



ユーザーガイド

AWS Resource Access Manager



AWS Resource Access Manager: ユーザーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS RAM	1
ビデオの概要	1
の利点 AWS RAM	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
アクセス AWS RAM	5
の料金 AWS RAM	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	6
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	16
管理アクセス許可のバージョン	17
リソースの共有	17
内でリソース共有を有効にする AWS Organizations	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	30
自分が共有先になっているリソースを使用する	32
共有リソースの使用	33
リージョナルリソースとグローバルリソース	33
リージョナルリソースとグローバルリソースの違い	34
リソース共有とそのリージョン	35
所有するリソース	36
作成したリソース共有の表示	37
リソース共有の作成	39

リソース共有の更新	48
共有リソースの表示	56
共有相手のプリンシパルの表示	57
リソース共有の削除	59
共有しているリソース	61
招待の受け入れと拒否	61
共有しているリソース共有の表示	65
自分が共有先になっているリソースの表示	67
共有相手のプリンシパルの表示	68
リソース共有の終了	70
アベイラビリティゾーン ID	73
共有可能なリソース	76
AWS App Mesh	78
AWS AppSync GraphQL API	78
Amazon API Gateway	79
Amazon Application Recovery Controller (ARC)	80
Amazon Aurora	82
AWS Backup	83
Amazon Bedrock	84
請求情報とコスト管理	85
AWS Billing サービスの表示	86
AWS Cloud Map	87
AWS クラウド WAN	87
Amazon CloudFront	88
AWS CloudHSM	89
AWS CodeBuild	90
AWS CodeConnections	92
Amazon DataZone	93
Amazon EC2	94
EC2 イメージビルダー	98
エラスティックロードバランシング	101
AWS End User Messaging SMS	102
Amazon FSx for OpenZFS	105
AWS Glue	106
AWS License Manager	109
AWS Marketplace	110

AWS Migration Hub Refactor Spaces	111
マルチパーティー承認	112
AWS Network Firewall	113
Oracle Database@AWS	116
AWS Outposts	118
Amazon S3 on Outposts	120
AWS Private Certificate Authority	121
AWS Resource Explorer	122
AWS Resource Groups	123
Amazon Route 53	124
Amazon Simple Storage Service	127
Amazon SageMaker AI	128
AWS Service Catalog AppRegistry	137
AWS Systems Manager Incident Manager	138
AWS Systems Manager	140
Amazon VPC	142
Amazon VPC Lattice	153
でのアクセス許可の管理AWS RAM	157
マネージドアクセス許可の表示	158
カスタマー管理アクセス許可の作成と使用	163
カスタマー管理アクセス許可を作成する	163
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	165
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	167
カスタマー管理アクセス許可のバージョンを削除する	169
カスタマー管理アクセス許可を削除する	170
管理アクセス許可のバージョンを更新する	171
カスタマー管理アクセス許可に関する考慮事項	173
マネージドアクセス許可のしくみ	174
管理アクセス許可のタイプ	176
セキュリティ	178
データ保護	179
ID とアクセス管理	180
が IAM と AWS RAM 連携する方法	180
AWS 管理ポリシー	183
サービスにリンクされたロールの使用	189
IAM ポリシーの例	191

SCP の例	194
組織との共有を無効にする	199
ログ記録とモニタリング	200
EventBridge を使用した のモニタリング	201
を使用した AWS RAM API コールのログ記録 AWS CloudTrail	202
コンプライアンス検証	205
耐障害性	205
インフラストラクチャセキュリティ	206
AWS PrivateLink	206
考慮事項	206
インターフェイスエンドポイントの作成	207
エンドポイントポリシーを作成する	207
トラブルシューティング	209
エラー:アカウント ID が存在しない	209
シナリオ	209
原因	209
ソリューション	209
エラー: アクセス拒否の例外	210
シナリオ	210
原因	210
ソリューション	210
エラー: 未知のリソース例外	212
シナリオ	212
原因	212
ソリューション	213
エラー: 組織外との共有は許可されていない	213
シナリオ	213
考えられる原因と解決策	214
エラー: 共有リソースが表示されない	215
シナリオ	215
考えられる原因と解決策	215
エラー: 制限超過の例外	217
シナリオ	217
原因	217
ソリューション	217
招待が届かない	217

シナリオ	217
原因	218
VPC を共有できない	218
シナリオ	218
原因	218
Service Quotas	219
AWS SDK の使用	222
ドキュメント履歴	223
.....	CCXXXvi

とは AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) を使用すると AWS アカウント、サポートされているリソースタイプの AWS Identity and Access Management (IAM) ロールとユーザー間で、組織または組織単位 (OUs) 内で、リソースを安全に共有できます。複数の [リソースタイプ](#) がある場合は AWS アカウント、リソースを 1 回作成し、を使用してそのリソース AWS RAM 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 [によって管理されている場合](#) AWS Organizations、組織内の他のすべてのアカウント、または 1 つ以上の指定された組織単位 (OUs) に含まれるアカウントのみとリソースを共有できます。アカウントが組織の一部であるかどうかにかかわらず、アカウント ID AWS アカウントごとに特定の [リソースタイプ](#) と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、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。

内容

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

ビデオの概要

次の動画では、[の概要 AWS RAM 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。

次の動画は、AWS リソースに AWS マネージドアクセス許可を適用する方法を示しています。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。

の利点 AWS RAM

を使用する理由 AWS RAM 以下のような利点があります。

- 運用オーバーヘッドを削減 – リソースを 1 回作成し、 を使用してそのリソースを他のアカウントと共有します。AWS RAM 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、 はアイデンティティベースのアクセス許可ポリシーを使用せずに、その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の付与 AWS RAM を簡素化します。
- [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によって管理されます。 は、さまざまなタイプの AWS リソースを共有するための一貫したエクスペリエンス AWS RAM を提供します。
- 可視性と監査可能性を提供 – AWS RAM と Amazon CloudWatch の統合を通じて、共有リソースの使用状況の詳細を表示します AWS CloudTrail。AWS RAM は、共有リソースとアカウントを包括的に可視化します。

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

の外部で AWS Identity and Access Management (IAM) プリンシパル (IAM ロールとユーザー) を識別する [リソースベースのポリシー](#) をアタッチ AWS アカウント することで、一部のタイプの AWS リソースを他の と共有できます AWS アカウント。ただし、ポリシーをアタッチしてリソースを共有しても、AWS RAM が提供する追加の利点は活用されません。を使用すると、次の機能 AWS RAM を利用できます。

- すべての AWS アカウント IDs 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、 を使用して Amazon VPC サブネット AWS RAM 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 コンソールでサブネットを表示し、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。
- 組織に含まれていないアカウントとリソースを共有すると、招待プロセス AWS RAM を開始します。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がある場合は、次のいずれかを実行して、それらのリソースをフル AWS RAM マネージドリソースに昇格させることができます。

- [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 アカウント消費アカウントと共有する場合、消費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を付与します。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、AWS アカウント 共有した のネイティブリソースのようになります。

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

では AWS RAM、リソース共有を作成して、所有している [リソースを共有](#) します。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。では AWS CLI、`--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。プリンシパルは、個人 AWS アカウント、組織内のアカウント、組織の組織単位 (OU) AWS Organizations、または個人 AWS Identity and Access Management (IAM) ロールまたはユーザーです。

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。

- 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。リソースにアクセスするには、関連するサービスのコンソール、AWS CLI コマンド、および API オペレーションを使用します。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。

その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、リソースを所有 AWS アカウントと同じ機能と制限があります。

- 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、米国東部 (バージニア北部)、 の AWS RAM コンソールとツールでのみ表示および管理できます us-east-1。

アクセス AWS RAM

は、次のいずれか AWS RAM の方法で操作できます。

AWS RAM コンソール

AWS RAM は、ウェブベースのユーザーインターフェイスである AWS RAM コンソールを提供します。にサインアップしている場合は AWS アカウント、 にサインイン [AWS マネジメントコンソール](#) し、AWS RAM コンソールのホームページ AWS RAM から を選択して、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 および 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。は Windows、 macOS、 および Linux でこれらのツール AWS をサポートしています。使用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。の コマンドの詳細については AWS RAM、 [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 SDKs

AWS には、さまざまなプログラミング言語用の API コマンドが用意されています。開始方法の詳細については、「[AWS SDK 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かを使用しない場合、AWS RAM HTTPS クエリ API は AWS RAM および へのプログラムによるアクセスを提供します AWS。AWS RAM API を使用すると、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ためのコードを含める必要があります。詳細については、「[APIリファレンスAWS RAM](#)」を参照してください。

の料金 AWS RAM

AWS RAM または を使用してリソース共有を作成し、アカウント間でリソースを共有する場合、追加料金は発生しません。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。が共有可能なリソースに AWS 請求する方法の詳細については、リソースの所有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、マーチャント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、保存、および送信をサポートし、Payment Card Industry (PCI) Data Security Standard (DSS) に準拠していることが確認されています。

PCI DSS の詳細 (AWS PCI コンプライアンスパッケージ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、米国東部 (バージニア北部)、AWS リージョン米国東部 (オハイオ)、米国西部 (北カリフォルニア)、米国西部 (オレゴン) で FedRAMP Moderate として承認されています。

AWS RAM は AWS GovCloud (米国西部) と AWS GovCloud (米国東部) AWS リージョンで FedRAMP High として承認されています。

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、認可、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 Control (SOC) コンプライアンスと国際標準化機構 (ISO) ISO 9001、ISO 27001、ISO 27017、ISO 27018、および ISO 27701 標準の対象となるワークロードに

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。

の開始方法 AWS RAM

を使用すると AWS Resource Access Manager、所有しているリソースを他のユーザーと共有できません AWS アカウント。アカウントが によって管理されている場合は AWS Organizations、組織内の他のアカウントとリソースを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。

内で共有を有効にしない場合 AWS Organizations、組織または組織内の組織単位 (OU) とリソースを共有することはできません。ただし、組織 AWS アカウント 内の個人とリソースを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。

内容

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

の用語と概念 AWS RAM

以下の概念は、AWS Resource Access Manager (AWS RAM) を使用してリソースを共有する方法を説明するのに役立ちます。

リソースの共有

を使用してリソースを共有するには AWS RAM、リソース共有を作成します。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 つ以上の 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すると、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許可できます。

- と AWS RAM の共有を有効にし AWS Organizations、共有するプリンシパルが共有アカウントと同じ組織にある場合、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アクセスできるようになります。
- Organizations と AWS RAM の共有を有効にしない場合でも、組織 AWS アカウント 内の個人と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、共有されているリソースと、AWS RAM 管理者が を使用してリソース共有を作成する AWS リソースが含まれています AWS RAM。

AWS RAM 管理者は、 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 アカウント。はリソースベースのポリシーをリソース共有のリソースにアタッチすることで AWS RAM 機能するため、AWS RAM 管理者はリソース共有に含まれる各リソースタイプの AWS のサービスで PutResourcePolicy オペレーション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

消費アカウントは、リソースが共有される 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。

AWS RAM は、リソース共有のコンシューマーとして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ています。

- もう AWS アカウント 1 つ — リソース共有は、共有アカウントに含まれるリソースを消費アカウントで利用できるようにします。
- 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の共有により、AWS サービスはユーザーに代わってアクションを実行し、運用上の負担を軽減できます。

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 によって管理されている場合 AWS Organizations、リソース共有は組織の ID を指定して、組織内のすべてのアカウントと共有できます。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 タッチするリソースベースのポリシーを使用するためです "Principal": "*"。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 ロールやユーザーなど、プリンシパルにアタッチするアイデンティティ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。は、リソース共有に提供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 AWS RAM 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。

によって生成されたリソースベースのポリシー AWS RAM 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、リソースにアクセスしようとしているプリンシパルにアタッチされた AWS Organizations された IAM アイデンティティベースのポリシーと、に適用される可能性のあるのサービスコントロールポリシー (SCPs) が含まれます AWS アカウント。によって生成された

リソースベースのポリシーは、他のすべての IAM ポリシーと同じポリシー評価ロジック AWS RAM に参加します。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、easy-to-use 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エクスペリエンスを提供します。

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の場合、 はリソースベースのポリシー AWS RAM を自動的に構築および管理します。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。たとえば、 を使用して共有 AWS RAM し、2 つの異なるリソース共有に含める Amazon SageMaker AI パイプライン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、他のリソース共有を使用して、1 つのアカウントに SageMaker AI 実行アクセス許可のみを付与できます。 は、これらの 2 つの異なるアクセス許可セット AWS RAM を複数のステートメントを持つ 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。この基盤となるリソースポリシーを表示するには、 [GetResourcePolicy](#) オペレーションを呼び出します。 AWS のサービス次に、そ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を実行しようとす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検出可能性 – を使用してリソースを共有すると AWS RAM、ユーザーは、共有されている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および API オペレーションで、それらのリソースがユーザーのアカウントに直接あったかのように直接表示できます。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、消費アカウントのユーザーは CodeBuild コンソールと実行された CodeBuild API オペレーションの結果でプロジェクトを表示できます。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。
- 共有所有者の管理性 – を使用してリソースを共有すると AWS RAM、共有アカウントのリソース所有者は、自分のリソースにアクセスできる他のアカウント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せん。

- 効率 – を使用してリソースを共有する場合 AWS RAM、複数のリソースを共有して 1 つのユニット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 – では AWS RAM、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。は、リソース共有にアタッチするために選択できる ready-to-use AWS 管理アクセス許可 AWS RAM を提供します。

を使用すると AWS RAM、リソースベースのポリシーをまだサポートしていない一部の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の場合、 は実際のアクセス許可の表現としてリソースベースのポリシー AWS RAM 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 生成されたリソースベースのポリシーの例

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

```
    },
    "Action": [
      "imagebuilder:GetImage",
      "imagebuilder:ListImages"
    ],
    "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
  }
]
}
```

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
      "Action": [
        "imagebuilder:GetImage",
        "imagebuilder:ListImages"
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
  ]
}
```

EC2 Image Builder イメージリソースを組織内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、は次の例のようなポリシー AWS RAM を生成し、リソース共有に含まれる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。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "imagebuilder:GetImage",
        "imagebuilder:ListImages"
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/testimage/1.0.0/44",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-123456789"
        }
      }
    }
  ]
}
```

"Principal": "*" をリソースベースのポリシーで使用するこゝの影響

"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、該当するアイデンティティポリシー、アクセス許可の境界ポリシー、またはセッションポリシーが暗黙的な Deny の (つまり、明示的な Allow が存在しない) 場合でも、そのリソースベース

のポリシーによってアクションへのアクセスを付与されているプリンシパルに対して Deny が適用されることにはなりません。

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。管理アクセス許可は、プリンシパルがを使用して共有リソースで実行できる一連の actions および 条件を一覧表示します AWS RAM。

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 マネージドアクセス許可

AWS 管理アクセス許可は、によって作成および管理 AWS され、一般的な顧客シナリオに対するアクセス許可を付与します。は、サポートされているリソースタイプごとに少なくとも 1 つの AWS 管理アクセス許可 AWS RAM を定義します。一部のリソースタイプは、複数の AWS 管理アクセス許可をサポートし、1 つの管理アクセス許可を AWS デフォルトとして指定します。特に指定しない限り、[デフォルトの AWS 管理アクセス許可](#)は関連付けられます。

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つ以上の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、共有する[リソースのリソースベースのポリシー](#)を作成するための入力としてマネージドアクセス許可を取得します。

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。または、新しいマネージドアクセス許可バージョン AWS を作成する場合は、既存のリソース共有ごとにマネージド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 マネージドアクセス許可バージョン

AWS は、AWS マネージドアクセス許可に対する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 マネージド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

を使用して所有しているリソースを共有するには AWS RAM、次の操作を行います。

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

注意事項

- リソースを所有 AWS アカウント する 以外のプリンシパルとリソースを共有しても、リソースを作成し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は変更されません。
- AWS RAM はリージョナルサービスです。共有するプリンシパルは、リソースが作成された AWS リージョン のリソース共有にのみアクセスできます。
- 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。

内でリソース共有を有効にする AWS Organizations

アカウントが によって管理されている場合 AWS Organizations、それを利用してリソースをより簡単に共有できます。組織の有無にかかわらず、ユーザーは個々のアカウントに共有できます。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) を使用して共有を有効にする必要があります AWS Organizations。組織内のリソースを共有する場合、AWS RAM はプリンシパルに招待を送信しません。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。

組織内でリソース共有を有効にすると、`iam:AttachRolePolicy` というサービスにリンクされたロール `AWSRAMServiceRoleForResourceAccessManager` を作成します `AWSRAMServiceRoleForResourceAccessManager`。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 を使用して、自分が所属する組織に関する情報を取得する AWS RAM アクセス許可を付与します `AWSRAMServiceRolePolicy`。

Note

デフォルトでは、との共有を有効にすると AWS Organizations、組織内のリソース共有によって、同じ組織内のコンシューマーへのアクセスが制限されます。コンシューマーアカウントが組織を離れると、そのアカウントはリソース共有内のリソースにアクセスできなくな

ります。この制限は、リソースを OU、組織全体、または組織内の個々のアカウントと共有する場合に適用されます。

組織内でのaccount-to-account共有の場合、新しいリソース共有を作成するときに `RetainSharingOnAccountLeaveOrganization` を `true` に設定することで、アカウントが離れ `true` でも共有アクセスを保持できます。この設定を有効にすると、招待 AWS RAM を送信します (外部アカウントとの共有と同様)。アカウントは、組織を離れても共有リソースへのアクセスを保持します。

`RetainSharingOnAccountLeaveOrganization` 設定には、次の要件と制限があります。

- `allowExternalPrincipals` である必要があります `true`
- 新しいリソース共有を作成する場合にのみ設定できます
- OUs または組織全体との共有には適用されません
- `RetainSharingOnAccountLeaveOrganization` が `true` に設定されている場合 `true`、リソース共有を使用して、[組織内でのみ共有できる](#) リソースを共有することはできません。

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、「[とのリソース共有の無効化 AWS Organizations](#)」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` コマンド AWS Organizations を使用して、との共有を有効にする必要があります。 [enable-sharing-with-aws-organization](#) AWS CLI これにより、`AWSServiceRoleForResourceAccessManager` サービスにリンクされた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` サービスにリンクされたロールは作成されず、組織内でリソースを共有することはできません。

Console

組織内でリソース共有を有効にするには

1. AWS RAM コンソールで [設定](#) ページを開きます。
2. 「共有を有効にする AWS Organizations」を選択し、「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。

このコマンドは任意ので使用でき AWS リージョン、AWS RAM がサポートされている AWS Organizations すべてのリージョンでとの共有を有効にします。

```
$ 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。

1. 共有するリソースを追加します。
2. 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 管理アクセス許可の 1 つ、既存のカスタマー管理アクセス許可から選択するか、新しいカスタマー管理アクセス許可を作成できます。
- AWS マネージドアクセス許可は、標準のユースケースをカバーする AWS ために 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 は自動的にデフォルトバージョンをアタッチします。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

- 後で共有に含めた AWS リソースを削除する必要がある場合は、まずそのリソースを含む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お勧めします。
- 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 はリージョナルサービスです。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で AWS リージョン サポートされている任意の からそれらのリソースにアクセスできます。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 および グローバルリソースの詳細については、「」を参照してください[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](#)。
- 共有元のアカウントが の組織の一部 AWS Organizations であり、組織内での共有が有効になっている場合、共有する組織内のプリンシパルには、招待を使用せずにリソース共有へのアクセス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。
- リソース共有にアクセスできる AWS アカウント を組織または OU に追加すると、その新しいメンバーアカウントは自動的にリソース共有にアクセスします。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せん。
- 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 タッチするリソースベースのポリシーを使用するためです `"Principal": "*"` 。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、個別に AWS アカウント を追加することも、サポートされているサービスの場合は、IAM ロールと組織外のユーザーをプリンシパルとしてリソース共有に追加することもできます。

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 に存在するため AWS リージョン、コンソールの右上隅 AWS リージョン にある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。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. を初めて使用する場合は AWS RAM、ホームページからリソース共有を作成するを選択します。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. [\[次へ\]](#) を選択します。
6. ステップ 2: 管理アクセス許可を各リソースタイプに関連付けるには、 によって作成された管理アクセス許可 AWS 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. [次へ] を選択します。
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、誰とでも共有を許可するが選択されます。つまり、それをサポートす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 AWS アカウント である を追加するには、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 タッチするリソースベースのポリシーが使用するためです "Principal": "*"。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。

- 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。
- 個人を選択した場合 AWS アカウント、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。

i 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、ID (、組織 AWS アカウント、

または OU の場合) または ARN (IAM ロールまたはユーザーの場合) を入力し、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 – を追加するには AWS アカウント、12 桁のアカウント ID を入力します。例えば、次のようになります。

```
123456789012
```

- 組織 – 組織 AWS アカウント 内のすべての を追加するには、組織の ID を入力します。例えば、次のようになります。

```
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
```

例えば、次のようになります。

```
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
```

例えば、次のようになります。

```
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`

例えば、次のようになります。

```
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. [次へ] を選択します。

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](#) コマンドを使用します。次のコマンドは、組織 AWS アカウント 内のすべてのと共有されるリソース共有を作成します。共有には AWS License Manager ライセンス設定が含まれており、そのリソースタイプの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

を使用して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 AWS Resource Access Manager、次のタスクを実行します。

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。

- の組織に属 AWS Organizations していて、組織内の共有が有効になっている場合、組織内のプリンシパルは招待なしで共有リソースに自動的にアクセスします。
- リソースを所有 AWS アカウント すると共有する場合、そのアカウントのプリンシパルは招待なしで共有リソースに自動的にアクセスします。

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、リソース共有が作成された AWS リージョン にのみ表示されます。予想される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 AWS リージョン を使用して別のリソース共有に切り替える必要がある場合があります。

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しないことを示します。

3. 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-bbbbbbb222222",
      "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ある場合は、サービスコンソールまたは API/CLI コマンド `AWS リージョン` で正しい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。リソースを表示するには `AWS RAM`、リソース共有 `AWS リージョン` が作成された に対して `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。](#)
 - [での共有リソースの表示 AWS RAM](#)
 - [でリソースを共有するプリンシパルを表示する AWS RAM](#)
 - [でのリソース共有の削除 AWS RAM](#)
- [共有している 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) がリージョンおよびグローバルリソースと連携する方法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。リージョンリソースには `aws:region` が表示されます AWS リージョン。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

共有できるほとんどのリソースはリージョン AWS RAM 別です。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。たとえば、`awscli` を使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを作成するには AWS マネジメントコンソール、インスタンスを作成する [を選択します AWS リージョン](#)。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。AWS SDKs はそれぞれ、オペレーションが使用するリージョンを指定するための独自の同等のメカニズムを持っています。

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。

AWS リージョン コンソールまたは コマンドで AWS CLI 別の `aws:region` を指定した場合、前のリージョンに表示されるリソースを表示したり操作したりできなくなります。

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 AWS リージョン

で 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ときに `--region` パラメータを指定しません。

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須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 クラウド 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場合、すべてのユーザーに対して一貫性があります。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 はリージョン別サービスで、リソース共有はリージョン別です。したがって、リソース共有には、リソース共有 AWS リージョン と同じ のリソースと、サポートされているすべて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ンリソースを共有するには、 を使用してリソース共有 `us-west-2` を作成するように AWS RAM コンソールを設定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) 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 us-east-1。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、共有後もグローバルリソースのままです。元のでアクセスできる任意のリージョン AWS アカウント から共有 でアクセスできます AWS アカウント。

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リージョンで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ンリソースを表示してリソース共有に含めるには、リージョン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、米国東部 (バージニア北部) 、を使用する必要があります us-east-1。
- 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。](#)
- [での共有リソースの表示 AWS RAM](#)
- [でリソースを共有するプリンシパルを表示する AWS RAM](#)
- [でのリソース共有の削除 AWS RAM](#)

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

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ごの影響](#)」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. [次へ] を選択します。
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. [次へ] を選択します。
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. [次へ] を選択します。

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 マネジメントコンソール 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. [次へ] を選択します。
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が確定され、以前のバージョンに戻ることはできなくなります。

8. [次へ] を選択します。
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こゝの影響」](#)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. [次へ] を選択します。

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。

での共有リソースの表示 AWS RAM

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 に存在するため AWS リージョン、コンソールの右上隅 AWS リージョン にある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. 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"
    }
  ]
}
```

でリソースを共有するプリンシパルを表示する AWS RAM

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 に存在するため AWS リージョン、コンソールの右上隅 AWS リージョン にある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. 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](#) コマンドを使用して、AWS リージョン 呼び出し元のアカウントの現在の で作成したリソース共有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のアカウントの組織であり AWS アカウント、2 つの異なるリソース共有の一部として別の です。リソース共有 AWS リージョン を含む 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
    }
]
}
```

でのリソース共有の削除 AWS RAM

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

AWS リソース共有に含めた リソースを削除する必要がある場合、AWS ではまず、そのリソースを含む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、削除後も短時間 AWS RAM コンソールに表示されますが、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 `リージョン` に存在するため AWS リージョン、コンソールの右上隅 `リージョン` があるドロップダウンリストから適切な `リージョン` 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. 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  
}
```

共有している AWS リソースにアクセスする

AWS Resource Access Manager (AWS RAM) を使用すると、自分が追加された先のリソース共有、アクセスできる共有リソース、リソースを自分と共有している AWS アカウントを表示できます。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。

内容

- [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

の組織のメンバー AWS アカウント である を介し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、招待を受け入れることなく共有リソースに自動的にアクセスできます。サービスプリンシパルは、招待を受け入れることなく、共有リソースに自動的にアクセスすることもできます。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せん。

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
- との共有時に組織内のアカウント AWS Organizations が有効になっていない

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「[共有先: 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 AWS リージョン にある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 AWS アカウントで利用可能なすべての招待のリストを取得します。AWS CLI query パラメータを使用すると、出力を に設定されている招待のみに制限できますstatusPENDING。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-
fbf6-4336-8377-06c559dfec49",
    "resourceShareName": "Test TrngAcct Resource Share",
    "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
    "senderAccountId": "111111111111",
    "receiverAccountId": "123456789012",
    "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
    "status": "PENDING"
  }
]
}
```

2. 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-fbf6-4336-8377-06c559dfec49
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfec49",
    "resourceShareName": "Test TrngAcct Resource Share",
    "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
    "senderAccountId": "111111111111",
    "receiverAccountId": "123456789012",
    "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
    "status": "ACCEPTED"
  }
}
```

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、招待を拒否したければ、同じパラメータを付けて [reject-resource-share-invitation](#) コマ
ンドを使用します。

```
$ 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 に存在するため AWS リージョン、コンソールの右上隅 AWS リージョン にある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. (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、次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、他の によって呼び出し元アカウント AWS リージョン と指定された で共有されているリソース共有のリストを示しています AWS アカウント。

```
$ 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 アカウン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. <https://console.aws.amazon.com/ram/home> で 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 に存在するため AWS リージョン、コンソールの右上隅 AWS リージョン にある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. 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](#) コマンドを使用して、 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 AWS アカウント。

次のコマンド例では、リソース共有を共有 AWS アカウント した の詳細を、指定された でオペレーションを呼び出すために使用したアカウントとともに表示します AWS リージョン。

```
$ 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。組織 AWS アカウント 内の によってリソース共有に追加され、との共有 AWS Organizations が有効になっている場合、リソース共有を残すことはできません。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 に存在するため AWS リージョン、コンソールの右上隅 AWS リージョン にある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. 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。

次のコマンド例では、コマンドを呼び出す AWS アカウントが、ARN で指定されたリソース共有によって共有されるリソースにアクセスできなくなります。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": [  
      {
```

```

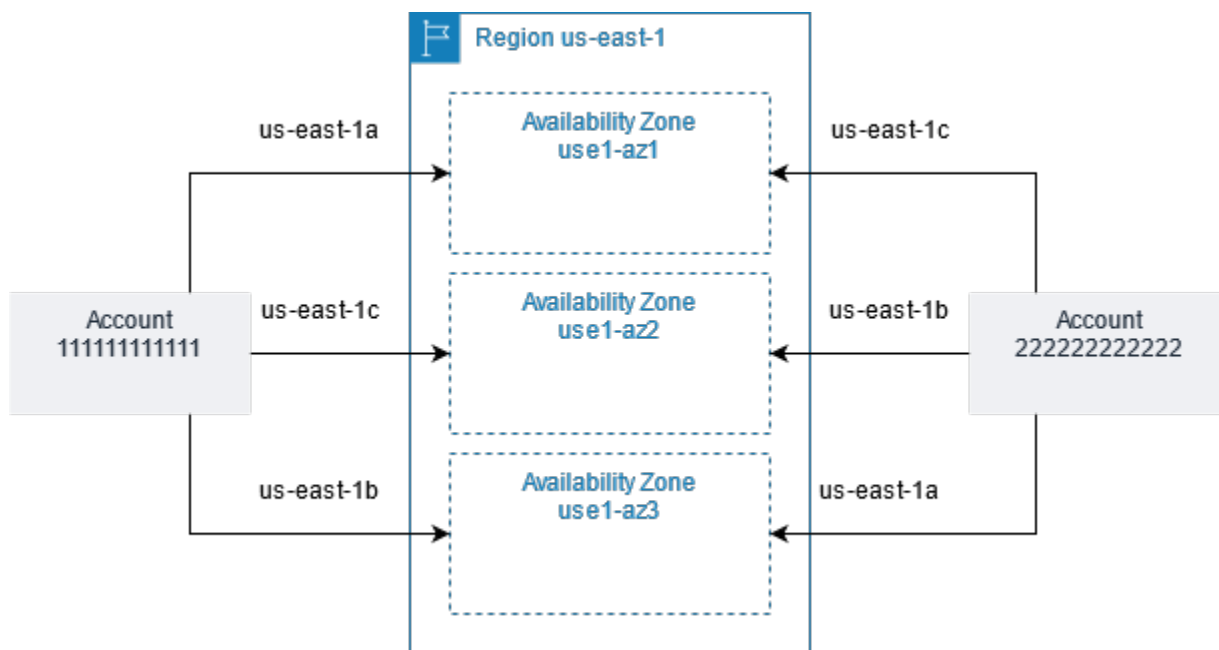
    "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
    "associatedEntity": "123456789012",
    "associationType": "PRINCIPAL",
    "status": "DISASSOCIATING",
    "external": false
  }
]
}

```

AWS リソースの Availability Zone ID

AWS は、物理 Availability Zone を AWS アカウントごとの Availability Zone 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 Availability Zone にリソースを分散するうえで役立ち、各リージョンの Availability Zone 「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 Availability Zone 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 Availability Zone」を参照してください。

次の図は、Availability Zone 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 [AWS リソース](#) 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。リソースは個人と共有できます 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、[AWS RAM](#) を使用して共有できるリソースタイプをグループ化して一覧表示 AWS のサービスします 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 - アカウントに加えて、このタイプのリソースを個々の AWS Identity and Access Management (IAM) ロールや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、「考慮事項」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 マネージドアクセス許可 AWS RAM をサポートしますが、この列の「はい」は、カスタマーマネージドアクセス許可がこのリソースタイプでもサポートされてい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
リンシパル
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
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「 共有メッシュの使用 」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
AppSync GraphQL API appsync:Apis	AWS AppSync GraphQL APIs一元管理し、他の AWS アカウントまたは組織と共有します。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、複数のアカウントで APIs を共有できます。詳細については、「AWS AppSync デベロッパーガイド」の 「マージされた APIs」 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 API Gateway

AWS RAMを使用して、以下の Amazon API Gateway 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
API Gateway プライベートカスタムドメイン <code>apigateway:Domainnames</code>	ドメイン名を一元的に作成および管理し、他の AWS アカウントや組織と共有します。これにより、複数のアカウントがプライベート API にマッピングされたドメイン名を呼び出すことができます。詳細については、Amazon API Gateway デベロッパーガイドの「 API Gateway でのプライベート API 用のカスタムドメイン名 」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

Amazon Application Recovery Controller (ARC)





AWS RAMを使用して、以下の Amazon Application Recovery Controller (ARC) 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
Route 53 ARC クラスタ <code>route53-recovery-control:Cluster</code>	ARC クラスタを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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の総数を削減できます。詳細については、「Amazon Application Recovery Controller デベロッパーガイド」の「 アカウント全体でのクラスタの共有 」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
ARC リージョンの切り替えプラン <code>arc-region-switch:Plan</code>	プランを一元的に作成して管理し、他の AWS アカウントや所属組織と共有します。これにより、複数のアカウントで、プランをホストするアカウントとは異なるアカウント	 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
	のリソースを使用できません。詳細については、「Amazon Application Recovery Controller (ARC) デベロッパーガイド」の「 リージョンの切り替え 」を参照してください。				

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
Aurora DB クラスタ <code>rds:Cluster</code>	DB クラスタ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 クラスタのクローンを作成できます。詳細については、 「Amazon	 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
	Aurora ユーザーガイド の「 Cross-account cloning with AWS RAM and Amazon Aurora 」を参照してください。				

AWS Backup

を使用して、次の AWS Backup 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
バックアップポールド <code>backup:BackupVault</code>	論理エアギャップポールドを一元的に作成および管理し、他の AWS アカウントまたは組織と共有します。このオプションを使用すると、複数のアカウントがポールドからバックアップにアクセスして復元できます。詳細については、「 AWS Backup デベロッパーガイド 」の「 論理エアギャップポールドの概	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
-------------	--------	---------------------	----------------	--------------------	-----------------

[要](#)」を参照してください。

Amazon Bedrock

AWS RAMを使用して、以下の Amazon Bedrock 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
-------------	--------	---------------------	----------------	--------------------	-----------------

Bedrock カスタムモデル

bedrock:CustomModel

カスタムモデルを一元的に作成して管理し、他の AWS アカウントや所属組織と共有します。これにより、複数のアカウントで生成 AI アプリケーションの同じカスタムモデルを使用できます。詳細については、「Amazon Bedrock ユーザーガイド」の「[別のアカウントのモデルを共有する](#)」を参照してください。



はい



はいえ

自分の組織内の AWS アカウントとのみ共有可能。







はい



はいえ

請求情報とコスト管理

AWS RAMを使用して、次の請求情報とコスト管理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
BCM ダッシュボード bcm-dashboards:dashboard	請求情報とコスト管理ダッシュボードを作成および管理し、組織内外の他の AWS アカウントと共有します。ダッシュボードを共有しても、共有されるのはダッシュボード設定のみで、参照元のデータは共有されません。共有先は、ダッシュボードのレイアウトやウィジェット設定にアクセスでき、独自のアクセス許可に基づいてデータが表示されます。この共有機能により、組織は共通のコストレポートプラクティスを確立し、さまざまなチームがコストデータを一貫して確認できるようになります。詳細については、「請求情報とコスト管理ユーザーガイド」の「 ダッ	 いいえ	 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
-------------	--------	---------------------	----------------	--------------------	-----------------

[シユボードの共有](#)」を参照してください。





AWS Billing サービスの表示

を使用して、次の AWS Billing View 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
請求ビュー billing:billingview	カスタム請求ビューを一元的に作成および管理し、他の AWS アカウントや組織と共有します。これにより、アプリケーションとビジネスユニットの所有者は、メンバーアカウントからビジネスユニットレベルの AWS 支出にアクセスできます。詳細については「AWS Cost Management ユーザーガイド」の「 カスタム請求ビューの共有 」を参照してください。	 はい	 はい 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 Cloud Map

を使用して、次の AWS Cloud Map 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
AWS Cloud Map 名前空間 <code>servicediscovery:Namespace</code>	名前空間を一元的に作成して管理し、組織内の他の AWS アカウントと共有します。これにより、複数の AWS アカウントが一時的な認証情報を必要とせずに、共有名前空間内のサービスとインスタンスを検出できます。詳細については、「AWS Cloud Map デベロッパーガイド」の「 共有 AWS Cloud Map 名前空間 」を参照してください。	 はい	 はい 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 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
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「 コアネットワークの共有 」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 CloudFront

AWS RAMを使用して、以下の Amazon CloudFront 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 CloudFront VPC オリジン cloudfront:t:VpcOrigin	CloudFront VPC オリジンを一元的に作成および管理し、他の AWS アカウントまたは組織と共有します。これにより、複数の AWS アカウントが CloudFront ディストリビューションの共有 VPC オリジンを使用できます。詳細については、「Amazon CloudFront デベロッパーガイド」の「 CloudFront での共有リソースの使用 」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 CloudHSM

を使用して、次の AWS CloudHSM 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
AWS CloudHSM バックアップ cloudhsm:Backup	AWS CloudHSM バックアップを一元管理し、他の AWS アカウントや組織と共有します。これにより、複数の AWS アカウントおよびユーザーが Backup AWS CloudHSM に関する情報を表示し、それを使用してクラスタを復元できます。詳細については、「AWS CloudHSM ユーザーガイド」の「 AWS CloudHSM バックアップの管理 」を参照してください。	 はい	 はい	 はい	 はい 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
CodeBuild プロジェクト <code>codebuild:Project</code>	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 または組織と共有します。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「 共有プロジェクトの使用 」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
CodeBuild レポートグループ <code>codebuild:ReportGroup</code>	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 およびユーザーがレポートグループとそのレポート、および各レポー	 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
	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「 共有プロジェクトの使用 」を参照してください。				

AWS CodeConnections





AWS RAMを使用して、以下の CodeConnections 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
コード接続 codeconnections:Connection	複数のアカウントでのコード接続の再利用を管理します。つまり、コード接続を共有すると、コード接続を必要とするすべてのアカウントで管理者の負担と管理者アクセスの必要	 いえ	 はい	 はい	 いえ
			すべての AWS アカ		

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
	性が軽減されます。詳細については、「開発者用コンソールユーザーガイド」の「 AWS アカウントで接続を共有する 」を参照してください。		アカウントと共有可能		

Amazon DataZone

AWS RAMを使用して、以下の DataZone 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	
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、複数のアカウントが Amazon DataZone ドメインを作成できます。詳細については、「Amazon DataZone ユーザーズガイド」の「 Amazon DataZone と		 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
-------------	--------	---------------------	----------------	--------------------	-----------------

[は](#)」を参照してください。

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	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に AWS アカウント 起動できます。詳細については、「Amazon EC2 ユーザーガイド」の「 共有キャパシティ予約の使用 」を参照してください。	 いえ	はい (任意の AWS アカウントと共有できません)。 キャパシティロックにはいいえ (独自の組織でのみ AWS アカウントと共有できます)。	 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>ML のキャパシティブロック (UltraServer CBs はまだサポートされていません) を他の AWS アカウント または組織と共有します。この機能を使用すると AWS アカウント、異なるで実行されているワークロードが所有しているキャパシティブロックに Amazon EC2 インスタンスを起動できるため、リザーブドキャパシティをより有効に活用してコストを削減できます。詳細については、Amazon EC2 ユーザーガイドの「共有キャパシティブロックの使用」を参照してください。</p>				

⚠ 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





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>る可能性がります。操作が失敗し、ユーザーがキャパシティ予約で 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。Amazon EC2 コンソールで表示して、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</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>することもできます。詳細については、「例: リソース共有障害時のアラート」を参照してください。</p>				
専用ホスト ec2:DedicatedHost	<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 ユーザーガイドの「共有専用ホストの使用」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
プレースメントグループ ec2:PlacementGroup	所有しているプレースメントグループを AWS アカウント組織全体で、組織内外で共有します。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ースメントグループで起動できます。詳細については、「Amazon EC2 ユーザーガイド」の「 プレースメントグループの共有 」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





EC2 イメージビルダー

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
Image Builder 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「EC2 Image Builder リソースの共有」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		
Image Builder コンテナレシピ imagebuilder:ContainerRecipe	<p>コンテナレシピを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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「EC2 Image Builder リソースの共有」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	 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
Image Builder のイメージ imagebuilder:Image	ゴールデンイメージを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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「 EC2 Image Builder リソースの共有 」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
Image Builder のイメージレシピ imagebuilder:ImageRecipe	イメージレシピを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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「 EC2 Image Builder リソースの共有 」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

エラスティックロードバランシング









AWS RAMを使用して、以下の Elastic Load Balancing 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
ELB トラストストア	Elastic Load Balancing トラストストアを一元的に作成および管理し、他の AWS アカ	 はい	 はい	 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
elasticloadbalancing:TrustStore	アカウントまたは組織と共有します。セキュリティ管理者は、1つまたは少数のトラストストアを管理し、複数の Application Load Balancer にわたって相互 TLS の設定を有効にできます。Elastic Load Balancing における HTTP ステータスコードについては、「Application Load Balancer のユーザーガイド」の「 Application Load Balancer の Elastic Load Balancing トラストストアを共有する 」を参照してください。				

AWS End User Messaging SMS

を使用して、次の AWS End User Messaging SMS 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
AWS SMS 音声 オプトアウトリスト sms-voice: :OptOutList	オプトアウトリストを作成し、組織 AWS アカウント内の他のと共有します。オプトアウトリストを共有して、他のアプリケーションがユーザーの電話番号を異なる AWS アカウントからオプトアウトしたり、ユーザーの電話番号のステータスを確認したりできる用になります。詳細については、「AWS End User Messaging SMS ユーザーガイド」の 「共有リソースの使用」 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	 はい	 いいえ
AWS SMS 音声 電話番号 sms-voice: :PhoneNumber	電話番号を作成して管理し、他の AWS アカウントや所属組織と共有します。これにより、複数の AWS アカウントが共有電話番号を使用してメッセージを送信できます。詳細については、「AWS End User Messaging SMS ユーザーガイド」	 いいえ	 はい すべての AWS アカウントと共有可能	 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
	の「 共有リソースの使用 」を参照してください。				
AWS SMS 音声プール sms-voice:Pool	プールを作成して管理し、他の AWS アカウントや組織と共有しません。これにより、複数の共有プールを使用して AWS アカウントメッセージを送信できません。詳細については、「AWS End User Messaging SMS ユーザーガイド」の「 共有リソースの使用 」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	 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
AWS SMS 音声送信者 IDs <code>sms-voice:SenderId</code>	送信元 ID 作成して管理し、他の AWS アカウントや所属組織と共有します。これにより、複数の AWS アカウントが共有送信者 ID を使用してメッセージを送信できます。詳細については、「AWS End User Messaging SMS ユーザーガイド」の「 共有リソースの使用 」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

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 ボリューム <code>fsx:Volume</code>	FSx for OpenZFS ボリュームを一元的に作成および管理し、他の AWS アカウントまたは組織と共有しま	 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>す。これにより、複数のアカウントが、FSx API CreateVolume または CopySnapshots hotAndUpdateVolume を通じ、共有ボリューム内の 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。詳細については、「Amazon FSx for OpenZFS ユーザーガイド」の「オンデマンドデータレプリケーション」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>		

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
AWS Glue 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す。詳細については、AWS Lake Formation デベロッパーガイド「 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 」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 Glue 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「 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 」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
AWS Glue 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「 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 」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 license-manager:LicenseConfiguration	ライセンス設定を一元的に作成および管理し、他の AWS アカウントや組織と共有します。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「 License Manager でのライセンス設定 」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





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「 AWS RAMでのリソース共有 」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 または組織のす	 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 および 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「 AWS RAMを使用したリファクタリングスペース環境の共有 」を参照してください。		アカウントと共有可能		

マルチパーティー承認





AWS RAMを使用して、以下のマルチパーティー承認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
マルチパーティー承認チーム	承認チームを作成して管理し、他の AWS アカウント や所属組織と共有します。これによ	 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
mpa:ApprovalTeam	り、他の AWS アカウントは保護されたオペレーションに関連付けられた承認チームを使用できます。保護されたオペレーションは、実行する前にチームの承認を必要とするオペレーションの事前定義されたリストです。詳細については、「マルチパーティー承認ユーザーガイド」の [用語と概念] を参照してください。		すべての AWS 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
Network Firewall	ファイアウォールを一元的に作成および管理し、他の AWS アカウントと共有し	 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
network-firewall:Firewall	<p>てファイアウォールエンドポイントを作成できるようにします。これにより、複数のアカウントを1つのファイアウォールで保護できます。詳細については、「AWS Network Firewall デベロッパーガイド」のAWS Network Firewall 「リソースの共有」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
Network Firewall ポリシー <code>network-firewall:FirewallPolicy</code>	ファイアウォールポリシーを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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 AWS Network Firewall 「リソースの共有」 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

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>Network Firewall ルールグループ</p> <p>network-fwirewall:StatefulRuleGroup</p> <p>network-fwirewall:StatelessRuleGroup</p>	<p>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および管理し、他の AWS アカウントまたは組織と共有します。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 AWS Network Firewall 「リソースの共有」 を参照してください。</p>	<p></p> <p>はい</p>	<p></p> <p>はい</p> <p>すべての AWS アカウントと共有可能</p>	<p></p> <p>はい</p>	<p></p> <p>はい</p>

Oracle Database@AWS





を使用して、次の Oracle Database@AWS 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
<p>Oracle Database@AWS Exadata インフラストラクチャ</p> <p>odbc:Cloud ExadataInfrastructure</p>	<p>を使用すると Oracle Database@AWS、Exadata インフラストラクチャと ODB ネットワークを同じ AWS 組織内 AWS アカウント内の複数の間で共有できます。これにより、インフラストラクチャを一度プロビジョニングすれば信頼できるアカウント間で再利用できるため、責任を分離しながらコストを削減できます。詳細については、「Oracle Database@AWS ユーザーガイド」の「でのリソース共有 Oracle Database@AWS」を参照してください。</p>	<p> いえ</p>	<p> いえ</p> <p>自分の組織内の AWS アカウントとのみ共有可能。</p>	<p> いえ</p>	<p> いえ</p>
<p>Oracle Database@AWS ODB ネットワーク</p> <p>odbc:OdbNetwork</p>	<p>を使用すると Oracle Database@AWS、Exadata インフラストラクチャと ODB ネットワークを同じ AWS 組織内 AWS アカウント内の複数の間で共有できます。これによ</p>	<p> いえ</p>	<p> いえ</p> <p>自分の組織内の AWS アカウント</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
	り、インフラストラクチャを一度プロビジョニングすれば信頼できるアカウント間で再利用できるため、責任を分離しながらコストを削減できます。詳細については、「 Oracle Database@AWS ユーザーガイド 」の「 でのリソース共有 Oracle Database@AWS 」を参照してください。		とのみ共有可能。		

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、	 いえ	 いえ	 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>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「共有 AWS Outposts リソースの使用」を参照してください。</p>		<p>自分の組織内の AWS アカウントとのみ共有可能。</p>		
<p>ローカルゲートウェイルートテーブル</p> <p>ec2:LocalGatewayRouteTable</p>	<p>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。詳細については、AWS Outposts ユーザーガイドの「共有可能な Outpost リソース」を参照してください。</p>	<p> いえ</p>	<p> いえ</p> <p>自分の組織内の AWS アカウントとのみ共有可能。</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
Outposts 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、「AWS Outposts ユーザーガイド」の「 共有 AWS Outposts リソースの使用 」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、「AWS Outposts ユーザーガイド」の「 共有 AWS Outposts リソースの使用 」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 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) acm-pca:CertificateAuthority	組織の内部パブリックキーインフラストラクチャ (PKI) のプライベート認証機関 (CAs) を作成および管理し、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「 プライベート CA へのアクセスの設定 」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





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
Resource Explorer ビュー resource-explorer-2:View	Resource Explorer ビューを一元的に作成して設定し、組織内 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「 Resource Explorer ビューの共有 」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、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「 AWS License Managerのホストリソースグループ 」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

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 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「 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 」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 いえ
Route 53 Profiles <code>route53profiles:Profile</code>	Route 53 を一Profile 元的に作成および管理し、他の AWS アカウントや組織と共有します。これにより、複数のアカウントが Route 53 Profiles で指定された DNS 設定を複数	 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
	<p>の VPC に適用できません。詳細については、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 Profiles」を参照してください。</p>				
<p>リゾルバールール</p> <p>route53resolver:ResolverRule</p>	<p>Resolver ルールを一元的に作成および管理し、他の AWS アカウントまたは組織と共有します。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 デベロッパーガイド」の「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」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
Resolver のクエリログ設定 <code>route53resolver:ResolverQueryLogConfig</code>	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「 Resolver クエリログ記録設定を他の AWS アカウントと共有する 」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
S3 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、Amazon Simple Storage Service ユーザーガイドの S3 Access Grants Cross-account 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	 はい





Amazon SageMaker AI





AWS RAMを使用して、以下の Amazon SageMaker AI 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
SageMaker AI リソースカタログ sagemaker:SagemakerCatalog	<p>検出性の向上 – アカウント所有者は、SageMaker AI 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性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 AI デベロッパーガイド」の「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」を参照してください。</p> <div style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p>Note</p> <p>SageMaker AI では、検出性とアクセスは別々のアクセス許可です。</p> </div>	 <small>いえ</small>	 <small>はい</small> すべての AWS アカウントと共有可能	 <small>はい</small>	 <small>いえ</small>

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 AI 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 AI デベロッパーガイド」の「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」を参照してください。</p> <div data-bbox="402 1304 743 1669" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>SageMaker AI では、検出性とアクセスは別々のアクセス許可です。</p> </div>	<p style="text-align: center;"></p> <p style="text-align: center;">はい</p>	<p style="text-align: center;"></p> <p style="text-align: center;">はい</p> <p style="text-align: center;">すべての AWS アカウントと共有可能</p>	<p style="text-align: center;"></p> <p style="text-align: center;">はい</p>	<p style="text-align: center;"></p> <p style="text-align: center;">いいえ</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
SageMaker AI ハブ sagemaker:Hub	Amazon SageMaker AI JumpStart を使用すると、sagemaker:Hub を一元的に作成および管理し、同じ組織内の他の AWS アカウントと共有できます。詳細については、「 Amazon SageMaker AI デベロッパーガイド 」の「Amazon SageMaker AI JumpStart で厳選されたプライベートハブを使用して基盤モデルアクセスを制御する」	 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
SageMaker AI 系統グループ sagemaker:LineageGroup	Amazon SageMaker AI では、パイプラインメタデータの系統グループを作成して、その履歴と関係をより深く理解することができます。系統グループを他の 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 および ユーザーが系統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 AI デベロッパーガイド」の「 クロスアカウントの系統追跡 」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

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 AI モデルカード sagemaker:ModelCard	Amazon SageMaker AI 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合理化します。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、「Amazon SageMaker AI デベロッパーガイド」の「 Amazon SageMaker AI モデルカード 」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

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>SageMaker AI モデルパッケージグループ</p> <p>sagemaker:model-package-group</p>	<p>Amazon SageMaker AI Model Registry を使用すると、<code>-sagemaker:model-package-group</code> 元的に作成および管理し、他のと共有してモデルバージョン AWS アカウントを登録できます。詳細については、「Amazon SageMaker デベロッパーガイド」の「Amazon SageMaker モデルレジストリ」を参照してください。</p>	<p></p> <p>はい</p>	<p></p> <p>はい</p>	<p></p> <p>はい</p>	<p></p> <p>いいえ</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
<p>SageMaker AI パートナーアプリケーション</p> <p>sagemaker:PartnerApp</p>	<p>SageMaker AI パートナー AI アプリケーションを使用すると、SageMaker AI パートナー AI アプリケーションを一元的に作成および管理し、他の AWS アカウントとアクセスを共有できます。詳細については、「Amazon SageMaker AI デベロッパーガイド」の「Amazon SageMaker AI パートナー AI アプリケーションのクロスアカウント共有の設定」を参照してください。Amazon SageMaker</p>	<p></p> <p>はい</p>	<p></p> <p>はい</p> <p>すべての AWS アカウントと共有可能</p>	<p></p> <p>いいえ</p>	<p></p> <p>いいえ</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
SageMaker AI パイプライン sagemaker:Pipeline	<p>Amazon SageMaker AI モデル構築パイプラインを使用すると、エンドツーエンドの大規模な機械学習ワークフローを作成、自動化、管理を行えます。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達成します。これにより、複数の AWS アカウントおよびユーザーが、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を使用して、パイプラインとその実行に関する情報を表示できます。詳細については、「Amazon SageMaker AI デベロッパーガイド」の「SageMaker パイプラインのクロスアカウントサポート」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	 いいえ

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
AppRegistry アプリケーション <code>servicecatalog:Applications</code>	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、アプリケーションと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 ユーザーズガイド」の「 アプリケーションの作成 」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 いえ
AppRegistry 属性グループ <code>servicecatalog:AttributeGroups</code>	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	 いえ	 いえ	 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
tributeGroups	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、「Service Catalog ユーザーズガイド」の「 属性グループの作成 」を参照してください。		自分の組織内の AWS アカウントとのみ共有可能。		

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
Incident Manager Contacts ssm-contacts:Contact	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 アカウントまたは組織と共有します。これにより、多くの ガインシ	 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
	<p>インシデント中に発生したインシデント対応計画 AWS アカウント を表示できます。</p> <div data-bbox="399 621 743 1129" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>現在、別のアカウントから共有された連絡先をインシデント対応計画に追加する機能はサポートされていません。</p> </div> <p>詳細については、AWS Systems Manager Incident Manager ユーザーガイドの「共有連絡先と対応計画の使用」を参照してください。</p>		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
Incident Manager レスポンスプラン <code>ssm-incidents:ResponsePlan</code>	対応計画を一元的に作成および管理し、他の AWS アカウントや組織と共有します。これにより、AWS アカウントは Amazon CloudWatch のアラームと Amazon EventBridge のイベントルールを対応計画に結び付け、インシデントの検出時に自動的にインシデントが作成されます。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「 共有連絡先と対応計画の使用 」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

AWS Systems Manager





を使用して、次の AWS Systems Manager リソースを共有できません 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
SSM JITNA 自動拒否ポリシー ssm:Document	Systems Managerを使用してジャストインタイムノードアクセスの承認ポリシーを作成します。アクセス拒否ポリシーを使用すると、指定したノードへのアクセスリクエストの自動承認を明示的に防ぐことができます。アクセス拒否ポリシーを他の AWS アカウントまたは組織と共有します。これにより、ジャストインタイムノードアクセスのアクセス拒否ポリシーが組織内のすべてのアカウントに適用されます。詳細については、「 AWS Systems Manager ユーザーガイド 」の「 Systems Manager を使用したジャストインタイムノードアクセス 」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





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
パラメータストアの詳細パラメータ <code>ssm:Parameter</code>	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、自動化ワークフローで参照できる設定データを保存します。パラメータを他の AWS アカウントまたは組織と共有します。これにより、複数の AWS アカウント および ユーザーが文字列に関する情報を確認し、データをコードから分離してセキュリティを強化できます。詳細については、「 AWS Systems Manager ユーザーガイド 」の「共有パラメータの使用」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 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 IPv4pool ec2:CoipPool	<p>AWS Outposts インストールプロセス中に、は、お客様がオンプレミスネットワークに関して提供した情報に基づいて、お客様所有の 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、AWS Outposts ユーザーガイドの「カ</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





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>IPAM プール 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、プールから各アカウントの VPCs などの AWS リソースに CIDRs を割り当てることができます。詳細については、「Amazon VPC IP Address Manager ユーザーズガイド」の「AWS RAMを使用して IPAM プールを共有する」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
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「 リソース検出を使用する 」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





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および管理し、他の AWS アカウントや組織と共有します。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「 共有プレフィックスリストの操作 」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





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 インスタンス、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「共有 VPC の使用」を参照してください。</p> <div data-bbox="402 1495 743 1869" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p>Note</p> <p>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</p> </div>	 <small>し</small> いえ	 <small>し</small> いえ 自分の組織内の AWS アカウントとのみ共有可能。	 <small>し</small> いえ	 <small>し</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
	<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
セキュリティグループ ec2:SecurityGroup	セキュリティグループを一元的に作成および管理し、他の AWS アカウントや組織と共有します。これにより、複数の AWS アカウントがセキュリティグループを Elastic ネットワークインターフェイスに関連付けることができます。詳細については、「Amazon VPC ユーザーガイド」の「 セキュリティグループの共有 」を参照してください。	 はい	 いいえ 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
Traffic Mirror ターゲット ec2:TrafficMirrorTarget	<p>トラフィックミラーターゲットを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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「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」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
Transit Gateway ec2:TransitGateway	<p>トランジットゲートウェイを一元的に作成および管理し、他の AWS アカウントや組織と共有します。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「Transit Gateway の共有」を参照してください。</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>Note</p> <p>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:DescribeTransi</p> </div>	 <small>し</small> いいえ	 <small>は</small> い すべての AWS アカウントと共有可能	 <small>し</small> いいえ	 <small>い</small> 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>tGateway 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 アカウントまたは組織と共有します。これにより、複数のグループメンバーまたはグループソースをマルチキャストドメインに登録 AWS アカウント および登録解除できます。詳細については、Transit Gateways ガイドの「共有マルチキャストドメインの使用」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:VerifiedAccess Group	AWS Verified Access 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、単一の共有エンドポイントセットを使用できます AWS Verified Access。詳細については、「AWS Verified Access ユーザーガイド」の「 を使用して AWS Verified Access グループを共有する AWS Resource Access Manager 」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

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 リソース設定 vpc-lattice:ResourceConfiguration	Amazon VPC Lattice でリソース設定を作成して、アカウントと VPC 間で VPC リソースを共有します。リソース設定では、そのリソースにアクセスできるユーザーを特定し、リソースの共有に使用するリソースゲートウェイを指定します。コンシューマーは、AWS PrivateLink で作成したリソース VPC エンドポイントを介して VPC リソースにアクセスできます。詳細については、「AWS PrivateLink ユーザーガイド」の「 AWS PrivateLink 経由で VPC リソースにアクセスする 」および「VPC Lattice ユーザーガイド」の「 VPC リソースのリソース設定 」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
Amazon VPC Lattice サービス vpc-lattice:Service	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サービス間の通信への接続、セキュリティの維持、監視を行うことができます。詳細については、「VPC Lattice ユーザーズガイド」の「 共有リソースの使用 」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
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サービス間の通信への接続、セキュリティの維持、監視を行うことができます。詳細については、「Amazon VPC Lattice ユーザーズガイド」の「 共有リソースの使用 」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

でのアクセス許可の管理AWS RAM

にはAWS RAM、[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](#)があります。AWS

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 は、リソースベースのポリシーの要素を完了します。AWS RAMその後、はその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。場合によっては、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、リソースタイプのAWSマネージドアクセス許可AWSを更新します。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

できるだけ早く新しいバージョンのAWSマネージドアクセス許可に更新することをお勧めします。これらの更新により、通常、を使用して追加のリソースタイプを共有AWSのサービスできる新規または更新されたのサポートが追加されますAWS RAM。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、「[マネージドアクセス許可の表示](#)」を参照してください。

トピック

- [マネージドアクセス許可の表示](#)
- [でのカスタマー管理アクセス許可の作成と使用 AWS RAM](#)
- [AWS マネージドアクセス許可を新しいバージョンに更新する](#)
- [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 AWS RAM](#)
- [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](#)

マネージド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せん。

- 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"
  }
}
```

でのカスタマー管理アクセス許可の作成と使用 AWS RAM

AWS Resource Access Manager (AWS RAM) は、共有できるリソースタイプごとに少なくとも 1 つの 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。提供された 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

カスタマー管理のアクセス許可は、に固有です AWS リージョン。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

- 次のいずれかを行います。
 - [\[マネージド許可ライブラリ\]](#) 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 マネージドアクセス許可を新しいバージョンに更新する

場合によっては、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 AWS を更新します。AWS がこれを行うと、AWS マネージド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、[\[リソース共有を更新\]](#) 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 マネージド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。

たとえば、次のサンプルコマンドは、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。

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 AWS RAM

カスタマー管理アクセス許可は、AWS リージョン 作成した のみ使用できます。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。でサポートされているリソースタイプのリストについては AWS Resource Access Manager、「」を参照してください [共有可能な AWS リソース](#)。

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。

- プリンシパルのプロパティの一致に使用される条件キー:
 - `aws:PrincipalOrgId`
 - `aws:PrincipalOrgPaths`
 - `aws:PrincipalAccount`
- サービスプリンシパルのアクセスを制限するために使用される条件キー:
 - `aws:SourceArn`
 - `aws:SourceAccount`
 - `aws:SourceOrgPaths`
 - `aws:SourceOrgID`
- システムタグ:
 - `aws:PrincipalTag/aws:`
 - `aws:ResourceTag/aws:`
 - `aws:RequestTag/aws:`

Note

この`aws:SourceAccount` 値は、サービスプリンシパルと共有するときに自動的に入力されます。

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ときは、共有する各リソースタイプにAWSマネージド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、は マネージドアクセス許可AWS RAMを使用して、各共有リソースにアタッチされたリソースベースのポリシーを生成します。

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。

Action

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。これは、のアクションAWS マネジメントコンソールでも、AWS Command Line Interface(AWS CLI) またはAWS API の オペレーションでもかまいません。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。

Condition

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、「サービス認可リファレンス」の[AWS「サービスのアクション、リソース、および条件キー](#)」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、「[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 AWS RAM](#)」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ときは、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、リソース所有サービスによって定義され、AWSによって管理されますAWS RAM。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 – がサポートするAWS RAMリソースタイプごとに 1 つのデフォルトの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管理アクセス許可の名前は、`<リソースタイプ>:AWSRAMDefaultPermission<ShareableResourceType>` の形式を使用しますAWSRAMDefaultPermission*ShareableResourceType*。たとえば、`ec2:Subnet`リソースタイプの場合、デフォルトのAWS管理アクセス許可の名前は `ec2:Subnet: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

と連携するすべてのAWSサービスは、少なくとも 1 つのデフォルトの管理アクセス許可 AWS RAM 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、「[マネージドアクセス許可の表示](#)」を参照してください。

追加のマネージドアクセス許可をサポートしていないサービスの場合、リソース共有を作成すると、は選択したリソースタイプに定義されたデフォルトのアクセス許可AWS RAM 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。

のセキュリティ AWS Resource Access Manager

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、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を活用できます。

セキュリティは、お客様と AWS お客様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、で AWS 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があります AWS クラウド。AWS また、では、安全に使用できるサービスも提供しています。[「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。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、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、を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS RAM。以下のトピックでは、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 AWS RAM ようにを設定する方法を示します。また、AWS RAM リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- [でのデータ保護 AWS Resource Access Manager](#)
- [の ID とアクセスの管理 AWS Resource Access Manager](#)
- [AWS RAM でのログ記録とモニタリング](#)
- [のコンプライアンス検証 AWS Resource Access Manager](#)
- [の耐障害性 AWS Resource Access Manager](#)
- [のインフラストラクチャセキュリティ AWS Resource Access Manager](#)
- [インターフェイスエンドポイント \(AWS PrivateLink\) AWS Resource Access Manager を使用したへのアクセス](#)

でのデータ保護 AWS Resource Access Manager

責任 AWS [共有モデル](#)、でのデータ保護に適用されます AWS Resource Access Manager。このモデルで説明されているように、AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスクもユーザーの責任となります。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に関するよくある質問](#)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。

データ保護の目的で、認証情報を保護し AWS アカウント、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設定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権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします：

- 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 は必須ですが、TLS 1.3 を推奨します。
- を使用して API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の[CloudTrail 証跡の使用](#)を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理された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 AWS を介して にアクセスするときに FIPS 140-3 検証済み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 \(FIPS\) 140-3](#)」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を、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含めないことを強くお勧めします。これは、コンソール AWS RAM、API、または SDK を使用して AWS CLI または他の AWS のサービス を操作する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、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。

の ID とアクセスの管理 AWS Resource Access Manager

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制御するのに役立つ AWS サービスです。IAM 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 (アクセス許可を付与する) かを制御します。IAM を使用して、のロール、ユーザー、グループなどのプリンシパルを作成します AWS アカウント。これらのプリンシパルが AWS リソースを使用してタスクを実行するためのアクセス許可を制御します。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

- [が IAM と AWS RAM 連携する方法](#)
- [AWS の 管理ポリシー AWS Resource Access Manager](#)
- [のサービスにリンクされたロールの使用 AWS RAM](#)
- [の IAM ポリシーの例 AWS RAM](#)
- [AWS Organizations および のサービスコントロールポリシーの例 AWS RAM](#)
- [とのリソース共有の無効化 AWS Organizations](#)

が IAM と AWS RAM 連携する方法

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。

- 以下のユーザーとグループ AWS IAM Identity Center:

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「[アクセス許可セットを作成する](#)」の手順に従ってください。

- IAM 内で、ID プロバイダーによって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します。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 \(フェデレーション\) 用のロールを作成する](#) を参照してください。

- IAM ユーザー:
 - ユーザーが担当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 ユーザーのロールの作成](#) を参照してください。
 - (お奨めできない方法) 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 には、多くのユーザーのニーズに対応するために使用できる AWS 管理ポリシーがいくつか用意されています。これらの詳細については、「[AWS の管理ポリシー AWS Resource Access Manager](#)」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。

以下のセクションでは、IAM アクセス許可ポリシーを構築するための AWS RAM 具体的な詳細について説明します。

目次

- [ポリシーの構造](#)
 - [効果](#)
 - [Action](#)
 - [\[リソース\]](#)
 - [Condition](#)

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>"
        }
    }
}]
}
```

効果

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。

Action

Action ステートメントは、ポリシーがアクセス許可を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]

Resource ステートメントは、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。

Condition

条件ステートメントはオプションです。ポリシーが適用される条件をさらに絞り込むために使用できます。は次の条件キー AWS RAM をサポートしています。

- `aws:RequestTag/${TagKey}` - 指定されたタグキーを含むタグがサービスリクエストに存在し、指定された値があるかどうかをテストします。
- `aws:ResourceTag/${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。外部プリンシパルは、の組織 AWS アカウント 外の です AWS Organizations。ここで `False` と評価された場合、このリソース共有は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 管理ポリシー AWS Resource Access Manager

AWS Resource Access Manager は現在、このトピックで説明されているいくつかの AWS RAM 管理ポリシーを提供しています。

AWS 管理ポリシー

- [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 RAM AWS 管理ポリシーの更新](#)

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 管理ポリシーは、によって作成および管理されるスタンドアロンポリシーです AWS。AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、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注意してください。ユースケースに固有の[カスタマー管理ポリシー](#)を定義して、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されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、AWS マネージドポリシーを更新する可能性が高くなります。

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

AWS マネージドポリシー: AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess ポリシーを IAM アイデンティティ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。

アクセス許可の詳細

このポリシーには、以下のアクセス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。

JSON

```
{
  "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 ポリシーを IAM アイデンティティ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。

アクセス許可の詳細

このポリシーには、以下のアクセス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。

JSON

```
{
```



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

AWS マネージドポリシー:

AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess ポリシーを IAM アイデンティティにアタッチできます。

このポリシーにより、プリンシパルは、このポリシーと共有されているリソース共有を承諾または拒否したり AWS アカウント、これらのリソース共有の詳細を表示したりできます。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。

アクセス許可の詳細

このポリシーには、以下のアクセス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。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",

```

```
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

AWS マネージドポリシー: AWSResourceAccessManagerServiceRolePolicy

AWS 管理ポリシーAWSResourceAccessManagerServiceRolePolicyは、サービスにリンクされたロールでのみ使用できます AWS RAM。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 AWS RAM、組織の構造への読み取り専用アクセスを に付与します。AWS RAM との統合を有効にすると AWS Organizations、は [AWSServiceRoleForResourceAccessManager](#) という名前のサービスにリンクされたロール AWS RAM を自動的に作成します。このロールは、AWS RAM コンソールで組織の構造を表示する場合など、組織とそのアカウントに関する情報を検索する必要があるときにサービスが引き受けます。

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。

アクセス許可の詳細

このポリシーには以下のアクセス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。

JSON

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

```

    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "organizations:DescribeAccount",
          "organizations:DescribeOrganization",
          "organizations:DescribeOrganizationalUnit",
          "organizations:ListAccounts",
          "organizations:ListAccountsForParent",
          "organizations:ListChildren",
          "organizations:ListOrganizationalUnitsForParent",
          "organizations:ListParents",
          "organizations:ListRoots"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
        "Effect": "Allow",
        "Action": [
          "iam:DeleteRole"
        ],
        "Resource": [
          "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
        ]
      }
    ]
  }
}

```

AWS RAM AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS RAM してからの の AWS 管理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アラートについては、AWS RAM ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWS Resource Access Manager が変更の追跡を開始しました	AWS RAM は既存の管理ポリシーを文書化し、変更の追跡を開始しました。	2021 年 9 月 16 日

のサービスにリンクされたロールの使用 AWS RAM

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 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、[IAM ロール](#)によって事前定義 AWS されており、ユーザーに代わって他の AWS サービスを呼び出す AWS RAM ために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、[IAM ロール](#)の設定 AWS RAM が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS RAM を定義します。特に定義されている場合を除き、[IAM ロール](#)のみがサービスにリンクされたロールを引き受け AWS RAM 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。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい]リンクを選択してください。

のサービスにリンクされたロールのアクセス許可 AWS RAM

AWS RAM は、[AWS RAM の共有](#)を有効にする `AWSServiceRoleForResourceAccessManager` ときに、`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 AWS Organizations。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。

- `iam.amazonaws.com`

`AWSServiceRoleForResourceAccessManagerServiceRolePolicy` という名前のロールアクセス許可ポリシーは、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に対して次のアクションを実行できます。

- 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 [AWSServiceRoleForResourceAccessManagerServiceRolePolicy](#) を参照してください。

プリンシパルが組織内での AWS RAM 共有を有効にするには、そのプリンシパル (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「[サービスリンクロールの許可](#)」を参照してください。

のサービスにリンクされたロールの作成 AWS RAM

サービスリンクロールを手動で作成する必要はありません。で組織内での共有を有効にする AWS RAM か AWS マネジメントコンソール、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、によってサービスにリンクされたロール AWS RAM が作成されます。

`enable-sharing-with-aws-organizations` を呼び出、サービスにリンクされたロールをアカウントに作成します。

このサービスにリンクされたロールを削除すると、には組織の構造の詳細を表示するアクセス許可 AWS RAM がなくなります。

のサービスにリンクされたロールの編集 AWS RAM

AWS RAM では、`AWSResourceAccessManagerServiceRolePolicy` 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。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照す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 を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの編集](#)」を参照してください。

のサービスにリンクされたロールの削除 AWS RAM

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。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、AWS CLI、または AWS API を使用し

て、`AWSResourceAccessManagerServiceRolePolicy` サービスにリンクされた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「サービスリンクロールの削除」を参照してください。

AWS RAM サービスにリンクされたロールでサポートされているリージョン

AWS RAM は、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ます。リージョンの詳細については、[AWS](#)の「Amazon Web Services 全般のリファレンスリージョンとエンドポイント」を参照してください。

の IAM ポリシーの例 AWS RAM

このトピックでは、特定のリソースとリソースタイプの共有と共有の制限 AWS RAM を示すの IAM ポリシーの例を示します。

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: 外部との共有を制限する AWS アカウント](#)

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 リソースネーム (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。

JSON

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

```
    "StringEqualsIfExists": {
      "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
    }
  }
}]
}
```

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。

アクション `AssociateResourceShare` および `CreateResourceShare` は、プリンシパルおよび `resourceArns` を独立した入力パラメータとして受け入れることができます。したがって、は各プリンシパルとリソースを個別に AWS RAM 承認するため、複数の [リクエストコンテキスト](#) が存在する可能性があります。つまり、プリンシパルが AWS RAM リソース共有に関連付けられている場合、`ram:RequestedResourceType` 条件キーはリクエストコンテキストに存在しません。同様に、リソースが AWS RAM リソース共有に関連付けられている場合、`ram:Principal` 条件キーはリクエストコンテキストに存在しません。したがって、プリンシパルを AWS RAM リソース共有に関連付ける `CreateResourceShare` と `AssociateResourceShare` を許可するには、[Null 条件演算子](#) を使用できます。

たとえば、次のポリシーでは、プリンシパルを Amazon Route 53 Resolver ルールのみ共有できるように制限し、プリンシパルをその共有に関連付けることができます。

JSON

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

```
    },
    {
      "Sid": "AllowAssociatingPrincipals",
      "Effect": "Allow",
      "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ram:Principal": "false"
        }
      }
    }
  ]
}
```

例 3: 外部との共有を制限する AWS アカウント

IAM ポリシーを使用して、プリンシパル AWS アカウントが AWS 組織外の リソースを共有できないようにすることができます。

たとえば、次の IAM ポリシーは、プリンシパルがリソース共有 AWS アカウントに外部を追加できないようにします。

JSON

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


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

AWS RAM は、サービスコントロールポリシー (SCP) をサポートしています。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、AWS アカウント [SCP をアタッチする要素の下にあるすべての](#) 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。これらは、組織のアクセスコントロールガイドラインを確実に AWS アカウント 順守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](#)
- [例 6: RetainSharingOnAccountLeaveOrganization を有効にしてリソース共有を防止する](#)

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。

AWS RAM はAPIs を個別に承認します。

JSON

```
{
  "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られないようにする

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。

JSON

```
{
  "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。

AWS RAM はAPIs を個別に承認します。

演算子 `StringEqualsIfExists` は、リクエストにリソースタイプパラメータが含まれていない場合、またはそのパラメータが含まれている場合はその値が指定したリソースタイプと完全に一致する場合に、リクエストを許可します。プリンシパルを含める場合は、`...IfExists` が必要です。

`...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。

JSON

```

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

```

```

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

```

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 AWS アカウント 内の個人、または IAM ロールまたはユーザーと共有できます。

AWS RAM は APIs を個別に承認します。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ram:Principal": [
            "arn:aws:organizations::*:organization/*",
            "arn:aws:organizations::*:ou/*"
          ]
        }
      }
    }
  ]
}

```

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。

StringNotEqualsIfExists のような否定条件演算子を持つ "Effect": "Deny" 要素を使用している場合は、条件キーがなくてもリクエストが拒否されます。Null 条件演算子を使用して、認可時に条件キーが存在していないかどうかを確認します。

AWS RAM は APIs を個別に承認します。

JSON

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

例 6: RetainSharingOnAccountLeaveOrganization を有効にしてリソース共有を防止する

次の SCP は、`ram:RetainSharingOnAccountLeaveOrganization` 条件キーが に設定されている場合に、ユーザーがリソース共有を作成または変更できないようにします `true`。

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

とのリソース共有の無効化 AWS Organizations

以前にとの共有を有効に AWS Organizations していて、組織全体または組織単位 (OUs) とリソースを共有する必要がなくなった場合は、共有を無効にすることができます。との共有を無効にすると AWS Organizations、作成したリソース共有からすべての組織または OUs が削除され、共有リソースにアクセスできなくなります。外部アカウント (招待によってリソース共有に追加されたアカウント) は影響を受けず、引き続きリソース共有に関連付けられます。

との共有を無効にするには AWS Organizations

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

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

⚠ Important

への信頼されたアクセスを無効にすると AWS Organizations、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にアクセスできなくなります。

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 サービスにリンクされた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 EventBridge

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。EventBridge 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、「[EventBridge AWS RAM を使用したモニタリング](#)」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、「[を使用した AWS RAM API コールのログ記録 AWS CloudTrail](#)」を参照してください。

EventBridge AWS RAM を使用したモニタリング

Amazon EventBridge 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。からのイベント AWS RAM は、ほぼリアルタイムで EventBridge 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 EventBridge 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。イベントを出力 AWS RAM しようとしたとき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 EventBridge 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。

リソース共有の失敗をモニタリングするには、AWS RAM リソース共有が失敗したときに警告する Amazon EventBridge 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 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. [次へ] を選択します。
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。

そのルールが有効になっている限り、失敗した AWS RAM リソース共有は、公開したトピックの受信者に SNS アラートを生成します。

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。

を使用した AWS RAM API コールのログ記録 AWS CloudTrail

AWS RAM は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスであると統合されています AWS RAM。CloudTrail は、AWS

RAM のすべての 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 コンソールからの呼び出しと 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。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、リクエストの実行先 AWS RAM、リクエスト元の IP アドレス、リクエスト、リクエストの実行日時などの詳細を確認します。

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。

AWS RAM CloudTrail の情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。アクティビティが発生すると AWS RAM、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、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対して、追跡を作成します。証跡により、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、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、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 ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については次を参照してください:

- [の証跡の作成 AWS アカウント](#)
- [AWS のサービス CloudTrail ログとの統合](#)
- [CloudTrail 用 Amazon SNS 通知の構成](#)
- [CloudTrail ログファイルを複数のリージョンから受け取る、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](#)に記載されています。たとえば、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テッドユーザーから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 サービス。

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

AWS RAM ログファイルエントリについて

「トレイル」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 のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典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、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出し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 botocore/1.11.2",
  "requestParameters": {
    "name": "foo"
  },
  "responseElements": {
    "resourceShare": {
      "allowExternalPrincipals": true,
      "name": "foo",

```

```
        "owningAccountId": "111122223333",
        "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
        "status": "ACTIVE"
    }
},
"requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
"eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

のコンプライアンス検証 AWS Resource Access Manager

AWS のサービスが特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「[コンプライアンスAWS のサービス プログラムによるスコープ](#)」の「コンプライアンス」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS 「コンプライアンスプログラム」](#)を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「[Downloading Reports in AWS Artifact](#)」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、[AWS 「セキュリティドキュメント」](#)を参照してください。

の耐障害性 AWS Resource Access Manager

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。は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティゾーン AWS リージョン を提供します。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よりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン および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。

のインフラストラクチャセキュリティ AWS Resource Access Manager

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 [ガインフラストラクチャ AWS](#) 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環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の [「Infrastructure Protection」](#) を参照してください。

AWS が発行した API コールを使用して、ネットワーク AWS RAM 経由でにアクセスします。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 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。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。

インターフェイスエンドポイント (AWS PrivateLink) AWS Resource Access Manager を使用した へのアクセス

を使用して AWS PrivateLink、VPC と の間にプライベート接続を作成できます AWS Resource Access Manager。インターネットゲートウェイ、NAT デバイス、VPN 接続、または Direct Connect 接続を使用せずに、VPC 内にある AWS RAM かのように にアクセスできます。VPC 内のインスタンスは AWS RAM にアクセスするためにパブリック IP アドレスを必要としません。

このプライベート接続を確立するには、AWS PrivateLink を利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、AWS RAM 宛てのトラフィックのエントリポイントとして機能するリクエスト管理型ネットワークインターフェイスです。

詳細については「AWS PrivateLink ガイド」の [「Access AWS のサービス through AWS PrivateLink」](#) を参照してください。

に関する考慮事項 AWS RAM

のインターフェイスエンドポイントを設定する前に AWS RAM、「AWS PrivateLink ガイド」の [「考慮事項」](#) を参照してください。

AWS RAM は、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートしています。

VPC エンドポイントポリシーがサポートされています AWS RAM。デフォルトでは、インターフェイスエンドポイント経由での AWS RAM への完全なアクセスが許可されます。

のインターフェイスエンドポイントを作成する AWS RAM

Amazon VPC コンソールまたは AWS Command Line Interface () AWS RAM を使用して、 のインターフェイスエンドポイントを作成できます AWS CLI。詳細については、「AWS PrivateLink ガイド」の「[インターフェイスエンドポイントを作成](#)」を参照してください。

次のサービス名 AWS RAM を使用して のインターフェイスエンドポイントを作成します。

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

インターフェイスエンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名を使用して、AWS RAM への API リクエストを実行できます。例えば、ram.us-east-1.amazonaws.com。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイント AWS RAM を介してへのフルアクセスを許可します。VPC AWS RAM からに許可されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドの[Control access to services using endpoint policies \(エンドポイントポリシーを使用してサービスへのアクセスをコントロールする\)](#)を参照してください。

例: AWS RAM アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされた AWS RAM アクションへのアクセスが許可されます。

JSON

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

に関する問題のトラブルシューティング AWS RAM

ガイドのこのセクションの情報は、AWS Resource Access Manager () を使用する際の一般的な問題の診断と修正に役立ちますAWS RAM。

トピック

- [エラー: 「アカウント ID が AWS 組織に存在しません」](#)
- [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: 「アカウント ID が AWS 組織に存在しません」

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 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 AWS Organizations。

ソリューション

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。

⚠ Important

への信頼されたアクセスを無効にすると AWS Organizations、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にアクセスできなくなります。

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. 「との共有を有効に AWS Organizations」ボックスを選択し、「設定の保存」を選択します。

これで、AWS RAM を使用して、組織内のアカウントや OUs とリソースを共有できるようになりました。

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た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。これは、に影響する AWS Organizations サービスコントロールポリシー (SCP) による制限によっても発生する可能性があります AWS アカウント。

ソリューション

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。

- 以下のユーザーとグループ AWS IAM Identity Center:

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「[アクセス許可セットを作成する](#)」の手順に従ってください。

- IAM 内で、ID プロバイダーによって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します。詳細については IAM ユーザーガイドの [サードパーティ ID プロバイダー \(フェデレーション\) 用のロールを作成する](#) を参照してください。

- IAM ユーザー:
 - ユーザーが担当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 ユーザーのロールの作成](#) を参照してください。
 - (お奨めできない方法) 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。

JSON

```
{
  "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](#) AWS Organizations を使用する代わりに [Organizations コンソール](#)または [Organizations EnableAWSServiceAccess API](#) を使用して AWS RAM との統合を有効にすると発生する可能性があります。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。ロールが作成され

ていないため、AWS RAM は組織内のアカウントまたは組織単位 (OUs) に関する詳細にアクセスできません。

ソリューション

この問題を解決するには、AWS RAM との統合をオフにします AWS Organizations。次に、AWS RAM [EnableSharingWithAwsOrganization](#) API オペレーションを呼び出すか、AWS マネジメントコンソール を使用して次の手順を実行して、再度オンにします。

Important

への信頼されたアクセスを無効にすると AWS Organizations、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にアクセスできなくなります。

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. 「との共有を有効に AWS Organizations」ボックスを選択し、「設定の保存」を選択します。

これで、AWS RAM を使用して、組織内のアカウントや OUs とリソースを共有できるようになりました。

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.」
- 「共有しようとしているリソースは、AWS 組織内でのみ共有できます。」

- 「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コネクション (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 との統合を有効にしたときにサービスにリンクされた `AWSServiceRoleForResourceAccessManager` されたロール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 AWS Organizations。

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。

Important

への信頼されたアクセスを無効にすると AWS Organizations、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にアクセスできなくなります。

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。

- 「との共有を有効に AWS Organizations」ボックスを選択し、「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

ではなく Organizations を使用して との共有 AWS Organizations が有効になっていた AWS RAM

ではなく Organizations を使用して を有効にした場合 AWS RAM、組織内での共有 AWS Organizations 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オン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。

Important

への信頼されたアクセスを無効にすると AWS Organizations、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にアクセスできなくなります。

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. 「との共有を有効に AWS Organizations」ボックスを選択し、「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 AWS アカウント を作成したで、[AWS RAM コンソール](#)で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のあるアカウント 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。

JSON

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

リソースが現在のコンソール設定 AWS リージョン とは異なる にある

AWS RAM はリージョナルサービスです。リソースは特定の に存在し AWS リージョン、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 を設定 AWS マネジメントコンソール する必要があります。

コンソールが現在アクセス AWS リージョンしている 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 AWS のサービス を作成した を使用して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。

ソリューション

- クォータを表示するには、エラーが表示される AWS アカウント で、到達するクォータのタイプに応じて、次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。

アカウントが 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 組織内であっても、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 VPC サブネットを別のアカウントと共有しようとする、共有オペレーションは成功します。ただし、消費アカウントでは、そのリソースLIMIT EXCEEDEDの が AWS RAM コンソールに表示されます。

原因

一部の個々のリソースタイプには、によって適用される制限とは別のサービス固有の制限があります AWS RAM。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、制限の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 Service Quotas



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、[サポート](#) 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> Note</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> Note</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 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 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。	<p data-bbox="829 226 886 260">250</p>

AWS SDK での AWS RAM の使用

AWS Software Development Kit (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
AWS SDK for C++	AWS SDK for C++ コードの例
AWS SDK for Go	AWS SDK for Go コードの例
AWS SDK for Java	AWS SDK for Java コードの例
AWS SDK for JavaScript	AWS SDK for JavaScript コードの例
AWS SDK for .NET	AWS SDK for .NET コードの例
AWS SDK for PHP	AWS SDK for PHP コードの例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コードの例
AWS SDK for Ruby	AWS SDK for Ruby コードの例

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

次の表に、AWS Resource Access Manager ドキュメントへの重要な追加事項を示します。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。

これらの更新に関する通知については、RSS AWS RAM フィードをサブスクライブできます。

変更	説明	日付
Amazon CloudFront のリソース共有サポートが追加されました。	Amazon CloudFront VPC オリジンを組織 AWS アカウント内の他のと共有できるようになりました。	2025 年 10 月 6 日
請求情報とコスト管理リソースを共有するためのサポートが追加されました。	Billing and Cost Management ダッシュボードを他の AWS アカウント または組織と共有できるようになりました AWS RAM。	2025 年 8 月 19 日
AWS Cloud Map リソース共有のサポートを追加	組織 AWS アカウント 内の他のと AWS Cloud Map 名前空間を共有できるようになりました。	2025 年 8 月 14 日
Amazon Application Recovery Controller (ARC) リソースを共有するためのサポートが追加されました。	Amazon Application Recovery Controller (ARC) プランを他の AWS アカウント または組織と共有できるようになりました AWS RAM。	2025 年 7 月 31 日
Oracle Database@AWS リソース共有のサポートを追加	Oracle Database@AWS Exadata インフラストラクチャと ODB ネットワークを組織 AWS アカウント 内の他のと共有できるようになりました。	2025 年 6 月 30 日

マルチパーティー承認リソースの共有のサポートが追加されました。	マルチパーティー承認チームを他のチーム AWS アカウント または組織内で共有できるようになりました。	2025 年 6 月 17 日
Amazon SageMaker AI のリソース共有サポートが追加されました。	を使用して AWS RAM、Amazon SageMaker AI パートナーアプリを他の AWS アカウント や組織と共有できるようになりました。	2025 年 6 月 6 日
AWS Network Firewall リソース共有のサポートを追加	AWS RAM を使用して AWS Network Firewall、ファイアウォールを他の AWS アカウント や組織と共有できるようになりました。	2025 年 5 月 28 日
AWS Systems Manager リソース共有のサポートを追加	アクセス AWS Systems Manager 拒否ポリシーは、他の AWS アカウント や組織と共有できません AWS RAM。	2025 年 4 月 30 日
AWS CodeConnections リソース共有のサポートを追加	AWS CodeConnections コード接続を組織内の他の AWS アカウント または と共有できるようになりました。	2025 年 3 月 5 日
AWS Billing リソース共有のサポートを追加	組織 AWS アカウント 内の他のと AWS Billing ビューを共有できるようになりました。	2024 年 12 月 20 日
Amazon VPC Lattice リソース設定の共有サポートが追加されました。	Amazon VPC Lattice リソース設定を他の AWS アカウント と共有できるようになりました。	2024 年 12 月 1 日

Amazon API Gateway リソースの共有サポートが追加されました。	API Gateway ドメイン名を他の AWS アカウント または組織内で共有できるようになりました。	2024 年 11 月 21 日
Amazon VPC リソースの共有サポートが追加されました。	Amazon VPC セキュリティグループを他の AWS アカウント または組織内で共有できるようになりました。	2024 年 10 月 30 日
AWS End User Messaging SMS リソースの共有のサポートを追加	AWS End User Messaging SMS リソースは、他の AWS アカウント や組織と共有できません AWS RAM。	2024 年 9 月 24 日
AWS PrivateLink	AWS PrivateLink for を使用すると AWS RAM、Virtual Private Cloud (VPC) のインターフェイスエンドポイントを使用して RAM に直接接続できます。	2024 年 9 月 9 日
共有のサポートを追加 AWS Backup	論理工アギャップポールトは、組織全体 AWS アカウント または組織内で共有できません。	2024 年 8 月 7 日
Elastic Load Balancing リソースの共有のサポートが追加されました。	Elastic Load Balancing トラストストアは、組織全体 AWS アカウント または組織内で共有できます。	2024 年 8 月 5 日
Amazon Bedrock カスタムモデルの共有のサポートが追加されました。	を使用して AWS RAM、Amazon Bedrock カスタムモデルを他の AWS アカウント や組織と共有できるようになりました。	2024 年 8 月 1 日

AWS CloudHSM バックアップの共有のサポートを追加	Backup AWS CloudHSM は、他の AWS アカウント や組織と共有できません AWS RAM。	2024 年 6 月 28 日
Amazon SageMaker AI の Model Registry リソースの共有サポートが追加されました。	詳細パラメータを安全かつ効率的に AWS アカウント 全体または所属する組織と共有できるようになりました。	2024 年 6 月 27 日
Amazon SageMaker AI JumpStart の共有サポートが追加されました	Amazon SageMaker AI JumpStart Hubs を組織内 AWS アカウント または組織内で共有できるようになりました。	2024 年 6 月 27 日
共有のサポートを追加 Amazon Route 53 Resolver Profiles	AWS RAM を使用して、組織 AWS アカウント 内の他のと共有 Amazon Route 53 Resolver Profiles できるようになりました。	2024 年 4 月 22 日
Parameter Store AWS Systems Manager リソースを共有するサポートを追加	詳細パラメータを安全かつ効率的に AWS アカウント 全体または所属する組織と共有できるようになりました。	2024 年 2 月 21 日
Amazon FSx for OpenZFS スナップショットを共有するサポートを追加	Amazon FSx for OpenZFS スナップショットを組織 AWS アカウント 内の他のと共有できるようになりました。	2023 年 12 月 19 日
Amazon Simple Storage Service リソースを共有するためのサポートを追加	Amazon Simple Storage Service Access Grants インスタンスを他の AWS アカウント 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

AWS Resource Explorer ビューを共有するためのサポートを追加	組織 AWS アカウント 内の他のと AWS Resource Explorer ビューを共有できるようになりました。	2023 年 11 月 14 日
Amazon Application Recovery Controller (ARC) リソースを共有するためのサポートが追加されました。	Amazon Application Recovery Controller (ARC) クラスターを他の AWS アカウント 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
Amazon DataZone リソースを共有するためのサポートを追加	Amazon DataZone リソースを他の AWS アカウント または組織と共有できるようになりました。	2023 年 10 月 4 日
サービスプリンシパル共有のサポートを追加	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
SageMaker Model Card リソースを共有するサポートを追加	SageMaker Model Card リソースを他の AWS アカウント 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
Amazon SageMaker Feature Store 特徴量グループと SageMaker AI Catalog を共有リソースとしてサポートしました。	Amazon SageMaker AI Feature Store の機能グループと SageMaker AI Catalog リソースを他の AWS アカウント 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

保留中の招待のサービス クォータ制限の引き上げ	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
共有可能なリソースとして AWS AppSync GraphQL APIs のサポートを追加	AWS AppSync GraphQL APIs 他の AWS アカウントと共有できるようになりました AWS RAM。	2023 年 5 月 24 日
共有可能なリソースとして AWS Verified Access グループ のサポートを追加	AWS Verified Access グループを一元的に作成および管理し、他の AWS アカウントや組織と共有できるようになりました。	2023 年 4 月 27 日
AWS RAM コンソールでカスタマー管理アクセス許可のサポートを追加	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
Amazon VPC Lattice サービス とサービスネットワーク共有 可能なリソースのサポートを 追加	Amazon VPC Lattice サービスおよびサービスネットワークリソースを他の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
共有可能なリソースとして AWS Marketplace Catalog エンティティのサポートを追加	Marketplace AWS アカウントで他のとエンティティを共有できるようになりました。	2023 年 3 月 27 日
AWS RAM コンソールでアクセス許可バージョンを管理するためのサポートを追加	AWS RAM コンソールを使用してバージョンの詳細を表示し、アクセス許可をデフォルトとして指定されたバージョンに更新できるようになりました。	2023 年 1 月 16 日

IAM ベストプラクティスの更新	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、「 IAM のセキュリティのベストプラクティス 」を参照してください。	2023 年 1 月 3 日
共有可能なリソースとして Amazon EC2 プレイメントグループのサポートを追加	Amazon EC2 プレイメントグループを他のと共有 AWS アカウントして、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
に関する 2 つの入門ビデオへのリンクを追加しました AWS RAM	リソースを他のと共有するためのウォークスルーを記述 AWS RAM し、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
Amazon SageMaker AI Pipelines のサポートが追加されました。	SageMaker Pipelines 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 8 月 2 日
共有可能なリソースタイプとして AWS Service Catalog AppRegistry アプリケーションと属性グループのサポートを追加	AppRegistry アプリケーションと属性グループを他の AWS アカウントと共有できるようになりました。	2022 年 6 月 17 日
AWS Resource Access Manager が SOC および ISO 認定を取得	AWS RAM は、Service Organization Control (SOC) および国際標準化機構 (ISO) ISO 9001、ISO 27001、ISO 27017、ISO 27018、および ISO 27701 標準に準拠していることが確認されています。	2022 年 5 月 31 日

AWS Resource Access Manager が FedRAMP 認定を受ける	AWS RAM は、Federal Risk and Authorization Management Program (FedRAMP) の認証を受けました。	2022 年 4 月 8 日
AWS Resource Access Manager PCI DSS 認定を取得	AWS RAM は、Payment Card Industry (PCI) データセキュリティ標準 (DSS) に準拠していることが確認されています。	2022 年 2 月 27 日
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。	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
グローバルリソースの共有サポートが追加されました。	グローバルリソースを他の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
共有可能なグローバルリソースとして AWS Cloud WAN コアネットワークのサポートを追加	Cloud WAN コアネットワークを他の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
Amazon VPC IP Address Manager (IPAM) プールの共有サポートが追加されました。	AWS RAM を使用して Amazon VPC IPAM プールを共有できます。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 12 月 1 日

[Amazon SageMaker AI のリソース共有サポート](#)

AWS RAM を使用して SageMaker AI 系統グループを共有できます。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サポート](#)

AWS RAM を使用して Migration Hub 環境を共有できます。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

[マネージド IAM アクセス許可ポリシーに関する情報を追加 AWS RAM AWS しました](#)

IAM コンソールでアクセスし、の IAM プリンシパルにアタッチできる利用可能な AWS 管理アクセス許可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。](#)

を使用して、S3 on Outposts AWS RAM を他の と共有できるようになりました AWS アカウント。

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、追加の AWS RAM 管理アクセス許可から選択し、個々の IAM ロールおよびユーザーとリソースを共有できます。

2021 年 6 月 10 日

AWS Systems Manager Incident Manager リソースの共有のサポートを追加	を使用して AWS RAM、AWS Systems Manager Incident Manager の連絡先と対応計画を他の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
Amazon Route 53 のリソース共有サポートが追加されました。	を使用して AWS RAM、Amazon Route 53 Resolver DNS Firewall ルールグループを他のと共有できるようになりました AWS アカウント。	2021 年 3 月 31 日
AWS Transit Gateway リソース共有のサポートを追加	を使用して AWS RAM、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と共有できるようになりました AWS アカウント。	2020 年 12 月 10 日
AWS Network Firewall リソース共有のサポートを追加	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 AWS RAM を他の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
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。	を使用して、Outposts およびローカルゲートウェイルートテーブル AWS RAM を他のと共有できるようになりました AWS アカウント。	2020 年 10 月 15 日
Route 53 クエリログの共有サポートが追加されました。	を使用して、Route 53 クエリログ AWS RAM を他のと共有できるようになりました AWS アカウント。	2020 年 9 月 7 日

AWS Private Certificate Authority リソース共有のサポートを追加	AWS RAM を使用して、AWS Private CA プライベート認証機関 (CAs) を他の 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
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を追加	AWS RAM を使用して AWS、Glue データカタログ、データベース、テーブルを他の と共有できるようになりました AWS アカウント。	2020 年 7 月 7 日
Amazon VPC プレフィックスリストの共有のサポートを追加	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
AWS Outposts 顧客所有の IPv4 アドレスの共有のサポートを追加	を使用して AWS RAM、AWS Outposts 顧客所有の IPv4 アドレスを他の 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
AWS App Mesh メッシュ共有のサポートを追加	を使用してメッシュ AWS RAM を他の 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
AWS CodeBuild プロジェクトとレポートグループの共有のサポートを追加	を使用して AWS RAM、AWS CodeBuild プロジェクトやレポートグループを他の 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

<u>追加リソースの共有サポートが追加されました。</u>	AWS RAM を使用して、Amazon EC2 Dedicated Hosts、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
<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>	を使用して、オンデマンドキャパシティ予約 AWS RAM を他の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
<u>Aurora DB クラスターの共有サポートが追加されました。</u>	AWS RAM を使用して、Aurora DB クラスターを他のと共有できるようになりました AWS アカウント。	2019 年 7 月 2 日
<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>	を使用して、トラフィックミラーリングターゲット AWS RAM を他の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
<u>ライセンス設定の共有サポートが追加されました。</u>	を使用して、AWS License Manager のライセンス設定 AWS RAM を他の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
<u>サブネットの共有サポートが追加されました。</u>	を使用して Amazon VPC サブネット AWS RAM を他の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。

を使用して AWS RAM、Amazon VPC トランジットゲートウェイを他の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。

を使用して、Route 53 Resolver ルール AWS RAM を他の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。