



ユーザーガイド

# AWS Resource Access Manager



# AWS Resource Access Manager: ユーザーガイド

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

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

# Table of Contents

AWS RAM とは? .....	1
ビデオの概要 .....	1
AWS RAM の利点 .....	2
リソースベースのポリシーによるクロスアカウントアクセス .....	2
リソース共有のしくみ .....	3
リソースの共有 .....	3
共有リソースの使用 .....	4
AWS RAM へのアクセス .....	5
AWS RAM の料金 .....	6
コンプライアンスと国際規格 .....	6
PCI DSS .....	6
FedRAMP .....	6
SOC および ISO .....	7
開始方法 .....	8
用語と概念 .....	8
リソースの共有 .....	8
共有アカウント .....	9
コンシューマープリンシパル .....	9
リソースベースのポリシー .....	11
管理アクセス許可 .....	15
管理アクセス許可のバージョン .....	16
リソースの共有 .....	17
AWS Organizations 内でリソース共有を有効にする .....	18
リソース共有を作成する .....	20
共有リソースの使用 .....	29
リソース共有の招待に応答する .....	29
自分が共有先になっているリソースを使用する .....	31
共有リソースの使用 .....	32
リージョナルリソースとグローバルリソース .....	32
リージョナルリソースとグローバルリソースの違い .....	33
リソース共有とそのリージョン .....	34
所有するリソース .....	35
作成したリソース共有の表示 .....	36
リソース共有の作成 .....	38

リソース共有の更新 .....	47
共有リソースの表示 .....	55
共有相手のプリンシパルの表示 .....	56
リソース共有の削除 .....	58
共有しているリソース .....	60
招待の受け入れと拒否 .....	60
共有しているリソース共有の表示 .....	64
自分が共有先になっているリソースの表示 .....	66
共有相手のプリンシパルの表示 .....	67
リソース共有の終了 .....	69
アベイラビリティゾーン ID .....	72
共有可能なリソース .....	75
AWS App Mesh .....	77
AWS AppSync GraphQL API .....	77
Amazon Aurora .....	78
AWS Private Certificate Authority .....	79
Amazon DataZone .....	80
AWS CodeBuild .....	81
Amazon EC2 .....	83
EC2 Image Builder .....	87
Amazon FSx for OpenZFS .....	90
AWS Glue .....	91
AWS License Manager .....	94
AWS Marketplace .....	95
AWS Migration Hub Refactor Spaces .....	96
AWS Network Firewall .....	97
AWS Outposts .....	99
Amazon S3 on Outposts .....	101
AWS Resource Explorer .....	102
AWS Resource Groups .....	103
Amazon Route 53 .....	104
Amazon Route 53 Application Recovery Controller .....	107
Amazon Simple Storage Service .....	108
Amazon SageMaker .....	109
AWS Service Catalog AppRegistry .....	115
AWS Systems Manager Incident Manager .....	116

AWS Systems Manager パラメータストア .....	118
Amazon VPC .....	119
Amazon VPC Lattice .....	129
AWS クラウド WAN .....	131
AWS RAM アクセス許可の管理 .....	132
管理アクセス許可の表示 .....	133
カスタマー管理アクセス許可の作成と使用 .....	138
カスタマー管理アクセス許可を作成する .....	138
カスタマー管理アクセス許可の新しいバージョンを作成する .....	140
カスタマー管理アクセス許可のデフォルトとなる別のバージョンを選択する .....	142
カスタマー管理アクセス許可のバージョンを削除する .....	144
カスタマー管理アクセス許可を削除する .....	145
管理アクセス許可のバージョンを更新する .....	146
カスタマー管理アクセス許可に関する考慮事項 .....	148
マネージドアクセス許可のしくみ .....	149
管理アクセス許可のタイプ .....	150
セキュリティ .....	153
データ保護 .....	153
Identity and Access Management .....	154
AWS RAM と IAM の連携について .....	155
AWS マネージドポリシー .....	158
サービスにリンクされたロールの使用 .....	163
IAM ポリシーの例 .....	165
SCP の例 .....	167
組織との共有を無効にする .....	171
ログ記録とモニタリング .....	172
CloudWatch Events を使用したモニタリング .....	173
AWS RAM による AWS CloudTrail API コールのログ記録 .....	174
耐障害性 .....	177
インフラストラクチャセキュリティ .....	177
トラブルシューティング .....	179
エラー: アカウント ID が存在しない .....	179
シナリオ .....	179
原因 .....	179
解決策 .....	179
エラー: アクセス拒否の例外 .....	180

シナリオ .....	180
原因 .....	180
解決策 .....	180
エラー: 未知のリソース例外 .....	182
シナリオ .....	182
原因 .....	182
解決策 .....	182
エラー: 組織外との共有は許可されていない .....	183
シナリオ .....	183
考えられる原因と解決策 .....	183
エラー: 共有リソースが表示されない .....	184
シナリオ .....	184
考えられる原因と解決策 .....	184
エラー: 制限超過の例外 .....	186
シナリオ .....	186
原因 .....	186
解決策 .....	186
招待が届かない .....	187
シナリオ .....	187
原因 .....	187
VPC を共有できない .....	187
シナリオ .....	187
原因 .....	187
Service Quotas .....	189
AWS SDK の使用 .....	192
ドキュメント履歴 .....	193
.....	cciii

# AWS Resource Access Manager とは？

AWS Resource Access Manager (AWS RAM) を使用すると、AWS アカウント 全体、組織または組織単位 (OU) 間、およびサポートされているリソースタイプの AWS Identity and Access Management (IAM) ロールやユーザーと安全にリソースを共有できます。複数の AWS アカウントがある場合、リソースを 1 回作成し、AWS RAM を使用してそのリソースを他のアカウントで使用できるようにすることができます。アカウントが AWS Organizations によって管理されている場合、リソースを共有できる相手は組織内の他のすべてのアカウント、または 1 つまたは複数の指定された組織単位 (OU) に含まれるアカウントのみです。アカウントが組織の一部かどうかにかかわらず、アカウント ID で特定の AWS アカウント と共有することも可能です。[サポートされているリソースタイプ](#)によっては、指定した IAM ロールやユーザーと共有することもできます。

## 目次

- [ビデオの概要](#)
- [AWS RAM の利点](#)
- [リソース共有のしくみ](#)
- [AWS RAM へのアクセス](#)
- [AWS RAM の料金](#)
- [コンプライアンスと国際規格](#)

## ビデオの概要

次のビデオでは、AWS RAM の概要とリソース共有の作成方法について説明します。詳細については、「[???](#)」を参照してください。

次のビデオでは、AWS リソースに AWS 管理アクセス許可を適用する方法について説明します。詳細については、「[???](#)」を参照してください。

このビデオでは、最小特権のベストプラクティスに従って、カスタマー管理アクセス許可の作成および関連付けを行う方法について説明します。詳細については、「[???](#)」を参照してください。

# AWS RAM の利点

AWS RAM を使用する理由 以下のような利点があります。

- [Reduces your operational overhead] (運用オーバーヘッドを削減) — リソースを一度作成すれば、AWS RAM を使用してそのリソースを他のアカウントと共有できます。これにより、複製したリソースをすべてのアカウントにプロビジョニングする必要がなくなるため、運用のオーバーヘッドが減少します。リソースを所有するアカウント内で AWS RAM を使用すると、ID ベースのアクセス許可ポリシーを使用しなくても、アカウントのすべてのロールとユーザーへのアクセス許可を簡単に付与できます。
- [Provides security and consistency] (セキュリティと一貫性を確保) - 単一のポリシーとアクセス許可セットを使用して、共有リソースのセキュリティ管理を簡素化します。代わりに、個別のすべてのアカウントに重複リソースを作成しようとする場合、同じポリシーとアクセス許可を実装するタスクがあり、それらのアカウント全体で同じリソースを維持する必要があります。代わりに、AWS RAM リソース共有のすべてのユーザーは、単一のポリシーとアクセス許可のセットで管理されます。AWS RAM は、異なるタイプの AWS リソースを共有する一貫したエクスペリエンスを提供します。
- [Provides visibility and auditability] (可視性と可監査性を提供) – AWS RAM と Amazon CloudWatch の統合および AWS CloudTrail を介して共有リソースの使用状況の詳細が表示されます。AWS RAM は、共有リソースとアカウントの包括的な可視性を提供します。

## リソースベースのポリシーによるクロスアカウントアクセス

ユーザーは、AWS アカウント の外の AWS Identity and Access Management (IAM) プリンシパル (IAM ロールおよびユーザー) を識別する [リソースベースのポリシー](#) をアタッチすることで、AWS リソースの一部のタイプを他の AWS アカウント と共有できます。しかし、ポリシーのアタッチによるリソースの共有では、AWS RAM が提供する付加的な利点を活かさせません。AWS RAM を使用すると、以下の機能を利用できるようになります。

- 全員の AWS アカウント ID を列挙しなくても、[組織または組織単位 \(OU\)](#) と共有できます。
- ユーザーからは、共有されたリソースを発信元の AWS のサービス コンソールや API オペレーションで、あたかもそのリソースがユーザーのアカウント内に直接存在するかのように見えます。例えば、AWS RAM を使用して Amazon VPC サブネットを別のアカウントと共有する場合、そのアカウントのユーザーは、Amazon VPC コンソール、およびそのアカウントで実行された Amazon VPC API オペレーションの結果でサブネットを確認できます。リソースベースのポリ



シーをアタッチして共有されたリソースはこのように表示されることはなく、代わりに Amazon リソースネーム (ARN) によってリソースを検出して明示的に参照する必要があります。

- リソースの所有者は、共有した個々のリソースにアクセスできるプリンシパルを確認できます。
- 組織外のアカウントとリソースを共有すると、AWS RAM によって招待プロセスが開始されます。プリンシパルが共有リソースにアクセスできるようにするには、受信者は招待を受け入れる必要があります。[組織内での共有機能を有効にすると](#)、組織内のアカウントと共有する際に招待を受け取る必要がなくなります。

リソースベースのアクセス許可ポリシーを使用して共有したリソースでは、次のいずれかを実行して、それらのリソースをフルマネージド AWS RAM リソースにすることができます。

- [PromoteResourceShareCreatedFromPolicy](#) API オペレーションを使用します。
- API オペレーションと同等の AWS Command Line Interface (AWS CLI) [promote-resource-share-created-from-policy](#) コマンドを使用します。

## リソース共有のしくみ

所有アカウントのリソースを別の AWS アカウント (コンシューマーアカウント) と共有する場合、コンシューマーアカウントのプリンシパルに共有リソースへのアクセス許可を付与することになります。コンシューマーアカウントのロールとユーザーに適用されるすべてのポリシーとアクセス許可は、共有リソースにも適用されます。共有内のリソースは、共有した AWS アカウント 内にあるネイティブのリソースのように見えます。

グローバルリソースとリージョナルリソースの両方を共有できます。詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。

## リソースの共有

AWS RAM を使用した[リソース共有](#)。これにより、自身が所有するリソースを共有できます。リソース共有を作成するには、以下を指定します。

- リソース共有を作成する AWS リージョン。コンソールの右上隅にある [リージョン] ドロップダウンメニューで選択します。AWS CLI で、`--region` パラメータを使用します。
- リソース共有には、そのリソース共有と同じ AWS リージョン にあるリージョナルリソースのみを含めることができます。

- リソース共有にグローバルリソースを含めることができるのは、そのリソース共有がグローバルリソースのホームである米国東部 (バージニア北部) us-east-1 にある場合のみです。
- リソース共有の名前。
- このリソース共有の一部としてアクセス権を付与したいリソースのリスト。
- リソース共有へのアクセス権の付与先になるプリンシパル。プリンシパルとなれるものは、個々の AWS アカウント、AWS Organizations 内の組織または組織単位 (OU) のアカウント、または個々の AWS Identity and Access Management (IAM) 。

#### Note

すべてのリソースタイプを IAM ロールやユーザーと共有できるわけではありません。これらのプリンシパルと共有できるリソースの詳細については、「[共有可能な AWS リソース](#)」を参照してください。

- リソース共有に含まれるリソースタイプごとに、1つの[管理アクセス許可](#)のみを関連付けることができます。他のアカウントのプリンシパルがリソース共有のリソースで実行できる操作は、管理アクセス許可によって決まります。

アクセス許可の動作はプリンシパルのタイプによって異なります。

- プリンシパルがリソースを所有しているアカウントとは別のアカウントに属している場合、リソース共有にアタッチされたアクセス許可が、それらのアカウントのロールとユーザーに付与できる最大のアクセス許可になります。その後、それらのアカウントの管理者は、IAM ID ベースのポリシーを使用して、個々のロールとユーザーに共有リソースへのアクセス権を付与する必要があります。これらのポリシーで付与されるアクセス許可は、リソース共有にアタッチされたアクセス許可で定義されているアクセス許可を超えることはできません。

リソース所有アカウントは、共有するリソースの完全な所有権を保持します。

## 共有リソースの使用

リソースの所有者がそのリソースをアカウントと共有している場合、ユーザーは、自分のアカウントが所有している場合と同じように、共有リソースにアクセスできます。リソースへのアクセスは、該当するサービスのコンソール、AWS CLI コマンド、API オペレーションを介して可能です。自分のアカウント内のプリンシパルが実行できる API オペレーションは、リソースのタイプによって異なり、リソース共有に付いている AWS RAM アクセス許可によって指定されます。アカウントで設定されているすべての IAM ポリシーとサービスコントロールポリシーも継続的に適用されます。これにより、セキュリティとガバナンスのコントロールに対する既存の投資を活用できます。

リソースのサービスを使用して共有リソースにアクセスする場合、そのリソースを所有する AWS アカウントと同じ能力と制限が適用されます。

- リージョナルリソースの場合は、そのリソースを所有しているアカウント内の AWS リージョンからのみアクセスできます。
- グローバルリソースの場合は、そのリソースのサービスコンソールとツールがサポートするすべての AWS リージョンからアクセスできます。リソース共有とそのグローバルリソースは、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 の AWS RAM コンソールとツールでのみ表示できます。

## AWS RAM へのアクセス

AWS RAM は次のいずれかの方法で使用できます。

### AWS RAM コンソール

AWS RAM には、AWS RAM コンソールというウェブベースのユーザーインターフェイスがあります。AWS アカウントにサインアップ済みの場合、[AWS Management Console](#) にサインインし、コンソールのホームページから AWS RAM を選択することで、AWS RAM コンソールにアクセスできます。

また、ブラウザで[AWS RAM コンソール](#)に直接移動することもできます。まだサインインしていない場合、コンソールが表示される前にログインするように求められます。

### AWS CLI と Tools for Windows PowerShell

AWS CLI および AWS Tools for PowerShell は、AWS RAM パブリック API オペレーションへの直接アクセスを提供します。AWS は、Windows、macOS、Linux でこれらのツールをサポートします。開始方法の詳細については、[AWS Command Line Interface ユーザーガイド](#)または[AWS Tools for Windows PowerShell ユーザーガイド](#)を参照してください。AWS RAM 用のコマンドの詳細については、[AWS CLI コマンドリファレンス](#)または[AWS Tools for Windows PowerShell コマンドレットリファレンス](#)を参照してください。

### AWS SDK

AWS は、一連のプログラミング言語に対応する API コマンドを提供します。開始方法の詳細については、「[AWS SDKs と ツールのリファレンスガイド](#)」を参照してください。

## Query API

サポートされているプログラミング言語のいずれも使用しない場合、AWS RAM HTTPS クエリ API を介して AWS RAM および AWS へのプログラムによるアクセスが可能です。AWS RAM API によって、HTTPS リクエストをサービスに直接発行できます。AWS RAM API を使用する場合は、認証情報を使用してリクエストにデジタル署名するコードを含める必要があります。詳細については、[AWS RAM API リファレンス](#)を参照してください。

## AWS RAM の料金

AWS RAM を使用してアカウント間でリソースを共有する際に追加料金はかかりません。リソースの利用料金はリソースのタイプによって異なります。共有可能なリソースについての AWS の料金請求の詳細については、リソースを所有するサービスのドキュメントを参照してください。

## コンプライアンスと国際規格

### PCI DSS

AWS RAM は、加盟店またはサービスプロバイダーによるクレジットカードデータの処理、ストレージ、および送信をサポートし、Payment Card Industry (PCI) データセキュリティスタンダード (DSS) に準拠していることが検証されています。

PCI DSS の詳細 (AWS PCI Compliance Package のコピーをリクエストする方法など) については、「[PCI DSS レベル 1](#)」を参照してください。

### FedRAMP

AWS RAM は、以下の AWS リージョンで FedRAMP Moderate として認可されています。米国東部 (バージニア北部)、米国東部 (オハイオ)、米国西部 (北カリフォルニア)、米国西部 (オレゴン)。

AWS RAM は、以下の AWS リージョンで FedRAMP High として認可されています。AWS GovCloud (US-West) および AWS GovCloud (US-East)。

Federal Risk and Authorization Management Program (FedRAMP) は米国政府全体のプログラムであり、クラウドの製品やサービスに対するセキュリティ評価、認証、および継続的なモニタリングに関する標準アプローチを提供しています。

FedRAMP コンプライアンスの詳細については、「[FedRAMP](#)」を参照してください。

## SOC および ISO

AWS RAM は、Service Organization Controls (SOC) コンプライアンスおよび国際標準化機構 (ISO) 規格 ISO 9001、ISO 27001、ISO 27017、ISO 27018、および ISO 27701 で規定されている対象ワークロードに使用できます。金融、ヘルスケア、その他の規制分野のお客様は、[AWS Artifact](#) の SOC レポート、AWS ISO、CSA STAR 証明書で確認できる、顧客データを保護するセキュリティプロセスやコントロールに関するインサイトを得ることができます。

SOC コンプライアンスの詳細については、「[SOC](#)」を参照してください。

ISO コンプライアンスの詳細については、「[ISO 9001](#)」、「[ISO 27001](#)」、「[ISO 27017](#)」、「[ISO 27018](#)」、および「[ISO 27701](#)」を参照してください。

# AWS RAM の開始方法

AWS Resource Access Manager では、所有しているリソースを自分以外の個々の AWS アカウントと共有できます。アカウントが AWS Organizations によって管理されている場合、組織内でリソースを他のアカウントと共有することもできます。他の AWS アカウント によって自分と共有されたリソースも使用できます。

AWS Organizations 内で共有が有効になっていない場合、リソースを組織または組織内の組織単位 (OU) と共有することはできません。ただし、組織内でリソースを個々の AWS アカウント と共有することはできます。[サポートされているリソースタイプ](#)について、組織内でリソースを個々の AWS Identity and Access Management (IAM) ロールまたはユーザーと共有することもできます。この場合、これらのプリンシパルは、組織の一部としてではなく、外部アカウントとして扱われます。共有リソースにアクセスするには、リソース共有に参加するための招待状を受け取ってその招待状を受け入れる必要があります。

## 目次

- [AWS RAM の用語と概念](#)
- [AWS リソースの共有](#)
- [共有 AWS リソースの使用](#)

## AWS RAM の用語と概念

以下の概念は、AWS Resource Access Manager (AWS RAM) を使用したリソース共有の理解に役立ちます。

### リソースの共有

AWS RAM を使用してリソース共有を作成することで、リソースを共有できます。リソース共有には次の 3 つの要素があります。

- 共有する 1 つまたは複数の AWS リソースのリスト。
- アクセスが付与される 1 つまたは複数の[プリンシパル](#)のリスト。
- 共有に含める各リソースタイプの[管理アクセス許可](#)。各管理アクセス許可は、リソース共有内の対象タイプのすべてのリソースに適用されます。

AWS RAM を使用してリソース共有を作成した後は、リソース共有で指定されたプリンシパルに共有のリソースへのアクセスを付与できます。

- AWS Organizations で AWS RAM 共有を有効にし、共有先のプリンシパルが共有アカウントと同じ組織に所属している場合、アカウント管理者が AWS Identity and Access Management (IAM) アクセス許可ポリシーを使用してリソースを使用するアクセス許可を付与すると、それらのプリンシパルはすぐにリソースにアクセスできるようになります。
- Organizations で AWS RAM 共有を有効にしない場合でも、組織内の個々の AWS アカウント とはリソースを共有できます。コンシューマーアカウントの管理者は、リソース共有に参加するための招待状を受け取ります。管理者が招待状を承諾すると、リソース共有で指定されたプリンシパルは共有リソースにアクセスできるようになります。
- リソースタイプでサポートされている場合は、組織外のアカウントと共有することもできます。コンシューマーアカウントの管理者は、リソース共有に参加するための招待状を受け取ります。管理者が招待状を承諾すると、リソース共有で指定されたプリンシパルは共有リソースにアクセスできるようになります。このタイプの共有がサポートされているリソースタイプについては、「[共有可能な AWS リソース](#)」の「組織外のアカウントと共有可能」列を参照してください。

## 共有アカウント

共有アカウントには共有リソースが含まれており、AWS RAM 管理者はこのリソースで AWS RAM を使用して AWS リソースを作成します。

AWS RAM 管理者は、AWS アカウント でリソース共有を作成および設定するアクセス許可を持つ IAM プリンシパルです。AWS RAM は、リソースベースのポリシーをリソース共有内のリソースにアタッチすることで機能するため、AWS RAM 管理者はリソース共有に含まれるリソースタイプごとに AWS のサービスで PutResourcePolicy を呼び出すアクセス許可も必要です。

## コンシューマープリンシパル

コンシューマーアカウントは、リソースの共有先の AWS アカウント です。リソース共有は、アカウント全体をプリンシパルとして指定することも、リソースタイプによってはアカウント内の個々のロールやユーザーを指定することもできます。このタイプの共有がサポートされているリソースタイプについては、「[共有可能な AWS リソース](#)」の「IAM ロールおよびユーザーと共有可能」列を参照してください。

また AWS RAM は、リソース共有のコンシューマーとしてのサービスプリンシパルもサポートしています。このタイプの共有がサポートされているリソースタイプについては、「[共有可能な AWS リソース](#)」の「サービスプリンシパルと共有可能」列を参照してください。



コンシューマーアカウントのプリンシパルは、以下の両方のアクセス許可で許可されているアクションのみを実行できます。

- リソース共有にアタッチされた管理アクセス許可。これは、コンシューマーアカウントのプリンシパルに付与できる最大のアクセス許可を指定します。
- コンシューマーアカウントの IAM 管理者が個々のロールまたはユーザーにアタッチする IAM ID ベースのポリシー。これらのポリシーは、指定されたアクションと、共有アカウントのリソースの [Amazon リソースネーム \(ARN\)](#) への Allow アクセスを許可する必要があります。

AWS RAM は、リソース共有のコンシューマーとして、次の IAM プリンシパルタイプをサポートします。

- 別の AWS アカウント - リソース共有により、共有アカウントに含まれるリソースをコンシューマーアカウントで使用できるようになります。
- 別のアカウントの個々の IAM ロールまたはユーザー — 一部のリソースタイプでは、個々の IAM ロールまたはユーザーとの直接共有がサポートされています。このプリンシパルタイプは ARN で指定します。
  - IAM ロール - `arn:aws:iam::123456789012:role/rolename`
  - IAM ユーザー - `arn:aws:iam::123456789012:user/username`
- サービスプリンシパル — リソースを AWS サービスと共有して、サービスにリソース共有へのアクセスを許可します。サービスプリンシパルと共有することで、AWS サービスがユーザーに代わってアクションを実行できるため、運用上の負荷を軽減することができます。

サービスプリンシパルと共有するには、[すべてのユーザーとの共有を許可] を選択して、[プリンシパルタイプの選択] のドロップボックスリストで [サービスプリンシパル] を選択します。サービスプリンシパルの名前を次の形式で指定します。

- `service-id.amazonaws.com`

混乱した代理のリスクを軽減するため、リソースポリシーでは `aws:SourceAccount` 条件キーにリソース所有者のアカウント ID が表示されます。

- 組織内のアカウント — 共有アカウントが AWS Organizations で管理されている場合、リソース共有は組織のすべてのアカウントと共有する組織の ID を指定できます。リソース共有では、組織単位 (OU) ID を指定して、その OU 内のすべてのアカウントと共有することもできます。共有アカウントは、自分の組織または自分の組織内の OU ID とのみ共有できます。組織または OU の ARN で組織内のアカウントを指定します。
  - 組織内のすべてのアカウント — 以下は、AWS Organizations にある組織の ARN の例です。



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

- 組織単位内のすべてのアカウント — 以下は、OU ID の ARN の例です。

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

### Important

組織または OU と共有し、スコープにリソース共有を所有するアカウントが含まれる場合、共有アカウントのすべてのプリンシパルは、共有内のリソースに自動的にアクセスできるようになります。付与されるアクセスは、共有に関連付けられている管理アクセス許可によって定義されます。これは、共有内の各リソースに AWS RAM がアタッチするリソースベースのポリシーで "Principal": "\*" が使用されるためです。詳細については、[「"Principal": "\\*" をリソースベースのポリシーで使用するごとの影響」](#)を参照してください。

他のコンシューマーアカウントのプリンシパルは、共有のリソースにすぐにはアクセスできません。他のアカウントの管理者は、まず ID ベースのアクセス許可ポリシーを適切なプリンシパルにアタッチする必要があります。これらのポリシーは、リソース共有内の個々のリソース ARN への Allow アクセスを付与する必要があります。これらのポリシーのアクセス許可は、リソース共有に関連付けられた管理アクセス許可で指定されているアクセス許可を超えることはできません。

## リソースベースのポリシー

リソースベースのポリシーは、IAM ポリシー言語を実装する JSON テキストドキュメントです。IAM ロール/ユーザーなど、プリンシパルにアタッチする ID ベースのポリシーとは異なり、リソースベースのポリシーをリソースにアタッチします。AWS RAM は、ユーザーがリソース共有で指定した情報に基づいて、ユーザーに代わってリソースベースのポリシーを作成します。ユーザーは、リソースにアクセスできるユーザーを決定する Principal ポリシー要素を指定する必要があります。詳細については、「IAM ユーザーガイド」の [「アイデンティティベースおよびリソースベースのポリシー」](#)を参照してください。

AWS RAM で生成されたリソースベースのポリシーは、他のすべての IAM ポリシータイプとともに評価されます。これには、リソースへのアクセスを試みているプリンシパルにアタッチされているすべての IAM ID ベースのポリシーと、AWS アカウントに適用される可能性のある AWS Organizations のサービスコントロールポリシー (SCP) が含まれます。AWS RAM で生成されたり

ソースベースのポリシーは、他のすべての IAM ポリシーと同じポリシー評価ロジックで評価されます。ポリシー評価の詳細結果および結果から導かれるアクセス許可の決定については、「IAM ユーザーズガイド」の「[ポリシーの評価論理](#)」を参照してください。

AWS RAM は、使いやすい抽象化リソースベースのポリシーを提供することで、シンプルで安全なリソース共有を実現します。

リソースベースのポリシーをサポートするリソースタイプについては、AWS RAM は自動的にリソースベースのポリシーを作成し管理します。指定されたリソースで、AWS RAM はそのリソースを含むすべてのリソース共有からの情報を組み合わせて、リソースベースのポリシーを作成します。例えば、2 つの異なるリソース共有を含み、AWS RAM を使用して共有する Amazon SageMaker Pipelines を考えてみましょう。1 つのリソース共有を使用して、組織全体に読み取り専用アクセス権を付与できます。その後、もう 1 つのリソース共有を使用して、1 つのアカウントに SageMaker の実行アクセス許可のみを付与できます。AWS RAM は、これら 2 つの異なるアクセス許可セットを複数のステートメントで 1 つのリソースポリシーに自動的に結合します。その後、結合されたリソースベースのポリシーをパイプラインリソースにアタッチします。ユーザーは、[GetResourcePolicy](#) を呼び出すことで基盤となるこのリソースポリシーを表示できます。次に AWS のサービスは、このリソースベースのポリシーを使用して、共有リソースに対してアクションの実行を試みるプリンシパルを承認します。

リソースベースのポリシーを手動で作成し、PutResourcePolicy を呼び出してリソースにアタッチすることもできますが、以下の利点があるため AWS RAM を使用することを推奨します。

- 共有コンシューマーの見つけやすさ — AWS RAM を使用してリソースを共有する場合、ユーザーは、共有されたすべてのリソースをリソースを所有するサービスのコンソールや API オペレーションで、あたかもそのリソースがユーザーのアカウント内に存在するかのように表示することができます。例えば、AWS CodeBuild プロジェクトを別のアカウントと共有する場合、コンシューマーアカウントのユーザーは、CodeBuild コンソールや CodeBuild API の実行結果でプロジェクトを表示することができます。リソースベースのポリシーを直接アタッチして共有したリソースは、この方法では表示されません。代わりに、リソースを探し、ARN を使用して明示的にリソースを参照する必要があります。
- 共有所有者の管理しやすさ — AWS RAM を使用してリソースを共有する場合、共有アカウントのリソースの所有者は、どのアカウントがリソースにアクセスできるかを一元的に確認できます。リソースベースのポリシーを使用してリソースを共有する場合、関連するサービスコンソールまたは API で個々のリソースのポリシーを調べることによってのみ、コンシューマーアカウントを確認できます。

- 効率性 — AWS RAM を使用してリソースを共有する場合、共有する複数のリソースを 1 つのリソースとして管理できます。リソースベースのポリシーのみを使用してリソースを共有する場合は、共有するすべてのリソースに個別のポリシーをアタッチする必要があります。
- シンプルさ — AWS RAM を使用すると、JSON ベースの IAM ポリシー言語を理解する必要はありません。AWS RAM は、リソース共有にアタッチするアクセス許可を選択できる、すぐに使用できる AWS 管理アクセス許可を提供します。

AWS RAM を使用すると、リソースベースのポリシーをサポートしていないリソースタイプを共有することもできます。このようなリソースタイプでは、AWS RAM は実際のアクセス許可を表すリソースベースのポリシーを自動的に生成します。ユーザーは、[GetResourcePolicy](#) を呼び出してこれを表示できます。これには、次のリソースタイプが含まれます。

- Amazon Aurora – DB クラスター
- Amazon EC2 — キャパシティ予約と専用ホスト
- AWS License Manager – ライセンス設定
- AWS Outposts - ローカルゲートウェイルートテーブル、アウトポスト、サイト
- Amazon Route 53 – 転送ルール
- Amazon Virtual Private Cloud — カスタマーが所有する IPv4 アドレス、プレフィックスリスト、サブネット、トラフィックミラーターゲット、トランジットゲートウェイ、トランジットゲートウェイマルチキャストドメイン

## AWS RAM で生成されたリソースベースのポリシーの例

EC2 Image Builder のイメージリソースを個々のアカウントと共有する場合、AWS RAM は次の例のようなポリシーを生成し、リソース共有に含まれるすべてのイメージリソースにアタッチします。

```
{
  "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"
    }
]
}

```

EC2 Image Builder のイメージリソースを別の AWS アカウント の IAM ロールまたはユーザーと共有する場合、AWS RAM は次の例のようなポリシーを生成し、リソース共有に含まれるすべてのイメージリソースにアタッチします。

```

{
  "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"
    }
  ]
}

```

EC2 Image Builder のイメージリソースを組織のすべてのアカウント、または OU アカウントと共有する場合、AWS RAM は次の例のようなポリシーを生成し、リソース共有に含まれるすべてのイメージリソースにアタッチします。

#### Note

このポリシーは "Principal": "\*" を使用し、その後 "Condition" 要素を使用して、指定された PrincipalOrgID と一致する ID のアクセス許可を制限します。詳細については、「[「Principal»: "\\*" をリソースベースのポリシーで使用するこゝの影響](#)」を参照してください。

```

{

```

```
"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"
      }
    }
  }
]
```

## "Principal": "\*" をリソースベースのポリシーで使用するごとの影響

"Principal": "\*" をリソースベースのポリシーに含めると、そのポリシーは、Condition 要素が存在する場合、その要素によって課せられる制限に従い、リソースを含むアカウント内のすべての IAM プリンシパルにアクセスを付与します。呼び出し元のプリンシパルに適用されるポリシーの明示的な Deny ステートメントは、このポリシーによって付与されたアクセス許可を上書きします。ただし、すべての適用可能な ID ポリシーでの 暗示的な Deny (つまり明示的な Allow の欠如)、アクセス許可の境界、またはプリンシパルに対して Deny しないセッションポリシーは、そのようなリソースベースのポリシーによってアクションへのアクセスを付与します。

この動作がユースケースで適切でない場合は、関連するロールやユーザーに影響を与える明示的な Deny ステートメントを ID ポリシー、アクセス許可の境界、またはセッションポリシーに追加することで、この動作を制限できます。

## 管理アクセス許可

管理アクセス許可は、リソース共有内のサポートされているリソースタイプに対して、プリンシパルがどのような条件でアクションを実行できるかを定義します。リソース共有を作成する際に、リソース共有に含まれるリソースタイプごとに、どの管理アクセス許可を使用するかを指定する必要があります。管理アクセス許可には、プリンシパルが AWS RAM を使用してリソース共有で実行できる一連の actions と条件が含まれます。

リソース共有では、リソースタイプごとに1つの管理アクセス許可のみをアタッチすることができます。特定のタイプの一部のリソースである管理アクセス許可を使用し、同じタイプの他のリソースでは別の管理アクセス許可を使用するようなリソース共有を作成することはできません。これを行うには、2つの異なるリソース共有を作成し、それらのリソースを分割して、それぞれのセットに異なる管理アクセス許可を付与する必要があります。管理アクセス許可には、2つの異なるタイプがあります。

## AWS 管理アクセス許可

AWS 管理アクセス許可は、AWS が作成および管理し、一般的なユーザーシナリオ向けのアクセス許可を付与します。AWS RAM は、サポートされているすべてのリソースタイプに対して少なくとも1つの AWS 管理アクセス許可を定義します。リソースタイプによっては、複数の AWS 管理アクセス許可をサポートし、そのうちの1つの管理アクセス許可を AWS デフォルトとして指定しているものもあります。特に指定しない限り、[デフォルトの AWS 管理アクセス許可](#)が関連付けられます。

## カスタマー管理アクセス許可

カスタマー管理アクセス許可は、AWS RAM で共有リソースを使用する場合に、どのような条件下でどのアクションを実行できるかを正確に指定する、ユーザーが作成し管理する管理アクセス許可です。例えば、大規模な IP アドレスの管理に役立つ Amazon VPC IP Address Manager (IPAM) プールの読み取りアクセスを制限する場合を考えてみます。IP アドレスの割り当てはできるものの、他の開発者アカウントが割り当てた IP アドレスの範囲は表示できないようなカスタマー管理アクセス許可を開発者に対して作成することができます。最小特権のベストプラクティスに従って、必要なアクセス許可のみを付与し、共有リソースでタスクを実行できるような環境を構築することができます。

[グローバルコンテキストキー](#)や[サービス固有のキー](#)などの条件を追加して、プリンシパルがリソースにアクセスする条件を指定するオプションを使用して、リソース共有内のリソースタイプに対して独自のアクセス許可を定義します。これらのアクセス許可は、1つまたは複数の AWS RAM 共有で使用できます。カスタマー管理アクセス許可はリージョンに固有のものです。

AWS RAM は、管理アクセス許可を入力として使用し、共有するリソースに関する[リソースベースのポリシー](#)を作成します。

## 管理アクセス許可のバージョン

管理アクセス許可を変更すると、管理アクセス許可の新しいバージョンが作成されます。新しいバージョンはすべての新しいリソース共有のデフォルトになります。各管理アクセス許可には、必ず 1

つのバージョンがデフォルトバージョンとして指定されています。ユーザーまたは AWS が管理アクセス許可の新しいバージョンを作成する際、既存のリソース共有ごとに管理アクセス許可を明示的に更新する必要があります。リソース共有に適用する前に、この手順で変更を評価できます。すべての新しいリソース共有は、対応するリソースタイプ用の新しいバージョンの管理アクセス許可を自動的に使用します。

## AWS 管理アクセス許可のバージョン

AWS は、AWS 管理アクセス許可へのすべての変更を処理します。このような変更で、新しい機能への対応や発見された不具合の除去を行うことができます。リソース共有には、デフォルトの管理アクセス許可のバージョンのみを適用できます。

## カスタマー管理アクセス許可のバージョン

カスタマー管理アクセス許可へのすべての変更は、ユーザーが行います。ユーザーは、新しいデフォルトバージョンを作成したり、古いバージョンをデフォルトとして設定したり、リソース共有に関連付けられていないバージョンを削除したりできます。各カスタマー管理アクセス許可には最大 5 つのバージョンを作成できます。

リソース共有を作成または更新する場合、指定した管理アクセス許可のデフォルトバージョンのみをアタッチできます。詳細については、「[AWS 管理アクセス許可を新しいバージョンに更新する](#)」を参照してください。

# AWS リソースの共有

AWS RAM を使用して、所有しているリソースを共有するには、以下の手順に従います。

- [AWS Organizations 内でリソース共有を有効にする](#) (オプション)
- [リソース共有を作成する](#)

### メモ

- リソースを所有する AWS アカウント 外のプリンシパルを含むリソース共有は、リソースが作成されたアカウント内のリソースに適用されるアクセス許可やクォータに影響することはありません。
- AWS RAM はリージョンでのサービスです。共有先のプリンシパルは、リソース共有が作成された AWS リージョン 内のみのアクセスが可能です。



- リソースによっては、共有に関する特別な考慮事項と前提条件があります。詳細については、「[共有可能な AWS リソース](#)」を参照してください。

## AWS Organizations 内でリソース共有を有効にする

アカウントが AWS Organizations によって管理されている場合、それを活用すればリソースを共有しやすくなります。組織の有無にかかわらず、ユーザーは個々のアカウントとリソースを共有できます。ただし、アカウントが組織内にある場合には、各アカウントを列挙しなくても、個々のアカウント、または組織内または OU 内のすべてのアカウントとの共有が可能です。

組織内でリソースを共有するには、まず AWS RAM コンソールまたは AWS Command Line Interface (AWS CLI) を使用して AWS Organizations との共有を有効にする必要があります。組織内でリソースを共有する場合、AWS RAM はプリンシパルに招待状を送信しません。組織内のプリンシパルは、招待状を交換せずに共有リソースにアクセスできます。

組織内でリソースの共有を有効にする場合、AWS RAM は **AWSServiceRoleForResourceAccessManager** と呼ばれるサービスがリンクされたロールを作成します。このロールは AWS RAM サービスのみが引き受けることができ、AWS 管理ポリシー **AWSResourceAccessManagerServiceRolePolicy** を使用して、そのサービスが所属する組織に関する情報を取得する AWS RAM 権限を付与します。

組織全体または OU とリソースを共有する必要がなくなった場合は、リソース共有を無効にすることができます。詳細については、「[AWS Organizations とのリソース共有の無効化](#)」を参照してください。

### 最小アクセス許可

以下の処理を実行するには、次のアクセス許可を持つ組織の管理アカウントのプリンシパルでサインインする必要があります。

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



## 要件

- これらの手順は、組織の管理アカウントのプリンシパルとしてサインインしている場合のみ実行できます。
- その組織で、すべての機能が有効になっている必要があります。詳細については、[AWS Organizations ユーザーガイド](#)の「組織内のすべての機能の有効化」を参照してください。

### Important

AWS RAM コンソールまたは [enable-sharing-with-aws-organization](#) AWS CLI コマンドを使用して AWS Organizations との共有を有効にする必要があります。これにより、AWSServiceRoleForResourceAccessManager サービスリンクロールが確実に作成されます。AWS Organizations コンソールまたは [enable-aws-service-access](#) AWS CLI コマンドを使用して AWS Organizations で信頼されたアクセスを有効にすると、AWSServiceRoleForResourceAccessManager サービスリンクロールが作成されず、組織内でリソースを共有できなくなります。

## Console

組織内でリソース共有を有効にするには

1. AWS RAM コンソールの [\[Settings\]](#) (設定) ページを開きます。
2. [\[Enable sharing with AWS Organizations\]](#) (との共有を有効にする) を選択してから [\[Save settings\]](#) (設定の保存) を選択します。

## AWS CLI

組織内でリソース共有を有効にするには

[enable-sharing-with-aws-organization](#) コマンドを使用します。

このコマンドはどの AWS リージョン でも使用でき、AWS RAM がサポートされているすべてのリージョンで AWS Organizations との共有が有効になります。

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

```
}
```

## リソース共有を作成する

所有するリソースを共有するには、リソース共有を作成します。プロセスの概要を次に示します。

- 共有するリソースを追加します。
- 共有に含める各リソースタイプで、リソースタイプで使用する [管理アクセス許可](#) を指定します。
  - 使用可能な AWS 管理アクセス許可および既存のカスタマー管理アクセス許可を選択することができます。または、新しいカスタマー管理アクセス許可を作成することもできます。
  - AWS 管理アクセス許可は、標準的なユースケースに対応するように AWS によって作成されます。
  - カスタマー管理アクセス許可を使用すると、セキュリティやビジネスニーズに合わせて独自の管理アクセス許可をカスタマイズできます。

### Note

選択した管理アクセス許可に複数のバージョンがある場合、AWS RAM はデフォルトバージョンを自動的にアタッチします。アタッチできるのは、デフォルトとして指定されているバージョンのみです。

- リソースにアクセスできるようにしたいプリンシパルを指定します。

### 考慮事項

- 共有に含めた AWS リソースを後で削除する必要がある場合は、そのリソースをリソース共有から削除するか、リソース共有を削除することを推奨します。
- リソース共有に含めることができるリソースタイプの一覧は「[共有可能な AWS リソース](#)」で確認できます。
- 共有できるのは自分が [所有する](#) リソースのみです。自分が共有先になっているリソースを共有リソースにすることはできません。
- AWS RAM はリージョンでのサービスです。リソースを他の AWS アカウント 内のプリンシパルと共有する場合、プリンシパルはリソースが作成されたのと同じ AWS リージョン から各リソースにアクセスする必要があります。サポートされているグローバルリソースについては、そのリソースのサービスコンソールとツールがサポートしているどの AWS リージョン からでもアクセ

できます。このようなリソース共有とそのグローバルリソースは、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 の AWS RAM コンソールとツールでのみ表示できます。AWS RAM とグローバルリソースの詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。

- 共有しているアカウントが AWS Organizations の組織の一部で、組織で共有が有効化されている場合、組織内のあらゆる共有先プリンシパルには、招待状なしでリソース共有にアクセスできるアクセス許可が自動的に付与されます。組織のコンテキスト外で共有するアカウントのプリンシパルは、リソース共有に参加するための招待を受け取り、招待を受け入れた後でのみ、共有リソースへのアクセス権が付与されます。
- サービスプリンシパルと共有する場合、他のプリンシパルをリソース共有に関連付けることはできません。
- 組織の一部であるアカウントまたはプリンシパル間で共有する場合、組織のメンバーシップを変更すると、リソース共有へのアクセスに動的に影響します。
- 組織またはリソース共有へのアクセス権を持つ OU に AWS アカウント を追加する場合、新しいメンバーに共有リソースへのアクセス許可が自動的に付与されます。その後、共有先のアカウント管理者は、アカウント内の個々のプリンシパルに、共有内のリソースへのアクセス権を付与できます。
- 組織またはリソース共有へのアクセス権を持つ OU からアカウントを削除する場合、そのアカウントのすべてのプリンシパルは、リソース共有からアクセス可能なリソースへのアクセス許可を自動的に失います。
- メンバーアカウント、またはメンバーアカウントの IAM ロールまたはユーザーと直接共有し、そのアカウントを組織から削除する場合、そのアカウントのすべてのプリンシパルは、そのリソース共有からアクセス可能なリソースへのアクセス許可を失います。

#### Important

組織または OU と共有し、スコープにリソース共有を所有するアカウントが含まれる場合、共有アカウントのすべてのプリンシパルは、共有内のリソースに自動的にアクセスできるようになります。付与されるアクセスは、共有に関連付けられている管理アクセス許可によって定義されます。これは、共有内の各リソースに AWS RAM がアタッチするリソースベースのポリシーで "Principal": "\*" が使用されるためです。詳細については、「["Principal": "\\*" をリソースベースのポリシーで使用するものの影響](#)」を参照してください。

他のコンシューマーアカウントのプリンシパルは、共有のリソースにすぐにはアクセスできません。他のアカウントの管理者は、まず ID ベースのアクセス許可ポリシーを適切なプリンシパルにアタッチする必要があります。これらのポリシーは、リソース共有内の

個々のリソース ARN への Allow アクセスを付与する必要があります。これらのポリシーのアクセス許可は、リソース共有に関連付けられた管理アクセス許可で指定されているアクセス許可を超えることはできません。

- リソース共有に追加できるのは、アカウントがメンバーとして所属する組織とその組織の OU のみです。組織の外部から OU または組織をプリンシパルとしてリソース共有に追加することはできません。ただし、個々の AWS アカウント、または組織外のサポートされているサービスの IAM ロールをリソース共有のプリンシパルとして追加することはできます。

#### Note

すべてのリソースタイプを IAM ロールやユーザーと共有できるわけではありません。これらのプリンシパルと共有できるリソースの詳細については、「[共有可能な AWS リソース](#)」を参照してください。

- 次のリソースタイプについては、7 日以内に共有への招待を受け入れる必要があります。7 日以内に招待を受け入れない場合、招待は期限切れになり、自動的に辞退したことになります。

#### Important

以下のリストに含まれていない共有リソースタイプについては、12 時間以内にリソース共有への招待を受け入れる必要があります。12 時間が経過すると、招待は期限切れになり、リソース共有のエンドユーザープリンシパルとの関連付けが解除されます。エンドユーザーは招待を受け入れることができなくなります。

- Amazon Aurora – DB クラスター
- Amazon EC2 — キャパシティ予約と専有ホスト
- AWS License Manager - ライセンス設定
- AWS Outposts - ローカルゲートウェイルートテーブル、アウトポスト、サイト
- Amazon Route 53 – 転送ルール
- Amazon VPC — カスタマーが所有する IPv4 アドレス、プレフィックスリスト、サブネット、トラフィックミラーターゲット、トランジットゲートウェイ、トランジットゲートウェイマルチキャストドメイン

## Console

リソース共有を作成するには

1. [AWS RAM コンソール](#)を開きます。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) us-east-1 に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。リソース共有にグローバルリソースを含める場合は、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 を選択する必要があります。
3. AWS RAM を初めて使用する場合は、ホームページから [Create a resource share] (リソース共有の作成) を選択します。それ以外の場合、[\[Shared by me : Resource shares\]](#) (自分が共有: リソース共有) から [Create resource share] (リソース共有の作成) を選択します。
4. [Step 1: Specify resource share details] (ステップ 1: リソース共有の詳細を指定する) で、以下の手順に従います。
  - a. [Name] (名前) に、リソース共有のわかりやすい名前を入力します。
  - b. [Resources] (リソース) で、リソース共有に追加するリソースを以下のように選択します。
    - [Select resource type] (ターゲットリソースの選択) で、共有するリソースのタイプを選択します。そうすることで、共有可能なリソースのリストが、選択したタイプのリソースのみに絞り込まれます。
    - 結果のリソースリストで、共有したい個々のリソースの横にあるチェックボックスをオンにします。選択したリソースが [Selected resources] (選択済みリソース) に移動します。


特定のアベイラビリティゾーンに関連付けられているリソースを共有する場合、アベイラビリティゾーン ID (AZ ID) を使用すると、アカウント間でこれらのリソースの場所を判別するのに役立ちます。詳細については、「[AWS リソースのアベイラビリティゾーン ID](#)」を参照してください。
  - c. (オプション) [タグをアタッチする](#)には、[Tags] (タグ) にタグのキーと値を入力します。[Add new tag] (新しいタグを追加) を選択して、他のユーザーを追加します。この手順を必要なだけ繰り返します。これらのタグは、リソース共有内のリソースには適用されず、リソース共有自体にのみ適用されます。

5. [Next] (次へ) をクリックします。
6. 「手順 2: 管理アクセス許可を各リソースタイプに関連付ける」では、AWS で作成された管理アクセス許可をリソースタイプに関連付けるか、既存のカスタマー管理アクセス許可を選択するか、サポートされているリソースタイプに対して独自のカスタマー管理アクセス許可を作成するかを選択できます。詳細については、「[管理アクセス許可のタイプ](#)」を参照してください。

[カスタマー管理アクセス許可の作成] を選択して、共有ユースケースの要件を満たすカスタマー管理アクセス許可を作成します。詳細については、「[カスタマー管理アクセス許可を作成する](#)」を参照してください。プロセスが完了したら



を選択し、[管理アクセス許可] ドロップダウンリストから新しいカスタマー管理アクセス許可を選択します。

 Note

選択した管理アクセス許可に複数のバージョンがある場合、AWS RAM はデフォルトバージョンを自動的にアタッチします。デフォルトとして指定されたバージョンのみをアタッチできます。

管理アタッチで許可されているアクションを表示するには、[この管理アタッチのポリシーテンプレートを表示] を展開します。

7. [Next] (次へ) をクリックします。
8. 「手順 3: プリンシパルにアクセス権限を付与する」で、以下を行います。
  - a. デフォルトでは、[すべてのユーザーとの共有を許可] が選択されています。つまり、サポートされているリソースタイプでは、組織外の AWS アカウント とリソースを共有できます。これは、Amazon VPC サブネットなど、組織内のみで共有できるリソースタイプには影響しません。[サポートされているリソースタイプ](#)の一部は、IAM ロールおよびユーザーと共有できます。

組織内のプリンシパルのみでリソース共有を制限するには、[自分の組織内でのみ共有を許可] を選択します。

- b. [Principals] (プリンシパル) について、以下の操作をします。


- 組織、組織単位 (OU) または組織の一部である AWS アカウント を追加するには、[Display organizational structure] (組織構造の表示) をオンにします。そうすると組織図が表示されます。次いで、追加したい各プリンシパルの横にあるチェックボックスをオンにします。

 Important

組織または OU と共有し、スコープにリソース共有を所有するアカウントが含まれる場合、共有アカウントのすべてのプリンシパルは、共有内のリソースに自動的にアクセスできるようになります。付与されるアクセスは、共有に関連付けられている管理アクセス許可によって定義されます。これは、共有内の各リソースに AWS RAM がアタッチするリソースベースのポリシーで "Principal": "\*" が使用されるためです。詳細については、「["Principal": "\\*" をリソースベースのポリシーで使用するの影](#)響」を参照してください。

他のコンシューマーアカウントのプリンシパルは、共有のリソースにすぐにはアクセスできません。他のアカウントの管理者は、まず ID ベースのアクセス許可ポリシーを適切なプリンシパルにアタッチする必要があります。これらのポリシーは、リソース共有内の個々のリソース ARN への Allow アクセスを付与する必要があります。これらのポリシーのアクセス許可は、リソース共有に関連付けられた管理アクセス許可で指定されているアクセス許可を超えることはできません。

- 組織 (o- で始まる ID) を選択した場合、組織内のすべての AWS アカウント のプリンシパルがリソース共有にアクセスできます。
- OU (ou- で始まる ID) を選択した場合、OU 内とその子 OU 内のすべての AWS アカウント のプリンシパルがリソース共有にアクセスできます。
- 個々の AWS アカウント を選択した場合、そのアカウントのプリンシパルのみがリソース共有にアクセスできます。

 Note

[Display organizational structure] (組織構造の表示) トグルが表示されるのは、AWS Organizations とのが有効になっていて、組織の管理アカウントにサインインしているときのみです。



この方法で組織外の AWS アカウント または IAM ロール/ユーザーを指定することはできません。代わりに、[組織構造を表示] を無効にし、ドロップダウンリストとテキストボックスを使用して ID または ARN を入力します。

- 組織外のプリンシパルを含む ID または ARN でプリンシパルを指定するには、プリンシパルごとにプリンシパルタイプを選択します。次に、(AWS アカウント、組織、または OU の) ID または (IAM ロールまたはユーザーの) ARN を入力して [追加] を選択します。使用可能なプリンシパルタイプと ID および ARN 形式は以下のとおりです。

- AWS アカウント — AWS アカウント を追加するには、12 桁のアカウント ID を入力します。例:

123456789012

- [Organization] (組織) — AWS アカウント のすべてを追加するには、組織の ID を入力します。例:

o-abcd1234

- [Organizational unit (OU)] (部門単位 (OU)) — OU を追加するには、OU の ID を入力します。例:


ou-abcd-1234efgh

- [IAM role] (IAM ロール) — IAM ロールを追加するには、ロールの ARN を入力します。次の構文を使用します。

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

例:

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

 Note

IAM ロールの一意的 ARN を取得するには、[IAM コンソールでロールのリストを表示](#)し、[get-role](#) AWS CLI コマンドまたは [GetRole](#) API アクションを使用します。


- [IAM user] (IAM ユーザー) — IAM ユーザーを追加するには、ユーザーの ARN を入力します。次の構文を使用します。



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

例:

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

 Note

IAM ユーザーの一意的 ARN を取得するには、[IAM コンソールでユーザーのリストを表示し](#)、[get-user](#) AWS CLI コマンドまたは [GetUser](#) API アクションを使用します。

- サービスプリンシパル — サービスプリンシパルを追加するには、[プリンシパルタイプの選択] ドロップボックスで [サービスプリンシパル] を選択します。AWS サービスプリンシパル名を入力します。次の構文を使用します。

- *service-id*.amazonaws.com

例:

pca-connector-ad.amazonaws.com

- c. [Selected principals] (選択されたプリンシパル) について、指定したプリンシパルがリストに入っていることを確認します。

9. [Next] (次へ) をクリックします。

10. [Step 4: Review and create] (ステップ 4: 確認して作成する) で、リソース共有に関する設定の詳細を見直します。任意のステップについて設定を変更するには、戻りたいステップに対応するリンクを選択して必要なだけ変更を加えます。

11. リソース共有を確認し終わった、[Create resource share] (リソース共有の作成) を選択します。

リソースとプリンシパルの関連付けが完了するまでに数分かかることがあります。リソース共有を使用する前にこのプロセスを完了させてください。

12. リソースとプリンシパルの追加および削除、リソース共有へのカスタムタグの適用はいつでもできます。リソース共有に含まれるリソースタイプのうち、デフォルトの管理アクセス許可以外をサポートするタイプについては、管理アクセス許可を変更できます。リソースを共有する必要がなくなったら、リソース共有を削除できます。詳細については、「[所有する AWS リソースの共有](#)」を参照してください。

## AWS CLI

リソース共有を作成するには

[create-resource-share](#) コマンドを実行します。次のコマンドは、組織内の AWS アカウント のすべてと共有されるリソース共有を作成します。共有は、AWS License Manager ライセンス設定を含み、これはそのリソースタイプに対するデフォルトの管理アクセス許可を付与します。

**Note**

このリソース共有のリソースタイプでカスタマー管理アクセス許可を使用する場合は、既存のカスタマー管理アクセス許可を使用するか、新しいカスタマー管理アクセス許可を作成します。カスタマー管理アクセス許可の ARN をメモし、リソース共有を作成します。詳細については、「[カスタマー管理アクセス許可を作成する](#)」を参照してください。

```
$ 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"
  }
}
```

## 共有 AWS リソースの使用

AWS Resource Access Manager を使用して自分のアカウントと共有されたリソースの使用を開始するには、以下のタスクを完了します。

### タスク

- [リソース共有の招待に応答する](#)
- [自分が共有先になっているリソースを使用する](#)

## リソース共有の招待に応答する

リソース共有の招待状を受け取った場合、共有リソースへのアクセス許可を得るには、その招待を受け入れる必要があります。

招待状は、次のシナリオでは使用されません。

- 自分が AWS Organizations の組織のメンバーであり、組織内での共有が有効になっている場合、組織内のプリンシパルには招待なしで共有リソースに対するアクセス許可が自動的に付与されます。
- リソースを所有する AWS アカウント と共有する場合、そのアカウントのプリンシパルは、招待なしで自動的に共有リソースにアクセスできます。

### Console

招待に応答するには

1. AWS RAM コンソールで [\[Shared with me : Resource shares\]](#) (自分と共有: リソース共有) ページを開きます。

#### Note

リソース共有は、それが作成された AWS リージョン 内でのみ表示されます。想定していたリソース共有がコンソールに表示されない場合は、右上隅のドロップダウンコントロールを使用して別の AWS リージョン への切り替えが必要な場合があります。

2. 自分にアクセスが付与されたリソース共有のリストを見直します。

[Status] (ステータス) 列は、リソース共有の現在の参加ステータスを示します。Pending ステータスは、受信者がリソース共有に追加されたけれども招待を受け入れても拒否してもいないことを示します。

- リソース共有の招待に応答するには、リソース共有 ID を選択し、[Accept resource share] (リソース共有を承諾する) または [Reject resource share] (リソース共有を拒否する) を選択します。招待を拒否すると、リソースにアクセスできなくなります。招待を受け入れると、リソースにアクセスできます。

## AWS CLI

開始するには、使用可能なリソース共有の招待状のリストを取得します。次のコマンド例は、us-west-2 リージョンで実行され、単一のリソース共有が PENDING 状態で利用可能であることを示します。

```
$ 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"
    }
  ]
}
```

前のコマンドで指定された招待状の Amazon リソースネーム (ARN) を次のコマンドでパラメータとして使用することで招待を受け入れることができます。

```
$ 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-bbbbbbb222222",
    "senderAccountId": "111122223333",
    "receiverAccountId": "444455556666",
    "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
    "status": "ACCEPTED"
  }
}
```

出力には `status` が `ACCEPTED` に変わったことが示されます。これで、そのリソース共有に含まれるリソースを受け入れ側アカウントのプリンシパルで使用できるようになりました。

## 自分が共有先になっているリソースを使用する

リソース共有への招待を受け入れると、共有リソースについて特定のアクションを実行できるようになります。これらのアクションはリソースのタイプによって異なります。詳細については、「[共有可能な AWS リソース](#)」を参照してください。リソースは、各リソースのサービスコンソールと API/CLI 操作で直接利用できます。リソースがリージョンに固有の場合は、サービスコンソールまたは API/CLI コマンドで正しい AWS リージョンを使用する必要があります。リソースがグローバルの場合は、指定されたホームリージョン (米国東部 (バージニア北部)、`us-east-1`) を使用する必要があります。AWS RAM のリソースを表示するには、リソース共有が作成された AWS リージョンで AWS RAM コンソールを開く必要があります。

# 共有 AWS リソースの使用

AWS Resource Access Manager (AWS RAM) を使用すると、所有している AWS リソースを共有したり、自分が共有先になっている AWS リソースにアクセスしたりできます。

## 目次

- [リージョナルリソースの共有とグローバルリソースの共有の比較](#)
  - [リージョナルリソースとグローバルリソースの違い](#)
  - [リソース共有とそのリージョン](#)
- [所有する AWS リソースの共有](#)
  - [AWS RAM で作成したリソース共有の表示](#)
  - [AWS RAM 内でのリソース共有の作成](#)
  - [AWS RAM 内のリソース共有を更新します。](#)
  - [AWS RAM 内の共有リソースの表示](#)
  - [AWS RAM 内のリソース共有相手のプリンシパルの表示するには](#)
  - [AWS RAM 内のリソース共有の削除](#)
- [自分と共有されている AWS リソースにアクセスする](#)
  - [リソース共有への招待の受け入れと拒否](#)
  - [共有しているリソース共有の表示](#)
  - [自分が共有先になっているリソースの表示](#)
  - [共有相手のプリンシパルの表示](#)
  - [リソース共有の終了](#)
    - [リソース共有を終了するための前提条件](#)
    - [リソース共有を終了するには](#)
- [AWS リソースのアベイラビリティーゾーン ID](#)

## リージョナルリソースの共有とグローバルリソースの共有の比較

このトピックでは、AWS Resource Access Manager (AWS RAM) でのリージョナルリソースとグローバルリソースの処理の違いについて説明します。

リソースには、リージョナルリソースとグローバルリソースの 2 つがあります。[Amazon リソースネーム \(ARN\)](#) の 4 番目のフィールドを使用して、リソースがリージョナルかグローバルかを識別できます。リージョナルリソースには、AWS リージョンが表示されます。何も表示されない場合、リソースはグローバルです。

## リージョナルリソースとグローバルリソースの違い

### リージョナルリソース

AWS RAM で共有できるリソースのほとんどはリージョナルリソースです。特定の AWS リージョンにリージョナルリソースを作成すると、リージョナルリソースはそのリージョンに存在するようになります。これらのリソースの表示や操作を行うには、そのリージョンに対してオペレーションを指示する必要があります。例えば、AWS Management Console を使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを作成するには、インスタンスを作成する [AWS リージョン](#) を選択します。AWS Command Line Interface (AWS CLI) を使用してインスタンスを作成する場合は、`--region` パラメータを含めます。各 AWS SDK には、オペレーションで使用するリージョンを指定する独自の等価メカニズムがあります。

リージョナルリソースを使用するのは、いくつかの理由があります。理由の 1 つは、リソースと、そのリソースへのアクセスに使用するサービスエンドポイントを、できるだけ顧客の近くに置くことです。これにより、レイテンシーが最小限に抑えられるため、パフォーマンスが向上します。もう 1 つの理由は、分離境界を設けることです。これにより、複数のリージョンに独立したリソースのコピーを作成することで、負荷を分散してスケーラビリティを向上させることができます。同時に、リソースを互いに分離することで可用性を向上させます。

コンソールまたは AWS CLI コマンドに別の AWS リージョンを指定した場合、以前のリージョンで表示できたリソースの表示や操作ができなくなります。

リージョナルリソースの [Amazon リソースネーム \(ARN\)](#) を表示すると、そのリソースを含むリージョンが ARN の 4 番目のフィールドとして指定されています。例えば、Amazon EC2 インスタンスはリージョナルリソースです。このようなリソースは、us-east-1 リージョンにある VPC の以下の例と似た ARN を持ちます。

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

### グローバルリソース

一部の AWS サービスは、グローバルにアクセスできるリソースをサポートしています。つまり、どこからでもリソースを使用できます。グローバルサービスのコンソールでは AWS リー

ジョンを指定しません。グローバルリソースにアクセスするには、サービスの AWS CLI および AWS SDK オペレーションを使用する際に `--region` を指定しません。

グローバルリソースは、特定のリソースのインスタンスが一度に 1 つしか存在できないことが必要なケースをサポートします。このようなシナリオでは、異なるリージョンのコピーとの間でレプリケーションや同期を行うことは適切ではありません。リソースのコンシューマーが変更内容を瞬時に確認できるようにするとレイテンシーが増加する可能性があるため、単一のグローバルエンドポイントにアクセスする必要があることは許容できると考えられます。例えば、AWS Cloud WAN コアネットワークをグローバルリソースとして作成すると、そのネットワークはすべてのユーザーに対して一貫性のあるものになります。これは、すべてのリージョンにまたがる 1 つの連続したグローバルネットワークのように見えます。

グローバルリソースの [Amazon リソースネーム \(ARN\)](#) には、リージョンは含まれません。次の Cloud WAN コアネットワークのサンプル ARN のように、このような ARN の 4 番目のフィールドは空です。

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

## リソース共有とそのリージョン

AWS RAM はリージョナルサービスで、リソース共有はリージョナルです。そのため、リソース共有には、そのリソース共有と同じ AWS リージョンのリソースや、サポートされている任意のグローバルリソースを含めることができます。リソース共有を作成するリージョンは、リソース共有のホームリージョンです。

### Important

現在、グローバルリソースを含むリソース共有は、指定されたホームリージョンである米国東部 (バージニア北部) リージョン `us-east-1` でのみ作成できます。リソース共有は 1 つのホームリージョンでのみ作成できますが、グローバル共有リソースは、そのサービスのコンソールまたは CLI と SDK の操作では、標準のグローバルリソースとして表示されます。ホームリージョンの制限はリソース共有にのみ適用され、共有に含まれるリソースには適用されません。

`us-west-2` リージョンで作成したリージョナルリソースを共有するには、そのリージョンで `us-west-2` を使用するように AWS RAM コンソールを設定して、作成する必要があります。異なる



AWS リージョンのリソースを含むリソース共有は作成できません。つまり、us-west-2 と eu-north-1 の両方のリソースを共有するには、2 つの異なるリソース共有を作成する必要があります。2 つの異なるリージョンのリソースを 1 つのリソース共有にまとめることはできません。

AWS RAM コンソールでグローバルリソースを共有するには、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 を使用するように AWS RAM コンソールを設定する必要があります。その後、指定されたホームリージョンにリソース共有を作成します。1 つのリソース共有にグローバルリソースを混在させることができるのは、us-east-1 リージョンのリソースだけです。

グローバルリソースは指定されたホームリージョンの AWS RAM リソース共有でのみ表示できますが、共有した後もグローバルリソースのままです。共有されたリソースには、元の AWS アカウントでアクセスできたどのリージョンの共有 AWS アカウント からでもアクセスできます。

### 考慮事項

- AWS RAM コンソールでリソース共有を作成するには、共有するリソースを含むリージョンを使用する必要があります。グローバルリソースを含める場合は、指定されたホームリージョンを使用して共有を作成する必要があります。例えば、AWS Cloud WAN コアネットワークを共有するには、us-east-1 リージョンにリソース共有を作成する必要があります。
- AWS RAM コンソールでリソース共有を表示または変更するには、リソース共有を含むリージョンを使用する必要があります。同様に、AWS RAM AWS CLI および SDK オペレーションでは、オペレーションで指定したリージョンにあるリソース共有のみを操作できます。グローバルリソースを含むリソース共有を表示または変更するには、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 を使用する必要があります。
- AWS RAM コンソールでリージョナルリソースを表示してリソース共有に含めるには、リージョナルリソースを含むリージョンを使用する必要があります。
- AWS RAM コンソールでグローバルリソースを表示してリソース共有に含めるには、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 を使用する必要があります。
- リージョナルリソースとグローバルリソースの両方を含むリソース共有は、指定されたホームリージョンである米国東部 (バージニア北部) リージョン us-east-1 でのみ作成できます。

## 所有する AWS リソースの共有

AWS Resource Access Manager (AWS RAM) を使用して、指定したプリンシパルと指定したリソースを共有できます。このセクションでは、新しいリソース共有の作成、既存のリソース共有の変更、不要になったリソース共有の削除方法について説明します。

## トピック

- [AWS RAM で作成したリソース共有の表示](#)
- [AWS RAM 内でのリソース共有の作成](#)
- [AWS RAM 内のリソース共有を更新します。](#)
- [AWS RAM 内の共有リソースの表示](#)
- [AWS RAM 内のリソース共有相手のプリンシパルの表示するには](#)
- [AWS RAM 内のリソース共有の削除](#)

## AWS RAM で作成したリソース共有の表示

作成したリソース共有のリストを表示できます。どのリソースをどのプリンシパルと共有しているかを確認できます。

### Console

リソース共有を表示するには

1. AWS RAM コンソールで [\[Shared by me : Resource shares\]](#) (自分が共有: リソース共有) ページを開きます。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. 結果にあるリソース共有で使用されている管理アクセス許可に、デフォルトとして指定されている管理アクセス許可の新しいバージョンが含まれている場合、ページに警告バナーが表示されます。ページ上部の [レビューしてすべて更新] を選択すると、管理アクセス許可のすべてのバージョンを一度に更新できます。

または、管理アクセス許可の新しいバージョンが 1 つ以上ある個々のリソース共有では、[ステータス] 列に [更新可能] と表示されます。このリンクを選択すると、更新された管理アクセス許可のバージョンの確認プロセスが開始され、リソース共有内の該当するリソースタイプのバージョンとして割り当てることができます。

4. (オプション) フィルタを適用して特定の共有リソースを見つけます。複数のフィルタを適用して検索を絞り込むことができます。リソース共有名の一部などのキーワードを入力する

と、そのキーワードが名前に含まれるリソース共有のみを一覧表示できます。テキストボックスを選択すると、推奨される属性フィールドのドロップダウンリストが表示されます。いずれかを選択してから、そのフィールドで選択可能な値をリストから選択できます。他の属性やキーワードを追加しながら目的のリソースが見つかるまで続けてください。

5. 確認するリソース共有の名前を選択します。コンソールには、リソース共有に関する以下の情報が表示されます。
  - 概要 — リソース共有名、ID、所有者、Amazon リソースネーム (ARN)、作成日、外部アカウントとの共有を許可するかどうか、および現在のステータスの一覧です。
  - マネージド許可 — このリソース共有にアタッチされている管理アクセス許可の一覧です。リソース共有には、リソースタイプごとに1つだけ管理アクセス許可を含めることができます。各管理アクセス許可には、そのリソース共有に関連付けられている管理アクセス許可のバージョンが表示されます。デフォルトバージョンでない場合、コンソールには [デフォルトバージョンに更新] のリンクが表示されます。このリンクを選択すると、デフォルトバージョンを使用するようにリソース共有を更新できます。
  - 共有リソース — リソース共有に含まれる個々のリソースの一覧です。リソースの ID を選択してブラウザで新しいタブを開き、ネイティブサービスのコンソールにリソースを表示します。
  - 共有プリンシパル — リソース共有相手のプリンシパルのリスト。
  - タグ - リソース共有自体にアタッチされているタグのキーと値のペアの一覧を表示します。これらは、リソース共有に含まれる個々のリソースにアタッチされているタグではありません。

## AWS CLI

リソース共有を表示するには

`--resource-owner` パラメータを `SELF` に設定して [get-resource-shares](#) コマンドを使用すると、AWS アカウント 内で作成したリソース共有の詳細を表示できます。

次の例は、呼び出し元 AWS アカウント について現在の AWS リージョン (`us-east-1`) 内で共有されているリソース共有を示しています。別のリージョンで作成されたリソース共有を取得するには、`--region <region-code>` パラメータを使用します。グローバルリソースを含むリソースシェアを含めるには、米国東部 (バージニア北部) `us-east-1` リージョンを指定する必要があります。

```
$ 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"
    }
  ]
}
```

## AWS RAM 内でのリソース共有の作成

所有するリソースを共有するには、リソース共有を作成します。プロセスの概要を次に示します。

- 共有するリソースを追加します。
- 共有に含める各リソースタイプで、リソースタイプで使用する[管理アクセス許可](#)を指定します。
  - 使用可能な AWS 管理アクセス許可および既存のカスタマー管理アクセス許可を選択することができます。または、新しいカスタマー管理アクセス許可を作成することもできます。
  - AWS 管理アクセス許可は、標準的なユースケースに対応するように AWS によって作成されます。
  - カスタマー管理アクセス許可を使用すると、セキュリティやビジネスニーズに合わせて独自の管理アクセス許可をカスタマイズできます。

**Note**

選択した管理アクセス許可に複数のバージョンがある場合、AWS RAM はデフォルトバージョンを自動的にアタッチします。アタッチできるのは、デフォルトとして指定されているバージョンのみです。

**3. リソースにアクセスできるようにしたいプリンシパルを指定します。****考慮事項**

- 共有に含めた AWS リソースを後で削除する必要がある場合は、そのリソースをリソース共有から削除するか、リソース共有を削除することを推奨します。
- リソース共有に含めることができるリソースタイプの一覧は「[共有可能な AWS リソース](#)」で確認できます。
- 共有できるのは自分が[所有する](#)リソースのみです。自分が共有先になっているリソースを共有リソースにすることはできません。
- AWS RAM はリージョンでのサービスです。リソースを他の AWS アカウント 内のプリンシパルと共有する場合、プリンシパルはリソースが作成されたのと同じ AWS リージョン から各リソースにアクセスする必要があります。サポートされているグローバルリソースについては、そのリソースのサービスコンソールとツールがサポートしているどの AWS リージョン からでもアクセスできます。このようなリソース共有とそのグローバルリソースは、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 の AWS RAM コンソールとツールでのみ表示できます。AWS RAM とグローバルリソースの詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
- 共有しているアカウントが AWS Organizations の組織の一部で、組織で共有が有効化されている場合、組織内のあらゆる共有先プリンシパルには、招待状なしでリソース共有にアクセスできるアクセス許可が自動的に付与されます。組織のコンテキスト外で共有するアカウントのプリンシパルは、リソース共有に参加するための招待を受け取り、招待を受け入れた後でのみ、共有リソースへのアクセス権が付与されます。
- サービスプリンシパルと共有する場合、他のプリンシパルをリソース共有に関連付けることはできません。
- 組織の一部であるアカウントまたはプリンシパル間で共有する場合、組織のメンバーシップを変更すると、リソース共有へのアクセスに動的に影響します。
  - 組織またはリソース共有へのアクセス権を持つ OU に AWS アカウント を追加する場合、新しいメンバーに共有リソースへのアクセス許可が自動的に付与されます。その後、共有先のアカウ

ント管理者は、アカウント内の個々のプリンシパルに、共有内のリソースへのアクセス権を付与できます。

- 組織またはリソース共有へのアクセス権を持つ OU からアカウントを削除する場合、そのアカウントのすべてのプリンシパルは、リソース共有からアクセス可能なリソースへのアクセス許可を自動的に失います。
- メンバーアカウント、またはメンバーアカウントの IAM ロールまたはユーザーと直接共有し、そのアカウントを組織から削除する場合、そのアカウントのすべてのプリンシパルは、そのリソース共有からアクセス可能なリソースへのアクセス許可を失います。

### Important

組織または OU と共有し、スコープにリソース共有を所有するアカウントが含まれる場合、共有アカウントのすべてのプリンシパルは、共有内のリソースに自動的にアクセスできるようになります。付与されるアクセスは、共有に関連付けられている管理アクセス許可によって定義されます。これは、共有内の各リソースに AWS RAM がアタッチするリソースベースのポリシーで "Principal": "\*" が使用されるためです。詳細については、「["Principal": "\\*" をリソースベースのポリシーで使用するの影響](#)」を参照してください。

他のコンシューマーアカウントのプリンシパルは、共有のリソースにすぐにはアクセスできません。他のアカウントの管理者は、まず ID ベースのアクセス許可ポリシーを適切なプリンシパルにアタッチする必要があります。これらのポリシーは、リソース共有内の個々のリソース ARN への Allow アクセスを付与する必要があります。これらのポリシーのアクセス許可は、リソース共有に関連付けられた管理アクセス許可で指定されているアクセス許可を超えることはできません。

- リソース共有に追加できるのは、アカウントがメンバーとして所属する組織とその組織の OU のみです。組織の外部から OU または組織をプリンシパルとしてリソース共有に追加することはできません。ただし、個々の AWS アカウント、または組織外のサポートされているサービスの IAM ロールをリソース共有のプリンシパルとして追加することはできます。

### Note

すべてのリソースタイプを IAM ロールやユーザーと共有できるわけではありません。これらのプリンシパルと共有できるリソースの詳細については、「[共有可能な AWS リソース](#)」を参照してください。



- 次のリソースタイプについては、7 日以内に共有への招待を受け入れる必要があります。7 日以内に招待を受け入れない場合、招待は期限切れになり、自動的に辞退したことになります。

### Important

以下のリストに含まれていない共有リソースタイプについては、12 時間以内にリソース共有への招待を受け入れる必要があります。12 時間が経過すると、招待は期限切れになり、リソース共有のエンドユーザープリンシパルとの関連付けが解除されます。エンドユーザーは招待を受け入れることができなくなります。

- Amazon Aurora – DB クラスター
- Amazon EC2 — キャパシティ予約と専用ホスト
- AWS License Manager – ライセンス設定
- AWS Outposts - ローカルゲートウェイルートテーブル、アウトポスト、サイト
- Amazon Route 53 – 転送ルール
- Amazon VPC — カスタマーが所有する IPv4 アドレス、プレフィックスリスト、サブネット、トラフィックミラーターゲット、トランジットゲートウェイ、トランジットゲートウェイマルチキャストドメイン

## Console

リソース共有を作成するには

1. [AWS RAM コンソール](#)を開きます。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。リソース共有にグローバルリソースを含める場合は、指定されたホームリージョンである米国東部 (バージニア北部) us-east-1 を選択する必要があります。
3. AWS RAM を初めて使用する場合は、ホームページから [Create a resource share] (リソース共有の作成) を選択します。それ以外の場合、[\[Shared by me : Resource shares\]](#) (自分が共有: リソース共有) から [Create resource share] (リソース共有の作成) を選択します。

4. [Step 1: Specify resource share details] (ステップ 1: リソース共有の詳細を指定する) で、以下の手順に従います。
  - a. [Name] (名前) に、リソース共有のわかりやすい名前を入力します。
  - b. [Resources] (リソース) で、リソース共有に追加するリソースを以下のように選択します。
    - [Select resource type] (ターゲットリソースの選択) で、共有するリソースのタイプを選択します。そうすることで、共有可能なリソースのリストが、選択したタイプのリソースのみに絞り込まれます。
    - 結果のリソースリストで、共有したい個々のリソースの横にあるチェックボックスをオンにします。選択したリソースが [Selected resources] (選択済みリソース) に移動します。

特定のアベイラビリティゾーンに関連付けられているリソースを共有する場合、アベイラビリティゾーン ID (AZ ID) を使用すると、アカウント間でこれらのリソースの場所を判別するのに役立ちます。詳細については、「[AWS リソースのアベイラビリティゾーン ID](#)」を参照してください。
  - c. (オプション) [タグをアタッチする](#) には、[Tags] (タグ) にタグのキーと値を入力します。[Add new tag] (新しいタグを追加) を選択して、他のユーザーを追加します。この手順を必要なだけ繰り返します。これらのタグは、リソース共有内のリソースには適用されず、リソース共有自体にのみ適用されます。
5. [Next] (次へ) をクリックします。
6. 「手順 2: 管理アクセス許可を各リソースタイプに関連付ける」では、AWS で作成された管理アクセス許可をリソースタイプに関連付けるか、既存のカスタマー管理アクセス許可を選択するか、サポートされているリソースタイプに対して独自のカスタマー管理アクセス許可を作成するかを選択できます。詳細については、「[管理アクセス許可のタイプ](#)」を参照してください。

[カスタマー管理アクセス許可の作成] を選択して、共有ユースケースの要件を満たすカスタマー管理アクセス許可を作成します。詳細については、「[カスタマー管理アクセス許可を作成する](#)」を参照してください。プロセスが完了したら



を選択し、[管理アクセス許可] ドロップダウンリストから新しいカスタマー管理アクセス許可を選択します。



**Note**

選択した管理アクセス許可に複数のバージョンがある場合、AWS RAM はデフォルトバージョンを自動的にアタッチします。デフォルトとして指定されたバージョンのみをアタッチできます。

管理アタッチで許可されているアクションを表示するには、[この管理アタッチのポリシーテンプレートを表示] を展開します。

7. [Next] (次へ) をクリックします。
8. 「手順 3: プリンシパルにアクセス権限を付与する」で、以下を行います。
  - a. デフォルトでは、[すべてのユーザーとの共有を許可] が選択されています。つまり、サポートされているリソースタイプでは、組織外の AWS アカウント とリソースを共有できます。これは、Amazon VPC サブネットなど、組織内のみで共有できるリソースタイプには影響しません。[サポートされているリソースタイプ](#)の一部は、IAM ロールおよびユーザーと共有できます。

組織内のプリンシパルのみでリソース共有を制限するには、[自分の組織内でのみ共有を許可] を選択します。


- b. [Principals] (プリンシパル) について、以下の操作をします。
  - 組織、組織単位 (OU) または組織の一部である AWS アカウント を追加するには、[Display organizational structure] (組織構造の表示) をオンにします。そうすると組織図が表示されます。次いで、追加したい各プリンシパルの横にあるチェックボックスをオンにします。

**Important**

組織または OU と共有し、スコープにリソース共有を所有するアカウントが含まれる場合、共有アカウントのすべてのプリンシパルは、共有内のリソースに自動的にアクセスできるようになります。付与されるアクセスは、共有に関連付けられている管理アクセス許可によって定義されます。これは、共有内の各リソースに AWS RAM がアタッチするリソースベースのポリシーで "Principal": "\*" が使用されるためです。詳細については、「["Principal": "\\*" をリソースベースのポリシーで使用する時の影響](#)」を参照してください。

他のコンシューマーアカウントのプリンシパルは、共有のリソースにすぐにはアクセスできません。他のアカウントの管理者は、まず ID ベースのアクセス許可ポリシーを適切なプリンシパルにアタッチする必要があります。これらのポリシーは、リソース共有内の個々のリソース ARN への Allow アクセスを付与する必要があります。これらのポリシーのアクセス許可は、リソース共有に関連付けられた管理アクセス許可で指定されているアクセス許可を超えることはできません。

- 組織 (o- で始まる ID) を選択した場合、組織内のすべての AWS アカウント のプリンシパルがリソース共有にアクセスできます。
- OU (ou- で始まる ID) を選択した場合、OU 内とその子 OU 内のすべての AWS アカウント のプリンシパルがリソース共有にアクセスできます。
- 個々の AWS アカウント を選択した場合、そのアカウントのプリンシパルのみがリソース共有にアクセスできます。

 Note

[Display organizational structure] (組織構造の表示) トグルが表示されるのは、AWS Organizations とのが有効になっていて、組織の管理アカウントにサインインしているときのみです。

この方法で組織外の AWS アカウント または IAM ロール/ユーザーを指定することはできません。代わりに、[組織構造を表示] を無効にし、ドロップダウンリストとテキストボックスを使用して ID または ARN を入力します。

- 組織外のプリンシパルを含む ID または ARN でプリンシパルを指定するには、プリンシパルごとにプリンシパルタイプを選択します。次に、(AWS アカウント、組織、または OU の) ID または (IAM ロールまたはユーザーの) ARN を入力して [追加] を選択します。使用可能なプリンシパルタイプと ID および ARN 形式は以下のとおりです。

- AWS アカウント — AWS アカウント を追加するには、12 桁のアカウント ID を入力します。例:

123456789012

- [Organization] (組織) — AWS アカウント のすべてを追加するには、組織の ID を入力します。例:

o-abcd1234

- [Organizational unit (OU)] (部門単位 (OU)) — OU を追加するには、OU の ID を入力します。例:


ou-abcd-1234efgh

- [IAM role] (IAM ロール) — IAM ロールを追加するには、ロールの ARN を入力します。次の構文を使用します。

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

例:

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

 Note


IAM ロールの一意的 ARN を取得するには、[IAM コンソールでロールのリストを表示](#)し、[get-role](#) AWS CLI コマンドまたは [GetRole](#) API アクションを使用します。

- [IAM user] (IAM ユーザー) — IAM ユーザーを追加するには、ユーザーの ARN を入力します。次の構文を使用します。

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

例:

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

 Note

IAM ユーザーの一意的 ARN を取得するには、[IAM コンソールでユーザーのリストを表示](#)し、[get-user](#) AWS CLI コマンドまたは [GetUser](#) API アクションを使用します。

- サービスプリンシパル — サービスプリンシパルを追加するには、[プリンシパルタイプの選択] ドロップボックスで [サービスプリンシパル] を選択します。AWS サービスプリンシパル名を入力します。次の構文を使用します。
- *service-id*.amazonaws.com

例:

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

- c. [Selected principals] (選択されたプリンシパル) について、指定したプリンシパルがリストに入っていることを確認します。

9. [Next] (次へ) をクリックします。

10. [Step 4: Review and create] (ステップ 4: 確認して作成する) で、リソース共有に関する設定の詳細を見直します。任意のステップについて設定を変更するには、戻りたいステップに対応するリンクを選択して必要なだけ変更を加えます。

11. リソース共有を確認し終わった、[Create resource share] (リソース共有の作成) を選択します。

リソースとプリンシパルの関連付けが完了するまでに数分かかることがあります。リソース共有を使用する前にこのプロセスを完了させてください。

12. リソースとプリンシパルの追加および削除、リソース共有へのカスタムタグの適用はいつでもできます。リソース共有に含まれるリソースタイプのうち、デフォルトの管理アクセス許可外をサポートするタイプについては、管理アクセス許可を変更できます。リソースを共有する必要がなくなったら、リソース共有を削除できます。詳細については、「[所有する AWS リソースの共有](#)」を参照してください。

## AWS CLI

リソース共有を作成するには

[create-resource-share](#) コマンドを実行します。次のコマンドは、組織内の AWS アカウント のすべてと共有されるリソース共有を作成します。共有は、AWS License Manager ライセンス設定を含み、これはそのリソースタイプに対するデフォルトの管理アクセス許可を付与します。

### Note

このリソース共有のリソースタイプでカスタマー管理アクセス許可を使用する場合は、既存のカスタマー管理アクセス許可を使用するか、新しいカスタマー管理アクセス許可を作成します。カスタマー管理アクセス許可の ARN をメモし、リソース共有を作成します。詳細については、「[カスタマー管理アクセス許可を作成する](#)」を参照してください。

```
$ 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"  
  }  
}
```

## AWS RAM 内のリソース共有を更新します。

AWS RAM 内のリソース共有は、以下の方法でいつでも更新できます。

- 作成したリソース共有にプリンシパル、リソース、またはタグを追加できます。
- デフォルトの AWS 管理アクセス許可以外をサポートするリソースタイプでは、各リソースタイプに適用する管理アクセス許可を選択できます。
- リソース共有にアタッチされている管理アクセス許可に新しいデフォルトバージョンがある場合は、管理アクセス許可を更新して新しいバージョンを使用できます。
- リソース共有 からプリンシパルまたはリソースを削除することで、共有リソースへのアクセスを取り消すことができます。アクセスを取り消すと、プリンシパルは共有リソースにアクセスできなくなります。

### Note

リソースを共有する相手のプリンシパルは、共有が空の場合、またはリソース共有の終了をサポートするリソースタイプのみが含まれている場合、リソース共有を終了できます。終了

をサポートしていないリソースタイプがリソース共有に含まれている場合、プリンシパルには共有所有者に連絡する必要があることを知らせるメッセージが表示されます。この場合、リソース共有の所有者は、リソース共有からプリンシパルを削除する必要があります。このアクションがサポートされないリソースタイプのリストについては、「[リソース共有を終了するための前提条件](#)」を参照してください。

## Console

リソース共有を更新するには

1. AWS RAM コンソールで [\[Shared by me : Resource shares\]](#) (自分が共有: リソース共有) に移動します。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. リソース共有を選択してから [Modify] (変更) を選択します。
4. [Step 1: Specify resource share details] (ステップ 1: リソース共有の詳細を指定する) で、リソース共有の詳細を見直し、必要に応じて以下のいずれかを更新します。
  - a. (オプション) リソース共有の名前を変更するには、[Name] (名前) を編集します。
  - b. (オプション) リソース共有にリソースを追加するには、[Resources] (リソース) の下でリソースのタイプを選択してからリソースの横にあるチェックボックスをオンにします。グローバルリソースは、AWS Management Console でリージョンを米国東部 (バージニア北部) (us-east-1) に設定した場合にのみ表示されます。
  - c. (オプション) リソース共有からリソースを削除するには、[Selected resources] (選択されたリソース) の下でリソースを見つけてからリソースの ID の横にある [X] を選択します。
  - d. (オプション) リソース共有にタグを追加するには、[Tags] (タグ) の下にある空のテキストボックスにタグのキーと値を入力します。タグのキーと値のペアを複数追加するには、[Add new tag] (新しいタグを追加) を選択します。最大 50 個のタグを追加できます。
  - e. リソース共有からタグを削除するには、[Tags] (タグ) の下で削除したいタグを見つけてその横にある [Remove] (削除) をクリックします。

5. [Next] (次へ) をクリックします。
6. (オプション) 「手順 2: 管理アクセス許可を各リソースタイプに関連付ける」では、AWS で作成された管理アクセス許可をリソースタイプに関連付けるか、既存のカスタマー管理アクセス許可を選択するか、独自のカスタマー管理アクセス許可を作成するかを選択できます。詳細については、「[管理アクセス許可のタイプ](#)」を参照してください。

[カスタマー管理アクセス許可の作成] を選択して、共有ユースケースの要件を満たすカスタマー管理アクセス許可を作成することもできます。詳細については、「[カスタマー管理アクセス許可を作成する](#)」を参照してください。プロセスが完了したら



を選択し、[管理アクセス許可] ドロップダウンリストから新しいカスタマー管理アクセス許可を選択します。

管理アタッチで許可されているアクションを表示するには、[この管理アタッチのポリシーテンプレートを表示] を展開します。

7. リソース共有に現在割り当てられている管理アクセス許可のバージョンが現在のデフォルトバージョンでない場合は、[デフォルトバージョンに更新] を選択してデフォルトバージョンに更新できます。

**Note**

最後のステップを終えてリソース共有に変更を保存するまでは、[以前のバージョンに戻す] を選択してバージョンの更新をキャンセルできます。ただし AWS 管理アクセス許可の場合、リソース共有を保存すると、変更は確定し、以前のバージョンに戻ることはできなくなります。

8. [Next] (次へ) をクリックします。
9. [Step 3: Choose principals that are allowed to access] (ステップ 3: アクセスを許可するプリンシパルを選択する) で、選択したプリンシパルを見直し、必要に応じて以下のいずれかを更新します。
  - a. (オプション) 組織内外のプリンシパルとの共有の有効化を変更するには、以下のオプションのいずれかを選択します。
    - 組織外の AWS アカウント、または個々の IAM ロール/ユーザーとリソースを共有するには、[外部のプリンシパルとの共有を許可] を選択します。



- AWS Organizations 内の組織内のプリンシパルのみにリソース共有を制限するには、[Allow sharing with principals in your organization only] (組織内のプリンシパルとの共有のみを許可する) を選択します。
- b. [Principals] (プリンシパル) について、以下の操作をします。
- (オプション) 組織、組織単位 (OU)、または組織内のメンバー AWS アカウント を追加するには、[組織構造を表示] をオンにして組織図のツリーを表示します。次いで、追加したい各プリンシパルの横にあるチェックボックスをオンにします。

#### Important

組織または OU と共有し、スコープにリソース共有を所有するアカウントが含まれる場合、共有アカウントのすべてのプリンシパルは、共有内のリソースに自動的にアクセスできるようになります。付与されるアクセスは、共有に関連付けられている管理アクセス許可によって定義されます。これは、共有内の各リソースに AWS RAM がアタッチするリソーススペースのポリシーで "Principal": "\*" が使用されるためです。詳細については、[「"Principal": "\\*" をリソーススペースのポリシーで使用するごとの影響」](#)を参照してください。

他のコンシューマーアカウントのプリンシパルは、共有のリソースにすぐにはアクセスできません。他のアカウントの管理者は、まず ID ベースのアクセス許可ポリシーを適切なプリンシパルにアタッチする必要があります。これらのポリシーは、リソース共有内の個々のリソース ARN への Allow アクセスを付与する必要があります。これらのポリシーのアクセス許可は、リソース共有に関連付けられた管理アクセス許可で指定されているアクセス許可を超えることはできません。

#### Note

[Display organizational structure] (組織構造の表示) トグルが表示されるのは、AWS Organizations との共有が有効になっていて、組織の管理アカウントにプリンシパルとしてサインインしているときのみです。

この方法で組織外の AWS アカウント または IAM ロール/ユーザーを指定することはできません。代わりに、プリンシパルの識別子を入力することでこれらのプリンシパルを追加する必要があり、識別子は [Display organizational



structure](組織構造の表示) スイッチの下にあるテキストボックスに表示されます。次の箇条書きを参照してください。

- (オプション) 識別子でプリンシパルを追加するには、ドロップダウンリストでプリンシパルタイプを選択してからプリンシパルの ID または ARN を入力します。最後に、[Add] (追加) を選択します。

個々の AWS アカウント を選択した場合、そのアカウントのみがリソース共有にアクセスできます。次のオプションのいずれかを選択できます。

- 別の AWS アカウント (リソース所有者以外) — リソースを他のアカウントが使用できるようにします。アカウントの管理者は、ID ベースのアクセス許可ポリシーを使用して、共有リソースへのアクセスを個々のロールやユーザーに付与して、プロセスを完了する必要があります。これらのアクセス許可は、リソース共有にアタッチされた管理アクセス許可で定義されているアクセス許可を超えることはできません。
- この AWS アカウント (リソース所有者) — リソース所有アカウントのすべてのロールとユーザーには、リソース共有にアタッチされた管理アクセス許可によって定義されたアクセスが自動的に付与されます。
- 追加内容は直ちに [Selected principals] (選択されたプリンシパル) リストに表示されません。

その後、この手順を繰り返して、アカウント、OU、または組織を追加できます。

- (オプション) プリンシパルを削除するには、[Selected principals] (選択されたプリンシパル) から対象のプリンシパルを見つけて、チェックボックスをオンにしてから [Deselect] (選択解除) を選択します。

10. [Next] (次へ) をクリックします。

11. [Step 4: Review and create] (ステップ 4: 確認して更新する) で、リソース共有に関する設定の詳細を見直します。

12. 任意のステップについて設定を変更するには、戻りたいステップに対応するリンクを選択して必要なだけ変更を加えます。

管理アクセス許可でデフォルト以外のバージョンを使用している場合は、[デフォルトバージョンに更新] を選択して変更することもできます。

13. 変更が終わったら [Update resource share] (リソース共有の更新) を選択します。

## AWS CLI

リソース共有を更新するには

以下の AWS CLI コマンドを使用してリソース共有を変更できます。

- リソース共有の名前を変更したり、外部プリンシパルを許可するかどうかを変更するには、[update-resource-share](#) コマンドを使用します。次の例では、指定したリソース共有の名前を変更し、その組織のプリンシパルのみを許可するように設定します。リソース共有を含む AWS リージョン のサービスエンドポイントを使用する必要があります。

```
$ 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
  }
}
```

- リソース共有にリソースを追加するには、[associate-resource-share](#) コマンドを使用します。次の例では、指定したリソース共有にサブネットを追加します。

```
$ 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
  ]
}

```

- リソース共有内のリソースタイプの管理アクセス許可を追加または置換するには、[list-permissions](#) コマンドおよび [associate-resource-share-permission](#) コマンドを使用します。リソース共有では、リソースタイプごとに1つの管理アクセス許可のみを割り当てることができます。既に管理アクセス許可を持っているリソースタイプに管理アクセス許可を追加しようとすると、`--replace` オプションを含まない場合はエラーが発生してコマンドが失敗します。

次のコマンド例では、Amazon Elastic Compute Cloud (Amazon EC2) サブネットで使用可能な管理アクセス許可のARNをリスト化し、これらのARNのいずれかを使用して、指定されたリソース共有内のそのリソースタイプに現在割り当てられているAWS管理アクセス許可を置き換えます。

```

$ 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
}

```

- リソース共有からリソースを削除するには、[disassociate-resource-share](#) コマンドを使用します。次の例では、指定したリソース共有から指定した ARN を持つ Amazon EC2 サブネットを削除します。

```
$ 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  
  ]  
}
```

- リソース共有にアタッチされたタグを変更するには、[tag-resource](#) コマンドおよび [untag-resource](#) コマンドを使用します。次の例では、指定されたリソース共有にタグ `project=lima` を追加します。

```
$ 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
```

次の例では、指定されたリソース共有から `project` のキーを持つタグを削除します。

```
$ 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
```

タグ付けコマンドが成功した場合、出力は生成されません。

## AWS RAM 内の共有リソースの表示

すべてのリソース共有にわたって、共有した個々のリソースのリストを表示できます。このリストは、現在共有しているリソース、そのリソースが含まれているリソース共有数、そのリソースにアクセスできるプリンシパルの数を確認するのに役立ちます。

### Console

現在共有しているリソースを表示するには

1. AWS RAM コンソールで [\[Shared by me : Shared resources\]](#) (自分が共有: 共有リソース) ページを開きます。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. 共有リソース別に以下の情報が表示されます。
  - [Resource ID] (リソース ID) — リソースの ID。リソースの ID を選択してブラウザで新しいタブを開き、ネイティブサービスのコンソールにリソースを表示します。
  - [Resource type] (リソースタイプ) — リソースのタイプ。
  - [Last share date] (最終共有日) - リソースが最後に共有された日付。
  - [Resource shares] (リソース共有) — リソースを含んでいるリソース共有の数。リソース共有のリストを表示するには、番号を選択します。
  - [Principals] (プリンシパル) — リソースにアクセスできるプリンシパルの数。プリンシパルを表示する値を選択します。

### AWS CLI

現在共有しているリソースを表示するには

`--resource-owner` パラメータを `SELF` に設定して [list-resources](#) コマンドを使用すると、現在共有しているリソースの詳細を表示できます。

次の例は、呼び出し元 AWS アカウント について AWS リージョン (us-east-1) 内のリソース共有に含まれているリソースを示しています。別のリージョンで共有されたリソースを取得するには、`--region <region-code>` パラメータを使用します。

```
$ 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"
    }
  ]
}
```

## AWS RAM 内のリソース共有相手のプリンシパルの表示するには

リソースを共有している相手のプリンシパルをすべてのリソース共有にわたって表示できます。プリンシパルのリストを表示することで、共有リソースにアクセスできるユーザーを判別できます。

### Console

リソース共有相手のプリンシパルの表示するには

1. AWS RAM コンソールで [\[Shared by me : Principals\]](#) (自分が共有: プリンシパル) に移動します。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-

east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。

3. フィルタを適用して特定のプリンシパルを見つけます。複数のフィルタを適用して検索を絞り込むことができます。テキストボックスを選択すると、推奨される属性フィールドのドロップダウンリストが表示されます。いずれかを選択してから、そのフィールドで選択可能な値をリストから選択できます。他の属性やキーワードの追加は、目的のリソースが見つかるまで可能です。
4. リストに表示された各プリンシパルについて、コンソールに以下の情報が表示されます。
  - [Principal ID] (プリンシパル ID) — プリンシパルの ID。ID を選択してブラウザで新しいタブを開き、プリンシパルをネイティブコンソールに表示します。
  - [Resources shares] (リソース共有) — 指定したプリンシパルと共有しているリソース共有の数。番号を選択すると、リソース共有のリストが表示されます。
  - [Resources] (リソース) — プリンシパルと共有しているリソースの件数。番号を選択すると、共有リソースのリストが表示されます。

## AWS CLI

リソース共有相手のプリンシパルの表示するには

[list-principals](#) コマンドを使用すると、呼び出し元アカウントについて現在の AWS リージョンで作成したリソース共有内で参照するプリンシパルのリストを取得できます。

次の例では、呼び出し元アカウントのデフォルトリージョンで作成された共有へのアクセス権を持つプリンシパルを一覧表示します。この例では、プリンシパルは呼び出し元アカウントの組織および別の AWS アカウントであり、2 つの異なるリソース共有の一部となっています。リソース共有を含む AWS リージョンのサービスエンドポイントを使用する必要があります。

```
$ 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
    }
]
}
```

## AWS RAM 内のリソース共有の削除

リソース共有はいつでも削除できます。リソース共有を削除すると、そのリソース共有に関連付けられていたすべてのプリンシパルが共有リソースにアクセスできなくなります。リソース共有を削除しても、リソースは削除されません。

### AWS リソースを削除するには

リソース共有に含めた AWS リソースを削除する場合は、AWS では、まずそのリソースを含むすべてのリソース共有からリソースを削除するか、リソース共有を削除することをお勧めします。

削除されたリソース共有は、削除後しばらくは AWS RAM コンソールに表示されたままになりますが、そのステータスは Deleted に変わります。

### Console

リソース共有を削除するには

1. AWS RAM コンソールで [\[Shared by me : Resource shares\]](#) (自分が共有: リソース共有) ページを開きます。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-



east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。

3. 削除したいリソース共有を選択します。

**⚠ Warning**

リソース共有を適切に選択したことを確認してください。削除したリソースを回復することはできません。

4. [Delete] (削除) を選択し、確認メッセージに応答して [Delete] (削除) を選択します。
5. 削除されたリソース共有は 2 時間後に表示されなくなります。それまでは、「削除済み」ステータスでコンプライアンスに表示され続けます。

## AWS CLI

リソース共有を削除するには

[delete-resource-share](#) コマンドを使用すると、不要になったリソース共有を削除できます。

次の例では、まず [get-resource-shares](#) コマンドを実行して、削除したいリソース共有の Amazon リソース名前 (ARN) を取得します。次いで、[delete-resource-share](#) コマンドを使用して、指定したリソース共有を削除します。

```
$ 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  
}
```

## 自分と共有されている AWS リソースにアクセスする

AWS Resource Access Manager (AWS RAM) を使用すると、自分が追加されたリソース共有、アクセスできる共有リソース、およびリソースを共有 AWS アカウント している を表示できます。共有リソースへのアクセスが不要になったら、リソース共有を終了することもできます。

### コンテンツ

- [リソース共有への招待の受け入れと拒否](#)
- [共有しているリソース共有の表示](#)
- [自分が共有先になっているリソースの表示](#)
- [共有相手のプリンシパルの表示](#)
- [リソース共有の終了](#)

## リソース共有への招待の受け入れと拒否

共有リソースにアクセスするには、リソース共有の所有者に自分をプリンシパルとして追加してもらう必要があります。所有者は以下のいずれかをプリンシパルとしてリソース共有に追加できます。

- 自分のアカウントが属する組織
- 自分のアカウントを含む組織単位 (OU)
- 自分の個人アカウント
- サポートされているリソースタイプの場合、自分の IAM ロールまたはユーザー

内の組織のメンバー AWS アカウント である を通じてリソース共有に追加され AWS Organizations、組織内での共有が有効になっている場合、招待を承諾しなくても共有リソースに自動的にアクセスできます。また、サービスプリンシパルは、招待を受け入れずに共有リソースに自動的にアクセスできます。その後、招待元のアカウントが組織から削除された場合、そのアカウントの

すべてのプリンシパルは、リソース共有からアクセス可能なリソースへのアクセスを自動的に失います。

以下のいずれかによって自分がリソース共有に追加された場合、リソース共有に参加するための招待状を受け取ります。

- の組織外のアカウント AWS Organizations
- との共有が有効になってい AWS Organizations ない場合の組織内のアカウント

リソース共有の招待状を受け取った場合、共有リソースへのアクセス権を得るには、その招待を受け入れる必要があります。招待を辞退した場合、共有リソースにアクセスすることはできません。

次のリソースタイプについては、7 日以内に共有への招待を受け入れる必要があります。7 日以内に招待を受け入れない場合、招待は期限切れになり、自動的に辞退したことになります。

#### Important

以下のリストに含まれていない共有リソースタイプについては、12 時間以内にリソース共有への招待を受け入れる必要があります。12 時間が経過すると、招待は期限切れになり、リソース共有のエンドユーザープリンシパルとの関連付けが解除されます。エンドユーザーは招待を受け入れることができなくなります。

- Amazon Aurora – DB クラスター
- Amazon EC2 — キャパシティ予約と専有ホスト
- AWS License Manager – ライセンス設定
- AWS Outposts – ローカルゲートウェイルートテーブル、アウトポスト、サイト
- Amazon Route 53 – 転送ルール
- Amazon VPC — カスタマーが所有する IPv4 アドレス、プレフィックスリスト、サブネット、トラフィックミラーターゲット、トランジットゲートウェイ、トランジットゲートウェイマルチキャストドメイン

## Console

リソース共有の招待に応答するには

1. AWS RAM コンソールの「[Share with me : リソース共有](#)」ページに移動します。

2. AWS RAM リソース共有は特定の に存在するため AWS リージョン、コンソールの右上隅にある AWS リージョン ドロップダウンリストから適切な を選択します。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部)、 () に設定する必要がありますus-east-1。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. 自分が追加された先のリソース共有のリストを見直します。

[Status] (ステータス) 列は、リソース共有の現在の参加ステータスを示します。Pending ステータスは、受信者がリソース共有に追加されたけれども招待を受け入れても拒否してもいいことを示します。

4. リソース共有の招待に応答するには、リソース共有 ID を選択し、[Accept resource share] (リソース共有を承諾する) または [Reject resource share] (リソース共有を拒否する) を選択します。招待を拒否すると、リソースにアクセスできなくなります。招待を受け入れると、リソースにアクセスできます。

## AWS CLI

リソース共有の招待に応答するには

以下のコマンドを使用して、リソース共有への招待を受け入れるか拒否できます。

- [get-resource-share-invitations](#)
- [accept-resource-share-invitation](#)
- [reject-resource-share-invitation](#)

1. 次の例では、[get-resource-share-invitations](#) コマンドを使用して、ユーザーの で使用可能なすべての招待のリストを取得します AWS アカウント。AWS CLI query パラメータを使用すると、出力を、 が status に設定されている招待のみに制限できます PENDING。この例では、アカウント 111111111111 から送られた 1 通の招待状が、指定された AWS リージョン の現在のアカウント PENDING で 123456789012であることを示しています。

```
$ aws ram get-resource-share-invitations \
  --region us-east-1 \
  --query 'resourceShareInvitations[?status==`PENDING`]'
{
  "resourceShareInvitations": [
    {
```

```

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

```

2. 受け入れたい招待状が見つかったら、次のコマンドで承諾できるように出力の `resourceShareInvitationArn` を書き留めます。

```

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

```

成功した場合、`status` が `PENDING` から `ACCEPTED` に変わったというレスポンスが示されま  
す。

代わりに招待を拒否したい場合は、同じパラメータを指定して [reject-resource-share-invitation](#) コ  
マンドを実行します。

```
$ 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"
  }
}
```

## 共有しているリソース共有の表示

アクセスできるリソース共有を表示できます。どのプリンシパルが自分どリソースを共有しているのかがわかります。

### Console

リソース共有を表示するには

1. AWS RAM コンソールで [\[Shared with me : Resource shares\]](#) (自分と共有: リソース共有) に移動します。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. (オプション) フィルタを適用して特定の共有リソースを見つけます。複数のフィルタを適用して検索を絞り込むことができます。リソース共有名の一部などのキーワードを入力すると、そのキーワードが名前に含まれるリソース共有のみを一覧表示できます。テキストボックスを選択すると、推奨される属性フィールドのドロップダウンリストが表示されます。い

いずれかを選択してから、そのフィールドで選択可能な値をリストから選択できます。他の属性やキーワードを追加しながら目的のリソースが見つかるまで続けてください。

4. AWS RAM コンソールには、以下の情報が表示されます。

- [Name] (名前) — リソース共有の名前。
- [ID] — リソース共有の ID。ID を選択すると、リソース共有の詳細ページが表示されます。
- [Owner] (所有者) — リソース共有を作成した AWS アカウント の ID。
- [Status] (ステータス) — リソース共有の現在のステータス。可能な値は以下のとおりです。
  - Active — リソース共有がアクティブで利用可能です。
  - Deleted — リソース共有が削除され、使用できなくなりました。
  - Pending — リソース共有の承諾を求める招待が応答待ちです。

## AWS CLI

リソース共有を表示するには

`--resource-owner` パラメータを `OTHER-ACCOUNTS` に設定して [get-resource-shares](#) コマンドを使用します。

次の例は、指定された AWS リージョン で共有されているリソース共有と共有元の他の AWS アカウント のリストを示します。

```
$ 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"
    }
  ]
}
```

## 自分が共有先になっているリソースの表示

アクセスできる共有リソースが表示されます。どのプリンシパルが自分とリソースを共有していて、どのリソース共有にそのリソースが含まれているかがわかります。

### Console

自分が共有先になっているリソースを表示するには

1. AWS RAM コンソールで [\[Shared with me : Shared resources\]](#) (自分と共有: 共有リソース) に移動します。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. フィルタを適用して特定の共有リソースを見つけます。複数のフィルタを適用して検索を絞り込むことができます。
4. 次の情報が利用可能です。
  - [Resource ID] (リソース ID) — リソースの ID。サービスコンソールに表示するリソースの ID を選択します。
  - [Resource type] (リソースタイプ) — リソースのタイプ。



- [Last share date] (最終共有日) - リソースを共有した日付。
- [Resource shares] (リソース共有) — リソースが含まれるリソース共有の数。共有リソースを表示するための値を選択します。
- [Owner ID] (所有者 ID) — リソースを所有しているプリンシパルの ID。

## AWS CLI

自分が共有先になっているリソースを表示するには

[list-resources](#) コマンドを使用して、共有しているリソースを表示できます。

以下は、別の AWS リージョン で指定された AWS アカун ト のリソース共有でアクセスできるリソースの詳細を表示するコマンドの例です。

```
$ 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"
    }
  ]
}
```

## 共有相手のプリンシパルの表示

リソースを共有しているすべてのプリンシパルのリストを表示できます。共有されているリソースおよびリソース共有を確認できます。

## Console

リソースを共有しているすべてのプリンシパルのリストを表示するには

1. AWS RAM コンソール (<https://console.aws.amazon.com/ram>) を開きます。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. ナビゲーションペインで、[Shared with me] (自分と共有)、[Principals] (プリンシパル) の順に選択します。
4. (オプション) フィルタを適用して特定のプリンシパルを検索できます。複数のフィルタを適用して検索を絞り込むことができます。
5. コンソールには、以下の情報が表示されます。
  - [Principal ID] (プリンシパル ID) - 自分の共有相手のプリンシパルの ID。
  - [Resource shares] (リソース共有) — プリンシパルが自分を追加したリソース共有の数。番号を選択すると、リソース共有のリストが表示されます。
  - [Resources] (リソース) - プリンシパルと共有しているリソースの件数。リソースのリストを表示する値を選択します。

## AWS CLI

リソースを共有しているすべてのプリンシパルのリストを表示するには

[list-principals](#) コマンドを使用すると、AWS アカウント とリソースを共有しているプリンシパルのリストを取得できます。

次のコマンド例では、指定した AWS リージョン でオペレーションの呼び出しに使用されたアカウントとリソース共有を共有した AWS アカウント に関する詳細を表示します。

```
$ aws ram list-principals \
  --region us-east-1 \
  --resource-owner OTHER-ACCOUNTS
{
  "principals": [
    {
      "id": "111111111111",
```

```

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

```

## リソース共有の終了

自分が共有先になっているリソースにアクセスする必要がなくなった場合は、いつでもリソース共有を終了できます。リソース共有を終了すると、共有リソースにアクセスする権利を失います。

### リソース共有を終了するための前提条件

- リソース共有を終了できるのは、リソース共有が個人の AWS アカウント として共有され、組織として共有されていない場合のみです。自分が組織内の AWS アカウント によって追加され、AWS Organizations との共有が有効になっている場合、リソース共有を終了することはできません。組織内のリソース共有へのアクセスは自動です。
- リソース共有を終了するには、リソース共有が空であるか、または共有の終了をサポートするリソースタイプのみが含まれていることを確認します。

リソース共有の終了は、以下のリソースタイプのみでサポートされています。

サービス	リソースタイプ
Amazon Aurora	rds:Cluster
Amazon EC2	ec2:CapacityReservation ec2:DedicatedHost
AWS License Manager	license-manager:LicenseConfiguration
AWS Outposts	ec2:LocalGatewayRouteTable outposts:Outpost

サービス	リソースタイプ
	outposts:Site
Amazon Route 53	route53resolver:ResolverRule
Amazon VPC	ec2:CoipPool ec2:PrefixList ec2:Subnet ec2:TrafficMirrorTarget ec2:TransitGateway ec2:TransitGatewayMulticastDomain

## リソース共有を終了するには

### Console

リソース共有を終了するには

1. AWS RAM コンソールで [\[Shared with me : Resource shares\]](#) (自分と共有: リソース共有) に移動します。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。
3. 終了したいリソース共有を選択します。
4. [Leave resource share] (リソース共有の終了) を選択し、確認ダイアログボックスで [Leave] (終了する) を選択します。

## AWS CLI

リソース共有を終了するには

[disassociate-resource-share](#) コマンドを使用してリソース共有を終了します。

以下のコマンド例では、コマンドを呼び出した AWS アカウント は、ARN で指定されたリソース共有で共有されているリソースへのアクセス権を失います。終了したいリソース共有を含む AWS リージョン 内のサービスエンドポイントにリクエストを送信する必要があります。

1. まず、リソース共有リストを取得し、終了したいリソース共有の ARN を取得します。

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

2. 次に、コマンドを実行して、リソース共有を終了します。アカウント 123456789012 が共有している指定されたリソース共有から関連付けを解除するには、自分のアカウント ID である 111111111111 をプリンシパルとして指定する必要があります。

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

```

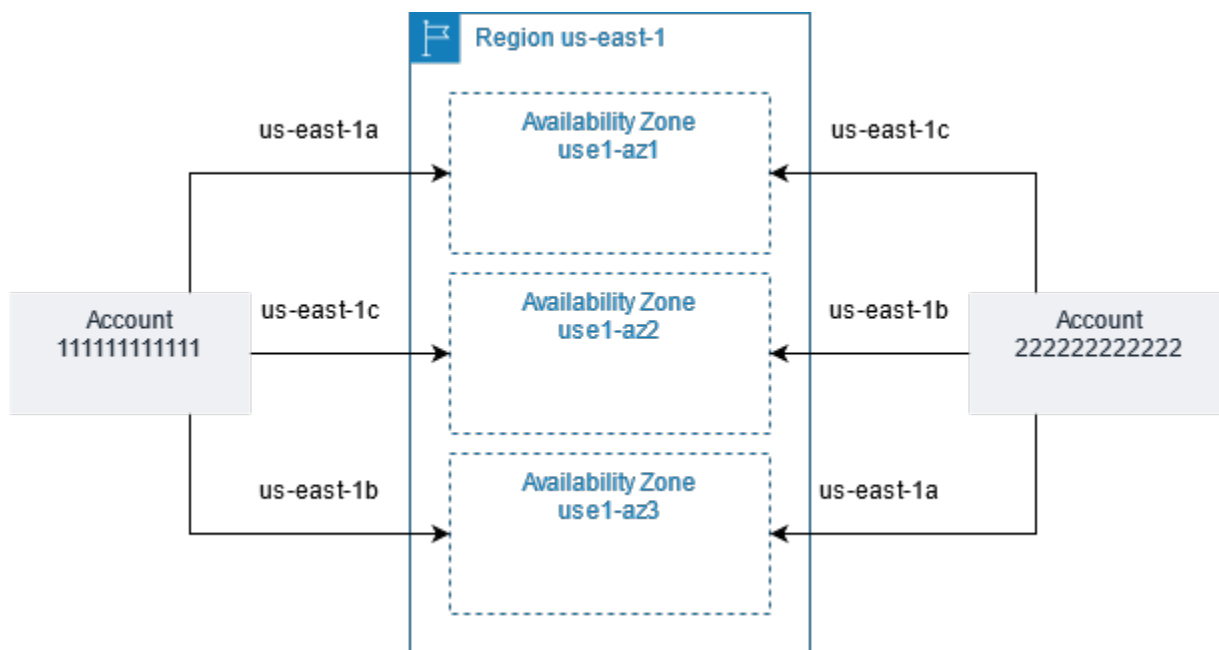
    "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
    "associatedEntity": "123456789012",
    "associationType": "PRINCIPAL",
    "status": "DISASSOCIATING",
    "external": false
  }
]
}

```

## AWS リソースのアベイラビリティゾーン ID

AWS は、物理アベイラビリティゾーンを AWS アカウント ごとのアベイラビリティゾーン名にランダムにマップします。このアプローチは、AWS リージョン 内のアベイラビリティゾーンにリソースを分散するうえで役立ち、各リージョンのアベイラビリティゾーン「a」にリソースが集中しなくて済みます。その結果、自分の AWS アカウントのアベイラビリティゾーン us-east-1a が、異なる AWS アカウントについては us-east-1a と同じ物理的な場所を表さない可能性があります。詳細については、[Amazon EC2 ユーザーガイド](#)の「リージョンとアベイラビリティゾーン」を参照してください。

次の図は、アベイラビリティゾーン名のマッピングがアカウントごとに異なる場合があっても各アカウントの AZ ID が同じになる様子を示しています。



一部のリソースについては、AWS リージョンのみでなくアベイラビリティゾーンの識別も必要です。例えば、Amazon VPC サブネットなどです。単一のアカウント内では、特定の名前へのアベイラビリティゾーンのマッピングは重要ではありません。しかし、AWS RAM を使用して他の AWS アカウントとリソースを共有しようとする場合、マッピングは重要です。このランダムなマッピングにより、共有リソースにアクセスしようとするアカウントには、どのアベイラビリティゾーンを参照すべきかがわからなくなります。その一助として、このようなリソースについては、アカウントに関係するリソースの実際の場所を AZ ID で特定することもできます。AZ ID は、すべての AWS アカウントにわたる同じアベイラビリティゾーンを一貫して示す一意の識別子です。例えば、use1-az1 は us-east-1 リージョン内のアベイラビリティゾーン ID であり、どの AWS アカウントでも同じ物理的な場所を表します。

AZ ID を使用すると、アカウント間でリソースの場所を区別できます。例えば、AZ ID use1-az2 のアベイラビリティゾーンにあるサブネットを別のアカウントと共有する場合、このサブネットは AZ ID が同じく use1-az2 であるアベイラビリティゾーンのそのアカウントでも利用できます。各サブネットの AZ ID は、Amazon VPC コンソールに表示され、AWS CLI を使用してクエリできます。

## Console

アカウントのアベイラビリティゾーンの AZ ID を表示するには

1. AWS RAM コンソールで [AWS RAM コンソール](#) ページに移動します。
2. [Your AZ ID] (お客様の AZ ID) の下に現在の AWS リージョンに関する AZ ID が表示されます。

## AWS CLI

アカウントのアベイラビリティゾーンの AZ ID を表示するには

次のコマンド例では、us-west-2 リージョン内のアベイラビリティゾーンの AZ ID とそれらが呼び出し側の AWS アカウントにどうマップされるかを示します。

```
$ 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"
  }
]
```



## 共有可能な AWS リソース

AWS Resource Access Manager (AWS RAM) を使用すると、他のによって作成および管理されているリソースを共有できます AWS のサービス。リソースは個々のと共有できません AWS アカウント。AWS Organizationsにおいて組織または組織単位 (OU) 内のアカウントとリソースを共有することもできます。サポートされているリソースタイプによっては、個々の AWS Identity and Access Management (IAM) ロールおよびユーザーとリソースを共有することもできます。

以下のセクションでは、を使用して共有 AWS のサービスできるリソースタイプを別にグループ化して一覧表示します AWS RAM。表の列には、各リソースタイプがサポートする機能を記載しています。

IAM ユーザーおよびロールと共有可能	 <p>はい - このタイプのリソースは、アカウントに加えて、個々の AWS Identity and Access Management (IAM) ロールおよびユーザーと共有できます。</p>  <p>いいえ - このタイプのリソースはアカウントとのみ共有できます。</p>
組織外のアカウントと共有可能	 <p>はい - このタイプのリソースは、組織内外で個々のアカウントと共有できるだけです。詳細については、「<a href="#">考慮事項</a>」を参照してください。</p>



いいえ - このタイプのリソースは、同じ組織のメンバーであるアカウントとのみ共有できます。

カスタマー  
管理アクセ  
ス許可を使  
用可能

でサポートされているすべてのリソースタイプは AWS 管理  
アクセス許可 AWS RAM をサポートしますが、この列のは  
いは、カスタマー管理アクセス許可がこのリソースタイプ  
でもサポートされることを意味します。



はい — このタイプのリソースでは、カスタマー管理アクセ  
ス許可を使用できます。



いいえ — このタイプのリソースでは、カスタマー管理アク  
セス許可は使用できません。

サービスブ  
リンシバル  
と共有可能







はい - このタイプのリソースは AWS のサービスと共有でき  
ます。



はい - このタイプのリソースは AWS のサービスと共有でき  
ません。

## AWS App Mesh

を使用して、次の AWS App Mesh リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
[Mesh] (メッシュ)  appmesh:Mesh	メッシュを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。共有メッシュを使用すると、異なるによって作成されたリソースが同じメッシュ内で相互に通信 AWS アカウント できます。詳細については、AWS App Mesh ユーザーガイドの「 <a href="#">共有メッシュの使用</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ





## AWS AppSync GraphQL API

を使用して、次の AWS AppSync GraphQL API リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
GraphQL API appsync:Apis	AWS AppSync GraphQL APIs一元管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、同じリージョン内の異なるアカウント間で複数のサブスキーマ API のデータにアクセスできる統合 AWS AppSync Merged API の作成 AWS AppSync APIs の一環として、複数のアカウントが APIs を共有できるようになります。詳細については、「AWS AppSync デベロッパーガイド」の「 <a href="#">マージされた APIs</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はいえ





## Amazon Aurora

AWS RAMを使用して、以下の Amazon Aurora リソースを共有できます。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
DB クラスター rds:Cluster	DB クラスターを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントが 1 つの一元的な共有マネージド DB クラスターのクローンを作成できます。詳細については、 <a href="#">「Amazon Aurora ユーザーガイド」の「AWS RAM および Amazon Aurora を使用したクロスアカウントクローン作成」</a> を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 はい	 はい

## AWS Private Certificate Authority

を使用して、次の AWS Private CA リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Private certificate Authority (CA) <code>acm-pca:CertificateAuthority</code>	組織の内部パブリックキーインフラストラクチャ (PKI) CAs) を作成および管理し、それらの CAs を他の AWS アカウント または組織と共有します。これにより、他のアカウント内の AWS Certificate Manager ユーザーが共有 CA によって署名された X.509 証明書を発行できます。詳細については、AWS Private Certificate Authority ユーザーガイドの「 <a href="#">プライベート CA へのアクセスの設定</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい いえ	 はい





## Amazon DataZone

を使用して、次の DataZone リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
DataZone ドメイン  datazone:Domain	ドメインを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントで Amazon DataZone ドメインを作成できます。詳細については、 <a href="#">「Amazon ユーザーガイド DataZone」</a> の「Amazon とは DataZone 」を参照してください。	 いえ	 はい  すべての AWS アカウントと共有可能	 いえ	 いえ





## AWS CodeBuild

を使用して、次の AWS CodeBuild リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
プロジェクト  codebuild:Project	プロジェクトを作成し、それを使用してビルドを実行します。プロジェクトを他の AWS アカウントま	 はい	 はい	 はい	 いえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p>または自分の組織と共有します。これにより、複数の AWS アカウント およびユーザーがプロジェクトに関する情報を表示してそのビルドを分析できます。詳細については、AWS CodeBuild ユーザーガイドの「<a href="#">共有プロジェクトの使用</a>」を参照してください。</p>		<p>すべての AWS アカウントと共有可能</p>		



リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
レポートグループ  codebuild:ReportGroup	レポートグループを作成し、プロジェクトを構築する際にレポートの作成に使用します。レポートグループを他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントとユーザーがレポートグループとそのレポート、および各レポートのテストケースの結果を表示できます。レポートを表示できる期限は作成後 30 日まであり、それを過ぎると表示できなくなります。詳細については、AWS CodeBuild ユーザーガイドの「 <a href="#">共有プロジェクトの使用</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 はい	 はいえ

## Amazon EC2





AWS RAMを使用して、以下の Amazon EC2 リソースを共有できます。





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
キャパシティ予約  ec2:CapacityReservation	<p>キャパシティ予約を一元的に作成および管理し、リザーブドキャパシティを他の AWS アカウントまたは自分の組織と共有します。これにより、複数の Amazon EC2 インスタンスを一元管理されたリザーブドキャパシティで AWS アカウント 起動できます。詳細については、「Amazon EC2 <a href="#">ユーザーガイド</a>」の「<a href="#">共有キャパシティ予約の使用</a>」を参照してください。</p> <p>Amazon EC2</p>	 いいえ	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ

**⚠ Important**

[キャパシティ予約を共有するための前提条件](#)をすべて満たしていない場合、共有操作が失敗する可能性があります。操作が失敗し、ユーザーがキャパシティ





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p>予約で Amazon EC2 インスタンスを起動しようとする、インスタンスはオンデマンドインスタンスとして起動し、コストが高くなる可能性があります。<a href="#">Amazon EC2 コンソール</a>で表示して、共有キャパシティ予約にアクセスできることを確認することをお勧めします。また、リソース共有の障害を監視して、高コストにつながる方法でユーザーがインスタンスを起動する前に是正措置を取れるようにすることもできます。詳細については、「<a href="#">例: リソース共有障害</a>」</p>				





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p><a href="#">時のアラート</a>」を参照してください。</p>				
<p>Dedicated Hosts ec2:DedicatedHost</p>	<p>Amazon EC2 専用ホストを一元的に割り当てて管理し、ホストのインスタンス容量を他の AWS アカウントまたは自分の組織と共有します。これにより、複数のがで Amazon EC2 インスタンスを一元管理された専用ホストに AWS アカウント 起動できます。詳細については、Amazon EC2 <a href="#">ユーザーガイド</a>」の「<a href="#">共有 Dedicated Hosts</a>の使用」を参照してください。</p>	 いいえ	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
プレイズメントグループ <code>ec2:PlacementGroup</code>	所有しているプレイズメントグループを AWS アカウント、組織内外の全体で共有します。Amazon EC2 インスタンスは、共有しているどのアカウントからでも共有プレイズメントグループで起動できます。詳細については、「 <a href="#">Amazon EC2 ユーザーガイド</a> 」の「 <a href="#">プレイズメントグループの共有</a> 」を参照してください。 Amazon EC2	 はい	 はい すべての AWS アカウントと共有可能	 はいえ	 はいえ





## EC2 Image Builder

AWS RAMを使用して、以下の EC2 Image Builder リソースを共有できます。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
コンポーネント	コンポーネントを一元的に作成して管理し、他の AWS アカウントまたは自分の組	 はい	 はい	 はい	 はいえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
imagebuilder:Component	<p>組織と共有します。イメージレシピで事前定義されたビルドおよびテストコンポーネントを使用できるユーザーを管理します。詳細については、EC2 Image Builder ユーザーガイドの「<a href="#">EC2 Image Builder リソースの共有</a>」を参照してください。</p>		すべての AWS アカウントと共有可能		
コンテナレシピ imagebuilder:ContainerRecipe	<p>コンテナレシピを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、事前定義されたドキュメントを使用してコンテナイメージビルドを複製できるユーザーを管理できます。詳細については、EC2 Image Builder ユーザーガイドの「<a href="#">EC2 Image Builder リソースの共有</a>」を参照してください。</p>	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はいえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
イメージ imagebuilder:Image	ゴールデンイメージを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。EC2 Image Builder で作成されたイメージを組織間で使用できるユーザーを管理します。詳細については、EC2 Image Builder ユーザーガイドの「 <a href="#">EC2 Image Builder リソースの共有</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい	 いいえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
イメージのレシピ  imagebuilder:ImageRecipe	イメージレシピを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、事前定義されたドキュメントを使用して AMI ビルドを複製できるユーザーを管理できます。詳細については、EC2 Image Builder ユーザーガイドの「 <a href="#">EC2 Image Builder リソースの共有</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 はい	 いいえ

## Amazon FSx for OpenZFS


AWS RAMを使用して、以下の Amazon FSx for OpenZFS リソースを共有できます。







リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
FSx ポリウム fsx:Volume	FSx for OpenZFS ポリウムを一元的に作成および管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントが FSx APIs CreateVolume または を介して共有ポリウムの OpenZfs スナップショットを使用してデータレプリケーションを実行できますCopySnaps hotAndUpdateVolume 。詳細については、「Amazon FSx for OpenZFS ユーザーガイド」の「 <a href="#">オンデマンドデータレプリケーション</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はい

## AWS Glue

を使用して、次の AWS Glue リソースを共有できます AWS RAM。





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
データカタログ glue:Catalog	中央データカタログを管理し、データベースとテーブルに関するメタデータを AWS アカウント または組織と共有します。これにより、ユーザーは複数のアカウントにわたるデータにクエリを実行できません。詳細については、AWS Lake Formation デベロッパーガイド「 <a href="#">AWS アカウント間のデータカタログのテーブルおよびデータベースの共有</a> 」を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 いえ	 いえ
データベース glue:Database	データカタログデータベースを一元的に作成および管理し、AWS アカウント または組織と共有します。データベースは、データカタログテーブルの集まりです。これにより、ユーザーは複数のアカウント間でデータを結合およびクエリできる抽出、変	 いえ	 はい すべての AWS アカウントと共有可能	 いえ	 いえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	換、ロード (ETL) のジョブを実行できるようになります。詳細については、AWS Lake Formation デベロッパーガイド「 <a href="#">AWS アカウント間のデータカタログのテーブルおよびデータベースの共有</a> 」を参照してください。				

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
テーブル glue:Table	データカタログテーブルを一元的に作成および管理し、AWS アカウントまたは組織と共有します。データカタログテーブルには、Amazon S3、JDBC データソース、Amazon Redshift、ストリーミングソース、およびその他のデータストア内のデータテーブルに関するメタデータが含まれています。これにより、ユーザーは、複数のアカウント間でデータを結合およびクエリできる ETL ジョブを実行できます。詳細については、AWS Lake Formation デベロッパーガイド「 <a href="#">AWS アカウント間のデータカタログのテーブルおよびデータベースの共有</a> 」を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 いえ	 いえ





## AWS License Manager

を使用して、次の AWS License Manager リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
ライセンス設定 <code>license-manager:LicenseConfiguration</code>	ライセンス設定を一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウント間でエンタープライズ契約の条項に基づいて、一元管理されたライセンスルールを一元的に施行できます。詳細については、License Manager ユーザーガイドの「 <a href="#">License Manager でのライセンス設定</a> 」を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 いえ	 いえ





## AWS Marketplace

を使用して、次の AWS Marketplace リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Marketplace カタログエンティティ <code>aws-marketplace:Entity</code>	で、組織全体 AWS アカウント または組織内のエンティティを作成、管理、共有します AWS Marketplace。詳細については、「AWS Marketplace Catalog API リファレンス」の「 <a href="#">AWS RAMでのリソース共有</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 いえ	 いえ

## AWS Migration Hub Refactor Spaces





を使用して、次の AWS Migration Hub Refactor Spaces リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
リファクタリングスペース環境 <code>refactor-spaces:Environment</code>	リファクタリングスペース環境を作成し、作成した環境にリファクタリングスペースアプリケーションを格納します。この環境を組織内の他の AWS アカウント または組織の	 はい	 はい すべての AWS アカ	 はい	 いえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	すべてのアカウントと共有します。これにより、複数の AWS アカウントとユーザーが環境とその中のアプリケーションに関する情報を表示できます。詳細については、「AWS Migration Hub Refactor Spaces ユーザーズガイド」の「 <a href="#">AWS RAMを使用したリファクタリングスペース環境の共有</a> 」を参照してください。		アカウントと共有可能		





## AWS Network Firewall

を使用して、次の AWS Network Firewall リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
ファイアウォールポリシー <code>network-firewall:F</code>	ファイアウォールポリシーを一元的に作成して管理し、他の AWS アカウント または自分	 はい	 はい	 はいえ	 はいえ









リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
firewallPolicy	<p>の組織と共有します。これにより、組織内の複数のアカウントが、共通のネットワークモニタリング、保護、およびフィルタリング動作を共有できるようになります。詳細については、AWS Network Firewall デベロッパーガイドの「<a href="#">ファイアウォールポリシーとルールグループの共有</a>」を参照してください。</p>		すべての AWS アカウントと共有可能		



リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
ルールグループ  network-firewall:StatefulRuleGroup  network-firewall:StatelessRuleGroup	ステートレスルールグループとステートフルルールグループを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、の組織内の複数のアカウント AWS Organizations が、ネットワークトラフィックを検査および処理するための一連の基準を共有できるようになります。詳細については、AWS Network Firewall デベロッパーガイドの「 <a href="#">ファイアウォールポリシーとルールグループの共有</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ

## AWS Outposts





を使用して、次の AWS Outposts リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Outposts outposts: Outpost	Outposts を一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントが、一元管理された共有 Outposts にサブネットと EBS ボリュームを作成できます。詳細については、「AWS Outposts ユーザーガイド」の「 <a href="#">共有 AWS Outposts リソースの使用</a> 」を参照してください。	 いえ	 いえ 自分の組織内の AWS アカウントとのみ共有可能。	 はい	 はい
ローカルゲートウェイルートテーブル ec2:LocalGatewayRouteTable	ローカルゲートウェイへの VPC 関連付けを一元的に作成および管理し、組織 AWS アカウント内の他のと共有します。これにより、複数のアカウントがローカルゲートウェイへの VPC アソシエーションを作成してルートテーブルと仮想インターフェイスの設定を表示できます。詳細につい	 いえ	 いえ 自分の組織内の AWS アカウントとのみ共有可能。	 いえ	 はい

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	ては、AWS Outposts ユーザーガイドの「 <a href="#">共有可能な Outpost リソース</a> 」を参照してください。				
サイト outposts: Site	Outpost サイトを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントが共有サイトで Outposts を作成して管理でき、Outpost リソースとサイトの間で分割制御がサポートされます。詳細については、「 <a href="#">AWS Outposts ユーザーガイド</a> 」の「 <a href="#">共有 AWS Outposts リソースの使用</a> 」を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 いえ	 いえ





## Amazon S3 on Outposts

AWS RAMを使用して、以下の Amazon S3 on Outposts リソースを共有できます。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
S3 on Outpost s3-outposts:Outpost	Outpost で Amazon S3 バケット、アクセスポイント、エンドポイントを作成および管理します。これにより、複数のアカウントが共有サイトで Outposts を作成して管理でき、Outpost リソースとサイトの間で分割制御がサポートされません。詳細については、「 <a href="#">AWS Outposts ユーザーガイド</a> 」の「 <a href="#">共有 AWS Outposts リソースの使用</a> 」を参照してください。	 いえ	 いえ 自分の組織内の AWS アカウントとのみ共有可能。	 はい	 はい





## AWS Resource Explorer

を使用して、次の AWS Resource Explorer リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
ビュー resource-explorer-2:View	Resource Explorer ビューを一元的に作成して設定し、組織 AWS アカウント 内の他のと共有します。これにより、複数の のロールとユーザーは、ビューからアクセス可能なリソース AWS アカウント を検索して検出できます。詳細については、「AWS Resource Explorer ユーザーガイド」の「 <a href="#">Resource Explorer ビューの共有</a> 」を参照してください。	 いえ	 いえ 自分の組織内の AWS アカウントとのみ共有可能。	 いえ	 いえ








## AWS Resource Groups





を使用して、次の AWS Resource Groups リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
リソースグループ  resource-groups:Group	ホストリソースグループを一元的に作成して管理し、組織 AWS アカウント内の他と共有します。これにより、AWS License Managerを使用して作成された Amazon EC2 Dedicated Hosts のグループを複数の AWS アカウントが共有できません。詳細については、AWS License Manager ユーザーガイドの「 <a href="#">AWS License Managerのホストリソースグループ</a> 」を参照してください。	 いえ	 はい  すべての AWS アカウントと共有可能	 いえ	 いえ




## Amazon Route 53

AWS RAMを使用して、以下の Amazon Route 53 リソースを共有できます。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Route 53 Resolver DNS Firewall ルールグループ <code>route53resolver:FirewallRuleGroup</code>	Route 53 Resolver DNS Firewall ルールグループを一元的に作成および管理し、他の AWS アカウント または自分の組織と共有します。これにより、複数のアカウントが、Route 53 リゾルバを介してアウトバウンド DNS クエリを検査および処理するための条件セットを共有できるようになります。詳細については、Amazon Route 53 デベロッパーガイドの「 <a href="#">AWS アカウントアカウント間で Route 53 Resolver DNS Firewall ルールグループを共有する</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はいえ	 はいえ
Route 53 Profiles <code>route53profiles:Profile</code>	Route 53 を一Profile 的に作成して管理し、他の AWS アカウント または自分の組織と共有します。これにより、複数のアカウントが Route 53 で指定さ	 はい	 はい すべての AWS アカ	 はい	 はいえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	れた DNS 設定 Profiles を複数の VPCs。詳細については、 <a href="#">「Amazon Route 53 Profiles デベロッパーガイド」</a> の「Amazon Route 53」を参照してください。		アカウントと共有可能		
リゾルバールール  route53resolver:ResolverRule	Resolver ルールを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントが、仮想プライベートクラウド (VPC) から、一元管理された共有リゾルバールールで定義された送信先 IP アドレスに DNS クエリを転送できます。詳細については、「Amazon Route 53 <a href="#">デベロッパーガイド</a> 」の「 <a href="#">Resolver ルールを他のと共有 AWS アカウントし、共有ルールを使用する</a> 」を参照してください。				
		いえ	はい	いえ	いえ
			すべての AWS アカウントと共有可能		



リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
ログのクエリ route53resolver:ResolverQueryLogConfig	クエリログを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントが、VPC で発生した DNS クエリを一元的にクエリログに記録できるようになります。詳細については、Amazon Route 53 デベロッパーガイドの「 <a href="#">Resolver クエリログ記録設定を他の AWS アカウントと共有する</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はいえ





## Amazon Route 53 Application Recovery Controller

AWS RAMを使用して、以下の Amazon Route 53 Application Recovery Controller リソースを共有できます。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Route 53 ARC クラスター  route53-recovery-control:Cluster	Route 53 ARC クラスターを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントが 1 つの共有クラスターにコントロールパネルとルーティングコントロールを作成できるようになり、管理が簡素化され、組織が必要とするクラスターの総数を削減できます。詳細については、「Amazon Route 53 Application Recovery Controller デベロッパーガイド」の「 <a href="#">アカウント全体でのクラスターの共有</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 はい	 はい  いえ

## Amazon Simple Storage Service

を使用して、次の Amazon Simple Storage Service リソースを共有できます AWS RAM。





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Access Grants s3:Access Grants	S3 Access Grants インスタンスを一元的に作成および管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントが共有リソースを表示および削除できます。詳細については、「 <a href="#">ユーザーガイド</a> 」の <a href="#">S3 Access Grants Cross-account Access</a> Amazon Simple Storage Service」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はい

## Amazon SageMaker





を使用して、次の Amazon SageMaker リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
SageMaker カタログ  sagemaker:SagemakerCatalog	<p>検出可能性のため – アカウント所有者は、SageMaker カタログ内のすべての特徴量グループリソースについて、他のアカウントに検出可能性のアクセス許可を付与できます。アクセスが付与されたアカウントのユーザーは、共有されている特徴量グループをカタログから閲覧できるようになります。詳細については、「Amazon SageMaker デベロッパーガイド」の「<a href="#">クロスアカウント特徴量グループの検出可能性とアクセス</a>」を参照してください。</p> <div data-bbox="399 1472 743 1835" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 20px;"> <p><b>Note</b></p> <p>検出可能性とアクセスは、では個別のアクセス許可です SageMaker。</p> </div>	<div style="text-align: center;">               いいえ           </div>	<div style="text-align: center;">               はい           </div> <p>すべての AWS アカウントと共有可能</p>	<div style="text-align: center;">               はい           </div>	<div style="text-align: center;">               はい           </div>

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
SageMaker 特徴量グループ  sagemaker:FeatureGroup	<p>アクセス — アカウント所有者は、特定の特徴量グループリソースについて、他のアカウントにアクセス許可を付与できます。アクセスが付与されたアカウントのユーザーは、共有されている特徴量グループを使用できるようになります。詳細については、「Amazon SageMaker デベロッパーガイド」の「<a href="#">クロスアカウント特徴量グループの検出可能性とアクセス</a>」を参照してください。</p> <div data-bbox="402 1304 743 1669" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 20px;"> <p><b>Note</b></p> <p>検出可能性とアクセスは、では個別のアクセス許可です SageMaker。</p> </div>	 はい	 はい  すべての AWS アカウントと共有可能	 はい	

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
システムグループ  sagemaker:LineageGroup	Amazon SageMaker では、パイプラインメタデータのシステムグループを作成して、その履歴と関係をより深く理解できます。システムグループを他の AWS アカウントまたは組織内のアカウントと共有します。これにより、複数の AWS アカウントとユーザーがシステムグループに関する情報を表示し、その中の追跡エンティティをクエリできます。詳細については、「Amazon SageMaker デベロッパーガイド」の「 <a href="#">クロスアカウントシステム追跡</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 はいえ	 はいえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
SageMaker モデルカード <code>sagemaker:ModelCard</code>	Amazon SageMaker はモデルカードを作成し、機械学習 (ML) モデルに関する重要な詳細を 1 か所に文書化して、ガバナンスとレポート作成を効率化します。Model Card を他の AWS アカウントまたは組織内のアカウントと共有して、機械学習運用のマルチアカウント戦略を実現できます。これにより AWS アカウント、は ML アクティビティのモデルカードアクセスを他のアカウントと共有できます。詳細については、 <a href="#">「Amazon デベロッパーガイド」の「Amazon SageMaker Model Cards」</a> を参照してください。 SageMaker	 はい	 はい すべての AWS アカウントと共有可能	 はいえ	





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
SageMaker パイプライン  sagemaker:Pipeline	Amazon SageMaker Model Building Pipelines を使用すると、end-to-end 機械学習ワークフローを大規模に作成、自動化、管理できます。パイプラインを他の AWS アカウントまたは組織内のアカウントと共有して、機械学習オペレーションのマルチアカウント戦略を実現します。これにより、複数の AWS アカウントとユーザーが、パイプラインとその実行に関する情報を表示し、他のアカウントからパイプラインを開始、停止、再試行するためのオプションアクセス権を持つことができます。詳細については、「Amazon SageMaker デベロッパーガイド」の <a href="#">SageMaker 「パイプライン」のクロスアカウント</a>	 はい	 はい  すべての AWS アカウントと共有可能	 はい	 いいえ







リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<a href="#">トサポート</a> 」を参照してください。				

## AWS Service Catalog AppRegistry









を使用して、次の AWS Service Catalog AppRegistry リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
アプリケーション  servicecatalog:Application	アプリケーションを作成し、それを使用して AWS 環境全体でそのアプリケーションに属するリソースを追跡します。アプリケーションを他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウント およびユーザーが、アプリケーションおよび関連するリソースに関する情報をローカルで表示できます。詳細については、「Service Catalog	 いえ	 いえ 自分の組織内の AWS アカウントとのみ共有可能。	 はい	 はい

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	「ユーザーズガイド」の「 <a href="#">アプリケーションの作成</a> 」を参照してください。				
属性グループ servicecatalog:AttributeGroup	属性グループを作成し、作成した属性グループを使用してアプリケーションに関連するメタデータを格納します。属性グループを他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントとユーザーが属性グループに関する情報を表示できます。詳細については、「 <a href="#">Service Catalog ユーザーズガイド</a> 」の「 <a href="#">属性グループの作成</a> 」を参照してください。	 いえ	 いえ 自分の組織内の AWS アカウントとのみ共有可能。	 はい	 いえ

## AWS Systems Manager Incident Manager





を使用して、次の AWS Systems Manager Incident Manager リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
問い合わせ <code>ssm-contacts:Contact</code>	連絡先とエスカレーション計画を一元的に作成および管理し、連絡先の詳細を他の AWS アカウント または自分の組織と共有します。これにより、多くの <b>ガインシデント</b> 中に発生したエンゲージメント AWS アカウント を表示できます。詳細については、AWS Systems Manager Incident Manager ユーザーガイドの「 <a href="#">共有連絡先と対応計画の使用</a> 」を参照してください。	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はい いえ
対応計画 <code>ssm-incidents:ResponsePlan</code>	対応計画を一元的に作成して管理し、他の AWS アカウント や自分の組織と共有します。これにより、は Amazon CloudWatch アラームと Amazon EventBridge イベントルールを対応計画 AWS アカウント に接続し、インシデント	 はい	 はい すべての AWS アカウントと共有可能	 はい	 はい いえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	が検出されると自動的にインシデントを作成できます。インシデントは、これらの他の AWS アカウントのメトリクスにもアクセスできます。詳細については、AWS Systems Manager Incident Manager ユーザーガイドの「 <a href="#">共有連絡先と対応計画の使用</a> 」を参照してください。				

## AWS Systems Manager パラメータストア





を使用して、次の AWS Systems Manager Parameter Store リソースを共有できます AWS RAM。





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
パラメータ ssm:Parameter	パラメータを作成し、スクリプト、コマンド、SSM ドキュメント、設定および自動化ワークフローで参照	 はい	 はい	 はい	 はい いえ





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p>できる設定データを保存するために使用します。パラメータを他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントとユーザーが文字列に関する情報を表示し、データをコードから分離することでセキュリティを強化できます。詳細については、「<a href="#">ユーザーガイド</a>」の「<a href="#">共有パラメータの使用</a>」を参照してください。</p>		<p>すべての AWS アカウントと共有可能</p>		

## Amazon VPC





AWS RAMを使用して、以下の Amazon Virtual Private Cloud (Amazon VPC) リソースを共有できません。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
カスタマー所有の IPv4 アドレス  ec2:CoipPool	<p>AWS Outposts インストールプロセス中に、は、オンプレミスネットワークに関して提供された情報に基づいて、顧客所有の IP アドレスプールと呼ばれるアドレスプール AWS を作成します。</p> <p>カスタマー所有の IP アドレス (CoIP) は、オンプレミスネットワークを介して Outpost サブネット内のリソースへのローカル接続または外部接続を提供します。これらのアドレスは、Elastic IP アドレスを使用するか、カスタマー所有の IP アドレスを自動的に割り当てるサブネット設定を使用して、EC2 インスタンスなどの Outpost 上のリソースに割り当てることができます。CoIP の詳細については、<a href="#">AWS Outposts ユーザーガイド</a>の「カ</p>	 いえ	 いえ  自分の組織内の AWS アカウントとのみ共有可能。	 いえ	 いえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p>「スタマー所有 IP アドレス」を参照してください。</p>				
<p>IP Address Manager (IPAM) プール</p> <p>ec2:IpamPool</p>	<p>Amazon VPC IPAM プールを他の AWS アカウント、IAM ロールまたはユーザー、またはの組織全体または組織単位 (OU) と一元的に共有します AWS Organizations。これにより、これらのプリンシパルは、プールから VPC などの AWS リソースに CIDRs をそれぞれのアカウントに割り当てることができます。VPCs 詳細については、「Amazon VPC IP Address Manager ユーザーズガイド」の「<a href="#">AWS RAMを使用して IPAM プールを共有する</a>」を参照してください。</p>	<p>はい</p>	<p>はい</p> <p>すべての AWS アカウントと共有可能</p>	<p>はい</p>	<p>はい</p> <p>いえ</p>

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
IP Address Manager (IPAM) リソース検出  ec2:IpamResourceDiscovery	リソース検出を他のと共有します AWS アカウント。リソース検出は、所有アカウントに属するリソースを Amazon VPC IPAM が管理および監視できるようにする IPAM コンポーネントです。詳細については、「Amazon VPC IPAM ユーザーズガイド」の「 <a href="#">リソース検出を使用する</a> 」を参照してください。	 いいえ	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ







リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
プレフィックスリスト  ec2:PrefixList	プレフィックスリストを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントが VPC セキュリティグループやサブネットルートテーブルなど、リソース内のプレフィックスリストを参照できます。詳細については、Amazon VPC ユーザーガイドの「 <a href="#">共有プレフィックスリストの操作</a> 」を参照してください。	 いいえ	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
サブネット ec2:Subnet	<p>サブネットを一元的に作成して管理し、自分の組織内の AWS アカウントと共有します。これにより、複数 AWS アカウントがそれらのアプリケーションリソースを一元管理された VPC に起動できます。これらのリソースには、Amazon EC2 Amazon Relational Database Service (RDS) データベース、Amazon Redshift クラスター、AWS Lambda 関数が含まれます。詳細については、Amazon VPC ユーザーガイドの「<a href="#">共有 VPC の使用</a>」を参照してください。</p>	 いいえ	 いいえ 自分の組織内の AWS アカウントとのみ共有可能。	 いいえ	 いいえ

**Note**

リソース共有を作成する際にサブネットを含めるには、ram:CreateResource





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p>Share に加えて <code>ec2:DescribeSubnets</code> および <code>ec2:DescribeVpcs</code> のアクセス許可が必要です。</p> <p>デフォルトサブネットは共有できません。共有できるのは自分で作成したサブネットだけです。</p>				

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Traffic Mirror ターゲット  ec2:TrafficMirrorTarget	トラフィックミラーターゲットを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントがミラーリングされたネットワークトラフィックをアカウント内のトラフィックミラーソースから、一元管理された共有トラフィックミラーターゲットに送信できます。詳細については、トラフィックミラーリングのガイドの「 <a href="#">クロスアカウントトラフィックミラーリングターゲット</a> 」を参照してください。	 <small>し</small> いえ	 <small>は</small> い  すべての AWS アカウントと共有可能	 <small>し</small> いえ	 <small>い</small> いえ

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Transit Gateway  ec2:TransitGateway	トランジットゲートウェイを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数の AWS アカウントが、一元管理されたマネージド Transit Gateway を介して VPC とオンプレミスネットワークの間を流れるトラフィックをルーティングできます。詳細については、Amazon VPC Transit Gateway の「 <a href="#">Transit Gateway の共有</a> 」を参照してください。	 いいえ	 はい  すべての AWS アカウントと共有可能	 いいえ	 いいえ

**Note**









リソース共有の作成時にトランジットゲートウェイを含めるには、ram:CreateResourceShare に加えて ec2:Descr

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	<p>ibeTransitGateway アクセス許可が必要です。</p>				
<p>Transit Gateway マルチキャストドメイン</p> <p>ec2:TransitGatewayMulticastDomain</p>	<p>Transit Gateway マルチキャストドメインを一元的に作成および管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のマルチキャストドメイン内のグループメンバーまたはグループソース AWS アカウントを登録および登録解除できます。詳細については、Transit Gateways ガイドの「<a href="#">共有マルチキャストドメインの使用</a>」を参照してください。</p>	<p> いえ</p>	<p> はい</p> <p>すべての AWS アカウントと共有可能</p>	<p> いえ</p>	<p> いえ</p>

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
AWS Verified Access グループ  ec2:VerifiedAccessGroup	AWS Verified Access グループを一元的に作成して管理し、他の AWS アカウントまたは自分の組織と共有します。これにより、複数のアカウントのアプリケーションは、単一の共有 AWS Verified Access エンドポイントセットを使用できます。詳細については、「 <a href="#">ユーザーガイド</a> 」の「 <a href="#">を使用して AWS Verified Access グループを共有する</a> 」 <a href="#">AWS Resource Access Manager</a> AWS Verified Access」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 はいえ	 はいえ

## Amazon VPC Lattice

AWS RAMを使用して、以下の Amazon VPC Lattice リソースを共有できます。





リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Amazon VPC Lattice サービス <code>vpc-lattice:Service</code>	Amazon VPC Lattice サービスを一元的に作成および管理し、個人 AWS アカウントまたは組織と共有します。これにより、サービス所有者はマルチアカウント環境で通信を接続、保護、監視 service-to-service でできます。詳細については、「VPC Lattice ユーザーズガイド」の「 <a href="#">共有リソースの使用</a> 」を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 はい	 いえ
Amazon VPC Lattice サービス ネットワーク <code>vpc-lattice:ServiceNetwork</code>	Amazon VPC Lattice サービスネットワークを一元的に作成および管理し、個人 AWS アカウントまたは組織と共有します。これにより、サービスネットワーク所有者は、マルチアカウント環境で service-to-service 通信を接続、保護、監視できます。詳細については、「Amazon VPC Lattice ユーザーズガイド」の「 <a href="#">共有リソースの使用</a> 」を参照してください。	 いえ	 はい すべての AWS アカウントと共有可能	 はい	 いえ



リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
	ド」の「 <a href="#">共有リソースの使用</a> 」を参照してください。				

## AWS クラウド WAN

を使用して、次の AWS Cloud WAN リソースを共有できます AWS RAM。

リソースタイプとコード	ユースケース	IAM ユーザーおよびロールと共有可能	組織外のアカウントと共有可能	カスタマー管理アクセス許可を使用可能	サービスプリンシパルと共有可能
Cloud WAN コアネットワーク  networkmanager:CoreNetwork	Cloud WAN コアネットワークを一元的に作成および管理し、他と共有します AWS アカウント。これにより、1 つの Cloud WAN コアネットワークで複数のホスト AWS アカウントにアクセスしてプロビジョニングできます。詳細については、「AWS Cloud WAN ユーザーズガイド」の「 <a href="#">コアネットワークの共有</a> 」を参照してください。	 はい	 はい  すべての AWS アカウントと共有可能	 はいえ	 はいえ

# AWS RAM アクセス許可の管理

AWS RAM には、AWS 管理アクセス許可とカスタマー管理アクセス許可の [2 種類の管理アクセス許可](#)があります。

管理アクセス許可は、コンシューマーがリソース共有内のリソースに対してどのような操作ができるかを定義します。リソース共有を作成する際に、リソース共有に含まれるリソースタイプごとに、どの管理アクセス許可を使用するかを指定する必要があります。管理アクセス許可のポリシーテンプレートには、プリンシパルとリソースを除いて、リソースベースのポリシーに必要なものがすべて含まれています。リソースベースのポリシーは、リソースの Amazon リソースネーム (ARN) とリソース共有に関連付けられたプリンシパルの ARN によって構成されます。次に AWS RAM は、リソース共有内のすべてのリソースにアタッチするリソースベースのポリシーを作成します。

各管理アクセス許可には、1 つまたは複数のバージョンを含めることができます。管理アクセス許可には、必ず 1 つのバージョンがデフォルトバージョンとして指定されています。新しいバージョンを作成し、その新しいバージョンをデフォルトとして指定することで、AWS がリソースタイプの AWS 管理アクセス許可を更新することがあります。新しいバージョンを作成して、カスタマー管理アクセス許可を更新することもできます。リソース共有に既にアタッチされている管理アクセス許可は自動的に更新されません。新しいデフォルトバージョンが使用可能になると AWS RAM コンソールに表示され、新しいデフォルトバージョンでの変更を以前のバージョンと比較して確認できます。

## Note

できるだけ早く AWS 管理アクセス許可の新しいバージョンに更新することをお勧めします。これらの更新では通常、AWS RAM を使用して追加のリソースタイプを共有できる新しいまたは更新された AWS のサービス に対するサポートが追加されます。新しいデフォルトバージョンでは、セキュリティの脆弱性に対処して修正することもできます。

## Important

リソース共有には、管理アクセス許可のデフォルトバージョンのみをアタッチできます。

使用可能なマネージドアクセス許可の一覧は、いつでも取得できます。詳細については、「[管理アクセス許可の表示](#)」を参照してください。

トピック

- [管理アクセス許可の表示](#)
- [AWS RAM でのカスタマー管理アクセス許可の作成と使用](#)
- [AWS 管理アクセス許可を新しいバージョンに更新する](#)
- [AWS RAM でカスタマー管理アクセス許可を使用する際の考慮事項](#)
- [マネージドアクセス許可のしくみ](#)
- [管理アクセス許可のタイプ](#)

## 管理アクセス許可の表示

リソース共有内のリソースタイプに割り当て可能な管理アクセス許可の詳細を表示できます。リソース共有に割り当てられている管理アクセス許可を特定できます。これらの詳細を表示するには、AWS RAM コンソールで [マネージド許可ライブラリ](#) を使用します。

### Console

AWS RAM で管理アクセス許可の詳細を表示するには

1. AWS RAM コンソールで [\[マネージド許可ライブラリ\]](#) ページに移動します。
2. AWS RAM リソース共有は特定の AWS リージョン 内に存在するので、コンソール右上のドロップダウンリストから適切な AWS リージョン を選択してください。グローバルリソースを含むリソース共有を表示するには、AWS リージョン を米国東部 (バージニア北部) (us-east-1) に設定する必要があります。グローバルリソース共有の詳細については、「[リージョナルリソースの共有とグローバルリソースの共有の比較](#)」を参照してください。すべてのリージョンで同じ AWS 管理アクセス許可を使用できますが、これは [Step 5](#) 内の各管理アクセス許可に表示される関連付けられたリソース共有の数に影響します。カスタマー管理アクセス許可は、作成したリージョンのみで使用できます。
3. [マネージド許可] リストで、詳細を表示する管理アクセス許可を選択します。検索ボックスに名前またはリソースタイプの一部を入力するか、ドロップダウンリストで管理アクセス許可タイプを選択すると、管理アクセス許可のリストをフィルタリングできます。
4. (オプション) 表示設定を変更するには、[マネージド許可] パネルの右上にある歯車アイコンを選択します。以下の設定を変更できます。
  - [Page size] (リソースサイズ) — 各ページに表示されるリソースの件数。
  - [Wrap lines] (行の折り返し) — 表内の行末で折り返すかどうかの指定。

- [Columns] (列) - リソースタイプおよび関連付けられた共有に関する情報を表示するか非表示にするかを指定します。

表示オプションを設定し終わったら [Confirm] (確認) を選択します。

5. 各管理アクセス許可について、リストには次の情報が表示されます。

- 管理アクセス許可名 — 管理アクセス許可の名前。
- リソースタイプ — 管理アクセス許可に関連付けられているリソースタイプ。
- 管理アクセス許可タイプ — 管理アクセス許可が AWS 管理アクセス許可かカスタマー管理アクセス許可のいずれであるか。
- 関連付けられた共有 — 管理アクセス許可に関連付けられているリソース共有の数。番号が表示された場合、その番号を選択すると、リソース共有のテーブルに以下の情報が表示されます。
  - リソース共有名 — 管理アクセス許可に関連付けられているリソース共有の名前。
  - 管理アクセス許可のバージョン — このリソース共有にアタッチされている管理アクセス許可のバージョン。
  - 所有者 — リソース共有所有者の AWS アカウント 番号。
  - 外部プリンシパルを許可 — そのリソース共有が AWS Organizations において組織外のプリンシパルとの共有を許可するかどうか。
  - ステータス — リソース共有と管理アクセス許可の間の関連付けの現在のステータス。
- ステータス — 管理アクセス許可の以下の状態を示します。
  - アタッチ可能 — 管理アクセス許可はリソース共有にアタッチできます。
  - アタッチ不可 — 管理アクセス許可はリソース共有にアタッチできません。
  - 削除中 — 管理アクセス許可は無効で、まもなく削除されます。
  - 削除済み — 管理アクセス許可は削除されました。管理アクセス許可ライブラリから削除されるまで 2 時間表示され続けます。

管理アクセス許可の名前を選択すると、その管理アクセス許可に関する詳細を表示できます。管理アクセス許可の詳細ページには、以下の情報が表示されます。

- リソースタイプ — この管理アクセス許可が適用される AWS リソースのタイプ。
- バージョンの数 - カスタマー管理アクセス許可には最大 5 つのバージョンを作成できます。

- デフォルトバージョン — どのバージョンをデフォルトにするかを指定し、この管理アクセス許可を使用するすべての新しいリソース共有に自動的に割り当てられます。異なるバージョンを使用する既存のリソース共有では、リソース共有をデフォルトバージョンに更新するように求めるプロンプトが表示されます。
- ARN — 管理アクセス許可の [Amazon リソースネーム \(ARN\)](#)。AWS 管理アクセス許可の ARN は以下の形式に従います。

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

[DefaultPermission] という部分文字列 (実際の ARN では括弧なし) は、そのリソースタイプでデフォルトに指定されている 1 つの管理アクセス許可の名前だけに存在しません。

- 管理アクセス許可のバージョン — このドロップダウンリストの下タブで表示されるバージョン情報を選択できます。
  - 詳細タブ:
    - 作成日時 — 管理アクセス許可のこのバージョンが作成された日付と時刻。
    - 最終更新時刻 — 管理アクセス許可のこのバージョンが最後に更新された日付と時刻。
  - ポリシーテンプレートタブ — このバージョンの管理アクセス許可で、関連付けられているリソースタイプに対してプリンシパルが実行できるサービスアクションと条件 (該当する場合) のリスト。
  - 関連付けられたリソース共有 — このバージョンの管理アクセス許可を使用するリソース共有のリスト。

## AWS CLI

AWS RAM で管理アクセス許可の詳細を表示するには

[list-permissions](#) コマンドを使用すると、呼び出し元アカウントについて現在の AWS リージョンにあるリソース共有で使用できる管理アクセス許可のリストを取得できます。

```
$ 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"
  }
]
}

```

特定の管理アクセス許可の ARN は、`list-permissions` AWS CLI コマンドの `--query` パラメータ内の名前を検索することもできます。次の例では、指定された名前と一致する `permissions` 配列結果の要素のみを含むように出力をフィルタリングします。また、結果には ARN フィールドのみを表示し、デフォルトの JSON の代わりにプレーンテキスト形式で表示するように指定しています。

```

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

```

目的の管理アクセス許可の ARN が見つかったら、[get-permission](#) コマンドを実行して JSON ポリシーテキストを含む詳細を取得できます。

```

$ aws ram get-permission \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
  "permission": {
    "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
    "version": "1",
    "defaultVersion": true,
    "name": "My-Test-CMP",
    "resourceType": "ec2:IpamPool",
    "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n\t\t\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"
  }
}
```

## AWS RAM でのカスタマー管理アクセス許可の作成と使用

AWS Resource Access Manager (AWS RAM) は、共有できるリソースタイプごとに 1 つ以上の AWS 管理アクセス許可を提供します。ただし、これらの管理アクセス許可では、共有のユースケースで **最小特権** しか付与されない場合があります。提供されている AWS 管理アクセス許可のいずれかが機能しない場合は、独自のカスタマー管理アクセス許可を作成できます。

カスタマー管理アクセス許可は、AWS RAM で共有リソースを使用する場合に、どのような条件下でどのアクションを実行できるかを正確に指定する、ユーザーが作成し管理する管理アクセス許可です。例えば、大規模な IP アドレスの管理に役立つ Amazon VPC IP Address Manager (IPAM) プールの読み取りアクセスを制限する場合を考えてみます。IP アドレスの割り当てはできるものの、他の開発者アカウントが割り当てた IP アドレスの範囲は表示できないようなカスタマー管理アクセス許可を開発者に対して作成することができます。最小特権のベストプラクティスに従って、必要なアクセス許可のみを付与し、共有リソースでタスクを実行できるような環境を構築することができます。

また、カスタマー管理アクセス許可は、必要に応じて更新または削除することができます。

### トピック

- [カスタマー管理アクセス許可を作成する](#)
- [カスタマー管理アクセス許可の新しいバージョンを作成する](#)
- [カスタマー管理アクセス許可のデフォルトとなる別のバージョンを選択する](#)
- [カスタマー管理アクセス許可のバージョンを削除する](#)
- [カスタマー管理アクセス許可を削除する](#)

## カスタマー管理アクセス許可を作成する

カスタマー管理アクセス許可は AWS リージョン に固有のものです。カスタマー管理アクセス許可は、適切なリージョンに作成するようにしてください。



## Console

カスタマー管理アクセス許可を作成するには

- 次のいずれかを実行します。
  - [\[マネージド許可ライブラリ\]](#) に移動し、[\[カスタマー管理アクセス許可の作成\]](#) を選択します。
  - コンソールの [\[カスタマー管理アクセス許可の作成\]](#) ページに直接移動します。
- [\[カスタマー管理アクセス許可の詳細\]](#) にカスタマー管理アクセス許可名を入力します。
- この管理アクセス許可を適用するリソースタイプを選択します。
- [\[ポリシーテンプレート\]](#) で、このリソースタイプで実行できる操作を定義します。
  - [\[マネージド型アクセス許可のインポート\]](#) を選択すると、既存の管理アクセス許可のアクションを使用できます。
  - ビジュアルエディタで、要件に合わせてアクセスレベル情報を選択または選択解除します。
  - [\[JSON エディタ\]](#) を使用して条件を追加または変更します。
- (オプション) タグを管理アクセス許可にアタッチするには、[\[タグ\]](#) にタグキーと値を入力します。タグを追加するには、[\[新しいタグを追加\]](#) を選択します。この手順を必要なだけ繰り返します。
- 終了したら、[\[カスタマー管理アクセス許可の作成\]](#) を選択します。

## AWS CLI

カスタマー管理アクセス許可を作成するには

- [create-permission](#) コマンドを実行して、名前、カスタマー管理アクセス許可を適用するリソースタイプ、およびポリシーテンプレートの本文を指定します。

以下のコマンドの例は、`imagebuilder:Component` リソースタイプ用の管理アクセス許可を作成します。

```
$ 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
  }
}
```

## カスタマー管理アクセス許可の新しいバージョンを作成する

カスタマー管理アクセス許可のユースケースが変更された場合は、管理アクセス許可の新しいバージョンを作成できます。これは既存のリソース共有には影響せず、カスタマー管理アクセス許可を使用する新しいリソース共有にのみ影響します。

各管理アクセス許可には最大 5 つのバージョンを設定できますが、関連付けることができるのはデフォルトバージョンのみです。

### Console

カスタマー管理アクセス許可の新しいバージョンを作成するには

1. [\[マネージド許可ライブラリ\]](#) に移動します。
2. 管理アクセス許可リストを [カスタマー管理] でフィルタリングするか、変更するカスタマー管理アクセス許可の名前を検索します。
3. 管理アクセス許可の詳細ページの [管理アクセス許可のバージョン] セクションで、[バージョンを作成] を選択します。
4. [ポリシーテンプレート] で、ビジュアルエディタまたは JSON エディタを使用してアクションと条件を追加または削除します。

また、[マネージド型アクセス許可のインポート] を選択して、既存のポリシーテンプレートを使用することもできます。

5. 終了したら、ページ下部の [バージョンを作成] を選択します。

## AWS CLI

カスタマー管理アクセス許可の新しいバージョンを作成するには

1. 新しいバージョンを作成する管理アクセス許可の Amazon リソースネーム (ARN) を見つけます。これを行うには、`--permission-type CUSTOMER_MANAGED` パラメータを含む [list-permissions](#) を呼び出して、カスタマー管理アクセス許可のみを含めます。

```
$ 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. ARN を取得したら、[create-permission-version](#) を呼び出して、更新されたポリシーテンプレートを指定します。

```
$ 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  
  }  
}
```

出力には新しいバージョンのバージョン番号が含まれます。

## カスタマー管理アクセス許可のデフォルトとなる別のバージョンを選択する

別のカスタマー管理アクセス許可のバージョンを新しいデフォルトバージョンとして設定できます。

### Console

カスタマー管理アクセス許可の新しいデフォルトバージョンを設定するには

1. [\[マネージド許可ライブラリ\]](#) に移動します。
2. 管理アクセス許可リストを [カスタマー管理] でフィルタリングするか、変更するカスタマー管理アクセス許可の名前を検索します。
3. [カスタマー管理アクセス許可の詳細] ページの [マネージド型アクセス許可のバージョン] セクションでドロップダウンリストを使用して、新しいデフォルトとして設定するバージョンを選択します。
4. [デフォルトバージョンとして設定] を選択します。
5. ダイアログボックスが表示されたら、このバージョンをこのカスタマー管理アクセス許可を使用するすべての新しいリソース共有のデフォルトにするかどうかを確認します。[デフォルトバージョンとして設定] を選択します。

### AWS CLI

カスタマー管理アクセス許可の新しいデフォルトバージョンを設定するには

1. [list-permission-versions](#) を呼び出して、デフォルトのバージョンとして設定するバージョン番号を見つけます。

次のコマンドの例は、指定した管理アクセス許可の現在のバージョンを取得します。

```
$ 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  
    }  
  ]  
}
```

- バージョン番号をデフォルトとして設定したら、[set-default-permission-version](#) を呼び出します。

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

このコマンドが正常に実行されると、出力が返されることはありません。[list-permission-versions](#) をもう一度実行して、選択したバージョンの defaultVersion フィールドが true に設定されたことを確認します。

## カスタマー管理アクセス許可のバージョンを削除する

各カスタマー管理アクセス許可には最大 5 つのバージョンを作成できます。不要になった場合には、バージョンを削除できます。カスタマー管理アクセス許可のデフォルトバージョンを削除することはできません。削除したバージョンは、最大 2 時間コンソールに「削除済み」ステータスで表示され、その後完全に削除されます。

### Console

カスタマー管理アクセス許可のバージョンを削除するには

1. [\[マネージド許可ライブラリ\]](#) に移動します。
2. 管理アクセス許可リストを [カスタマー管理] でフィルタリングするか、削除するカスタマー管理アクセス許可のバージョン名を検索します。
3. 削除するバージョンが現在デフォルトバージョンでないことを確認します。
4. ページの [バージョン] セクションの [関連付けられたリソース共有] タブを選択して、このバージョンを使用している共有がないか確認します。

関連付けられている共有がある場合は、このバージョンを削除する前に、カスタマー管理アクセス許可のバージョンを変更する必要があります。

5. [バージョン] セクションの右側にある [バージョンの削除] を選択します。
6. 確認ダイアログボックスで [削除] を選択して、カスタマー管理アクセス許可のこのバージョンを削除することを確認します。

カスタマー管理アクセス許可のバージョンを削除しない場合は、[キャンセル] を選択します。

### AWS CLI

カスタマー管理アクセス許可のバージョンを削除するには

1. [list-permission-versions](#) を呼び出して、使用可能なバージョン番号を取得します。

- バージョン番号を取得したら、そのバージョン番号を [delete-permission-version](#) のパラメータとして指定します。

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

このコマンドが正常に実行されると、出力が返されることはありません。[list-permission-versions](#) をもう一度実行して、削除したバージョンが出力に含まれていないことを確認します。

## カスタマー管理アクセス許可を削除する

カスタマー管理アクセス許可が不要になった場合、または使用していない場合、カスタマー管理アクセス許可を削除できます。共有リソースに関連付けられているカスタマー管理アクセス許可を削除することはできません。削除されたカスタマー管理アクセス許可は、2 時間後に表示されなくなります。それまでは、[管理アクセス許可ライブラリ] に「削除済み」ステータスで表示され続けます。

### Console

カスタマー管理アクセス許可を削除するには

- [\[マネージド許可ライブラリ\]](#) に移動します。
- 管理アクセス許可リストを [カスタマー管理] でフィルタリングするか、削除するカスタマー管理アクセス許可の名前を検索します。
- カスタマー管理アクセス許可を選択する前に、管理アクセス許可リストで関連付けられている共有が 0 であることを確認します。

管理アクセス許可に関連付けられているリソース共有がある場合は、続行する前にすべてのリソース共有に別の管理アクセス許可を割り当てる必要があります。

- [カスタマー管理アクセス許可の詳細] ページの右上隅で、[マネージド型アクセス許可の削除] を選択します。
- 確認ダイアログボックスが表示されたら、[削除] を選択して管理アクセス許可を削除します。

## AWS CLI

カスタマー管理アクセス許可を削除するには

1. カスタマー管理アクセス許可のみが含まれるように `--permission-type CUSTOMER_MANAGED` パラメータを含む [list-permissions](#) を呼び出して、削除する管理アクセス許可の ARN を見つけます。

```
$ 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. 削除する管理アクセス許可の ARN を取得したら、取得した ARN を [delete-permission](#) のパラメータとして指定します。

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

## AWS 管理アクセス許可を新しいバージョンに更新する

AWS では、特定のリソースタイプのリソース共有にアタッチできる AWS 管理アクセス許可が更新されることがあります。AWS で更新が実行されると、AWS 管理アクセス許可の新しいバージョン



が作成されます。指定されたリソースタイプを含むリソース共有は、最新バージョンの管理アクセス許可を使用するように自動更新されません。ユーザーは、リソース共有ごとに管理アクセス許可を明示的に更新する必要があります。これは、リソース共有に適用する前に、変更を評価するために必要な手順です。

## Console

リソース共有に関するアクセス許可を一覧表示するページがコンソールに表示され、そのうちの1つまたは複数がアクセス許可のデフォルトバージョン以外を使用している場合、コンソールページの上部にバナーが表示されます。バナーには、リソース共有がデフォルトバージョン以外を使用していることが示されます。

また、個々のアクセス許可で現在のバージョン番号がデフォルトでない場合は、バージョン番号の横に [デフォルトバージョンに更新] ボタンが表示されることがあります。

このボタンを選択すると、[リソース共有の更新](#)ウィザードが起動します。ウィザードのステップ2では、アクセス許可のデフォルト以外のバージョンを更新して、デフォルトバージョンを使用するように変更できます。

ウィザードの最後のページで [送信] を選択してウィザードを完了するまで、変更は保存されません。

### Note

アタッチできるのはデフォルトバージョンだけで、別のバージョンには戻せません。カスタマー管理アクセス許可の場合、アクセス許可をデフォルトバージョンに更新した後は、最初に他のバージョンをデフォルトに設定しない限り、別のバージョンをリソース共有に適用することはできません。例えば、アクセス許可をデフォルトバージョンに更新した後に、ロールバックが必要なエラーが見つかった場合は、以前のバージョンをデフォルトとして指定します。新しい別のバージョンを作成して、デフォルトとして指定することもできます。これらのオプションのいずれかを実行したら、現在のデフォルトバージョンを使用するようにリソース共有を更新します。

## AWS CLI

AWS 管理アクセス許可のバージョンを更新するには

1. `--permission-arn` パラメータを指定して [get-resource-shares](#) コマンドを実行し、更新する管理アクセス許可の [Amazon リソースネーム \(ARN\)](#) を指定します。この結果、コマンドはその管理アクセス許可を使用するリソース共有のみを返します。

例えば、次のコマンドの例は、Amazon EC2 キャパシティ予約のデフォルトの AWS 管理アクセス許可を使用するすべてのリソース共有の詳細を返します。

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

出力には、管理アクセス許可によってアクセスが制御されている 1 つ以上のリソースを持つすべてのリソース共有の ARN が含まれます。

2. 前のコマンドで指定したリソース共有ごとに、[associate-resource-share-permission](#) コマンドを実行します。更新するリソース共有を指定するための `--resource-share-arn`、更新する AWS 管理アクセス許可を指定するための `--permission-arn`、管理アクセス許可の最新バージョンを使用するように共有を更新することを指定するための `--replace` パラメータを含めます。バージョン番号を指定する必要はありません。デフォルトバージョンが自動的に使用されます。

```
$ 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. ステップ 1 のコマンドの結果で受け取った各 `ResourceShareArn` で、前のステップのコマンドを繰り返します。

## AWS RAM でカスタマー管理アクセス許可を使用する際の考慮事項

カスタマー管理アクセス許可は、作成した AWS リージョン のみで使用できます。すべてのリソースタイプがカスタマー管理アクセス許可をサポートしているわけではありません。AWS Resource Access Manager でサポートされているリソースタイプの一覧については、「[共有可能な AWS リソース](#)」を参照してください。

複数のステートメントを含むカスタマー管理アクセス許可はサポートされていません。カスタマー管理アクセス許可では、非否定演算子は 1 つしか使用できません。

カスタマー管理アクセス許可では、以下の条件はサポートされていません。

- 関連組織のプリンシパル:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`
- 特定のサービス関連のプリンシパル:
  - `aws:SourceArn`
  - `aws:SourceAccount`
- システムタグ:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

## マネージドアクセス許可のしくみ

概要については、管理アクセス許可を使用して AWS リソースに最小特権でアクセスするというベストプラクティスを適用する方法について説明する以下の動画を参照してください。

このビデオでは、最小特権のベストプラクティスに従って、カスタマー管理アクセス許可の作成および関連付けを行う方法について説明します。詳細については、「[???](#)」を参照してください。

リソース共有を作成する際に、リソースタイプごとに AWS 管理アクセス許可を関連付けます。管理アクセス許可に複数のバージョンがある場合、新しいリソース共有では常にデフォルトとして指定されたバージョンが使用されます。

リソース共有を作成すると、AWS RAM は管理アクセス許可を使用してリソースベースのポリシーを生成し、それを各共有リソースにアタッチします。

管理アクセス許可のポリシーテンプレートは、以下を指定します。

## 効果

共有リソースについてオペレーションを実行するプリンシパルのアクセス許可を Allow するか Deny するかを示します。管理アクセス許可の場合、効果は常に Allow です。詳細については、ユーザーガイドの「[効果](#)」を参照してください。

## アクション

プリンシパルに実行アクセス許可が付与されているオペレーションのリスト。AWS Management Console ではアクション、AWS Command Line Interface (AWS CLI) もしくは AWS API ではオペレーションです。アクションは、AWS アクセス許可で定義されます。詳細については、[IAM ユーザーガイド](#)の「アクション」を参照してください。

## 条件

プリンシパルがリソース共有内のリソースをいつ、どのように操作できるか。条件は、共有リソースに追加のセキュリティレイヤーを加えます。これらを使用して、機密データへの操作に対する共有リソースへのアクセスを制限します。例えば、特定の企業の IP アドレス範囲からアクションを実行するように要求する条件や、多要素認証で認証されたユーザーのみにアクションの実行権限を付与する条件を含めることができます。条件の詳細については、「IAM ユーザーズガイド」の「[AWS グローバル条件コンテキストキー](#)」を参照してください。サービス固有の条件の詳細については、「サービス認証リファレンス」の「[AWS サービスのアクション、リソース、条件キー](#)」を参照してください。

### Note

条件は、カスタマー管理アクセス許可、および AWS 管理アクセス許可のサポートされているリソースタイプで使用することができます。

カスタマー管理アクセス許可で使用できない条件については、「[AWS RAM でカスタマー管理アクセス許可を使用する際の考慮事項](#)」を参照してください。

## 管理アクセス許可のタイプ

リソース共有を作成する際、リソース共有に含める各リソースタイプに関連付ける管理アクセス許可を選択します。AWS 管理アクセス許可は、AWS リソース所有サービスによって定義され、AWS RAM によって管理されます。独自のカスタマー管理アクセス許可は、ユーザーが作成し管理します。

- **AWS 管理アクセス許可** — AWS RAM がサポートするリソースごとに 1 つのデフォルト管理アクセス許可があります。追加の管理アクセス許可のいずれかを明示的に選択しない限り、デフォルトの管理アクセス許可がリソースタイプで使用されます。デフォルトの管理アクセス許可は、指定されたタイプのリソースを共有するという最も一般的な顧客シナリオをサポートすることを目的としています。デフォルトマネージドアクセス許可では、プリンシパルは、リソースタイプのサービスによって定義された特定のアクションを実行できます。例えば、Amazon VPC `ec2:Subnet` リソースタイプの場合、デフォルトマネージドアクセス許可では、プリンシパルは以下のアクションを実行できます。
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

デフォルトの AWS 管理アクセス許可

は、`AWSRAMDefaultPermission`*ShareableResourceType* の形式で名前が付けられます。例えば、`ec2:Subnet` リソースタイプの場合、デフォルト AWS マネージドアクセス許可の名前は `AWSRAMDefaultPermissionSubnet` です。

#### Note

デフォルトの管理アクセス許可は、管理アクセス許可のデフォルト[バージョン](#)とは異なります。すべての管理アクセス許可は、デフォルトであるか、一部のリソースタイプでサポートされている追加の管理アクセス許可であるかを問わず、読み取り/書き込みアクセスや読み取り専用アクセスなど、さまざまな共有シナリオをサポートするさまざまな効果とアクションを備えた個別の完全な権限です。管理アクセス許可は、AWS がカスタマー管理かを問わず、複数のバージョンを持つことができ、そのうちの 1 つがその権限のデフォルトバージョンです。

例えば、フルアクセス (Read および Write) 管理アクセス許可と読み取り専用管理アクセス許可の両方をサポートするリソースタイプを共有する場合、ユーザーは完全なアクセスを付与する管理アクセス許可を含む管理者向けのリソースを 1 つ作成することができます。その後、[最小特権の付与というベストプラクティス](#)に従い、読み取り専用の管理アクセス許可を使用して他の開発者とのリソース共有を作成できます。

**Note**

AWS RAM と連携するすべての AWS サービスは、少なくとも 1 つのデフォルト管理アクセス許可をサポートします。各 AWS のサービスで使用可能なアクセス許可は、[マネージド許可ライブラリ](#) ページで確認できます。このページには、現時点でアクセス許可に関連付けられているリソース共有、外部プリンシパルとの共有が許可されているかどうか (該当する場合) を含め、使用可能なマネージドアクセス許可ごとの詳細が表示されます。詳細については、「[管理アクセス許可の表示](#)」を参照してください。

追加マネージドアクセス許可をサポートしないサービスの場合、リソース共有を作成すると、AWS RAM は、選択したリソースタイプに定義されたデフォルトアクセス許可を自動的に適用します。サポートされている場合、ユーザーは [\[マネージド型アクセス許可を関連付ける\]](#) ページで [\[カスタマー管理アクセス許可の作成\]](#) オプションを選択できます。

- **カスタマー管理アクセス許可** - カスタマー管理アクセス許可は、AWS RAM で共有リソースを使用する場合に、どのような条件下でどのアクションを実行できるかを正確に指定する、ユーザーが作成し管理する管理アクセス許可です。例えば、大規模な IP アドレスの管理に役立つ Amazon VPC IP Address Manager (IPAM) プールの読み取りアクセスを制限する場合を考えてみます。IP アドレスの割り当てはできるものの、他の開発者アカウントが割り当てた IP アドレスの範囲は表示できないようなカスタマー管理アクセス許可を開発者に対して作成することができます。最小特権のベストプラクティスに従って、必要なアクセス許可のみを付与し、共有リソースでタスクを実行できるような環境を構築することができます。

# AWS RAM のセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。AWS の顧客は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWS と顧客の間の責任共有です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウド 内で AWS のサービスを実行するインフラストラクチャを保護する責任を担います。また、AWS は、ユーザーが安全に使用できるサービスも提供します。[AWS コンプライアンスプログラム](#)の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Resource Access Manager (AWS RAM) に適用するコンプライアンスプログラムの詳細については、「[コンプライアンスプログラムによる AWS 対象範囲内のサービス](#)」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。また、お客様は、データの機密性、お客様の会社の要件、および適用される法律および規制など、その他の要因についても責任を負います。

このドキュメントは、AWS RAM を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。次のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために AWS RAM を設定する方法を示します。また、AWS リソースのモニタリングや保護に役立つ、他の AWS RAM のサービスの使用方法についても説明します。

## トピック

- [AWS RAM でのデータ保護](#)
- [AWS RAM のためのアイデンティティおよびアクセス管理](#)
- [AWS RAMでのログ記録とモニタリング](#)
- [AWS RAM での耐障害性](#)
- [AWS RAM でのインフラストラクチャセキュリティ](#)

## AWS RAM でのデータ保護

AWS [責任共有モデル](#)は、AWS Resource Access Manager でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバルインフラ



トラクチャを保護する責任を負います。顧客は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。このコンテンツには、使用される AWS のサービスのセキュリティ構成と管理タスクが含まれます。データプライバシーの詳細については、「[データプライバシーのよくある質問](#)」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「[AWS 責任共有モデルおよび GDPR](#)」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、次の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 および TLS 1.3 をお勧めします。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS のサービス 内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、[連邦情報処理規格 \(FIPS\) 140-2](#) を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で AWS RAM または他の AWS のサービス を使用する場合も同様です。タグ、または名前に使用される自由形式のテキストフィールドに入力されるデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

## AWS RAM のためのアイデンティティおよびアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全にコントロールするために役立つ AWS のサービスです。IAM コントロールの管理者は、誰を認証 (サインイン) し、誰に AWS リソースの使用を許可する (アクセス許可を持たせる) かを制御します。IAM を使用して、ロール、ユーザー、グループなどのプリンシパルを AWS アカウント に作成します。



ユーザーは、プリンシパルが AWS リソースでタスクを実行するためのアクセス許可をコントロールします。IAM は追加料金なしでご利用いただけます。カスタム IAM ポリシーの管理と作成の詳細については、「IAM ユーザーズガイド」の「[IAM ポリシーを管理する](#)」を参照してください。

## トピック

- [AWS RAM と IAM の連携について](#)
- [AWS の AWS RAM 管理ポリシー](#)
- [AWS RAM のサービスにリンクされたロールの使用](#)
- [AWS RAM の IAM ポリシー例](#)
- [AWS Organizations および AWS RAM のサービスコントロールポリシーの例](#)
- [AWS Organizations とのリソース共有の無効化](#)

## AWS RAM と IAM の連携について

デフォルトでは、IAM プリンシパルには AWS RAM リソースを作成または変更するためのアクセス許可はありません。IAM プリンシパルがリソースを作成または変更してタスクを実行できるようにするには、以下の手順のいずれかを実行します。これらのアクションは、特定のリソースおよび API アクションを使用するアクセス許可を付与します。

アクセスを提供するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「[シークレットの作成と管理](#)」の手順に従ってください。

- ID プロバイダーを通じて IAM で管理されているユーザー:

ID フェデレーションのロールを作成する。詳細については、「IAM ユーザーガイド」の「[サードパーティー ID プロバイダー \(フェデレーション\) 用のロールの作成](#)」を参照してください。

- IAM ユーザー:

- ユーザーが設定できるロールを作成します。手順については、「IAM ユーザーガイド」の「[IAM ユーザー用ロールの作成](#)」を参照してください。

- (非推奨) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。「IAM ユーザーガイド」の「[ユーザー \(コンソール\) へのアクセス許可の追加](#)」の指示に従います。

AWS RAM は、多くのユーザーのニーズに対応するうえで役立ついくつかの AWS マネージドポリシーを提供します。これらの詳細については、「[AWS の AWS RAM 管理ポリシー](#)」を参照してください。

ユーザーに付与するアクセス許可を細かく制御する必要がある場合、IAM コンソールで独自のポリシーを構築できます。ポリシーを作成して IAM ロールとユーザーにアタッチする方法については、「AWS Identity and Access Management ユーザーズガイド」の「[IAM でのポリシーとアクセス許可](#)」を参照してください。

以降のセクションでは、IAM アクセス許可ポリシーを構築するための AWS RAM 固有の詳細について説明します。

## 目次

- [ポリシーの構造](#)
  - [エフェクト](#)
  - [アクション](#)
  - [リソース](#)
  - [条件](#)

## ポリシーの構造

IAM アクセス許可ポリシーは 効果、アクション、リソース、および条件を含む JSON ドキュメントです。通常、IAM ポリシーは以下の形式をとります。

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

## エフェクト

効果文は、ポリシーでアクションを実行するプリンシパルアクセスを許可するか拒否するかを示します。指定できる値は、Allow および Deny などです。

## アクション

アクション文は、ポリシーで許可または拒否する AWS RAM API アクションを指定します。許可されるアクションの詳細な一覧については、IAM ユーザーガイドの「[AWS Resource Access Manager で定義されるアクション](#)」を参照してください。

## リソース

リソース文は、ポリシーの影響を受ける AWS RAM リソースを指定します。ステートメント内でリソースを指定するには、一意の Amazon リソースネーム (ARN) を使用する必要があります。許可されるリソースの詳細な一覧については、IAM ユーザーガイドの「[AWS Resource Access Manager で定義されるリソース](#)」を参照してください。

## 条件

条件ステートメントはオプションです。これらを使用すると、ポリシーが適用される条件をさらに絞り込めます。AWS RAM では次の条件キーがサポートされています。

- `aws:RequestTag/${TagKey}` - サービスリクエストに指定されたタグキーを含むタグが存在し、指定された値を持っているかどうかをテストします。
- `aws:ResourceTag/${TagKey}` - サービスリクエストの対象となるリソースに、ポリシーで指定したタグキーが付いたタグがアタッチされているかどうかをテストします。

次の条件例では、サービスリクエストで参照されているリソースに、キー名「Owner」、値「Dev Team」のタグがアタッチされているかどうかを確認します。

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

- `aws:TagKeys` - リソース共有の作成またはタグ付けに使用すべきタグキーを指定します。
- `ram:AllowsExternalPrincipals` - サービスリクエスト内のリソース共有が外部プリンシパルとの共有を許可しているかどうかをテストします。外部プリンシパルの例として、AWS

Organizations における組織外の AWS アカウント があります。False でのテストにパスした場合は、このリソースシェアを同じ組織内のアカウントでのみ共有できます。

- `ram:PermissionArn` - サービスリクエストで指定されたアクセス許可 ARN が、ポリシーで指定した ARN 文字列と一致するかどうかをテストします。
- `ram:PermissionResourceType` - サービスリクエストで指定されたアクセス許可が、ポリシーで指定したリソースタイプで有効かどうかをテストします。リソースタイプは、[共有可能なリソースタイプ](#)の一覧に示す形式に従って指定する必要があります。
- `ram:Principal` - サービスリクエストで指定されたプリンシパルの ARN が、ポリシーで指定した ARN 文字列と一致するかどうかをテストします。
- `ram:RequestedAllowsExternalPrincipals` - サービスリクエストに `allowExternalPrincipals` パラメータが含まれているかどうか、またその引数がポリシーで指定した値と一致するかどうかをテストします。
- `ram:RequestedResourceType` - 処理対象リソースのリソースタイプが、ポリシーで指定したリソースタイプ文字列と一致するかどうかをテストします。リソースタイプは、[共有可能なリソースタイプ](#)の一覧に示す形式に従って指定する必要があります。
- `ram:ResourceArn` - サービスリクエストの処理対象リソースの ARN が、ポリシーで指定した ARN と一致するかどうかをテストします。
- `ram:ResourceShareName` - サービスリクエストの処理対象リソースの名前が、ポリシーで指定した文字列と一致するかどうかをテストします。
- `ram:ShareOwnerAccountId` - サービスリクエストの処理対象リソースのアカウント ID 番号が、ポリシーで指定した文字列と一致するかどうかをテストします。

## AWS の AWS RAM 管理ポリシー

現時点で AWS Resource Access Manager は、このトピックで説明する AWS RAM マネージドポリシーを提供しています。

### AWS マネージドポリシー

- [AWS マネージドポリシー: `AWSResourceAccessManagerReadOnlyAccess`](#)
- [AWS マネージドポリシー: `AWSResourceAccessManagerFullAccess`](#)
- [AWS マネージドポリシー: `AWSResourceAccessManagerResourceShareParticipantAccess`](#)
- [AWS マネージドポリシー: `AWSResourceAccessManagerServiceRolePolicy`](#)
- [AWS マネージドポリシーの AWS RAM 更新](#)

前のリストでは、最初の 3 つのポリシーを IAM ロール、グループ、およびユーザーにアタッチして、アクセス許可を付与できます。リスト内の最後のポリシーは、AWS RAM サービスのサービスリンクロールです。

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケース別に [カスタマー管理ポリシー](#) を定義することで、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「[AWS 管理ポリシー](#)」を参照してください。

## AWS マネージドポリシー: AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、AWS アカウント が所有するリソース共有について読み取り専用アクセス許可を提供します。

これは、Get\* または List\* オペレーションのいずれかを実行するアクセス許可を付与することによって実現されます。リソース共有を変更する機能は用意されていません。

### 許可の詳細

このポリシーには、以下の許可が含まれています。

- ram - プリンシパルは、アカウントが所有するリソース共有に関する詳細を表示できるようになります。

```
{
```

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

## AWS マネージドポリシー: AWSResourceAccessManagerFullAccess

AWSResourceAccessManagerFullAccess ポリシーは IAM ID にアタッチできます。

このポリシーでは、AWS アカウント が所有するリソース共有を表示または変更できるフル管理アクセス権を提供します。

これは、あらゆる ram オペレーションを実行するアクセス許可を付与することで実現されます。

### 許可の詳細

このポリシーには、以下の許可が含まれています。

- ram - プリンシパルは、AWS アカウント が所有するリソース共有に関する情報を表示または変更できるようになります。

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

## AWS マネージドポリシー:

### AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、プリンシパルに、この AWS アカウント と共有されるリソース共有の承諾または拒否、およびそれらのリソース共有に関する詳細を表示する能力を提供します。これらのリソース共有を変更する機能は用意されていません。

これは、一部の ram オペレーションを実行するアクセス許可を付与することで実現されます。

#### 許可の詳細

このポリシーには、以下の許可が含まれています。

- ram - プリンシパルは、リソース共有の招待を受け入れるか拒否でき、アカウントと共有されているリソース共有の詳細を表示できるようになります。

```
{
  "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 マネージドポリシー: AWSResourceAccessManagerServiceRolePolicy

AWS マネージドポリシー `AWSResourceAccessManagerServiceRolePolicy` は、AWS RAM のサービスリンクロールでのみ使用できます。このポリシーをアタッチ、デタッチ、変更、または削除することはできません。

このポリシーは、組織構造への読み取り専用アクセス権を持つ AWS RAM を提供します。AWS RAM と AWS Organizations の統合を有効にすると、AWS RAM は [AWSServiceRoleForResourceAccessManager](#) という名前のサービスリンクロールを自動的に作成し、AWS RAM コンソールで組織の構造を表示するときなど、組織とそのアカウントに関する情報を調べる必要があるときにサービスが想定しているロールを作成します。

これは、組織の構造とアカウントの詳細を提供する `organizations:Describe` と `organizations:List` のオペレーションを実行するための読み取り専用アクセス許可を付与することによって実現されます。

### 許可の詳細

このポリシーには、以下の許可が含まれています。

- `organizations` - プリンシパルは、組織単位を含む組織構造に関する情報、およびそれらに含まれる AWS アカウント を表示できるようになります。

```
{
  "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 マネージドポリシーの AWS RAM 更新

このサービスがこれらの変更の追跡を開始してからの、AWS の AWS RAM マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、AWS RAM [Document history] (ドキュメントの履歴) ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
AWS Resource Access Manager は変更の追跡を開始しました	AWS RAM では、既存のマネージドポリシーに関するドキュメントを用意し、変更の追跡を開始しました。	2021 年 9 月 16 日

## AWS RAM のサービスにリンクされたロールの使用

AWS Resource Access Manager は AWS Identity and Access Management (IAM) [サービスにリンクされたロール](#)を使用します。サービスにリンクされたロールは、AWS RAM のサービスに直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、AWS による事前定義済みのロールであり、ユーザーに代わって AWS RAM から AWS の他のサービスを呼び出すために必要なすべてのアクセス許可を備えています。

サービスにリンクされたロールを使用すると、必要な許可を手動で追加する必要がなくなるため、AWS RAM の設定が簡単になります。AWS RAM は、このサービスにリンクされたロールの許可を定義します。特に定義されている場合を除き、AWS RAM のみとそのサービスにリンクされたロールを引き受けることができます。定義した許可には、信頼ポリシーと許可ポリシーの両方が含まれます。この許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「[IAM と連携するAWS サービス](#)」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。そのサービスに関するサービスにリンクされたロールのドキュメントを表示するには、リンクが設定されている [Yes] (はい) を選択します。

## AWS RAM のサービスにリンクされたロールのアクセス許可

AWS Organizations で共有を有効化すると、AWS RAM は `AWSServiceRoleForResourceAccessManager` という名前のサービスにリンクされたロールを使用します。このロールは、メンバーアカウントのリストや各アカウントが所属する組織単位など、組織の詳細を表示するアクセス許可を AWS RAM サービスに付与します。

このサービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- `ram.amazonaws.com`

アクセス許可ポリシー「`AWSResourceAccessManagerServiceRolePolicy`」がこのサービスにリンクされたロールにアタッチされ、AWS RAM は指定されたリソースで以下のアクションを完了できるようになります。

- アクション: 組織構造の詳細を取得する読み取り専用アクション。アクションの完全なリストについては、IAM コンソールで [AWSResourceAccessManagerServiceRolePolicy](#) を参照してください。

プリンシパルが組織内での AWS RAM 共有を有効化するには、プリンシパル (ユーザー、グループ、ロールなどの IAM エンティティ) に、サービスにリンクされたロールを作成するためのアクセス許可が必要です。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの許可](#)」を参照してください。

## AWS RAM のサービスにリンクされたロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。AWS Management Console で組織内での AWS RAM 共有を有効にするか、AWS CLI または AWS API を使用してアカウントで [EnableSharingWithAwsOrganization](#) を実行すると、AWS RAM はサービスにリンクされたロールを自動的に作成します。

このサービスにリンクされたロールを削除すると、組織構造の詳細を表示する AWS RAM の権限は失われます。

## AWS RAM のサービスにリンクされたロールの編集

AWS RAM で、AWSResourceAccessManagerServiceRolePolicy のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの編集](#)」を参照してください。

## AWS RAM のサービスにリンクされたロールの削除

IAM コンソール、AWS CLI、または AWS API を使用して、サービスにリンクされたロールを手動で削除できます。

IAM を使用してサービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSResourceAccessManagerServiceRolePolicy サービスリンクロールを削除します。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの削除](#)」を参照してください。

## AWS RAM のサービスにリンクされたロールをサポートするリージョン

AWS RAM では、このサービスが利用可能なすべてのリージョンで、サービスにリンクされたロールの使用をサポートしています。詳細については、[AWS](#) の「Amazon Web Services 全般のリファレンスのリージョンとエンドポイント」を参照してください。

## AWS RAM の IAM ポリシー例

このトピックでは、特定のリソースやリソースタイプを共有し、共有を制限することを示す AWS RAM のIAM ポリシーの例を紹介します。

### IAM ポリシーの例

- [例 1: 特定のリソースの共有を許可する](#)
- [例 2: 特定のリソースタイプの共有を許可する](#)
- [例 3: 外部 AWS アカウント との共有を制限する](#)

### 例 1: 特定のリソースの共有を許可する

IAM アクセス許可ポリシーを使用して、特定のリソースのみをリソース共有に関連付けるようにプリンシパルを制限できます。

例えば、以下のポリシーでは、指定した Amazon リソース名 (ARN) のリゾルバールールのみを共有するようにプリンシパルを制限しています。StringEqualsIfExists 演算子は、要求に ResourceArn パラメータが含まれていないか、またはパラメータが含まれている場合、値が指定された ARN と完全に一致する要求を許可します。

...IfExists 演算子を使用するタイミングと理由の詳細については、「IAM ユーザーズガイド」の「[...IfExists 条件演算子](#)」を参照してください。

```
{
  "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"
      }
    }
  }]
}
```

## 例 2: 特定のリソースタイプの共有を許可する

IAM ポリシーを使用して、特定のリソースのみをリソース共有に関連付けるようにプリンシパルを限定できます。

例えば、以下のポリシーでは、リゾルバールールのみを共有するようにプリンシパルを制限しています。

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

```
    }  
  }]  
}
```

### 例 3: 外部 AWS アカウント との共有を制限する

IAM ポリシーを使用して、プリンシパルがその AWS アカウント 組織の外にある AWS リソースを共有するのを防ぐことができます。

例えば、次の IAM ポリシーでは、プリンシパルによるリソース共有への外部 AWS アカウント の追加を防ぎます。

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

## AWS Organizations および AWS RAM のサービスコントロールポリシーの例

AWS RAM は、サービスコントロールポリシー (SCP) をサポートします。SCP は、組織内のアクセス許可を管理する目的で組織内の要素にアタッチされるポリシーです。SCP は、[SCP がアタッチされた要素の下位](#)にあるすべての AWS アカウント に適用されます。SCP では、組織のすべてのアカウントで使用可能な最大アクセス許可を一元的に制御できます。これは AWS アカウント が組織のアクセスコントロールガイドラインに従っていることを確認するのに役立ちます。詳細については、AWS Organizations ユーザーガイドの「[サービスコントロールポリシー](#)」を参照してください。

### 前提条件

SCP を使用するには、まず以下のことをする必要があります。

- 組織内のすべての機能の有効化。詳細については、[AWS Organizations ユーザーガイド](#)の「組織内のすべての機能の有効化」を参照してください。
- SCP を有効にして組織内で使用できるようにするには 詳細については、AWS Organizations ユーザーガイドの「[ポリシータイプの有効化と無効化](#)」を参照してください。
- 必要な SCP を作成します。SCP の作成の詳細については、AWS Organizations ユーザーガイドの「[SCP の作成および更新](#)」を参照してください。

## サービスコントロールポリシーの例

### 目次

- [例 1: 外部共有を禁止する](#)
- [例 2: 組織外の外部アカウントからのリソース共有への招待をユーザーが受け付けられないようにする](#)
- [例 3: 特定のアカウントに特定のリソースタイプの共有を許可する](#)
- [例 4: 組織全体または組織単位との共有を禁止する](#)
- [例 5: 特定のプリンシパルのみとの共有を許可する](#)

以下の例では、組織内のリソース共有のさまざまな側面を制御する方法を説明します。

### 例 1: 外部共有を禁止する

以下の SCP は、共有ユーザーの組織外にいるプリンシパルとの共有を許可するリソース共有をユーザーが作成できないようにするものです。

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

```

    }
  ]
}

```

### 例 2: 組織外の外部アカウントからのリソース共有への招待をユーザーが受け付けないようにする

次の SCP は、影響を受けるアカウントのプリンシパルがリソース共有を使用する招待を受け入れることをブロックします。共有アカウントと同じ組織内の他のアカウントと共有されているリソース共有では招待状は生成されないため、この SCP の影響を受けません。

```

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

```

### 例 3: 特定のアカウントに特定のリソースタイプの共有を許可する

以下の SCP では、アカウント 111111111111 と 222222222222 のみが、Amazon EC2 プレフィックスリストを共有する新しいリソース共有を作成し、プレフィックスリストを既存のリソース共有に関連付けることができます。

```

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

```

```

        ]
      },
      "StringEqualsIfExists": {
        "ram:RequestedResourceType": "ec2:PrefixList"
      }
    }
  ]
}

```

#### 例 4: 組織全体または組織単位との共有を禁止する

次の SCP は、組織全体または任意の組織単位とリソースを共有するリソース共有をユーザーが作成できないようにします。ユーザーは、組織内の個々の AWS アカウント、または IAM ロールもしくはユーザーとリソースを共有できます。

```

{
  "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/*"
          ]
        }
      }
    }
  ]
}

```

#### 例 5: 特定のプリンシパルのみとの共有を許可する

以下の SCP の例では、ユーザーは組織 o-12345abcdef、組織単位 ou-98765fedcba、および AWS アカウント 111111111111 のみとリソースを共有できます。



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

## AWS Organizations とのリソース共有の無効化

以前に AWS Organizations との共有を有効にしたことがあり、組織全体または組織単位 (OU) とリソースを共有する必要がなくなった場合、共有を無効にできます。AWS Organizations との共有を無効にすると、作成したリソース共有からすべての組織または OU が削除され、共有リソースへのアクセス権が失われます。

AWS Organizations との共有を無効にするには

1. AWS Organizations [disable-aws-service-access](#) AWS CLI コマンドを使用して AWS Organizations への信頼アクセスを無効にします。

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

**⚠ Important**

AWS Organizations への信頼できるアクセスを無効にすると、組織内のプリンシパルはすべてのリソース共有から削除され、それらの共有リソースへのアクセス権が失われます。

2. IAM コンソール、AWS CLI、または IAM API オペレーションを使用し、AWSServiceRoleForResourceAccessManager サービスリンクロールを削除します。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの削除](#)」を参照してください。

## AWS RAMでのログ記録とモニタリング

モニタリングは、AWS RAM と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS には、AWS RAM リソースをモニタリングし、潜在的なインシデントに対応するための複数のツールが用意されています。

### Amazon CloudWatch Events

AWS リソースの変更を示すシステムイベントのほぼリアルタイムのストリームを提供します。CloudWatch Events で自動イベント駆動型コンピューティングを有効にすると、特定のイベントを監視するルールを記述し、これらのイベントが発生したときに他の AWS のサービスで自動アクションをトリガーできます。詳細については、「[CloudWatch Events を使用した AWS RAM のモニタリング](#)」を参照してください。

### AWS CloudTrail

AWS アカウントにより、またはそのアカウントに代わって行われた API コールや関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出し日時を特定できます。詳細については、「[AWS RAM による AWS CloudTrail API コールのログ記録](#)」を参照してください。

## CloudWatch Events を使用した AWS RAM のモニタリング

Amazon CloudWatch Events を使用して、AWS RAM 内にある特定のイベントに関する自動通知を設定できます。AWS RAM からのイベントは、ほぼリアルタイムで CloudWatch Events に配信されます。イベントをモニタリングし、リソース共有の変更を示すイベントにตอบสนองしてターゲットを呼び出すように CloudWatch Events を設定できます。リソース共有への変更は、リソース共有の所有者およびリソース共有へのアクセスを許可されたプリンシパルの両方についてイベントをトリガーします。

イベントパターンを作成するとき、ソースは `aws.ram` です。

### Note

これらのイベントに依存するコードの記述には注意が必要です。これらのイベントは保証されていませんが、ベストエフォートベースで送信されます。AWS RAM がイベントの送信を試みる際にエラーが発生した場合、サービスはさらに数回試行します。ただし、タイムアウトになり、その特定のイベントが失われる可能性があります。

詳細については、「[Amazon CloudWatch Events ユーザーガイド](#)」を参照してください。

### 例: リソース共有障害時のアラート

Amazon EC2 のキャパシティ予約を組織の他のアカウントと共有するシナリオを考えてみましょう。これはコストを削減する良い方法です。

ただし、[キャパシティ予約を共有するための前提条件](#)をすべて満たしていない場合、リソース共有に関連する非同期タスクの実行が失敗する可能性があります。共有操作が失敗し、他のアカウントのユーザーがそれらのキャパシティ予約のいずれかでインスタンスを起動しようとする、Amazon EC2 はキャパシティ予約を受け付けられない状態であるかのように動作し、代わりにオンデマンドインスタンスとしてインスタンスを起動します。その結果、想定以上のコストが発生する可能性があります。

リソース共有の障害を監視するには、AWS RAM リソース共有が失敗するたびに警告する Amazon CloudWatch Events ルールを設定します。次のチュートリアルでは、Amazon Simple Notification Service (SNS) トピックを使用して、EventBridge がリソース共有障害を検出するたびに、トピックサブスクライバー全員に通知を送信します。Amazon SNS の詳細については、[Amazon Simple Notification Service デベロッパーガイド](#) を参照してください。

リソース共有が失敗したときに通知するルールを作成するには

1. [\[Amazon EventBridge console\]](#) (Amazon EventBridge コンソール) を開きます。
2. ナビゲーションペインで [ルール] を選択し、[ルール] リストで [ルールの作成] を選択します。
3. 名前を入力し、必要に応じてルールの説明を入力して [次へ] を選択します。
4. [イベントパターン] ボックスまでスクロールして、[カスタムパターン] を選択します。
5. 以下のイベントパターンをコピーして貼り付けます。

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

6. [Next] (次へ) をクリックします。
7. [ターゲット 1] の [ターゲットタイプ] で、AWS のサービス を選択します。
8. [ターゲットの選択] で、[SNS トピック] を選択します。
9. [トピック] で、通知を送信する SNS トピックを選択します。このトピックはすでに作成されている必要があります。
10. [次へ] を選択し、もう一度 [次へ] を選択して設定を確認します。
11. オプションに問題がなければ、[ルールの作成] を選択します。
12. [ルール] ページに戻り、新しいルールが [有効] になっていることを確認します。必要な場合、ルール名の横にあるラジオボタンを選択し、[有効] を選択します。

ルールが有効になっている場合、AWS RAM リソース共有に障害が発生すると、送信先のトピック受信者に SNS アラートが送信されます。

共有先のアカウントの [Amazon EC2 コンソールで共有されたキャパシティ予約を表示して](#)、キャパシティ予約がアクセス可能であることを確認することもできます。

## AWS RAM による AWS CloudTrail API コールのログ記録

AWS RAM は AWS CloudTrail という、AWS RAM のユーザーやロール、または AWS のサービスによって実行されたアクションを記録するサービスと統合しています。CloudTrail は、AWS RAM のす

すべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、AWS RAM コンソールの呼び出しと、AWS RAM API オペレーションへのコード呼び出しが含まれます。追跡を作成する場合は、AWS RAM のイベントなど、指定する Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集される情報を利用すると、具体的には AWS RAM へのリクエスト、リクエスト元の IP アドレス、リクエスト、リクエスト日時、その他の詳細を把握できます。

CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

## CloudTrail での AWS RAM 情報

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。AWS RAM でアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、[表示、検索、ダウンロード](#)できます。AWS アカウント 詳細については、「[CloudTrail イベント履歴でのイベントの表示](#)」を参照してください。

AWS RAM のイベントなど、AWS アカウント のイベントの継続的な記録については、追跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、以下を参照してください。

- [AWS アカウント の追跡の作成](#)
- [AWS のサービスと CloudTrail ログの統合](#)
- [Amazon SNS の CloudTrail の通知の設定](#)
- 「[Receiving CloudTrail log files from multiple Regions](#)(CloudTrail ログファイルを複数のリージョンから受け取る)」、「[Receiving CloudTrail log files from multiple accounts](#)(複数のアカウントから CloudTrail ログファイルを受け取る)」

すべての AWS RAM アクションは CloudTrail によってログに記録され、[AWS RAM API リファレンス](#)に記録されます。例え

ば、CreateResourceShare、AssociateResourceShare、EnableSharingWithAwsOrganization の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストを行ったユーザーに関する情報が含まれます。

- AWS アカウント ルート認証情報
- AWS Identity and Access Management (IAM) ロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報
- IAM ユーザーからの長期的なセキュリティ認証情報
- 別の AWS のサービス

詳細については、「[CloudTrail userIdentity 要素](#)」を参照してください。

## AWS RAM ログファイルエントリの理解

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、CreateResourceShare アクションの CloudTrail ログエントリを示しています。

```
{
  "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 boto3/1.11.2",
  "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"
}
```

## AWS RAM での耐障害性

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティゾーンを中心に構築されています。AWS リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立・隔離されたアベイラビリティゾーンがあります。アベイラビリティゾーンでは、アベイラビリティゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティゾーンは、従来の単一または複数のデータセンターインフラストラクチャに比べて、可用性、耐障害性、および拡張性に優れています。

AWS リージョン とアベイラビリティゾーンの詳細については、「[AWS グローバルインフラストラクチャ](#)」を参照してください。

## AWS RAM でのインフラストラクチャセキュリティ

マネージドサービスである AWS Resource Access Manager は AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「[AWS クラウドセキュリティ](#)」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 - AWS Well-Architected Framework」の「[インフラストラクチャ保護](#)」を参照してください。

AWS の発行済み API コールを使用して、ネットワーク経由で AWS RAM にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS) TLS 1.2 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service \(AWS STS\)](#) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。



# AWS RAM で問題のトラブルシューティング

本ガイドのこのセクションの情報は、AWS Resource Access Manager (AWS RAM) を使用する際の一般的な問題のトラブルシューティングと解決に役立ちます。

## トピック

- [エラー: 「Your account ID does not exist in an AWS organization」](#)
- [エラー: 「AccessDeniedException」](#)
- [エラー: 「UnknownResourceException」](#)
- [エラー: 組織外のアカウントと共有しようとするエラーが発生する](#)
- [共有先アカウントで共有リソースが表示されない](#)
- [エラー: 制限を超過した](#)
- [組織内の他のアカウントに招待が送信されない](#)
- [VPC サブネットを共有できない](#)

## エラー: 「Your account ID does not exist in an AWS organization」

### シナリオ

組織内のアカウントまたは組織単位 (OU) とリソースを共有しようとする、「Your account ID does not exist in an AWS organization」というエラーが表示されます。

### 原因

このエラーは、AWS Resource Access Manager と AWS Organizations の統合を有効化する際に、サービスにリンクされたロール [AWSServiceRoleForResourceAccessManager](#) が正常に作成されなかった場合に発生します。

### 解決策

必要なサービスにリンクされたロールを再度作成するには、次の手順を実行して統合を無効にして再度有効にします。

1. IAM ロールまたは管理者アクセス許可を持つユーザーを使用して、組織の管理アカウントにサインインします。
2. [AWS Organizations コンソールのサービスページ](#)に移動します。

3. [RAM] を選択します。
4. [Disable trusted access] (信頼されたアクセスを無効にする) を選択します。
5. [AWS RAM コンソールの設定ページ](#)に移動します。
6. [AWS Organizations との共有の有効化] ボックスを選択して、[設定の保存] を選択します。

これで、AWS RAM を使用して組織のアカウントや OU とリソースを共有できるようになります。

## エラー: 「AccessDeniedException」

### シナリオ

リソースを共有しようとしたり、リソース共有を表示したりしようとする、と、「Access Denied」と表示されます。

### 原因

必要なアクセス許可なしにリソース共有を作成しようとする、このエラーが表示されることがあります。これは、AWS Identity and Access Management (IAM) プリンシパルにアタッチされているポリシーのアクセス許可が不十分であることが原因である可能性があります。また、AWS アカウントに影響する AWS Organizations サービスコントロールポリシー (SCP) の制限が原因で発生することもあります。

### 解決策

アクセスを提供するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「[シークレットの作成と管理](#)」の手順に従ってください。

- ID プロバイダーを通じて IAM で管理されているユーザー:

ID フェデレーションのロールを作成する。詳細については、「IAM ユーザーガイド」の「[サードパーティー ID プロバイダー \(フェデレーション\) 用のロールの作成](#)」を参照してください。

- IAM ユーザー:

- ユーザーが設定できるロールを作成します。手順については、「IAM ユーザーガイド」の「[IAM ユーザー用ロールの作成](#)」を参照してください。

- (非推奨) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。「IAM ユーザーガイド」の「[ユーザー \(コンソール\) へのアクセス許可の追加](#)」の指示に従います。

このエラーを解決するには、リクエストを行ったプリンシパルが使用するアクセス許可ポリシーの Allow ステートメントによって、アクセス許可が付与されていることを確認する必要があります。また、アクセス許可が組織の SCP でブロックされていないことを確認する必要があります。

リソース共有を作成するには、次の 2 つのアクセス許可が必要です。

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

リソース共有を表示するには、次のアクセス許可が必要です。

- `ram:GetResourceShares`

リソース共有にアクセス許可をアタッチするには、次のアクセス許可が必要です。

- *`resourceOwningService:PutPolicyAction`*

これはプレースホルダーです。共有するリソースを所有するサービスの「PutPolicy」アクセス許可 (または同等の権限) でこれを置き換える必要があります。例えば、Route 53 リゾルバールールを共有する場合、必要な権限は `route53resolver:PutResolverRulePolicy` になります。複数のリソースタイプを含むリソース共有の作成を許可する場合は、許可するリソースタイプごとに関連するアクセス許可を含める必要があります。

以下は、このような IAM アクセス許可ポリシーの例です。

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

```
        "ram:GetResourceShares",
        "resourceOwningService:PutPolicyAction"
    ],
    "Resource": "*"
}
]
```

## エラー: 「UnknownResourceException」

### シナリオ

次のいずれかのエラーが表示されます。

- 「CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit ou-xxxx could not be found」
- 「CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou-xxxx could not be found」

### 原因

これらのエラーは、[AWS RAM コンソールを使用](#)する代わりに、[Organizations コンソール](#)または [Organizations の EnableAWSServiceAccess API](#) を使用して AWS RAM と AWS Organizations の統合を有効化した場合に発生することがあります。Organizations コンソールまたは API を使用して統合を有効化しても、サービスはアカウントに `AWSServiceRoleForResourceAccessManager` ロールを作成しません。このロールは、組織に関する情報にアクセスするために必要です。このロールが作成されていないため、AWS RAM は組織のアカウントや組織単位 (OU) に関する詳細にアクセスできません。

### 解決策

この問題を解決するには、AWS RAM と AWS Organizations の統合を無効にします。その後、AWS RAM [EnableSharingWithAwsOrganization](#) API を呼び出すか、AWS Management Console を使用し、次の手順を実行して、再度有効にします。

1. IAM ロールまたは管理者アクセス許可を持つユーザーを使用して、組織の管理アカウントにサインインします。

2. [AWS Organizations コンソールのサービスページ](#)に移動します。
3. [RAM] を選択します。
4. [Disable trusted access] (信頼されたアクセスを無効にする) を選択します。
5. [AWS RAM コンソールの設定ページ](#)に移動します。
6. [AWS Organizations との共有の有効化] ボックスを選択して、[設定の保存] を選択します。

これで、AWS RAM を使用して組織のアカウントや OU とリソースを共有できるようになります。

## エラー: 組織外のアカウントと共有しようとするエラーが発生する

### シナリオ

組織外のアカウントとリソースを共有しようとする、以下のいずれかのエラーが表示されます。

- 「You cannot share the resource outside your organization.」
- 「The resource you are attempting to share can only be shared within your AWS Organization.」
- 「InvalidParameterException: Principal Account-ID is not in your AWS organization. You do not have permission to add external AWS アカウント to a resource share.」
- 「OperationNotPermittedException: The resource you are attempting to share can only be shared within your AWS Organization.」

### 考えられる原因と解決策

一部のリソースタイプは、同じ組織のアカウントとしか共有できないものがあります。

一部のリソースタイプは、組織のメンバーではないアカウントとは共有できないものがあります。この制限のあるリソースタイプの例は、Amazon Elastic Compute Cloud (Amazon EC2) の一部である仮想プライベート接続 (VPC) です。

特定のリソースタイプを組織外のアカウントやプリンシパルと共有できるかどうかを確認するには、「[共有可能な AWS リソース](#)」を参照してください。

## サービスにリンクされたロールが正常に作成されない

この問題は、AWS RAM と AWS Organizations の統合を有効にしたときに、サービスにリンクされたロール `AWSServiceRoleForResourceAccessManager` が正常に作成されなかった場合に発生する可能性があります。

組織の一部であるアカウントとリソースを共有しようとしたときにこのようなエラーが発生した場合は、次の手順を実行してサービスにリンクされたロールを削除して再作成してください。

1. IAM ロールまたは管理者アクセス許可を持つユーザーを使用して、組織の管理アカウントにサインインします。
2. [AWS Organizations コンソールのサービスページ](#)に移動します。
3. [RAM] を選択します。
4. [Disable trusted access] (信頼されたアクセスを無効にする) を選択します。
5. [AWS RAM コンソールの設定ページ](#)に移動します。
6. [AWS Organizations との共有の有効化] ボックスを選択して、[設定の保存] を選択します。

## 共有先アカウントで共有リソースが表示されない

### シナリオ

ユーザーは、他の AWS アカウント から自分に共有されているはずのリソースを表示することができません。

### 考えられる原因と解決策

AWS Organizations との共有が AWS RAM ではなく Organizations を使用して有効化された

AWS RAM ではなく Organizations を使用して AWS Organizations を有効にした場合、組織内での共有は失敗します。これが問題の原因かどうかを確認するには、[AWS RAM コンソールの設定ページ](#)に移動し、[AWS Organizations との共有の有効化] チェックボックスが有効になっているかどうかを確認します。

- チェックボックスが有効の場合、このエラーは他の原因によるものです。
- チェックボックスが無効の場合、このエラーはこの原因による可能性があります。ここでは、このチェックボックスを有効にしないでください。問題を解決するには、次の手順を実行します。

1. IAM ロールまたは管理者アクセス許可を持つユーザーを使用して、組織の管理アカウントにサインインします。
2. [AWS Organizations コンソールのサービスページ](#)に移動します。
3. [RAM] を選択します。
4. [Disable trusted access] (信頼されたアクセスを無効にする) を選択します。
5. [AWS RAM コンソールの設定ページ](#)に移動します。
6. [AWS Organizations との共有の有効化] ボックスを選択して、[設定の保存] を選択します。

[共有を更新し、共有する組織内のアカウントまたは組織単位を指定する](#)必要がある場合があります。

リソース共有では、このアカウントをプリンシパルとして指定していない

リソース共有を作成した AWS アカウント で、[AWS RAM コンソールのリソース共有を表示します](#)。リソースにアクセスできないアカウントがプリンシパルとして表示されているかどうかを確認します。表示されていない場合は、[共有を更新してアカウントをプリンシパルとして追加します](#)。

アカウントのロールまたはユーザーに必要なアクセス許可がない

アカウント A のリソースを別のアカウント B と共有しても、アカウント B のロールとユーザーは共有内のリソースに自動的にアクセスできません。アカウント B の管理者は、まず、リソースにアクセスする必要があるアカウント B の IAM ロールとユーザーにアクセス許可を付与する必要があります。例えば、次のポリシーは、アカウント A のリソースについて、アカウント B のロールとユーザーに読み取り専用アクセス許可を付与する方法を示しています。このポリシーでは、[Amazon リソースネーム \(ARN\)](#) でリソースを指定します。

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

## リソースは現在のコンソール設定と異なる AWS リージョン にある

AWS RAM はリージョンでのサービスです。リソースは特定の AWS リージョン に存在し、それらを表示するにはそのリージョンのリソースを表示するように AWS Management Console を設定する必要があります。

コンソールが現在アクセスしている AWS リージョン は、コンソールの右上隅に表示されます。これを変更するには、現在のリージョン名を選択し、ドロップダウンメニューからリソースを表示するリージョンを選択します。

## エラー: 制限を超過した

### シナリオ

リソースを共有すると「You have reached the limit on the number of resources you can share」または「ResourceShareLimitExceededException」が表示されます。

### 原因

これらのエラーは、AWS RAM サービスまたは共有しようとしているリソースを作成した AWS のサービスを使用する際に、共有できるリソースの最大数に達したときに発生します。このクォータ (以前は「制限」と呼ばれていました) は、リソースの共有元アカウントおよび共有先アカウントの両方に影響します。

### 解決策

- クォータを確認するには、エラーが表示されている AWS アカウント で、制限に達しているクォータの種類に応じて、以下のいずれかのページに移動します。
  - [Service Quotas コンソールのサービスの AWS RAM ページ](#)
  - [クォータで制限されているリソースの AWS のサービス ページ](#)
- 下にスクロールして、関連するクォータを選択します。
- このクォータで利用できる場合は、[クォータの増加をリクエスト] を選択します。
- クォータに新しい値を入力して、[リクエスト] を選択します。
- リクエストは [クォータリクエスト履歴](#) ページに表示され、リクエストが確定するまでリクエストのステータスを確認できます。



## 組織内の他のアカウントに招待が送信されない

### シナリオ

AWS Organizations が管理する同じ組織の別のアカウントとリソースを共有しても、アカウントには招待が届きません。

### 原因

これは、自分のアカウントで[AWS 組織での共有が有効になっている](#)場合に想定される動作です。

このオプションが有効になっている場合に組織内の別のアカウントと共有すると、招待は送信されず、承諾も必要ありません。リソース共有でプリンシパルとして参照しているすべての組織アカウントは、すぐに共有内のリソースへのアクセスを開始できます。

自分のアカウントで AWS 組織内での共有を有効にしていない場合、他のアカウントと共有すると、同じ AWS 組織に属していても、スタンドアロンアカウントとして扱われます。ユーザーが共有内のリソースにアクセスするには、招待を受取、招待を承認する必要があります。

## VPC サブネットを共有できない

### シナリオ


AWS RAM を使用して別のアカウントと VPC サブネットを共有しようとする、共有は正常に行われます。ただし、AWS RAM コンソールのリソースのコンシューマーアカウントでは LIMIT EXCEEDED と表示されます。

### 原因

一部のリソースタイプには、AWS RAM によって適用される制限とは別にサービス固有の制限があります。これらの制限の中には、AWS RAM のいずれかの制限に達していなくても、共有を妨げるものがあります。制限はこれら制約の一例です。Amazon Virtual Private Cloud (Amazon VPC) は、別の個人アカウントと共有できるサブネットの数を制限します。すでに最大数のサブネットを含むコンシューマーアカウントとサブネットを共有しようとする、そのコンシューマーアカウントのコンソールに LIMIT EXCEEDED が表示されます。詳細については、「Amazon Virtual Private Cloud ユーザーズガイド」の「[Amazon VPC クォータ - VPC 共有](#)」を参照してください。

この問題を解決するには、まず、影響を受けたアカウントと指定されたリソースを共有している可能性のある他のリソース共有を確認し、不要な共有を削除します。サポートされている場合は、制限の

引き上げをリクエストすることもできます。制限の引き上げをリクエストする際は、[Service Quotas コンソール](#)を使用します。

 Note

AWS RAM は制限引き上げの変更を自動的に検出しません。変更を検出するには、リソースまたはプリンシパルを RAM のリソース共有に再度関連付ける必要があります。

## AWS RAM のサービスクォータ



AWS アカウント には AWS Resource Access Manager (AWS RAM) に関する以下の制限があります。これらの制限の一部は、リクエストによって引き上げることができます。制限の引き上げをリクエストするには、[AWS Support](#) にお問い合わせください。

### Note

以下のクォータの説明には、次の定義が適用されます。

- **リソース** — Amazon S3 バケットまたは Amazon EC2 インスタンスなど、AWS のサービスによって作成される共有する個別の要素。リソース共有で参照されるリソースごとに、1 クォータとカウントされます。同じリソースを 3 つの異なるリソース共有で共有すると、3 クォータとカウントされます。
- **リソース共有** — リソースの共有に使用できる AWS RAM によって作成されるコンテナ。各リソース共有は、含まれているリソースの数に関係なく、1 クォータとカウントされます。
- **共有プリンシパル** - リソース共有に関連付けられる ID。これには AWS Identity and Access Management (IAM) ロールやユーザー、AWS アカウント ID、組織単位、または組織全体が含まれます。リソース共有で参照する共有プリンシパルごとに、1 クォータとカウントされます。ID を参照して組織全体と共有した場合、1 クォータとカウントされます。
- **カスタマー管理アクセス許可** — 特定のユースケースに対応するために作成する管理アクセス許可で、最小特権で共有リソースの使用方法を管理します。

リソース	デフォルトの制限
AWS リージョン ごとのリソース共有の最大数	25,000
リソース共有あたりのリソース関連付けの最大数	5,000
リソース共有あたりのプリンシパル関連付けの最大数	5,000

リソース	デフォルトの制限
カスタマー管理アクセス許可の最大数	1,500
リソースタイプあたりのカスタマー管理アクセス許可の最大数	10
カスタマー管理アクセス許可あたりのバージョンの最大数	5
AWS リージョン 内のリソース共有全体のリソースの関連付けの最大数	25,000
<p> <b>Note</b></p> <p>リソース共有に含まれる各リソースは、この制限にカウントされます。あるリソースが 10 個の異なるリソース共有に含まれている場合は、この制限に対して 10 カウントされます。</p>	
AWS リージョン 内のリソース共有全体のプリンシパルの関連付けの最大数	25,000
<p> <b>Note</b></p> <p>リソース共有に含まれる各プリンシパルは、この制限にカウントされます。あるプリンシパルが 10 個の異なるリソース共有に含まれている場合は、この制限に対して 10 カウントされます。</p>	

リソース	デフォルトの制限
<p data-bbox="115 226 784 260">共有アカウントあたりの保留中の招待の最大数</p> <ul data-bbox="115 310 784 739" style="list-style-type: none"><li data-bbox="115 310 784 436">• このクォータは、同じ AWS Organizations に属さないアカウントと共有している送信アカウントにのみ適用されます。</li><li data-bbox="115 457 784 541">• 受信側アカウントで保有できる保留中の招待数のクォータはありません。</li><li data-bbox="115 562 784 739">• 招待は、同じ AWS Organizations の一部であるアカウント間で共有する場合、また、AWS Organizations 内で有効にしたリソース共有には使用されません。</li></ul>	<p data-bbox="829 226 886 260">250</p>

# AWS SDK での AWS RAM の使用

AWS ソフトウェア開発キット (SDK) は、多くの一般的なプログラミング言語で使用できます。各 SDK には、開発者が好みの言語でアプリケーションを構築しようとする際に役立つ API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	コードの例
<a href="#">AWS SDK for C++</a>	<a href="#">AWS SDK for C++ コードの例</a>
<a href="#">AWS SDK for Go</a>	<a href="#">AWS SDK for Go コードの例</a>
<a href="#">AWS SDK for Java</a>	<a href="#">AWS SDK for Java コードの例</a>
<a href="#">AWS SDK for JavaScript</a>	<a href="#">AWS SDK for JavaScript コードの例</a>
<a href="#">AWS SDK for .NET</a>	<a href="#">AWS SDK for .NET コードの例</a>
<a href="#">AWS SDK for PHP</a>	<a href="#">AWS SDK for PHP コードの例</a>
<a href="#">AWS SDK for Python (Boto3)</a>	<a href="#">AWS SDK for Python (Boto3) コードの例</a>
<a href="#">AWS SDK for Ruby</a>	<a href="#">AWS SDK for Ruby コードの例</a>

## 可用性の例

必要なものが見つからなかった場合。フィードバックリンクを使用してコード例をリクエストします。

# AWS RAM ユーザーガイドのドキュメント履歴

次の表は、このドキュメントに追加された重要な内容をまとめたものです。AWS Resource Access Manager また、お客様からいただいたフィードバックに対応するために、ドキュメントを更新します。

AWS RAM RSS フィードを購読すると、これらの更新に関する通知を受け取ることができます。

変更	説明	日付
<a href="#">共有のサポートが追加されました。Amazon Route 53 ResolverProfiles</a>	AWS RAM を使用して、Amazon Route 53 Resolver Profiles AWS アカウント 組織内の他のユーザーと共有できるようになりました。	2024 年 4 月 22 日
<a href="#">AWS Systems Manager パラメータストアリソースの共有がサポートされるようになりました。</a>	AWS アカウント 高度なパラメータを組織全体または組織内で安全かつ効率的に共有できるようになりました。	2024 年 2 月 21 日
<a href="#">Amazon FSx for OpenZFS スナップショットを共有するためのサポートが追加されました。</a>	OpenZFS 用 Amazon FSx AWS アカウント のスナップショットを組織内の他のユーザーと共有できるようになりました。	2023 年 12 月 19 日
<a href="#">リソース共有のサポートが追加されました。Amazon Simple Storage Service</a>	Amazon Simple Storage Service Access Grants AWS アカウント インスタンスを他のユーザーまたは組織と共有できるようになりました AWS RAM。	2023 年 11 月 27 日
<a href="#">AWS Resource Explorer ビューを共有するためのサポートが追加されました。</a>	AWS Resource Explorer AWS アカウント 組織内の他のユーザー	2023 年 11 月 14 日

	ザーとビューを共有できるようになりました。	
<a href="#">Amazon Route 53 Application Recovery Controller のリソース共有サポートが追加されました。</a>	Amazon Route 53 AWS アカウント アプリケーションリカバリコントローラクラスターを他のユーザーまたは組織と共有できるようになりました AWS RAM。	2023 年 10 月 18 日
<a href="#">Amazon DataZone リソースを共有するためのサポートが追加されました。</a>	Amazon DataZone AWS アカウント リソースを他のユーザーまたは自分の組織と共有できるようになりました。	2023 年 10 月 4 日
<a href="#">サービスプリンシパル共有のサポートが追加されました。</a>	サービスプリンシパルをリソース共有に関連付けることができるようになりました。これにより、指定したサービスはユーザーのリソースに必要なアクションをユーザーの代わりに管理できるようになります。	2023 年 8 月 29 日
<a href="#">SageMaker モデルカードリソースの共有がサポートされるようになりました。</a>	SageMaker AWS アカウント モデルカードのリソースを他のユーザーまたは組織と共有できるようになりました。	2023 年 8 月 18 日
<a href="#">共有可能なリソースとして Amazon SageMaker Feature Store SageMaker 機能グループとカタログのサポートが追加されました。</a>	Amazon SageMaker Feature Store SageMaker AWS アカウント 機能グループとカタログリソースを他のユーザーまたは組織と共有できるようになりました。	2023 年 7 月 20 日



<a href="#">保留中の招待のサービス クォータ制限の引き上げ。</a>	共有アカウントごとの保留中の招待の最大数が 20 件から 250 件に引き上げられました。	2023 年 6 月 8 日
<a href="#">共有可能なリソースとしての AWS AppSync GraphQL API のサポートを追加しました。</a>	AWS AppSync GraphQL API AWS アカウントを他のユーザーと共有できるようになりました。AWS RAM	2023 年 5 月 24 日
<a href="#">AWS Verified Access 共有可能なリソースとしてのグループのサポートが追加されました。</a>	AWS Verified Access グループを一元的に作成、管理し、AWS アカウント 他のユーザーや組織と共有できるようになりました。	2023 年 4 月 27 日
<a href="#">AWS RAM コンソールでの顧客管理権限のサポートが追加されました。</a>	サポートされているリソースタイプの詳細なリソースアクセス制御を安全に作成し、管理できるようになりました。	2023 年 4 月 19 日
<a href="#">Amazon VPC Lattice サービスとサービスネットワークのリソース共有サポートが追加されました。</a>	Amazon VPC Lattice サービスとサービスネットワークリソースを他のユーザーと共有できるようになりました。 AWS アカウント	2023 年 3 月 31 日
<a href="#">共有可能なリソースとしての AWS Marketplace Catalog エンティティのサポートが追加されました。</a>	これで、エンティティを Marketplace AWS アカウントの他のユーザーと共有できます。	2023 年 3 月 27 日
<a href="#">AWS RAM コンソールでの権限バージョンの管理がサポートされるようになりました。</a>	AWS RAM コンソールを使用してバージョンの詳細を表示したり、デフォルトとして指定されているバージョンへの権限を更新したりできるようになりました。	2023 年 1 月 16 日

<a href="#">IAM ベストプラクティスの更新</a>	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「 <a href="#">IAM のセキュリティのベストプラクティス</a> 」を参照してください。	2023 年 1 月 3 日
<a href="#">Amazon EC2 プレイメントグループのリソース共有サポートが追加されました。</a>	Amazon EC2 AWS アカウントプレイメントグループを他のユーザーと共有してインスタンスを起動できるようになりました。	2022 年 11 月 8 日
<a href="#">AWS RAMに関する 2 つの紹介動画へのリンクを追加しました。</a>	AWS RAM リソースを他のユーザーと共有する方法を説明し、ウォークスルーを提供する概要ビデオを追加しました。AWS アカウント	2022 年 8 月 29 日
<a href="#">Amazon SageMaker パイプラインのサポートが追加されました。</a>	SageMaker パイプラインを他のユーザーと共有できるようになりました。AWS アカウント	2022 年 8 月 2 日
<a href="#">AWS Service Catalog AppRegistry 共有可能なリソースタイプとしてアプリケーションと属性グループのサポートが追加されました。</a>	AppRegistry アプリケーションと属性グループを他のユーザーと共有できるようになりました。AWS アカウント	2022 年 6 月 17 日
<a href="#">AWS Resource Access Manager SOC および ISO 認証を受けています。</a>	AWS RAM サービス組織管理 (SOC) および国際標準化機構 (ISO) のISO 9001、ISO 27001、ISO 27017、ISO 27018、ISO 27701規格に準拠していることが検証されています。	2022 年 5 月 31 日

<a href="#">AWS Resource Access Manager FedRAMP認定を受けています。</a>	AWS RAM 連邦リスクおよび権限管理プログラム (FedRAMP) に準拠していることが検証されています。	2022 年 4 月 8 日
<a href="#">AWS Resource Access Manager PCI DSS 認定を受けています。</a>	AWS RAM ペイメントカード業界 (PCI) データセキュリティ基準 (DSS) に準拠していることが検証されています。	2022 年 2 月 27 日
<a href="#">Amazon VPC IPAM リソース検出のリソース共有サポートが追加されました。また、IPAM プールを組織外のアカウントと共有できるようになりました。</a>	IPAM リソースの検出を他の AWS アカウントと共有できるようになりました。	2022 年 1 月 25 日
<a href="#">グローバルリソースの共有サポートが追加されました。</a>	グローバルリソースを他のユーザーと共有できるようになりました。AWS アカウント	2021 年 12 月 2 日
<a href="#">共有可能なグローバルリソースとして AWS Cloud WAN コアネットワークがサポートされるようになりました。</a>	Cloud WAN AWS アカウントコアネットワークを他のユーザーと共有できるようになりました。	2021 年 12 月 2 日
<a href="#">Amazon VPC IP Address Manager (IPAM) プールの共有サポートが追加されました。</a>	AWS RAM を使用して Amazon VPC IP アドレス管理プールを共有できます。詳細については、ユーザーガイドの「 <a href="#">AWS 共有可能なリソース</a> 」を参照してください。AWS RAM	2021 年 12 月 1 日

[Amazon SageMaker リソースの共有のSupport](#)

AWS RAM SageMaker を使用して系統グループを共有できません。詳細については、「AWS RAM ユーザーガイド」の「[共有可能な AWS リソース](#)」を参照してください。

2021 年 11 月 30 日

[AWS Migration Hub リファクタリングスペースリソースの共有のSupport](#)

AWS RAM を使用してMigration Hub 環境を共有できません。詳細については、「AWS RAM ユーザーガイド」の「[共有可能な AWS リソース](#)」を参照してください。

2021 年 11 月 29 日

[AWS RAM AWS マネージド IAM アクセス権限ポリシーに関する情報を追加しました。](#)

IAM コンソールでアクセスでき、の IAM プリンシパルにアタッチできる、使用可能な AWS-managed アクセス権限ポリシーに関する詳細を公開しました。AWS アカウント

2021 年 9 月 16 日

[S3 on Outposts のリソース共有サポートが追加されました。](#)

AWS RAM を使用して、Outposts の S3 AWS アカウントを他のユーザーと共有できるようになりました。

2021 年 8 月 5 日

[追加の管理アクセス許可および IAM プリンシパルとのリソース共有のサポートが追加されました。](#)

サポートされているリソースタイプでは、AWS RAM 追加の管理権限から選択して、個々の IAM ロールやユーザーとリソースを共有できます。

2021 年 6 月 10 日

<a href="#"><u>AWS Systems Manager インシデントマネージャーリソースの共有のサポートが追加されました</u></a>	AWS RAM を使用して、AWS Systems Manager インシデントマネージャーの連絡先と対応計画を他のユーザーと共有できるようになりました AWS アカウント。	2021 年 5 月 10 日
<a href="#"><u>Amazon Route 53 のリソース共有サポートが追加されました。</u></a>	AWS RAM を使用して Amazon Route 53 リゾルバー DNS AWS アカウントファイアウォールルールグループを他のユーザーと共有できるようになりました。	2021 年 3 月 31 日
<a href="#"><u>AWS Transit Gateway リソース共有のサポートが追加されました。</u></a>	AWS RAM を使用して、AWS アカウントトランジットゲートウェイのマルチキャストドメインを他のユーザーと共有できるようになりました。	2020 年 12 月 10 日
<a href="#"><u>AWS Network Firewall リソース共有のサポートが追加されました。</u></a>	AWS RAM を使用して、AWS Network Firewall ファイアウォールポリシーとルールグループを他のユーザーと共有できるようになりました AWS アカウント。	2020 年 11 月 17 日
<a href="#"><u>Outposts および ローカルゲートウェイルートテーブルの共有サポートが追加されました。</u></a>	AWS RAM を使用して Outposts AWS アカウントとローカルゲートウェイルートテーブルを他のユーザーと共有できるようになりました。	2020 年 10 月 15 日
<a href="#"><u>Route 53 クエリログの共有サポートが追加されました。</u></a>	AWS RAM を使用して Route 53 AWS アカウントのクエリログを他のユーザーと共有できるようになりました。	2020 年 9 月 7 日

<a href="#"><u>AWS Private Certificate Authority リソース共有のサポートが追加されました。</u></a>	AWS RAM AWS Private CA を使用してプライベート認証局 (CA) を他のユーザーと共有できるようになりました AWS アカウント。	2020 年 8 月 17 日
<a href="#"><u>AWS Glue データカタログ、データベース、テーブルの共有のサポートが追加されました。</u></a>	AWS RAM を使用して、AWS Glue データカタログ、データベース、AWS アカウント テーブルを他のユーザーと共有できるようになりました。	2020 年 7 月 7 日
<a href="#"><u>Amazon VPC プレフィックスリストの共有サポートが追加されました。</u></a>	AWS RAM を使用してプレフィックスリストを共有できるようになりました。	2020 年 6 月 29 日
<a href="#"><u>AWS Outposts 顧客所有の IPv4 アドレスの共有がサポートされるようになりました。</u></a>	AWS RAM を使用して、AWS Outposts 顧客所有の IPv4 アドレスを他のユーザーと共有できるようになりました。AWS アカウント	2020 年 4 月 22 日
<a href="#"><u>メッシュ共有のサポートが追加されました。AWS App Mesh</u></a>	AWS RAM を使用してメッシュを他のユーザーと共有できるようになりました。AWS アカウント	2020 年 1 月 17 日
<a href="#"><u>AWS CodeBuild プロジェクトとレポートグループの共有がサポートされるようになりました。</u></a>	AWS RAM を使用して、AWS CodeBuild プロジェクトやレポートグループを他のユーザーと共有できるようになりました AWS アカウント。	2019 年 12 月 13 日

<a href="#"><u>追加リソースの共有サポートが追加されました。</u></a>	AWS RAM を使用して Amazon EC2 専用ホスト、AWS Resource Groups リソースグループ、Amazon EC2 Image Builder コンポーネント、イメージ、イメージレシピを他のユーザーと共有できるようになりました AWS アカウント。	2019 年 12 月 2 日
<a href="#"><u>オンデマンドキャパシティ予約の共有サポートが追加されました。</u></a>	AWS RAM を使用してオンデマンドキャパシティ予約を他のユーザーと共有できるようになりました AWS アカウント。	2019 年 7 月 29 日
<a href="#"><u>Aurora DB クラスターの共有サポートが追加されました。</u></a>	AWS RAM を使用して Aurora DB AWS アカウントクラスターを他のユーザーと共有できるようになりました。	2019 年 7 月 2 日
<a href="#"><u>トラフィックミラーリングターゲットの共有サポートが追加されました。</u></a>	AWS RAM を使用してトラフィックミラーリングターゲットを他のユーザーと共有できるようになりました。 AWS アカウント	2019 年 6 月 25 日
<a href="#"><u>ライセンス設定の共有サポートが追加されました。</u></a>	AWS RAM を使用して、AWS License Manager のライセンス構成を他のユーザーと共有できるようになりました AWS アカウント。	2018 年 12 月 5 日

[サブネットの共有サポートが追加されました。](#)

AWS RAM を使用して Amazon VPC サブネットを他のユーザーと共有できるようになりました。AWS アカウント

2018 年 11 月 27 日

[中継ゲートウェイの共有サポートが追加されました。](#)

AWS RAM を使用して Amazon VPC トランジットゲートウェイを他のユーザーと共有できるようになりました。AWS アカウント

2018 年 11 月 26 日

[リゾルバールールの共有サポートが追加されました。](#)

AWS RAM を使用して Route 53 リゾルバールールを他のユーザーと共有できるようになりました。AWS アカウント

2018 年 11 月 20 日



翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。