oder Ihrer Organisation nutzen. Auf diese Weise können mehrere ihre EC2 Amazon-Instances in zentral verwalteten reservierten Kapazitäten AWS-Konten starten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsamen Kapazitätsreservierungen im EC2Amazon-Benutzerhandbuch.</p> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Important</p> <p>Wenn Sie nicht alle Voraussetzungen für das Teilen einer Kapazität</p> </div>	<p> N</p>	<p> Ja</p> <p>Kann mit jedem AWS-Konto geteilt werden.</p>	<p> N</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>sreservierung erfüllen, kann der Vorgang zur gemeinsamen Nutzung fehlschlagen. Wenn dies passiert und ein Benutzer versucht, eine EC2 Amazon-Instance mit dieser Kapazität sreservierung zu starten, wird sie als On-Demand-Instance gestartet, für die höhere Kosten anfallen können. Wir empfehlen Ihnen, zu überprüfen, ob Sie auf die Reservierung für gemeinsame Kapazität</p>				

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

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

[gemeinsamen Nutzung von Ressourcen.](#)

<p>Dedicated Hosts ec2:DedicatedHost</p>	<p>Weisen Sie Amazon 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 EC2 Amazon-Instances auf zentral verwalteten dedizierten Hosts AWS-Konten starten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Dedicated Hosts im EC2Amazon-Benutzerhandbuch.</p>	<p> N</p>	<p> Ja Kann mit jedem geteilt werden AWS-Konto.</p>	<p> N</p>	<p> Nein</p>
----------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 EC2 Amazon-Instances von jedem Konto aus starten, mit dem Sie eine gemeinsame Platzierungsgruppe teilen. Weitere Informationen finden Sie unter Platzierungsgruppe teilen im EC2Amazon-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Nein	 Nein

EC2Image 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Komponenten</p> <p>imagebuilder:Component</p>	<p>Erstellen und verwalten Sie Komponenten zentral und teilen Sie sie mit anderen Personen Ihrer Organisation. Verwalten Sie, wer vordefinierte Build- und Testkomponenten in seinen Image-Rezepten verwenden kann. Weitere Informationen finden Sie unter Freigeben von EC2 Image Builder Builder-Ressourcen im EC2Image Builder Builder-Benutzerhandbuch.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> Ja</p>	<p> Nein</p>
<p>Container-Rezepte</p> <p>imagebuilder:ContainerRecipe</p>	<p>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</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden</p>	<p> Ja</p>	<p> Nein</p>

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	, wer vordefinierte Dokumente verwenden kann, um Container-Image-Builds zu duplizieren. Weitere Informationen finden Sie unter Freigeben von EC2 Image Builder Builder-Ressourcen im EC2Image Builder Builder-Benutzerhandbuch.		AWS-Konto.		

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Bilder</p> <p>imagebuilder:Image</p>	<p>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 Ihrer gesamten Organisation verwenden kann. Weitere Informationen finden Sie unter Freigeben von EC2 Image Builder Builder-Ressourcen im EC2Image Builder Builder-Benutzerhandbuch.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> Ja</p>	<p> Nein</p>

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 festlegen, wer vordefinierte Dokumente zum Duplizieren von AMI Builds verwenden kann. Weitere Informationen finden Sie unter Freigeben von EC2 Image Builder Builder-Ressourcen im EC2Image Builder Builder-Benutzerhandbuch.	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Nein

AWS Endbenutzer-Messaging SMS

Sie können die folgende AWS Endbenutzer-Messaging SMS Ressource gemeinsam nutzen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>OptOutList</p> <p>sms-voice:opt-out-list</p>	<p>Erstellen Sie eine OptOutList und teilen Sie sie mit anderen AWS-Konten in Ihrer Organisation. Sie können das teilen, OptOutList sodass die anderen Anwendungen die Rufnummern anderer Benutzer deaktivieren können, AWS-Konten oder sie können den Status der Telefonnummer des Benutzers überprüfen. Weitere Informationen finden Sie im AWS Endbenutzer-Messaging SMS Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Ressourcen.</p>	<p> N</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> Ja</p>	<p> Nein</p>
<p>PhoneNumber</p> <p>sms-voice:phone-number</p>	<p>Erstelle und verwalte eine Telefonnummer, um sie mit anderen AWS-Konten oder</p>	<p> N</p>	<p> Ja</p>	<p> Ja</p>	<p> Ja</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>deiner Organisation zu teilen. Auf diese Weise können mehrere AWS-Konten Personen Nachrichten unter Verwendung der gemeinsam genutzten Telefonnummer senden. Weitere Informationen finden Sie im AWS Endbenutzer-Messaging SMS Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Ressourcen.</p>		<p>Kann mit jedem geteilt werden AWS-Konto.</p>		

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SenderId sms-voice :sender-id	Erstelle und SenderId verwalte sie und teile sie mit anderen AWS-Konten oder deiner Organisation. Auf diese Weise können mehrere Nachrichten über die gemeinsame Nutzung AWS-Konten senden SenderId. Weitere Informationen finden Sie im AWS Endbenutzer-Messaging SMS Benutzerhandbuch unter Arbeiten mit gemeinsam genutzten Ressourcen .	 N	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Ja	 Ja

Amazon FSx für Open ZFS

Sie können die folgenden Amazon FSx for ZFS Open-Ressourcen mit anderen teilen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
FSx-Volume fsx:Volume	Sie können ZFS Volumes FSx für OpenZfs zentral erstellen und verwalten und sie mit anderen AWS-Konten oder Ihrer Organisation teilen. Auf diese Weise können mehrere Konten die Datenreplikation mithilfe von OpenZfs Snapshots auf gemeinsam genutzten Volumes über FSx APIs CreateVolume oder CopySnapshotAndUpdateVolume durchführen. Weitere Informationen finden Sie unter On-Demand-Datenreplikation im Amazon FSx for ZFS Open-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 seiner 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 Konto übergreifendes Teilen von Datenkatalogtabellen und Datenbanken im AWS Lake Formation Entwicklerhandbuch.	 N	 Ja	 N	 Nein
Datenbanken glue:Database	Erstellen und verwalten Sie Datenkatalogdatenbanken zentral und teilen Sie sie mit AWS-Konten oder Ihrer Organisation	 N	 Ja	 N	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>ion. Datenbanken sind Sammlungen von Datenkatalogtabellen. Auf diese Weise können Benutzer Abfragen ausführen und Jobs extrahieren, transformieren und laden (ETL), 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.</p>		<p>Kann mit jedem geteilt werden AWS-Konto.</p>		

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Tabellen</p> <p><code>glue:Table</code></p>	<p>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 mehrerer Konten verknüpft und abgefragt werden können. Weitere Informationen finden Sie unter AWS Kontenübergreifendes Teilen von Datenkatalogtabellen und Datenbanken im AWS Lake Formation Entwicklerhandbuch.</p>	<p> N</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> N</p>	<p> Nein</p>

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 seiner 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 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Marketplace-Katalogentität <code>aws-marketplace:Entity</code>	Erstellen, verwalten und teilen Sie Entitäten innerhalb AWS-Konten oder innerhalb Ihrer Organisation in AWS Marketplace. Weitere Informationen finden Sie AWS RAM in der AWS Marketplace Catalog API Referenz unter Gemeinsame Nutzung von Ressourcen .	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

AWS Migration Hub Refactor Spaces

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 seiner 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 für Netzwerküberwachung, Schutz und Filterung nutzen. Weitere Informationen finden Sie im AWS Network Firewall Entwicklungshandbuch unter Gemeinsame Nutzung von Firewallrichtlinien und Regelgruppen .	 Ja	 Ja Kann mit jedem geteilt werden AWS-Konto.	 N	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Regelgruppen</p> <p><code>network-firewall:StatefulRuleGroup</code></p> <p><code>network-firewall:StatelessRuleGroup</code></p>	<p>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 Entwicklungshandbuch unter Gemeinsame Nutzung von Firewallrichtlinien und Regelgruppen.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> Nein</p>	<p> Nein</p>

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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Outposts</p> <p>outposts: Outpost</p>	<p>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 in Ihren gemeinsamen, zentral verwalteten Outposts erstellen. Weitere Informationen finden Sie im AWS Outposts Benutzerhandbuch unter Arbeiten mit gemeinsam AWS genutzten Outposts-Ressourcen.</p>	<p> N</p>	<p> N</p> <p>Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.</p>	<p> Ja</p>	<p> Nein</p>
<p>Routing-Tabelle für das lokale Gateway</p> <p>ec2:LocalGatewayRouteTable</p>	<p>Sie können VPC Verknüpfungen zu einem lokalen Gateway zentral erstellen und verwalten und sie für andere Benutzer AWS-Konten in Ihrer Organisation freigeben</p>	<p> N</p>	<p> N</p> <p>Kann nur mit der eigenen AWS-Konten</p>	<p> N</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>. Auf diese Weise können mehrere Konten VPC Verknüpfungen zu einem lokalen Gateway erstellen und die Routentabelle und die Konfiguration der virtuellen Schnittstelle einsehen. Weitere Informationen finden Sie unter Shareable Outpost-Ressourcen im AWS Outposts Benutzerhandbuch.</p>		<p>Organisation geteilt werden.</p>		

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 mit anderen teilen, indem Sie AWS RAM.

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>S3 auf Outpost</p> <p>s3-outposts:Outpost</p>	<p>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.</p>	<p> N</p>	<p> N</p> <p>Kann nur mit AWS-Konten der eigenen Organisation geteilt werden.</p>	<p> Ja</p>	<p> Nein</p>

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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Ansichten</p> <p>resource-explorer-2:View</p>	<p>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.</p>	<p> N</p>	<p> N</p> <p>Kann nur innerhalb AWS-Konten der eigenen Organisation geteilt werden.</p>	<p> N</p>	<p> Nein</p>

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 seiner 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 erstellt wurden AWS License Manager. 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Route 53 Resolver DNS Firewall-Regelgruppen</p> <p><code>route53resolver:FirewallRuleGroup</code></p>	<p>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 Anfragen verwenden, die über Route 53 Resolver gesendet werden. Weitere Informationen finden Sie unter Gemeinsame Nutzung von Route DNS 53-Resolver-Firewall-Regelgruppen AWS-Konten im Amazon Route 53-Entwicklerhandbuch.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem AWS-Konto geteilt werden.</p>	<p> Nein</p>	<p> Nein</p>

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 Anfragen von ihren virtuellen privaten Clouds (VPCs) an die Ziel-IP-Adressen weiterleiten, die in gemeinsamen, zentral verwalteten Resolver-Regeln definiert sind. Weitere Informationen finden Sie unter Resolver-Regeln mit anderen teilen AWS-Konten und gemeinsame Regeln verwenden im Amazon Route 53 Developer Guide.	 N	 Ja Kann mit jedem AWS-Konto geteilt werden.	 N	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Logs abfragen</p> <p><code>route53resolver:ResolverQueryLogConfig</code></p>	<p>Erstellen und verwalten Sie Abfrageprotokolle zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere DNS Abfragen AWS-Konten , die ihren Ursprung in ihrem eigenen Abfrageprotokoll haben VPCs, 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.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem AWS-Konto geteilt werden.</p>	<p> Ja</p>	<p> Nein</p>

Amazon Application Recovery Controller (ARC)

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>ARC-Cluster</p> <p><code>route53-recovery-control:Cluster</code></p>	<p>Sie können ARC Cluster zentral erstellen und verwalten und sie gemeinsam mit anderen Personen AWS-Konten oder Ihrer Organisation nutzen. Auf diese Weise können mehrere Konten Control Panels und Routing-Kontrollen in einem einzigen gemeinsamen 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 Applicati</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> Ja</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	on Recovery Controller (ARC) Developer Guide.				

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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Zugangsschlüsse <code>s3:AccessGrants</code>	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.	 Ja	 Ja Kann mit jedem AWS-Konto geteilt werden.	 Ja	 Ja

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	Weitere Informationen finden Sie im Amazon Simple Storage Service Benutzerhandbuch unter S3 Access gewährt kontoübergreifenden Zugriff.				

Amazon SageMaker KI

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

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
SageMaker KI-Katalog <code>sagemaker:sagemakerCatalog</code>	Aus Gründen der Auffindbarkeit — ermöglicht es Kontoinhabern, anderen Konten für alle Featuregruppen-Ressourcen im SageMaker	 Nein	 Ja Kann mit jedem AWS-	 Ja	 Nein

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>AI-Katalog Auffindbarkeitsberechtigungen zu gewähren. Sobald der Zugriff gewährt wurde, können Benutzer dieser Konten die Funktionsgruppen, die mit ihnen geteilt wurden, im Katalog einsehen. Weitere Informationen finden Sie unter Auffindbarkeit und Zugriff auf kontoübergreifende Funktionsgruppen im Amazon SageMaker AI Developer Guide.</p> <div data-bbox="399 1335 743 1745" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Auffindbarkeit und Zugriff sind separate Berechtigungen in KI. SageMaker</p> </div>		Konto geteilt werden.		

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>SageMaker Gruppe „AI-Funktionen“</p> <p>sagemaker:FeatureGroup</p>	<p>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 AI Developer Guide.</p> <div data-bbox="402 1541 743 1818" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Auffindbarkeit und Zugriff sind separate Berechtig</p> </div>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem AWS-Konto geteilt werden.</p>	<p> Ja</p>	<p> Nein</p>

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

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

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

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

Amazon SageMaker AI Developer Guide.

SageMaker AI Model Registry Modellpaketgruppe <code>sagemaker:model-package-group</code>	Mit Amazon SageMaker AI Model Registry können Sie sie <code>sagemaker:model-package-group</code> zentral erstellen und verwalten und mit anderen teilen, AWS-Konten um Modellversionen zu registrieren. Weitere Informationen finden Sie unter Amazon SageMaker AI Model Registry im Amazon SageMaker AI Developer Guide.	 Ja	 Ja	 Ja	 Nein
---------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------

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

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

AWS Service Catalog AppRegistry

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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	 Nein	 Nein Kann nur mit AWS-	 Ja	 Nein

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>Ihrer gesamten AWS Umgebung zu verfolgen. Teilen Sie die Anwendung mit anderen AWS-Konten 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.</p>		<p>Konten der eigenen Organisation geteilt werden.</p>		

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Attribut-Gruppe <code>servicecatalog:AttributeGroup</code>	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.	 Nein	 Nein 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Kontakte</p> <p>ssm-contacts:Contact</p>	<p>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.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> Ja</p>	<p> Nein</p>
<p>Reaktionspläne</p> <p>ssm-incidents:ResponsePlan</p>	<p>Erstellen und verwalten Sie Reaktionspläne zentral und teilen Sie sie mit anderen AWS-</p>	<p> Ja</p>	<p> Ja</p>	<p> Ja</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>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.</p>		<p>Kann mit jedem geteilt werden AWS-Konto.</p>		

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 seiner 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 Benutzerinformationen 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 seiner 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 (AmazonVPC) -Ressourcen gemeinsam nutzen, indem Sie AWS RAM.

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

Kundeneigene Adressen IPv4
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



N



Nein

Kann nur AWS-Konten mit der eigenen Organisation geteilt werden.

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Pools des IP-Adress-Managers (IPAM) ec2:IpamPool	Teilen Sie VPC IPAM Amazon-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 Prinzipale AWS Ressourcen CIDRs aus dem Pool zuweisen, z. B. VPCs in ihren jeweiligen Konten. Weitere Informationen finden Sie AWS RAM im Amazon VPC IP Address Manager-Benutzerhandbuch unter Freigeben eines IPAM Pools mithilfe .	 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Erkennung von Ressourcen im IP Address Manager (IPAM)</p> <p><code>ec2:IpamResourceDiscovery</code></p>	<p>Teilen Sie Ressourcenenntdeckungen mit anderen AWS-Konten. Eine Ressourcensuche ist eine VPC IPAM Amazon-Komponente, die es ermöglicht, Ressourcen IPAM zu verwalten und zu überwachen, die zum Eigentümerkonto gehören. Weitere Informationen finden Sie unter Arbeiten mit Ressourcenentdeckungen im VPCIPAM Amazon-Benutzerhandbuch.</p>	<p> N</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> N</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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. Auf diese Weise können mehrere Präfixlisten in ihren Ressourcen AWS-Konten referenzieren, z. B. in VPC Sicherheitsgruppen und Subnetz-Routing-Tabellen. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Präfixlisten im VPCAmazon-Benutzerhandbuch.	 Nein	 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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Subnetze <code>ec2:Subnet</code>	Erstellen und verwalten Sie Subnetze zentral und geben Sie sie AWS-Konten innerhalb Ihrer Organisation frei. Auf diese Weise können AWS-Konten mehrere Benutzer ihre Anwendung ressourcen zentral verwaltenVPCs. Zu diesen Ressourcen gehören EC2 Amazon-Instances, Amazon Relational Database Service (RDS) - Datenbanken, Amazon Redshift Redshift-Cluster und AWS Lambda Funktionen. Weitere Informationen finden Sie unter Arbeiten mit VPC Teilen im VPCAmazon-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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p> Note</p> <p>Um bei der Erstellung einer Ressourcennfreigabe ein Subnetz einzubeziehen, benötigen Sie zusätzlich zu <code>ram:CreateResourceShare</code> die <code>ec2:DescribeVpcs</code> Berechtigungen <code>ec2:DescribeSubnets</code> und Standard-Subnetze können nicht gemeinsam genutzt werden. Sie können nur Subnetze teilen, die Sie selbst erstellt haben.</p>				

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

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Ziele von Traffic Mirror</p> <p><code>ec2:TrafficMirrorTarget</code></p>	<p>Erstellen und verwalten Sie Traffic-Mirror-Ziele zentral und teilen Sie sie mit anderen AWS-Konten Personen 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.</p>	<p> N</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden. AWS-Konto</p>	<p> N</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
Transit Gateways ec2:TransitGateway	Erstellen und verwalten Sie Transit-Gateways zentral und teilen Sie sie mit anderen AWS-Konten oder Ihrer Organisation. Auf diese Weise können mehrere AWS-Konten Personen den Verkehr zwischen ihren VPCs und lokalen Netzwerken über ein gemeinsam genutztes, zentral verwaltetes Transit-Gateway weiterleiten. Weitere Informationen finden Sie unter Gemeinsame Nutzung eines Transit-Gateways in den Amazon VPC Transit Gateways.	 Nein	 Ja Kann mit jedem geteilt werden AWS-Konto.	 Nein	 Nein
<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Um bei der Erstellung einer gemeinsamen Nutzung von Ressource</p> </div>					

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>n ein Transit-Gateway einzubeziehen, benötigen Sie zusätzlich zu <code>ram:CreateResourceShare</code> die <code>ec2:DescribeTransitGateway</code> entsprechende Berechtigung.</p>				

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Transit-Gateway-Multicast-Domänen</p> <p><code>ec2:TransitGatewayMulticastDomain</code></p>	<p>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.</p>	<p> N</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden. AWS-Konto</p>	<p> N</p>	<p> Nein</p>

Ressourcentyp und -code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner 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 geteilt werden AWS-Konto.	 Nein	 Nein

VPCAmazon-Gitter

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 seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>Amazon VPC Lattice-Dienst</p> <p><code>vpc-lattice:Service</code></p>	<p>Erstellen und verwalten Sie Amazon VPC Lattice-Dienste zentral und teilen Sie sie mit Einzelpersonen AWS-Konten oder Ihrer Organisation. Auf diese Weise können Servicebetreiber die service-to-service Kommunikation in einer Umgebung mit mehreren Konten verbinden, sichern und beobachten. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten Ressourcen im VPCLattice-Benutzerhandbuch.</p>	<p> Nein</p>	<p> Ja</p> <p>Kann mit jedem AWS-Konto geteilt werden.</p>	<p> Ja</p>	<p> Nein</p>
<p>Amazon VPC Lattice-Service-Netzwerk</p> <p><code>vpc-lattice:ServiceNetwork</code></p>	<p>Erstellen und verwalten Sie Amazon VPC Lattice-Service-Netzwerke zentral und teilen Sie sie mit Einzelpersonen AWS-</p>	<p> Nein</p>	<p> Ja</p> <p>Kann mit jedem AWS-</p>	<p> Ja</p>	<p> Nein</p>

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
	<p>Konten oder Ihrer Organisation. Auf diese Weise können Besitzer von Servicetzwerken 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.</p>		<p>Konto geteilt werden.</p>		

AWS Wolke WAN

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

Ressourcentyp und Code	Anwendungsfall	Kann mit IAM Benutzern und Rollen geteilt werden	Kann mit Konten außerhalb seiner Organisation teilen	Kann vom Kunden verwaltete Berechtigungen verwenden	Kann mit Service Principals teilen
<p>WANCloud-Kernnetzwerk</p> <p><code>networkmanager:CoreNetwork</code></p>	<p>Erstellen und verwalten Sie ein WAN Cloud-Core-Netzwerk zentral und teilen Sie es mit anderen AWS-Konten. Auf diese Weise können mehrere Hosts in einem einzigen WAN Cloud-Core-Netzwerk AWS-Konten aufrufen und bereitstellen. Weitere Informationen finden Sie im AWS WANCloud-Benutzerhandbuch unter Ein Kernnetzwerk gemeinsam nutzen.</p>	<p> Ja</p>	<p> Ja</p> <p>Kann mit jedem geteilt werden AWS-Konto.</p>	<p> N</p>	<p> Nein</p>

Sie können die Liste der verfügbaren verwalteten Berechtigungen jederzeit abrufen. Weitere Informationen finden Sie unter [Verwaltete Berechtigungen anzeigen](#).

Themen

- [Verwaltete Berechtigungen anzeigen](#)
- [Vom Kunden verwaltete Berechtigungen erstellen und verwenden in AWS RAM](#)
- [Aktualisierung AWS verwalteter Berechtigungen auf eine neuere Version](#)
- [Überlegungen zur Verwendung von vom Kunden verwalteten Berechtigungen in AWS RAM](#)
- [So funktionieren verwaltete Berechtigungen](#)
- [Arten von verwalteten Berechtigungen](#)

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 der AWS RAM Konsole.

Console

Einzelheiten zu den verwalteten Berechtigungen finden Sie unter AWS RAM

1. Navigieren Sie in der AWS RAM Konsole zur Seite [Bibliothek für verwaltete Berechtigungen](#).
2. Da es bestimmte AWS RAM Ressourcenfreigaben gibt, wählen Sie die entsprechende AWS-Region aus der Dropdownliste oben rechts in der Konsole aus. Zum Anzeigen von Ressourcenanteilen, die globale Ressourcen enthalten, müssen Sie die AWS-Region auf USA Ost (Nord-Virginia), (us-east-1) setzen. Weitere Informationen über das Teilen globaler Ressourcen finden Sie unter [Gemeinsame Nutzung regionaler Ressourcen im Vergleich zu globalen Ressourcen](#). Zwar haben alle Regionen dieselben verfügbaren AWS verwalteten Berechtigungen, dies wirkt sich jedoch auf die Anzahl der zugehörigen Ressourcenanteile aus, die für jede verwaltete Berechtigung in angezeigt werden [Step 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 eine AWS 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** — Die AWS-Konto Nummer des Resource Share-Besitzers.
 - **Externe Auftraggeber zulassen** — Ob diese Ressourcennutzung die gemeinsame Nutzung mit Prinzipalen außerhalb der Organisation ermöglicht AWS 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 — Der AWS 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 für AWS 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 unter [AWS RAM](#)

Sie können den [list-permissions](#) Befehl verwenden, um eine Liste der verwalteten Berechtigungen abzurufen, die für Ressourcenfreigaben in der aktuellen Version AWS-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\t\"Effect\": \"Allow\",\n\t\t\"Action\": [\n\t\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\t\"ec2:GetIpamPoolCidrs\",\n\t\t\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\t\"ec2:AssociateVpcCidrBlock\",\n\t\t\t\"ec2:CreateVpc\",\n\t\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t\t\"ec2:ReleaseIpamPoolAllocation\"\n\t\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 in AWS RAM

AWS Resource Access Manager (AWS RAM) stellt mindestens eine AWS 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 bereitgestellten AWS verwalteten Berechtigungen nicht funktioniert, können Sie Ihre eigene vom Kunden verwaltete Berechtigung erstellen.

Kundenverwaltete Berechtigungen sind verwaltete Berechtigungen, die Sie erstellen und verwalten, indem Sie genau angeben, welche Aktionen unter welchen Bedingungen mit gemeinsam genutzten Ressourcen ausgeführt werden können AWS RAM. Sie möchten beispielsweise den Lesezugriff für Ihre Amazon VPC IP Address Manager (IPAM) -Pools einschränken, die Ihnen helfen, Ihre IP-Adressen in großem Umfang zu verwalten. Sie können 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](#)
- [Erstellen Erstellen Sie eine vom Kunden verwalteten Richtlinie, d. h. es werden keine Kunden verwalteten Richtlinie](#)
- [Wählen Sie eine andere Version als Standard für eine vom Kunden verwaltete Berechtigung](#)
- [Eine vom Kunden verwaltete Berechtigungsversion löschen](#)
- [Eine vom Kunden verwaltete Berechtigung löschen](#)

Eine vom Kunden verwaltete Berechtigung erstellen

Vom Kunden verwaltete Berechtigungen sind spezifisch für ein AWS-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 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-version](#) Vorgang 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-version](#)Vorgang 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-versions](#)Vorgang 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-versions](#)Vorgang 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-versions](#)es 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 Bestätigungsdiaologfeld 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"
}
```

Aktualisierung AWS verwalteter Berechtigungen auf eine neuere Version

AWS aktualisiert gelegentlich die AWS verwalteten Berechtigungen, die für das Anhängen an eine Ressourcenfreigabe für einen bestimmten Ressourcentyp verfügbar sind. Wenn AWS dies der Fall ist, wird eine neue Version der AWS 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 einer AWS verwalteten Berechtigung zu aktualisieren

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

Der folgende Beispielbefehl gibt beispielsweise Details für jede Ressourcenfreigabe zurück, die die standardmäßige AWS verwaltete Berechtigung für Amazon EC2-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, welche AWS 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 in AWS RAM

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

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

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

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

- Bedingungsschlüssel, die verwendet werden, um den Zugriff für Dienstprinzipale einzuschränken:
 - `aws:SourceArn`
 - `aws:SourceAccount`
 - `aws:SourceOrgPaths`
 - `aws:SourceOrgID`
- System-Tags:
 - `aws:PrincipalTag/aws:`
 - `aws:ResourceTag/aws:`
 - `aws:RequestTag/aws:`

Note

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

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 Ihre AWS 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, eine AWS 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 `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 der AWS Management Console oder eine Operation in der AWS Command Line Interface (AWS CLI) oder AWS API sein. Die Aktionen werden durch die AWS Berechtigung definiert. Weitere Informationen finden Sie unter [Aktion](#) im IAM-Benutzerhandbuch.

Bedingung

Wann und wie ein Principal mit einer Ressource in 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 [AWS Globale Bedingungskontextschlüssel](#) Principal -Schlüssel. Weitere Informationen zu dienstspezifischen Bedingungen finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste](#) in der Service Authorization-Referenz.

Note

Bedingungen sind für vom Kunden verwaltete Berechtigungen und unterstützte Ressourcentypen für AWS verwaltete Berechtigungen verfügbar.

Informationen zu Bedingungen, die von der Verwendung mit vom Kunden verwalteten Berechtigungen ausgeschlossen sind, finden Sie unter [Überlegungen zur Verwendung von vom Kunden verwalteten Berechtigungen in AWS 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 derAWS verwalteten Standardberechtigungen verwenden das folgende Format:AWSRAMDefaultPermission*ShareableResourceType*. Für den`ec2:Subnet` Ressourcentyp lautet der Name der standardmäßigenAWS verwalteten Berechtigung beispielsweiseAWSRAMDefaultPermissionSubnet.

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, 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 (ReadundWrite) 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

Alle AWS Dienste, die damit arbeiten, AWS RAM unterstützen mindestens eine verwaltete Standardberechtigung. Sie können die jeweils verfügbaren Berechtigungen AWS-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 Ressourcenfreigabe AWS 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 können AWS RAM. Sie möchten beispielsweise den Lesezugriff für Ihre Amazon VPC IP Address Manager (IPAM) -Pools einschränken, die Ihnen helfen, Ihre IP-Adressen in großem Umfang zu verwalten. Sie können 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

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

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

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

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

Themen

- [Datenschutz in AWS RAM](#)
- [Identitäts- und Zugriffsmanagement für AWS RAM](#)
- [Einloggen und Überwachen AWS RAM](#)
- [Ausfallsicherheit in AWS RAM](#)
- [Infrastruktursicherheit in AWS RAM](#)
- [Zugriff AWS Resource Access Manager mithilfe eines Schnittstellenendpunkts \(AWS PrivateLink\)](#)

Datenschutz in AWS RAM

Das [Modell der AWS gemeinsamen Verantwortung](#) und geteilter Verantwortung gilt für den Datenschutz in AWS Resource Access Manager. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie im [Abschnitt Datenschutz FAQ](#). Informationen zum Datenschutz in Europa finden Sie im [AWS Shared Responsibility Model und](#) im GDPR Blogbeitrag auf dem AWS Security Blog.

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

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

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole arbeiten AWS RAM oder sie anderweitig AWS-Services verwenden, API, AWS CLI oder. AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn

Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen in den angebenURL, um Ihre Anfrage an diesen Server zu überprüfen.

Identitäts- und Zugriffsmanagement für AWS RAM

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

Themen

- [Wie AWS RAM funktioniert mit IAM](#)
- [AWS Von verwaltete Richtlinien für AWS RAM](#)
- [Verwenden von serviceverknüpften Rollen für AWS RAM](#)
- [Beispiel-IAM-Richtlinien für AWS RAM](#)
- [Beispiele für Dienststeuerungsrichtlinien für AWS Organizations und AWS RAM](#)
- [Deaktivieren der Ressourcenfreigabe mit AWS Organizations](#)

Wie AWS RAM funktioniert mit IAM

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

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

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, IAM die über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Folgen Sie den Anweisungen [unter Erstellen einer Rolle für einen externen Identitätsanbieter \(Verband\)](#) im IAMBenutzerhandbuch.

- IAMBenutzer:
 - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen [unter Eine Rolle für einen IAM Benutzer erstellen](#) im IAMBenutzerhandbuch.
 - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Folgen Sie den Anweisungen [unter Hinzufügen von Berechtigungen für einen Benutzer \(Konsole\)](#) im IAMBenutzerhandbuch.

AWS RAM bietet mehrere AWS verwaltete Richtlinien, die Sie verwenden können, um den Bedürfnissen vieler Benutzer gerecht zu werden. Weitere Informationen dazu finden Sie unter [AWS Von verwaltete Richtlinien für AWS RAM](#).

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

Die folgenden Abschnitte enthalten AWS RAM spezifische Informationen zum Erstellen einer IAM Berechtigungsrichtlinie.

Inhalt

- [Richtlinienstruktur](#)
 - [Auswirkung](#)
 - [Aktion](#)
 - [Ressource](#)
 - [Bedingung](#)

Richtlinienstruktur

Eine IAM Berechtigungsrichtlinie ist ein JSON Dokument, das die folgenden Aussagen enthält: Wirkung, Aktion, Ressource und Bedingung. Eine IAM Richtlinie hat in der Regel die folgende Form.

```
{
```

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

Auswirkung

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

Aktion

Die Aktionserklärung gibt die AWS RAM API Aktionen an, für die die Richtlinie die Genehmigung zulässt oder verweigert. Eine vollständige Liste der zulässigen Aktionen finden Sie AWS Resource Access Manager im IAM Benutzerhandbuch unter [Definierte Aktionen von](#).

Ressource

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

Bedingung

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

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

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

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

AWS Von verwaltete Richtlinien für AWS RAM

AWS Resource Access Manager bietet derzeit mehrere AWS RAM verwaltete 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 für AWS RAM die 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. AWS aktualisiert 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 gehören AWS-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 Ihres AWS-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 der AWS-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

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

Diese Richtlinie bietet AWS RAM mit schreibgeschütztem Zugriff auf die Struktur Ihrer Organisation. Wenn Sie die Integration aktivieren zwischen AWS RAM und AWS Organizations, AWS RAM erstellt automatisch eine dienstverknüpfte Rolle mit dem Namen [AWSServiceRoleForResourceAccessManager](#) dass 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 der AWS RAM Konsole.

Dies geschieht, indem es eine schreibgeschützte Berechtigung zum Ausführen von `organizations:Describe` und `organizations:ListOperations`, 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, und AWS-Konten zu sehen.

```
{
  "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 Änderungsverfolgung gestartet	AWS RAM dokumentierte die bestehenden Richtlinien und begann, Änderungen zu verfolgen.	16. September 2021

Verwenden von serviceverknüpften Rollen für AWS RAM

AWS Resource Access Manager verwendet [serviceverknüpfte Rollen](#) von AWS 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 -AWS Services 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 aktivieren AWS 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 Console oder die [EnableSharingWithAwsOrganization](#) in Ihrem Konto mithilfe der AWS CLI oder einer AWS API ausführen, AWS RAM erstellt die serviceverknüpfte Rolle für Sie.

Rufen Sie `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 teilen AWS-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 Richtlinien zur Dienststeuerung (SCPs). SCPs sind Richtlinien, die Sie an Elemente in einer Organisation anhängen, um Berechtigungen innerhalb dieser Organisation zu verwalten. Eine SCP gilt für alle AWS-Konten [unter dem Element, an das Sie das anhängen SCP](#). SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation. Sie können Ihnen dabei helfen, sicherzustellen, dass Sie die Richtlinien Ihrer Organisation für die Zugriffskontrolle einhalten. AWS-Konten Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.

Voraussetzungen

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

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

Beispiel für Service-Kontrollrichtlinien

Inhalt

- [Beispiel 1: Externes Teilen verhindern](#)
- [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

Im Folgenden SCP wird verhindert, dass Benutzer Ressourcenfreigaben erstellen, die die gemeinsame Nutzung mit Prinzipalen ermöglichen, die sich außerhalb der Organisation des teilenden 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

Im Folgenden SCP wird verhindert, dass alle Benutzer in einem betroffenen Konto eine Einladung zur Nutzung einer Ressourcenfreigabe annehmen. Ressourcenfreigaben, die für andere Konten in derselben Organisation wie das Sharing-Konto freigegeben wurden, generieren keine Einladungen und sind daher davon nicht betroffen SCP.

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

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

Im Folgenden SCP sind nur Konten 111111111111 und 222222222222 das Erstellen neuer Ressourcenfreigaben mit gemeinsamen EC2 Amazon-Präfixlisten oder das Zuordnen von Präfixlisten zu bestehenden Ressourcenfreigaben zulässig.

```
{
  "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

Im Folgenden SCP wird verhindert, dass Benutzer gemeinsam genutzte Ressourcen für die gesamte Organisation oder für beliebige Organisationseinheiten erstellen. Benutzer können Inhalte mit einzelnen AWS-Konten Personen 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

Im folgenden Beispiel SCP können Benutzer Ressourcen nur mit der o-12345abcdef, Organisationseinheit ou-98765fedcba der Organisation und AWS-Konto 111111111111 gemeinsam nutzen.

```

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

```

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 deaktivieren AWS 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 deaktivieren AWS Organizations, werden Prinzipale innerhalb Ihrer Organisation aus allen Ressourcenfreigaben entfernt und verlieren den Zugriff auf diese gemeinsam genutzten Ressourcen.

2. Verwenden Sie die IAM-Konsole AWS 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.

Einloggen und Überwachen AWS RAM

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

Amazon EventBridge

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

AWS CloudTrail

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

erfolgten. Weitere Informationen finden Sie unter [Protokollierung von AWS RAM-API-Aufrufen mit AWS CloudTrail](#).

Überwachung AWS RAM mit EventBridge

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

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

Note

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

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Beispiel: Warnung bei Fehlern bei der gemeinsamen Nutzung von Ressourcen

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

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

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

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

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

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

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

12. Vergewissern Sie sich, dass Ihre neue Regel wieder auf der Seite Regeln als Aktiviert markiert ist. Wählen Sie bei Bedarf das Optionsfeld neben Ihrem Regelnamen und wählen Sie dann Aktivieren aus.

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

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

Protokollierung von AWS RAM-API-Aufrufen mit AWS CloudTrail

AWS RAM ist in integriert AWS CloudTrail, einen Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS -Service durchgeführten Aktionen bereitstellt AWS RAM. CloudTrail erfasst alle API-Aufrufe für AWS 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, aktivieren AWS 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 CloudTrail Benutzerhandbuch](#).

AWS RAM Informationen in CloudTrail

CloudTrail wird AWS-Konto beim Erstellen Ihres für Sie aktiviert. Die in AWS RAM auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderen AWS -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 andere AWS -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](#)

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

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

- AWS-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](#).

Infrastruktursicherheit in AWS RAM

Als verwalteter Dienst AWS Resource Access Manager ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

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

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Zugriff AWS Resource Access Manager mithilfe eines Schnittstellenendpunkts (AWS PrivateLink)

Sie können Folgendes verwenden ... AWS PrivateLink um eine private Verbindung zwischen deinem VPC und herzustellen AWS Resource Access Manager. Sie können darauf zugreifen AWS RAM als ob es in Ihrem wäreVPC, ohne die Verwendung eines Internet-Gateways, NAT Geräts, einer VPN Verbindung oder AWS Direct Connect Verbindung. Für den Zugriff auf Ihre Instanzen sind VPC keine öffentlichen IP-Adressen erforderlich AWS RAM.

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

Weitere Informationen finden Sie unter Access [AWS-Services durch AWS PrivateLink](#) in der AWS PrivateLink Führer.

Überlegungen zu AWS RAM

Bevor Sie einen Schnittstellenendpunkt einrichten für AWS RAM, lesen Sie [Überlegungen](#) im AWS PrivateLink Leitfadens.

AWS RAM unterstützt das Aufrufen all seiner API Aktionen über den Schnittstellenendpunkt.

VPCEndpunktrichtlinien werden unterstützt für AWS RAM. Standardmäßig voller Zugriff auf AWS RAM ist über den Schnittstellenendpunkt erlaubt.

Erstellen Sie einen Schnittstellenendpunkt für AWS RAM

Sie können einen Schnittstellenendpunkt erstellen für AWS RAM entweder mit der VPC Amazon-Konsole oder dem AWS Command Line Interface (AWS CLI). Weitere Informationen finden Sie unter [Erstellen eines Schnittstellenendpunkts](#) in der AWS PrivateLink Leitfadens.

Erstellen Sie einen Schnittstellenendpunkt für AWS RAM mit dem folgenden Dienstnamen:

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

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

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM Ressource, die Sie an einen Schnittstellenendpunkt anhängen können. Die standardmäßige Endpunktrichtlinie ermöglicht vollen Zugriff auf AWS RAM über den Endpunkt der Schnittstelle. Um den Zugriff zu kontrollieren, der erlaubt ist AWS RAM Fügen Sie von Ihrem VPC dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

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

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf Dienste mithilfe von Endpunktrichtlinien](#) in der AWS PrivateLink Leitfadens.

Beispiel: VPC Endpunktrichtlinie für AWS RAM actions

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

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

Behebung von Problemen mit AWS RAM

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

Themen

- [Fehler: „Ihre Konto-ID ist in einer AWS Organisation nicht vorhanden“](#)
- [Fehler: "AccessDeniedException"](#)
- [Fehler: "UnknownResourceException"](#)
- [Fehler beim Versuch, Inhalte mit Konten außerhalb meiner Organisation zu teilen](#)
- [Geteilte Ressourcen werden im Zielkonto nicht angezeigt](#)
- [Fehler: Limit überschritten](#)
- [Das andere Konto in meiner Organisation erhält nie eine Einladung](#)
- [Sie können ein VPC Subnetz nicht gemeinsam nutzen](#)

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

Szenario

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

Ursache

Dieser Fehler kann auftreten, wenn die serviceverknüpfte Rolle [AWSServiceRoleForResourceAccessManager](#) nicht erfolgreich erstellt wurde, wenn Sie die Integration zwischen AWS Resource Access Manager und AWS Organizations aktivieren.

Lösung

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

Important

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

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

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

Fehler: "AccessDeniedException"

Szenario

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

Ursache

Dieser Fehler kann auftreten, wenn Sie versuchen, eine Ressourcenfreigabe zu erstellen, obwohl Sie nicht über die erforderlichen Berechtigungen verfügen. Dies kann durch unzureichende Berechtigungen in Richtlinien verursacht werden, die Ihrem Prinzipal AWS Identity and Access Management (IAM) zugeordnet sind. Dies kann auch aufgrund von Einschränkungen aufgrund einer AWS Organizations Dienststeuerungsrichtlinie (SCP) geschehen, die sich auf Ihren auswirkt AWS-Konto.

Lösung

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

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, IAM die über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Folgen Sie den Anweisungen [unter Erstellen einer Rolle für einen externen Identitätsanbieter \(Verband\)](#) im IAMBenutzerhandbuch.

- IAMBenutzer:

- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen [unter Eine Rolle für einen IAM Benutzer erstellen](#) im IAMBenutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Folgen Sie den Anweisungen [unter Hinzufügen von Berechtigungen für einen Benutzer \(Konsole\)](#) im IAMBenutzerhandbuch.

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

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

- `ram:CreateResourceShare`
- `ram:AssociateResourceShare`

Um eine Ressourcenfreigabe anzuzeigen, benötigen Sie die folgende Berechtigung:

- `ram:GetResourceShares`

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

- `resourceOwneringService:PutPolicyAction`

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

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

```
{
  "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 AWS Organizations mithilfe der [Organisationskonsole oder des Organizations EnableAWSServiceAccess](#) aktivieren, API anstatt [die AWS RAM Konsole zu verwenden](#). Wenn Sie die Integration mithilfe der Organisationskonsole oder aktivierenAPI, erstellt der Dienst die `AWSServiceRoleForResourceAccessManager` Rolle nicht in Ihrem Konto. Diese Rolle ist erforderlich, um auf Informationen über Ihre Organisation zuzugreifen. Da die Rolle nicht erstellt wurde, AWS RAM kann nicht auf Details zu den Konten oder Organisationseinheiten (OUs) in Ihrer Organisation zugegriffen werden.

Lösung

Um das Problem zu beheben, deaktivieren Sie die Integration zwischen AWS RAM und AWS Organizations. Schalten Sie es dann wieder ein, indem Sie den AWS RAM [EnableSharingWithAwsOrganization](#) API Vorgang aufrufen oder mit AWS Management Console dem die folgenden Schritte ausführen.

Important

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

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

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

Fehler beim Versuch, Inhalte mit Konten außerhalb meiner Organisation zu teilen

Szenario

Wenn Sie versuchen, Ressourcen mit Konten außerhalb Ihrer Organisation zu teilen, wird einer der folgenden Fehler angezeigt:

- „Sie können die Ressource nicht außerhalb Ihrer Organisation gemeinsam nutzen.“
- „Die Ressource, die Sie teilen möchten, kann nur innerhalb Ihrer AWS Organisation gemeinsam genutzt werden.“
- "InvalidParameterException: Die Hauptkonto-ID befindet sich nicht in Ihrer AWS Organisation. Sie sind nicht berechtigt, externe Ressourcen AWS-Konten zu einer Ressourcenfreigabe hinzuzufügen.“
- "OperationNotPermittedException: Die Ressource, die Sie teilen möchten, kann nur innerhalb Ihrer AWS Organisation gemeinsam genutzt werden.“

Mögliche Ursachen und Lösungen

Einige Ressourcentypen können nur mit Konten in derselben Organisation gemeinsam genutzt werden

Einige Ressourcentypen können nicht mit Konten geteilt werden, die nicht Mitglied dieser Organisation sind. Ein Beispiel für einen Ressourcentyp mit dieser Einschränkung sind virtuelle private Verbindungen (VPCs), die Teil von Amazon Elastic Compute Cloud (AmazonEC2) sind.

Informationen darüber, ob Sie einen bestimmten Ressourcentyp mit Konten und Prinzipalen außerhalb Ihrer Organisation teilen können, finden Sie unter [Gemeinsam nutzbare AWS Ressourcen](#).

Die mit dem Dienst verknüpfte Rolle wurde nicht erfolgreich erstellt

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

Wenn Sie versuchen, eine Ressource mit einem Konto zu teilen, das Teil Ihrer Organisation ist, einer dieser Fehler angezeigt wird, führen Sie die folgenden Schritte aus, um die dienstverknüpfte Rolle zu löschen und neu zu erstellen.

Important

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

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

Geteilte Ressourcen werden im Zielkonto nicht angezeigt

Szenario

Benutzer können die Ressourcen nicht sehen, von denen sie glauben, dass sie von anderen mit ihnen geteilt wurden AWS-Konten.

Mögliche Ursachen und Lösungen

Teilen mit AWS Organizations wurde aktiviert, indem Organizations verwendet wurden, anstatt AWS RAM

Wenn statt mithilfe von Organizations aktiviert AWS Organizations wurde AWS RAM, schlägt das Teilen innerhalb der Organisation fehl. Um zu überprüfen, ob dies die Ursache des Problems ist, navigieren Sie [in der AWS RAM Konsole zur Seite „Einstellungen“](#) und stellen Sie sicher, dass das AWS Organizations Kontrollkästchen Teilen aktivieren mit aktiviert ist.

- Wenn das Kontrollkästchen aktiviert ist, ist dies nicht die Ursache.
- Wenn das Kontrollkästchen nicht aktiviert ist, ist dies möglicherweise die Ursache. Markieren Sie das Kontrollkästchen noch nicht. Gehen Sie wie folgt vor, um die Situation zu korrigieren.

⚠ Important

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

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

Möglicherweise müssen Sie [die Freigabe aktualisieren und die Konten oder Organisationseinheiten innerhalb der Organisation angeben](#), für die das Teilen verwendet werden soll.

Die Ressourcenfreigabe gibt dieses Konto nicht als Hauptbenutzer an

[Sehen Sie sich in der AWS-Konto Datei, die die Ressourcenfreigabe erstellt hat, die Ressourcenfreigabe](#) in der [AWS RAM Konsole](#) an. Vergewissern Sie sich, dass das Konto, das nicht auf die Ressourcen zugreifen kann, als Principal aufgeführt ist. Ist dies nicht der Fall, [aktualisieren Sie den Share, um das Konto als Principal hinzuzufügen](#).

Für die Rolle oder den Benutzer im Konto sind keine Mindestberechtigungen erforderlich

Wenn Sie eine Ressource in Konto A mit einem anderen Konto B teilen, erhalten Rollen und Benutzer in Konto B nicht automatisch Zugriff auf die Ressourcen in der Freigabe. Der Administrator von

Konto B muss zunächst den IAM Rollen und Benutzern in Konto B, die auf die Ressource zugreifen müssen, die entsprechenden Berechtigungen erteilen. Als Beispiel zeigt die folgende Richtlinie, wie Sie Rollen und Benutzern in Konto B für eine Ressource aus Konto A schreibgeschützten Zugriff gewähren können. Die Richtlinie spezifiziert die Ressource anhand ihres [Amazon-Ressourcennamens \(\) ARN](#).

```
{
  "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 Dienst. Ressourcen sind in einer bestimmten Region vorhanden AWS-Region, und um sie sehen zu können, AWS Management Console müssen sie so konfiguriert sein, dass sie die Ressourcen in dieser Region anzeigen.

Die AWS-Region Datei, auf die die Konsole gerade zugreift, wird in der oberen rechten Ecke der Konsole angezeigt. Um ihn zu ändern, wählen Sie den Namen der aktuellen Region und dann im Dropdownmenü die Region aus, deren Ressourcen Sie sehen möchten.

Fehler: Limit überschritten

Szenario

Wenn Sie versuchen, Ressourcen gemeinsam zu nutzen, erhalten Sie die Meldung "Sie haben das Limit für die Anzahl der Ressourcen erreicht, die Sie teilen können ResourceShareLimitExceededException" oder "".

Ursache

Diese Fehler treten auf, wenn Sie die maximale Anzahl an Ressourcen erreichen, die Sie gemeinsam nutzen können, entweder mit dem AWS RAM Dienst oder mit dem Dienst AWS-Service , der die Ressource erstellt hat, die Sie teilen möchten. Dieses Kontingent (früher als Limit bezeichnet) kann sich sowohl auf das Sharing-Konto als auch auf das Konto auswirken, mit dem Sie die Ressource teilen.

Lösung

1. Um Ihre Kontingente einzusehen, rufen Sie an der AWS-Konto Stelle, an der der Fehler angezeigt wird, je nachdem, welche Art von Kontingent Sie erreicht haben, zu einer der folgenden Seiten auf:
 - Die [AWS RAM Seite in der Service Quotas Quotas-Konsole](#)
 - Die [Seite für diejenigen AWS-Service](#), deren Ressourcen vom Kontingent betroffen sind
2. Scrollen Sie nach unten und wählen Sie das entsprechende Kontingent aus.
3. Wenn es für dieses Kontingent verfügbar ist, wählen Sie Kontingenterhöhung beantragen.
4. Geben Sie einen neuen Wert für das Kontingent ein und wählen Sie dann „Anfrage“.
5. Die Anfrage wird auf der Seite mit dem [Verlauf der Kontingentanträge](#) angezeigt, auf der Sie den Status der Anfrage überprüfen können, bis sie abgeschlossen ist.

Das andere Konto in meiner Organisation erhält nie eine Einladung

Szenario

Wenn Sie Ressourcen mit einem anderen Konto in derselben Organisation teilen, das von verwaltet wird AWS Organizations, erhält dieser keine Einladungen.

Ursache

Dieses Verhalten ist zu erwarten, wenn für Ihr Konto die [gemeinsame Nutzung innerhalb der AWS Organisation](#) aktiviert ist.

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

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

Sie können ein VPC Subnetz nicht gemeinsam nutzen

Szenario

Wenn Sie versuchen, ein VPC Subnetz mit einem anderen Konto gemeinsam AWS RAM zu nutzen, ist der Freigabevorgang erfolgreich. Das verbrauchende Konto wird jedoch `LIMIT EXCEEDED` für diese Ressource in der AWS RAM Konsole angezeigt.

Ursache

Für einige einzelne Ressourcentypen gelten dienstspezifische Einschränkungen, die sich von den Einschränkungen unterscheiden, die von durchgesetzt wurden. AWS RAM Einige dieser Einschränkungen können die gemeinsame Nutzung effektiv verhindern, selbst wenn Sie eine der Einschränkungen von noch nicht erreicht haben. AWS RAM Grenzwerte sind ein Beispiel für diese Einschränkungen. Amazon Virtual Private Cloud (AmazonVPC) begrenzt die Anzahl der Subnetze, die Sie mit einem anderen individuellen Konto teilen können. Wenn Sie versuchen, ein Subnetz mit einem verbrauchenden Konto gemeinsam zu nutzen, das bereits die maximale Anzahl von Subnetzen enthält, wird dieses verbrauchende Konto `LIMIT EXCEEDED` in der Konsole für diese Ressource angezeigt. Weitere Informationen zu diesem Limit finden Sie unter [Amazon VPC Quotas — VPC Sharing](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Um dieses Problem zu beheben, suchen Sie zunächst nach anderen Ressourcenfreigaben, die die angegebene Ressource möglicherweise gemeinsam mit dem betroffenen Konto nutzen, und entfernen Sie die Freigaben, die Sie möglicherweise nicht mehr benötigen. Sie können auch eine Erhöhung für ein Limit beantragen, das Anpassungen unterstützt. Verwenden Sie die [Service Quotas Quotas-Konsole](#), um eine Erhöhung des Limits anzufordern.

Note

AWS RAM erkennt Änderungen der Limiterhöhung nicht automatisch. Sie müssen die Ressource oder den Prinzipal erneut der Ressourcenfreigabe zuordnenRAM, damit die Änderung erkannt wird.

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	25,000

 **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.

Ressource	Standardlimit
<p>Maximale Anzahl von Hauptverbänden für alle Ressourcenanteile in einem AWS-Region</p> <div data-bbox="115 352 792 762" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>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.</p></div>	25,000
<p>Maximale Anzahl ausstehender Einladungen pro Sharing-Konto</p> <ul style="list-style-type: none">• 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 Organizations 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.

Wenn Sie über diese Updates informiert werden möchten, können Sie den AWS RAM RSS Feed abonnieren.

Änderung	Beschreibung	Datum
Unterstützung für das Teilen von AWS Billing Ressourcen wurde hinzugefügt.	Sie können jetzt AWS Billing Ansichten mit anderen AWS-Konten in Ihrer Organisation teilen.	20. Dezember 2024
Unterstützung für die gemeinsame Nutzung von Amazon API Gateway-Ressourcen hinzugefügt.	Sie können API Gateway-Domainnamen jetzt mit anderen AWS-Konten oder innerhalb Ihrer Organisation teilen.	21. November 2024
Unterstützung für die gemeinsame Nutzung von VPC Amazon-Ressourcen hinzugefügt.	Sie können jetzt Amazon VPC Security-Gruppen mit anderen AWS-Konten oder innerhalb Ihrer Organisation teilen.	30. Oktober 2024
Unterstützung für die gemeinsame Nutzung von AWS Endbenutzer-Messaging SMS Ressourcen hinzugefügt.	Sie können AWS Endbenutzer-Messaging SMS Ressourcen mit anderen AWS-Konten oder Ihren Organisationen teilen AWS RAM.	24. September 2024
AWS PrivateLink	Mit AWS PrivateLink für können Sie eine direkte Verbindung herstellen AWS RAM, RAM indem Sie einen Schnittstellenendpunkt in	9. September 2024

	Ihrer virtuellen privaten Cloud verwenden (VPC).	
<u>Unterstützung für das Teilen wurde hinzugefügt AWS Backup.</u>	Sie können Tresore mit logischem Air-Gap innerhalb AWS-Konten oder innerhalb Ihrer Organisation gemeinsam nutzen.	7. August 2024
<u>Unterstützung für das Teilen von Amazon Bedrock Custom Models hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um benutzerdefinierte Amazon Bedrock-Modelle mit anderen AWS-Konten und mit Ihrer Organisation zu teilen.	1. August 2024
<u>Unterstützung für das Teilen von AWS CloudHSM Backups hinzugefügt.</u>	Sie können AWS CloudHSM Backups mit anderen AWS-Konten oder Ihren Organisationen teilen AWS RAM.	28. Juni 2024
<u>Unterstützung für die gemeinsame Nutzung von Amazon SageMaker AI hinzugefügt Model Registry Ressourcen.</u>	Sie können jetzt erweiterte Parameter sicher und effizient innerhalb AWS-Konten oder innerhalb Ihrer Organisation teilen.	27. Juni 2024
<u>Unterstützung für die gemeinsame Nutzung von Amazon SageMaker AI wurde hinzugefügt JumpStart.</u>	Sie können Amazon SageMaker AI JumpStart Hubs jetzt mit AWS-Konten oder innerhalb Ihrer Organisation teilen.	27. Juni 2024

<u>Unterstützung für das Teilen hinzugefügt Amazon Route 53 ResolverProfiles.</u>	Sie können es jetzt AWS RAM zum Teilen verwenden Amazon Route 53 Resolver Profiles mit anderen AWS-Konten innerhalb Ihrer Organisation.	22. April 2024
<u>Unterstützung für die gemeinsame Nutzung von AWS Systems Manager Parameter Store-Ressourcen wurde hinzugefügt.</u>	Sie können jetzt erweiterte Parameter sicher und effizient innerhalb Ihrer Organisation AWS-Konten oder innerhalb Ihrer Organisation teilen.	21. Februar 2024
<u>Unterstützung für das Teilen von Amazon FSx for Open ZFS Snapshots wurde hinzugefügt.</u>	Sie können Amazon FSx for Open ZFS Snapshots jetzt mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	19. Dezember 2023
<u>Unterstützung für die gemeinsame Nutzung von Amazon Simple Storage Service Ressourcen hinzugefügt.</u>	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
<u>Unterstützung für das Teilen von AWS Ressourcen Explorer Ansichten wurde hinzugefügt.</u>	Sie können jetzt AWS Ressourcen Explorer Ansichten mit anderen AWS-Konten innerhalb Ihrer Organisation teilen.	14. November 2023
<u>Unterstützung für die gemeinsame Nutzung von Amazon Application Recovery Controller (ARC) -Ressourcen hinzugefügt.</u>	Sie können jetzt Amazon Application Recovery Controller (ARC) -Cluster mit anderen AWS-Konten oder Ihrer Organisation teilen AWS RAM.	18. Oktober 2023

Unterstützung für die gemeinsame Nutzung von DataZone Amazon-Ressourcen hinzugefügt.	Sie können jetzt DataZone Amazon-Ressourcen mit anderen AWS-Konten oder Ihrer Organisation teilen.	04. Oktober 2023
Unterstützung für die gemeinsame Nutzung von Service Principal wurde hinzugefügt.	Sie können nun Service Principals mit Ressourc nfreigaben verknüpfen. Auf diese Weise können bestimmte Dienste die erforderlichen Aktionen für Kundenressourcen in Ihrem Namen verwalten.	29. August 2023
Unterstützung für die gemeinsame Nutzung von SageMaker Model Card-Ressourcen wurde hinzugefügt.	Sie können SageMaker Model Card-Ressourcen jetzt mit anderen AWS-Konten oder Ihrer Organisation teilen.	18. August 2023
Unterstützung für Amazon SageMaker AI Feature Store-Funktionsgruppen und SageMaker KI-Katalog als gemeinsam nutzbare Ressourcen hinzugefügt.	Sie können jetzt Amazon SageMaker AI Feature Store-Funktionsgruppen und SageMaker KI-Katalogressourcen mit anderen AWS-Konten oder Ihrer Organisation teilen.	20. Juli 2023
Erhöhung des Servicekontingents für ausstehende Einladungen.	Die maximale Anzahl ausstehender Einladungen pro Sharing-Konto wurde von 20 auf 250 erhöht.	08. Juni 2023
Unterstützung für AWS AppSync GraphQL APIs als gemeinsam nutzbare Ressourcen hinzugefügt.	Sie können AWS AppSync GraphQL jetzt APIs AWS-Konten mit AWS RAM anderen teilen.	24. Mai 2023

<u>Unterstützung für AWS Verified Access Gruppen als gemeinsam nutzbare Ressourcen hinzugefügt.</u>	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
<u>Unterstützung für vom Kunden verwaltete Berechtigungen in der AWS RAM Konsole hinzugefügt.</u>	Sie können jetzt auf sichere Weise detaillierte Ressourcenzugriffskontrollen für unterstützte Ressourcentypen erstellen und verwalten.	19. April 2023
<u>Unterstützung für gemeinsam nutzbare Amazon VPC Lattice-Service- und Service-Netzwerkressourcen hinzugefügt.</u>	Sie können jetzt Service- und Servicenetzwerkressourcen von Amazon VPC Lattice mit anderen AWS-Konten teilen.	31. März 2023
<u>Unterstützung für AWS Marketplace Katalogentitäten als gemeinsam nutzbare Ressourcen hinzugefügt.</u>	Sie können Ihre Entitäten jetzt mit anderen AWS-Konten im Marketplace teilen.	27. März 2023
<u>Unterstützung für die Verwaltung von Berechtigungsversionen in der AWS RAM Konsole hinzugefügt.</u>	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

[IAMAktualisierung der bewährten Verfahren.](#)

Aktualisierter Leitfaden zur Anpassung an die IAM bewährten Verfahren. Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden unter IAM.](#)

3. Januar 2023

[Unterstützung für EC2 Amazon-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 hinzugefügt AWS RAM.](#)

Es wurden Übersichtsvideos hinzugefügt, die das Teilen einer Ressource mit anderen beschreiben AWS RAM und erläutern. AWS-Konten

2p. August 2022

[Unterstützung für Amazon SageMaker AI-Pipelines hinzugefügt.](#)

Sie können jetzt SageMaker KI-Pipelines 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 SOC und ISO zertifiziert.	AWS RAM wurde als konform mit den Normen ISO 9001, ISO 27001, ISO 27017, ISO 27018 und 27701 der Service Organization Control (SOCISO) und der International Organization for Standardization () validiert. ISO	31. Mai 2022
AWS Resource Access Manager erhält die Fed-Zertifizierung. RAMP	AWS RAM wurde als konform mit dem Federal Risk and Authorization Management Program (FedRAMP) validiert.	8. April 2022
AWS Resource Access Manager erhält eine PCI DSS Zertifizierung.	AWS RAM wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert.	27. Februar 2022
Unterstützung für VPC IPAM Amazon-Ressourcendeckungen als gemeinsam nutzbare Ressourcen hinzugefügt. Außerdem können Sie jetzt IPAM Pools mit Konten außerhalb einer Organisation teilen.	Sie können IPAM Ressourcendeckungen jetzt 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 WAN Cloud-Kernnetzwerke als gemeinsam nutzbare globale Ressourcen hinzugefügt.	Sie können WAN Cloud-Cor e-Netzwerke jetzt mit anderen AWS-Konten teilen.	2. Dezember 2021

[Support für die gemeinsame Nutzung von Amazon VPC IP Address Manager \(IPAM\) - Pools](#)

Sie können VPC IPAM Amazon-Pools verwenden AWS RAM , um sie gemeinsam zu nutzen. Weitere Informationen finden Sie unter [Gemeinsam nutzbare AWS Ressourcen](#) im AWS RAM Benutzerhandbuch.

1. Dezember 2021

[Support für die gemeinsame Nutzung von Amazon SageMaker AI-Ressourcen](#)

Sie können es verwenden AWS RAM , um SageMaker KI-Abstammungsgruppen gemeinsam zu nutzen. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch [unter Gemeinsam nutzbare AWS Ressourcen](#).

30. November 2021

[Support für die gemeinsame Nutzung von AWS Migration Hub Refactor Spaces-Ressourcen](#)

Sie können es verwenden AWS RAM , um Migration Hub Hub-Umgebungen gemeinsam zu nutzen. Weitere Informationen finden Sie unter [Gemeinsam nutzbare AWS Ressourcen](#) im AWS RAM Benutzerhandbuch.

29. November 2021

[Es wurden Informationen zu AWS RAMAWS-verwalteten IAM Berechtigungsrichtlinien hinzugefügt.](#)

Veröffentlichte Details zu den verfügbaren AWS-verwalteten Berechtigungsrichtlinien, auf die Sie in der IAM Konsole zugreifen und sie den IAM Prinzipalen in Ihrer hinzufügen können. AWS-Konto

16. September 2021

<u>Unterstützung für die gemeinsame Nutzung von S3 auf Outposts-Ressourcen hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um S3 auf Outposts mit anderen AWS-Konten zu teilen.	05. August 2021
<u>Unterstützung für zusätzliche verwaltete Berechtigungen und die gemeinsame Nutzung von Ressourcen mit IAM Prinzipalen hinzugefügt</u>	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
<u>Unterstützung für die gemeinsame Nutzung von AWS Systems Manager Incident Manager-Ressourcen hinzugefügt</u>	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
<u>Unterstützung für die gemeinsame Nutzung von Amazon Route 53-Ressourcen hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um Amazon Route 53 Resolver DNS Firewall-Regelgruppen mit anderen AWS-Konten zu teilen.	31. März 2021
<u>Unterstützung für die gemeinsame Nutzung AWS Transit Gateway von Ressourcen hinzugefügt</u>	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 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 es jetzt verwenden AWS RAM , um AWS Glue-Datenkataloge, Datenbanken und Tabellen mit anderen AWS-Konten zu teilen.

7. Juli 2020

[Unterstützung für das Teilen von VPC Amazon-Präfixlisten hinzugefügt.](#)

Sie können sie jetzt AWS RAM zum Teilen von Präfixlisten verwenden.

29. Juni 2020

<u>Unterstützung für das Teilen von AWS Outposts kundeneigenen IPv4 Adressen wurde hinzugefügt.</u>	Sie können es jetzt verwenden AWS RAM , um AWS Outposts kundeneigene IPv4 Adressen mit anderen zu teilen. AWS-Konten	22. April 2020
<u>Unterstützung für das Teilen AWS App Mesh von Meshes hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um Meshes mit anderen zu teilen. AWS-Konten	17. Januar 2020
<u>Unterstützung für das Teilen von AWS CodeBuild Projekten und Berichtsgruppen hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um AWS CodeBuild Projekte und Berichtsgruppen mit anderen zu teilen AWS-Konten.	13. Dezember 2019
<u>Unterstützung für die gemeinsame Nutzung zusätzlicher Ressourcen hinzugefügt</u>	Sie können es jetzt verwenden , AWS RAM um Amazon EC2 Dedicated Hosts, AWS Resource Groups Ressourcenrgruppen und Amazon EC2 Image Builder Builder-Komponenten, Images und Image-Rezepte mit anderen zu teilen AWS-Konten.	02. Dezember 2019
<u>Unterstützung für die gemeinsame Nutzung von Kapazitätsreservierungen auf Abruf hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um On-Demand-Kapazitätsreservierungen mit anderen zu teilen AWS-Konten.	29. Juli 2019
<u>Unterstützung für die gemeinsame Nutzung von Aurora-DB-Clustern hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um Aurora-DB-Cluster mit anderen zu teilen AWS-Konten.	2. Juli 2019

<u>Unterstützung für die gemeinsame Nutzung von Traffic Mirroring-Zielen hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um Traffic Mirroring-Ziele mit anderen zu teilen. AWS-Konten	25. Juni 2019
<u>Unterstützung für die gemeinsame Nutzung von Lizenzkonfigurationen wurde hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um AWS License Manager Manager-Lizenzkonfigurationen mit anderen zu teilen AWS-Konten.	5. Dezember 2018
<u>Unterstützung für die gemeinsame Nutzung von Subnetzen hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um VPC Amazon-Subnetze mit anderen AWS-Konten zu teilen.	27. November 2018
<u>Unterstützung für die gemeinsame Nutzung von Transit-Gateways hinzugefügt</u>	Sie können es jetzt verwenden AWS RAM , um Amazon VPC Transit Gateways mit anderen AWS-Konten zu teilen.	26. November 2018
<u>Unterstützung für die gemeinsame Nutzung von Resolver-Regeln hinzugefügt</u>	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.