AWS Resource Access Manager

ユーザーガイド

AWS Resource Access Manager: ユーザーガイド

Table of Contents

AWS RAM とは

AWS Resource Access Manager(AWS RAM) を使用すると、リソースを任意の AWS アカウントと共有したり、 を介して共有したりできますAWS Organizations。複数の AWS アカウントがある場合は、リソースを一元的に作成し、AWS RAM を使用してそれらのリソースを他のアカウントと共有できます。

目次

Benefits

AWS RAM には以下のような利点があります。

- 運用のオーバーヘッドを削減—リソースを一元的に作成し、AWS RAM を使用してそれらのリソースを他のアカウントと共有できます。これにより、複製したリソースをすべてのアカウントにプロビジョニングする必要がなくなるため、運用のオーバーヘッドが減少します。
- セキュリティと一貫性を実現—既存のポリシーとアクセス許可を使用して共有リソースの消費を管理することで、セキュリティとコントロールを実現します。AWS RAM 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を提供します。
- 可視性と監査機能を提供—Amazon CloudWatch および AWS CloudTrail との統合により、共有リソースの使用状況の詳細が表示されます。AWS RAM は、共有リソースとアカウントの包括的な可視性を提供します。

リソース共有のしくみ

リソースを他のアカウントと共有すると、そのアカウントにそのリソースへのアクセス許可が付与されます。リソースを共有しているアカウントに適用されるポリシーとアクセス許可は、共有リソースに適用されます。

リソースの共有

リソースの共有 を作成することで、お客様が所有しているリソースを共有できます。リソースの共有 を作成するときは、名前、共有するリソース、共有相手のプリンシパルを指定します。プリンシパルとしては、AWS アカウントを指定するか、組織単位 を指定するか、または AWS Organizations の組織全体を指定できます。お客様のアカウントは、お客様が共有してい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お客様のアカウントと共有している場合、お客様は、お客様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。それぞれのサービスのコンソール、AWS CLI、API を使用してリソースにアクセスできます。ユーザーが実行を許可されているアクションは、リソースのタイプによって異なります。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が適用されます。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。

サービス制限

AWS アカウントに AWS RAM に関連した以下の制限があります。これらの制限のいくつかは、リクエストによって引き上げることができます。制限の引き上げをリクエストするには、AWS サポート にお問い合わせください。

Resource	デフォルトの制限
アカウントあたりの リソースの共有 の最大数	5000
アカウントあたりの共有プリンシパルの最大数	5000
アカウントあたりの共有リソースの最大数	5000
アカウントあたりの保留中の招待の最大数	20

AWS RAM へのアクセス

AWS RAM は次のいずれかの方法で使用できます。

AWS RAM コンソール

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

AWS Command Line Interface (AWS CLI)

AWS CLI では、AWS RAM のパブリック API オペレーションへの直接アクセスが可能です。Windows、 macOS 、および Linux でサポートされています。開始方法の詳細については、AWS Command Line Interface ユーザーガイド を参照してください。AWS RAM 用のコマンドの詳細については、「AWS CLI Command Reference」を参照してください。

AWS Tools for Windows PowerShell

AWSは、PowerShell環境でスクリプトを記述するユーザー向けに、さまざまな AWS 製品用のコマンドを提供しています。開始方法の詳細については、AWS Tools for Windows PowerShell ユーザーガイドを参照してください。AWS RAM のコマンドレットの詳細については、「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。

クエリ API

AWS RAM HTTPS クエリ API を使用すると、AWS RAM および AWS にプログラムでアクセスできます。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コードを含める必要があります。詳細については、AWS RAM API リファレンス を参照してください。

Pricing

リソースの共有 を作成してアカウント間でリソースを共有するための追加料金はありません。リソースの利用料金はリソースのタイプによって異なります。共有リソースに対する課金方法の詳細については、各サービスのドキュメントを参照してください。

共有可能なリソース

AWS RAMでは、他の AWS サービスでプロビジョニングされて管理されているリソースを共有できます。AWS RAM ではリソースを管理できませんが、 AWS アカウント間でリソースを利用できるようにする機能を提供します。

以下のセクションでは、 AWS RAM と統合される サービスと、共有をサポートするリソースを一覧表示します。

サービス

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。

Resource	ユースケース
メッシュ	メッシュ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ます。共有メッシュでは、異なるAWSアカウントで作成されたリソースが同じメッシュ内で相互に通信できます。詳細については、 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AWS App Mesh。

Amazon Aurora

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

Resource	ユースケース
DB クラスター	DB クラスター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ます。これにより、複数のAWSアカウントで共有され一元管理された DB クラスターのクローンを作成できます。詳細につ

Resource	ユースケース
	いては、Amazon Aurora ユーザーガイドの「クロスアカウント Aurora DB クラスターのクローン作成」を参照してください。

AWS Certificate Manager Private Certificate Authority

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

Resource	ユースケース
プライベート認証機関 (CA)	組織の内部 PKI 用のプライベート認証機関 (CA) を作成および管理し、他のAWSアカウントと共有します。これにより、他のアカウントのAWS Certificate Managerユーザーは共有 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 Certificate Manager Private Certificate Authority ユーザーガイドの「プライベート CA へのアクセスを有効にする」を参照してください。

AWS CodeBuild

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

Resource	ユースケース
プロジェクト	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。他のAWSアカウントまたはユーザーとプロジェクトを共有します。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、そのビルドを分析できます。詳細については、 https://docs.aws.amazon.com/codebuild/latest/userguide/project-sharing.html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 CodeBuild
レポート グループ	レポートグループを作成し、プロジェクトを構築するときにレポートを作成するために使用します。レポートグループを他のAWSアカウントまたはユーザーと共有します。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、および各レポートのテストケース結果を表示できます。レポートは、作成から 30 日間表示することができ、さらに期限切れになるため、表示することはできません。詳細については、 https://docs.aws.amazon.com/codebuild/latest/userguide/project-sharing.htmlユーザーガイドの「共有レポートグループのAWS CodeBuild操作」を参照してください。

Amazon EC2

を使用して、次のAmazon EC2リソースを共有できますAWS RAM。

Resource	ユースケース
Capacity Reservations	キャパシティー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ーを他の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ーに起動できます。Amazon EC2詳細については、次のガイドの「共有キャパシティー予約の使用」を参照してくださいLinux インスタンス用 Amazon EC2 ユーザーガイド。
Dedicated Hosts	Amazon EC2Dedicated Host の割り当てと管理を一元的に行い、ホストのインスタンスキャパシティーを他のAWSアカウントと共有します。これにより、複数のAWSアカウントがインスタンスを一元管理された Dedicated Host に起動できます。Amazon EC2詳細については、次のガイドの「共有専有ホストの使用」を参照してくださいLinux インスタンス用 Amazon EC2 ユーザーガイド。

Amazon EC2Image Builder

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

Resource	ユースケース
コンポーネント	コンポーネント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。イメージレシピで事前定義済みの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 のリソース共有」を参照してください。
イメージ	golden イメージを一元管理し、他の AWS アカウントおよび組織と共有します。組織全体で EC2 Image Builder で作成されたイメージ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 のリソース共有」を参照してください。
イメージレシピ	イメージレシピを一元的に作成および管理し、他の AWS アカウントおよび組織と共有します。これにより、定義済みのドキュメントを使用して、必要な設定の繰り返し可能なイメージパイプラインを自動化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 のリソース共有」を参照してください。

AWSグルー

を使用して、次の AWS Glue リソースを共有できますAWS RAM。

Resource	ユースケース
データカタログ	一元的な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 アカウントとエンタープライズ内の組織と共有します。これにより、ユーザーは複数のアカウントのデータに対してクエリを実行できます。詳細については、AWS Lake Formation Guide の「AWS アカウント間でのデータカタログテーブルとデータベースの共有」を参照してください。
データベース	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 アカウントおよびエンタープライズ内の組織と共有します。データベースはデータカタログテーブルのコレクションです。これにより、ユーザーはクエリを実行し、複数のアカウント間でデータの結合とクエリを行うことができる (ETL) ジョブを抽出、変換、ロードすることができます。詳細については、AWS Lake Formation Guide の「AWS アカウント間でのデータカタログテーブルとデータベースの共有」を参照してください。
テーブル	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 アカウントおよびエンタープライズ内の組織と共有します。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のデータテーブルに関するメタデータが含まれます。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クエリおよび ETL ジョブを実行できます。詳細については、AWS Lake Formation Guide の「AWS アカウント間でのデータカタログテーブルとデータベースの共有」を参照してください。

AWS ライセンスマネージャー

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

Resource	ユースケース
ライセンス 設定	ライセンス設定の作成と管理を一元的に行い、他のAWSアカウントと共有します。これにより、複数のAWSアカウント間でエンタープライズ契約の条件に基づく一元管理されたライセンスルールを適用できます。詳細については、AWS License Manager ユーザーガイドの「ライセンス設定の使用」を参照してください。

AWS Outposts

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

Resource	ユースケース
オイポスト	Outposts を一元的に作成および管理し、AWS組織内で共有します。これにより、複数のアカウントで共有され一元管理された 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、 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。AWS Outposts
Local gateway ルートテーブル	Outpost でローカルゲートウェイルートテーブルを一元的に作成および管理し、AWS組織内で共有します。これにより、マルチプルアカウントはローカルゲートウェイへの VPC の関連付けを作成し、Outpost のローカルゲートウェイ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、 https://docs.aws.amazon.com/outposts/latest/userguide/sharing-outposts.html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AWS Outposts。
Subnets	Outpost のサブネットを一元的に作成および管理し、AWS組織内で共有します。これにより、複数のアカウントで Outpost の共有サブネットで EC2 インスタンスを起動して実行できます。詳細については、 https://docs.aws.amazon.com/outposts/latest/userguide/sharing-outposts.html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AWS Outposts。

AWS リソースグループ

を使用して、次のAWS リソースグループリソースを共有できますAWS RAM。

Resource	ユースケース
リソース グループ	ホストリソースグループを一元的に作成および管理し、他のAWSアカウントと共有します。これにより、複数のAWSアカウントが を使用して作成された Amazon EC2 Dedicated Hosts グループを共有AWS License Managerできるようになります。詳細については、 AWS License Managerユーザーガイドの「ホストリソースグループ」を参照してください。AWS License Manager

Amazon Route 53

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

Resource	ユースケース
転送 ルール	転送ル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ます。これにより、複数のAWSアカウントがそれぞれの DNS クエリVPCsを、共有され一元管理されたリゾルバールールに定義されているターゲット IP アドレスに転送できます。詳細については、 の「他の AWS アカウントとの転送ルールの共有」および「共有ルールの使用」を参照してくださいAmazon Route 53 開発者ガイド。
クエリログ	クエリログ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ます。これにより、Multipe AWS アカウントは、DNS クエリをログ記録して、ログから一元的に管理されたクエリログVPCsを作成できます。詳細については、 の「共有リゾルバーのクエリログ記録の設定」を参照してくださいAmazon Route 53 開発者ガイド。

Amazon VPC

を使用して、次のAmazon VPCリソースを共有できますAWS RAM。

Resource	ユースケース
顧客所有IPv4の住所	AWS Outpostsインストールプロセス中に、AWS は、オンプレミスネットワークに関してお客様が提供した情報に基づいて、お客様が所有する IP アドレスプールと呼ばれるアドレスプールを作成します。 顧客所有の IP アドレスは、オンプレミスネットワークを通じて Outpost サブネット内のリソースへのローカルまたは外部接続を提供します。これらのアドレスは、Elastic IP アドレスを使用して EC2 インスタンスなどの Outpost のリソースに割り当てることができます。
プレフィックスリスト	プレフィックスリストを一元管理し、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、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、リソース内でプレフィックスリストを参照できます。詳細については、次のガイドの「共有プレフィックスリストの使用」を参照してくださいAmazon VPC ユーザーガイド。
Subnets	サブネットの作成と管理を一元的に行い、 から同じ組織内にある他のアカウントや組織単位と共有AWS Organizationsします。これにより、複数の AWS アカウントがアプリケーションリソースを一元管理された に起動VPCs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

Resource	ユースケース
	タベース、 Amazon Redshift クラスター、 関数が含まれます。AWS Lambda詳細については、次のガイドの「VPC 共有の使用」を参照してくださいAmazon VPC ユーザーガイド。
Traff icmirror targets	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アカウントと共有します。これにより、複数のAWSアカウントがアカウント内のトラフィックミラーソースから、共有され一元管理されたトラフィックミラーターゲットに、ミラーリングされたネットワークトラフィックを送信できるようになります。詳細については、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Traffic Mirroring。
トランジットゲートウェイ	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アカウントと共有します。これにより、複数のAWSアカウントが、共有され一元管理されたトランジットゲートウェイを介して、ネットワークVPCsとオンプレミスネットワーク間でトラフィックをルーティングできます。詳細については、トランジットゲートウェイガイドの「トランジットゲートウェイの共有」を参照してください。

AWS RAM の使用を開始する

AWS RAM では、お客様が所有しているリソースを個々の AWS アカウントと、または AWS Organizations を介して共有できます。また、他の AWS アカウントから、または AWS Organizations を介してお客様が共有先になっているリソースを使用できます。

トピック

リソースの共有

AWS RAM を使用して、お客様が所有しているリソースの共有を開始するには、以下の手順に従います。

> Note
>
> 一部のリソースには、共有するための特別な考慮事項と前提条件があります。詳細については、を参照してください 共有可能なリソース (p. 3)。

AWS Organizations との共有を有効にする

組織または組織単位とリソースを共有する場合は、AWS RAMコンソールまたは CLI コマンドを使用してとの共有を有効にする必要がありますAWS Organizations。組織内でリソースを共有する場合、AWS RAM はプリンシパルに招待を送信しません。組織内のプリンシパルは、招待を交換せずに共有リソースにアクセスできます。

組織全体または組織単位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。詳細については、を参照してください とのAWS Organizations 共有の無効化 (p. 26)。

Requirements

- 管理アカウントアカウントのみが とのAWS Organizations 共有を有効にできます。
- この組織はすべての機能で有効になっている必要があります。詳細については、 https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html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AWS Organizations。

> Important
>
> - AWS Organizations との共有を有効にしていない場合、お客様の組織全体で、または組織内の組織単位 とリソースを共有することはできません。ただし、組織内の個々の AWS アカウントとリソースを共有することはできます。この場合、アカウントは外部プリンシパルとして扱われます。リソース共有に参加するための招待を受け取り、共有リソースにアクセスするために招待を受け入れる必要があります。
> - AWS Organizationsコンソールまたは AWS RAMenable-sharing-with-aws-organization AWS CLIコマンドを使用して、 との共有を有効にする必要があります。これにより、`AWSServiceRoleForResourceAccessManager`サービスにリンクされたロールを確実に作成できます。AWS Organizationsコンソールまたは AWS Organizationsenable-aws-service-access コマンドを使用して、 で信頼されたアクセスを有効にした場合、AWS CLI

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。`AWSServiceRoleForResourceAccessManager`

との共有を有効にするには AWS Organizations (コンソール)

1. ram/home#Settings で AWS RAM コンソールの [Settings] ページを開きますhttps://console.aws.amazon.com/。
2. [Enable sharing with AWS Organizations (AWS Organizations との共有を有効にする)] を選択します。

AWS Organizations(AWS CLI) との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リージョンで使用でき、AWS RAM がサポートされているすべてのリージョンで AWS Organizations との共有を有効にします。

リソース共有を作成する

お客様が所有しているリソースを共有するには、リソースの共有 を作成し、共有するリソースを追加して、共有相手の プリンシパル を指定します。

Considerations

- お客様が所有しているリソースのみを共有リソースに設定できます。お客様が共有先になっているリソースを共有リソースに設定することはできません。
- お客様が AWS Organizations の組織のメンバーであり、組織内での共有が有効になっている場合、組織内の プリンシパル には共有リソースに対するアクセス許可が自動的に付与されます。それ以外の場合、プリンシパル は リソースの共有 への参加の招待を受け取り、その招待を受け入れた後で、共有リソースに対するアクセス許可が付与されます。
- 組織を リソースの共有 に追加した後、OU または組織に対する変更はリソース共有に影響します。たとえば、組織に新しいアカウントを追加した場合、そのアカウントは共有リソースにアクセスできます。
- 以下を リソースの共有に として追加することはできませんプリンシパル: IAM ユーザー、IAMロール、OUsまたは の組織外の組織AWS Organizations。

を作成するには リソースの共有 (コンソール)

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. 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。それ以外の場合は、[リソースの共有] リソースの共有 ページから [Create (の作成)] を選択します。
3. [Description (説明)] の [Name (名前)] に、リソースの共有 のわかりやすい名前を入力します。
4. (オプション) [Resources (リソース)] で、以下のように リソースの共有 に追加するリソースを選択します。

   a. [リソースタイプを選択します] で、リソースのタイプを選択します。これにより、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に絞り込まれます。

   b. 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。

      ゾーンのリソースを共有する場合は、アベイラビリティーゾーン ID (AZ ID) を使用すると、アカウント間での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、を参照してください リソースの AZIDs (p. 20)。
5. (オプション) [プリンシパル] で、以下の手順に従います。

a. デフォルトでは、任意の AWS アカウントとリソースを共有できます。リソース共有を AWS Organizations の組織に制限するには、[Allow external accounts (外部アカウントを許可)] をオフにします。
b. プリンシパル ごとに、その ID を指定し、[Add (追加)] を選択します。

   - 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。たとえば、`123456789012` と指定します。
   - OU を追加するには、OU の ID を入力します。たとえば、`ou-abcd1234-mnop5678qrst9098uv76` と指定します。
   - 組織全体を追加するには、組織の ID を入力します。たとえば、`o-abcd1234efgh5678` と指定します。

6. (オプション) [Tags (タグ)] に、タグのキーと値のペアを入力します。別のタグを追加するには、[タグの追加] を選択し、タグのキーと値のペアを入力します。これらのタグは、リソースの共有 に含まれるリソースには適用されません。
7. [作成リソースの共有] 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。リソースの共有 を使用する前にこのプロセスを完了させてください。
8. リソースと プリンシパル の追加および削除、リソースの共有 へのカスタムタグの適用はいつでもできます。リソースを共有する必要がなくなったら、リソースの共有 を削除できます。詳細については、を参照してください お客様が所有しているリソースの共有 (p. 14)。

リソースの共有 を作成するには (AWS CLI)

create-resource-share コマンドを使用します。

共有リソースの使用

共有リソースを使用し始めるには、以下の手順に従います。

リソース共有の招待に応答する

リソースの共有 への参加の招待を受け取った場合、共有リソースに対する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。お客様が AWS Organizations の組織のメンバーであり、組織内での共有が有効になっている場合、組織内の プリンシパル には、これらの招待は送信されることなく、共有リソースに対するアクセス許可が自動的に付与されます。

招待に応答するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[自分と共有]、[Resource shares (リソース共有)] の順に選択します。
3. お客様が追加された先の リソースの共有 のリストを確認します。

   [Status (ステータス)] 列は、リソースの共有 の現在の参加ステータスを示します。`Pending` ステータスは、お客様は リソースの共有 に追加されたが、まだ招待を受け入れていないか、辞退していないことを示します。
4. リソースの共有 招待に応答するには、リソースの共有 ID を選択し、[リソースの共有を承認] を選択して招待を受け入れるか、[リソースの共有を拒否] を選択して招待を辞退します。招待を辞退した場

合、リソースにアクセスすることはできません。招待を受け入れた場合、リソースにアクセスすることができます。

お客様が共有先になっているリソースを使用する

リソースの共有 への参加の招待を受け入れたら、共有リソースに対して特定のアクションを実行できます。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、を参照してください 共有可能なリソース (p. 3)。

共有リソースでの作業

お客様が所有している AWS リソースを共有したり、お客様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

お客様が所有しているリソースの共有

AWS RAM を使用すると、指定したリソースを、指定した プリンシパル と共有できます。作成した リソースの共有 はいつでも変更でき、それらの共有が不要になったら削除できます。

目次

リソース共有の作成

お客様が所有しているリソースを共有するには、リソースの共有 を作成し、共有するリソースを追加して、共有相手の プリンシパル を指定します。

リソースの共有 を作成するには、「リソースの共有 (p. 10)」の手順に従います。

リソース共有の更新

リソースの共有 はいつでも更新できます。作成した リソースの共有 に プリンシパル、リソース、または タグを追加できます。リソースの共有 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。

コンソールを使用して リソースの共有 を更新するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[共有ファイル]、[リソースの共有] の順に選択します。
3. リソースの共有 を選択してから、[変更] を選択します。
4. (オプション) リソースの共有 の名前を変更するには、[Name (名前)」を編集します。
5. (オプション) リソースの共有 にリソースを追加するには、[Resources (リソース)] でリソースのタイプを選択し、リソースの横にあるチェックボックスをオンにします。
6. (オプション) リソースを削除するには、[Selected resources (選択済みリソース)] パネルでリソースを見つけ、[X] を選択します。
7. (オプション) プリンシパル を追加するには、AWS アカウントの OU または組織の ID を入力し、[Add (追加)] を選択します。
8. (オプション) プリンシパル を削除するには、[Selected principals (選択済みプリンシパル)] パネルでそのプリンシパルを見つけ、[X] を選択します。
9. (オプション) リソースの共有 にタグを追加するには、[Tags (タグ)] で [タグの追加] を選択し、タグのキーと値のペアを入力します。
10. リソースの共有 からタグを削除するには、タグを見つけ、[タグの削除] を選択します。
11. [Save changes] を選択します。

AWS CLI を使用して リソースの共有 を更新するには

次のコマンドを使用します。

- associate-resource-share
- disassociate-resource-share
- tag-resource
- update-resource-share

リソース共有の表示

作成したすべての リソースの共有 のリストを表示できます。お客様がどのリソースをどの プリンシパル と共有しているのかを確認できます。

コンソールを使用して リソースの共有 を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[共有ファイル]、[リソースの共有] の順に選択します。
3. フィルタを適用して特定の リソースの共有 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. 確認する リソースの共有 を選択します。以下の情報が表示されます。

    - [Summary (概要)]—名前、ID、所有者、Amazon リソースネーム (ARN)、作成日、現在のステータスなど、リソースの共有 に関する情報を一覧表示します。

- [Shared resources (共有リソース)—リソースの共有 に含まれるリソースを一覧表示します。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。
- [Shared principals (共有プリンシパル)]—リソースを共有している相手の プリンシパル を一覧表示します。
- [Tags (タグ)]—リソースの共有 のタグのキーと値のペアを一覧表示します。

AWS CLI を使用して リソースの共有 を表示するには

get-resource-shares コマンドを使用します。

共有リソースの表示

アカウントによって共有されているリソースをすべての リソースの共有 にわたって表示できます。これにより、お客様が現在共有しているリソース、それらのリソースが含まれる リソースの共有 の数、それらのリソースにアクセスできる プリンシパル の数を判別できます。

コンソールを使用して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 (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[共有ファイル]、[Shared resources (共有リソース)] の順に選択します。
3. 共有リソース別に以下の情報が表示されます。

   - [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。
   - [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)]—リソースが含まれる リソースの共有 の数。リソースの共有 を一覧表示する値を選択します。
   - [プリンシパル]—リソースを共有している相手の 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 を使用して共有しているリソースを表示するには

list-resources コマンドを使用します。

共有相手のプリンシパルの表示

お客様とリソースを共有している プリンシパル をすべての リソースの共有 にわたって表示できます。お客様の共有相手のプリンシパルを表示することで、お客様の共有リソースにアクセスできるプリンシパルを判別できます。

コンソールを使用してお客様の共有相手の プリンシパル を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[共有ファイル]、[プリンシパル] の順に選択します。
3. プリンシパル 別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。
   - [Resource shares (リソース共有)]—お客様が プリンシパル と共有した リソースの共有 の数。リソースの共有 を表示する値を選択します。
   - [Resources (リソース)]—お客様が プリンシパル と共有したリソースの数。共有リソースを表示する値を選択します。

AWS CLI を使用してお客様の共有相手の プリンシパル を表示するには

list-principals コマンドを使用します。

リソース共有の削除

リソースの共有 はいつでも削除できます。リソースの共有 を削除すると、リソースの共有 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。リソースの共有 を削除しても、共有リソースは削除されません。

削除された リソースの共有 は、削除後しばらくの間コンソールに表示されたままになりますが、そのステータスは `Deleted` に変わります。

コンソールを使用して リソースの共有 を削除するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[共有ファイル]、[リソースの共有] の順に選択します。
3. リソースの共有 を選択します。必ず正しい リソースの共有 を選択してください。リソースの共有 は削除後に回復することはできません。
4. [Delete (削除)] を選択し、確認メッセージを入力して、[Delete (削除)] を選択します。

AWS CLI を使用して リソースの共有 を削除するには

delete-resource-share コマンドを使用します。

共有リソースでサポートされているアクション

AWS CLI を使用して、プリンシパル が共有リソースに対して実行できるアクションを表示できます。詳細については、get-resource-policies コマンドを参照してください。

お客様が共有先になっているリソースへのアクセス

AWS RAM を使用すると、お客様が追加された先の リソースの共有、アクセスできる共有リソース、お客様とリソースを共有している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、リソースの共有 を終了することもできます。

目次

招待の承認と却下

共有リソースにアクセスするには、プリンシパル がお客様を リソースの共有 に追加する必要があります。

お客様が AWS Organizations の組織のアカウントによって リソースの共有 に追加され、組織内での共有が有効になっている場合、お客様には共有リソースに対するアクセス許可が自動的に付与されます。

お客様が以下のいずれかによって リソースの共有 に追加された場合は、リソースの共有 への参加の招待を受け取ります。

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

リソースの共有 への参加の招待を受け取った場合、共有リソースにアクセスするには、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。

リソースの共有 への参加の招待を受け入れるまで 7 日間の猶予があります。7 日以内に招待を受け入れない場合は、自動的に、招待を辞退したことになります。

招待に応答するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[自分と共有]、[Resource shares (リソース共有)] の順に選択します。
3. お客様が追加された先の リソースの共有 のリストを確認します。

   [Status (ステータス)] 列は、リソースの共有 の現在の参加ステータスを示します。`Pending` ステータスは、お客様は リソースの共有 に追加されたが、まだ招待を受け入れていないか、辞退していないことを示します。
4. リソースの共有 招待に応答するには、リソースの共有 ID を選択し、[リソースの共有を承認] を選択して招待を受け入れるか、[リソースの共有を拒否] を選択して招待を辞退します。招待を辞退した場合、リソースにアクセスすることはできません。招待を受け入れた場合、リソースにアクセスすることができます。

招待に応答するには (AWS CLI)

次のコマンドを使用します。

- accept-resource-share-invitation
- reject-resource-share-invitation

リソース共有の表示

お客様が追加された先の リソースの共有 を表示できます。どの プリンシパル がお客様とどのリソースを共有しているのかを確認できます。

コンソールを使用して リソースの共有 を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[自分と共有]、[Resource shares (リソース共有)] の順に選択します。
3. フィルタを適用して特定の リソースの共有 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. 以下の情報が表示されます。

   - [Name (名前)]—リソースの共有 の名前。
   - [ID]—リソースの共有 の ID。リソースの共有 を表示する ID を選択します。
   - [Owner (所有者)]—リソースの共有 を作成した AWS アカウントの ID。
   - [Status (ステータス)]—リソースの共有 の現在のステータス。以下に示しているのは、可能な値です。
     - [Active (アクティブ)]—リソースの共有 はアクティブで使用可能です。
     - [Deleted (削除済み)]—"リソースの共有 は削除されたため、使用できなくなりました。

- [Pending (保留中)]—リソースの共有 への参加の招待は保留中です。

AWS CLI を使用して リソースの共有 を表示するには

get-resource-shares コマンドを使用します。

共有リソースの表示

お客様がアクセスできる共有リソースを表示できます。どの プリンシパル がお客様とリソースを共有していて、どの リソースの共有 にリソースが含まれているかを確認できます。

コンソールを使用して共有リソースを表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[自分と共有]、[Shared resources (共有リソース)] の順に選択します。
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. 以下の情報が表示されます。

   - [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。
   - [リソースタイプ]—リソースのタイプ。
   - [Last share date (最終共有日)]—お客様がリソースの共有先になった日付。
   - [Resource shares (リソース共有)]—リソースが含まれる リソースの共有 の数。リソースの共有 を表示する値を選択します。
   - [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 を使用して共有リソースを表示するには

list-resources コマンドを使用します。

お客様の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。お客様が共有先になっているリソースと リソースの共有 を確認できます。

コンソールを使用して、お客様とリソースを共有している プリンシパル を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[自分と共有]、[プリンシパル] の順に選択します。
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。
4. 以下の情報が表示されます。

   - [Principal ID (プリンシパル ID)]—お客様の共有相手の プリンシパル の ID。
   - [Resource shares (リソース共有)]—プリンシパル がお客様を追加した先の リソースの共有 の数。リソースの共有 を表示する値を選択します。
   - [Resources (リソース)]—プリンシパル がお客様と共有しているリソースの数。リソースを表示する値を選択します。

AWS CLI を使用して、お客様とリソースを共有している プリンシパル を表示するには

list-principals コマンドを使用します。

リソース共有の終了

お客様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 リソースの共有 を終了できます。リソースの共有 を終了すると、共有リソースへのアクセスが失われます。

お客様が組織内のアカウントによって リソースの共有 に追加され、AWS Organizations との共有が有効になっている場合、その共有を終了することはできません。

コンソールを使用して リソースの共有 を終了するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[自分と共有]、[Resource shares (リソース共有)] の順に選択します。
3. リソースの共有 を選択します。
4. [Leave resource share (リソース共有の終了)] を選択し、確認テキストを入力して、[Leave resource share (リソース共有の終了)] を選択します。

AWS CLI を使用して リソースの共有 を終了するには

disassociate-resource-share コマンドを使用します。

リソースの AZIDs

リソースがリージョンの複数のアベイラビリティーゾーンに分散されるようにするために、アベイラビリティーゾーンは各アカウントの名前に個別にマッピングされます。たとえば、お客様の AWS アカウントのアベイラビリティーゾーン `us-east-1a` は別の AWS アカウントのアベイラビリティーゾーン `us-east-1a` と同じ場所にはない可能性があります。詳細については、『 ユーザーガイド』の「Amazon EC2 リージョンとアベイラビリティーゾーン」を参照してください。

アカウントに対するリソースの場所を特定するには、AZ ID を使用する必要があります。これは、アベイラビリティーゾーンの一意で一貫した識別子です。たとえば、`use1-az1` は `us-east-1` リージョンの AZ ID であり、すべての AWS アカウントで同じ場所を示します。

アカウントのアベイラビリティーゾーンIDsの AZ を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. ナビゲーションペインで、[Resource Access Manager] を選択します。
3. 現在のリージョンIDsの AZ はお客様の AZ ID の下にあります。

AZ を表示すると、あるアカウントのリソースの場所を別のアカウントのリソースに対して決定できます。IDsたとえば、AZ ID のアベイラビリティー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 であるアベイラビリティーゾーンのそのアカウントで利用できますuse-az2。use-az2 各サブネットの AZ ID がAmazon VPCコンソールに表示されます。

IDsを使用して AZ を表示するにはAWS CLI

- describe-availability-zones
- DescribeAvailabilityZones

AWS RAM のセキュリティ

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

セキュリティは、AWS とお客様の間の共有責任です。共有責任モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、AWS クラウド内で AWS サービスを実行するインフラストラクチャを保護する責任を担います。また、AWS は、使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Resource Access Manager に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任はお客様が使用する AWS のサービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントでは、AWS RAM を使用する際に責任共有モデルを適用する方法について説明します。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ように AWS RAM を設定する方法について説明します。また、AWS RAM リソースのモニタリングやセキュリティ保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

AWS Resource Access Manager でのデータ保護

AWS Resource Access Manager は、データ保護の規制やガイドラインを含む AWS 責任共有モデルに準拠しています。AWS は、AWS のすべてのサービスを実行するグローバルなインフラストラクチャを保護する責任を担います。また、AWS は、カスタマーコンテンツおよび個人データを取り扱うためのセキュリティ構成の統制など、このインフラストラクチャ上でホストされるデータ管理を維持します。データコントローラーまたはデータプロセッサとして機能する AWS のお客様と APN パートナーは、AWS クラウドに保存された個人データに対する責任を担います。

データ保護目的の場合、AWS アカウント認証情報を保護して IAM (AWS Identity and Access Management) で個々のユーザーアカウントをセットアップし、そのユーザーに各自の職務を果たすために必要なアクセス許可のみが付与されるようにすることをお勧めします。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。

- SSL/TLS を使用して AWS リソースと通信します。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS 暗号化ソリューションを、AWS サービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- などの高度なマネージドセキュリティサービスAmazon Macieを使用します。

顧客のアカウント番号などの機密の識別情報を、[名前] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール、API、 AWS RAM 、または を使用して や他の AWS サービスを使用する場合も同様AWS CLIAWSです。SDKs AWS RAMや他のサービスに入力したすべてのデータは、診断ログに取り込まれる可能性があります。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

データ保護の詳細については、 AWS セキュリティブログのブログ投稿「AWSの責任共有モデルとGDPR」を参照してください。

AWS RAM の Identity and access management

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ために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS リソースの使用を承認する (アクセス権限を持たせる) かを制御します。IAM を使用すると、AWS アカウントでユーザーとグループを作成できます。ユーザーが AWS リソースを使用してタスクを実行するために必要なアクセス許可を制御します。IAM は追加料金なしで使用できます。カスタム IAM ポリシーの管理と作成の詳細については、「IAM; ポリシーの管理」を参照してください。

トピック

AWS RAM で IAM を使用する方法

デフォルトでは、 IAM ユーザーには AWS RAM リソースを作成または変更するためのアクセス許可はありません。IAMユーザーがリソースを作成または変更、およびタスクを実行できるようにするには、特定のリソースと API アクションを使用するアクセス許可を付与するIAMポリシーを作成する必要があります。次に、それらのアクセス権限が必要なユーザーまたはグループにそのポリシーをアタッチします。IAM

トピック

ポリシーの構造

IAMポリシーは、次のステートメントを含む JSON ドキュメントで
す。Effect、Action、Resource、Condition。IAMポリシーは通常、次の形式です。

```
{
     "Statement":[{
         "Effect":"effect",
         "Action":"action",
```

```
        "Resource":"arn",
        "Condition":{
            "condition":{
                "key":"value"
            }
        }
    }]
}
```

Effect

Effect ステートメントは、ポリシーがアクションを実行するユーザーのアクセス許可を許可または拒否するかどうかを示します。指定できる値は、以下の通りです。`Allow`および `Deny` 。

Action

アクションステートメントは、ポリシーがアクセス許可を許可または拒否する API アクションを指定します。AWS RAM許可されるアクションの完全なリストについては、の「 により定義されたアクションAWS Resource Access Manager」を参照してくださいIAM ユーザーガイド。

Resource

Resource ステートメントでは、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。許可された リソースの完全なリストについては、の「 により定義された リソースAWS Resource Access Manager」を参照してくださいIAM ユーザーガイド。

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。 AWS RAMは次の条件キーをサポートします。

- リソースの共有を作成またはタグ付けするときに使用する必要があるタグのキーと値のペア`aws:RequestTag/${TagKey}`—を指定します。
- a 指定されたタグキーと値のペアがあるリソースでのみアクションを実行できる`ws:ResourceTag/${TagKey}`—ことを示します。
- リソースの共有を作成またはタグ付けするときに使用できるタグキー`aws:TagKeys`—を指定します。
- 外部プリンシパルとの共有を許可または拒否するリソースの共有でのみアクションを実行できる`ram:AllowsExternalPrincipals`—ことを示します。外部プリンシパルはAWS、組織外のAWSアカウントです。
- 指定されたプリンシパルでのみアクションを実行できる`ram:Principal`—ことを示します。
- 指定されたリソースタイプでのみアクションを実行できる`ram:RequestedResourceType`—ことを示します。リソースタイプは次の形式で指定する必要があります。
  - リソースの共有を作成またはタグ付けするときに使用する必要があるタグのキーと値のペア`aws:RequestTag/${TagKey}`—を指定します。
  - a 指定されたタグキーと値のペアがあるリソースでのみアクションを実行できる`ws:ResourceTag/${TagKey}`—ことを示します。
  - リソースの共有を作成またはタグ付けするときに使用できるタグキー`aws:TagKeys`—を指定します。
  - 外部プリンシパルとの共有を許可または拒否するリソースの共有でのみアクションを実行できる`ram:AllowsExternalPrincipals`—ことを示します。外部プリンシパルはAWS、組織外のAWSアカウントです。
  - 指定されたプリンシパルでのみアクションを実行できる`ram:Principal`—ことを示します。
  - 指定されたリソースタイプでのみアクションを実行できる`ram:RequestedResourceType`—ことを示します。リソースタイプは次の形式で指定する必要があります。

- AWS App Mesh
  - `appmesh:Mesh`
- Amazon Aurora
  - `rds:Cluster`
- AWS Certificate Manager Private Certificate Authority
  - `acm-pca:CertificateAuthority`
- AWS CodeBuild
  - `codebuild:Project`
  - `codebuild:ReportGroup`
- Amazon EC2
  - `ec2:CapacityReservation`
  - `ec2:DedicatedHost`
- Amazon EC2Image Builder
  - `imagebuilder:Component`
  - `imagebuilder:Image`
  - `imagebuilder:ImageRecipe`
- AWSグルー
  - `glue:Catalog`
  - `glue:Database`
  - `glue:Table`
- AWS License Manager
  - `license-manager:LicenseConfiguration`
- AWS Outposts
  - `outposts:Outpost`
- AWS リソースグループ
  - `resource-groups:Group`
- Amazon Route 53
  - `route53resolver:ResolverRule`
  - `route53resolver:ResolverQueryLogConfig`
- Amazon VPC
  - `ec2:PrefixList`
  - `ec2:Subnet`
  - `ec2:TrafficMirrorTarget`
  - `ec2:TransitGateway`
  - `ec2:LocalGatewayRouteTable`

- 指定された ARN のあるリソースでのみアクションを実行できる`ram:ResourceArn`—ことを示します。
- 指定された名前のリソースの共有でのみアクションを実行できる`ram:ResourceShareName`—ことを示します。
- 特定のアカウントによって所有されているリソースの共有でのみアクションを実行できる`ram:ShareOwnerAccountId`—ことを示します。

- 指定された ARN のあるリソースでのみアクションを実行できる`ram:ResourceArn`—ことを示します。
- 指定された名前のリソースの共有でのみアクションを実行できる`ram:ResourceShareName`—ことを示します。
- 特定のアカウントによって所有されているリソースの共有でのみアクションを実行できる`ram:ShareOwnerAccountId`—ことを示します。

IAM ポリシーの例

例

例 1: 特定のリソースの共有を許可する

IAM ポリシーを使用して、特定のリソースのみを リソースの共有 に関連付けるように プリンシパル を制限できます。

たとえば、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。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "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、特定のリソースタイプのみを リソースの共有 に関連付けるように プリンシパル を制限できます。

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

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

例 3: 外部 AWS アカウントとの共有を制限する

IAM ポリシーを使用して、プリンシパル が AWS 組織外の AWS アカウントとリソースを共有するのを防ぐことができます。

たとえば、以下の IAM ポリシーでは、プリンシパル が外部 AWS アカウントを リソースの共有 に追加するのを防いでいます。

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

との共有の無効化AWS Organizations

以前に AWS Organizations との共有を有効にしていて、組織全体または組織単位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、すべての組織または組織単位AWS Organizationsが、作成した から削除され、共有リソースへのアクセスが失われます。リソースの共有

との共有を無効にするにはAWS Organizations

1. AWS OrganizationsAWS Organizationsdisable-aws-service-access https://docs.aws.amazon.com/cli/latest/reference/organizations/disable-aws-service-access.htmlコマンドを使用して、 への信頼されたアクセスを無効にします。AWS CLI

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

   Important

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

2. IAMコンソール、 IAM AWS CLI 、または IAM API を使用して、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、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IAM ユーザーガイド。

AWS RAM アクセス許可

AWS RAMアクセス許可は、 で使用されるポリシーフラグメントAWS RAMです。これらは、共有されているリソースに対してプリンシパルが実行できるアクションを制御します。AWS RAMアクセス許可は、共有リソースにアタッチされているリソースベースのポリシーを生成するために使用されます。

AWS RAMには、サポートされている共有可能なリソースタイプごとに、デフォルトの 管理アクセス許可が含まれています。AWSこれらのマネージド型のアクセス許可は、 AWS によって作成および管理され、共有可能なリソースタイプごとに許可されるアクションを定義します。によって管理されるデフォルトのアクセス許可の詳細については、「」を参照してくださいAWS。AWS管理のアクセス許可 (p. 27)

トピック

- AWS管理のアクセス許可 (p. 27)

AWS RAMアクセス許可の仕組み

リソース共有を作成すると、 AWS RAMは関連付けられている各リソースタイプのデフォルトのアクセス権限を自動的にリソース共有にアタッチします。たとえば、リソース共有を作成し、サブネットとキャパシティー予約を関連付ける場合、 AWS RAMはサブネットとキャパシティー予約のアクセス許可をリソース共有に自動的にアタッチします。

リソース共有が作成されると、それぞれのリソース所有サービスにアクセス許可が提供されます。リソース所有サービスは、提供されたアクセス許可を使用して、リソース共有に含まれるリソースごとにリソースベースのポリシーを作成します。リソース所有サービスによって作成されたリソースベースのポリシーには、次の要素が含まれます。

- リソース共有に含まれるリソース。`Resource`—
- `Effect`—AWS RAMアクセス許可の効果。常に `allow` になります。
- リソース共有に関連付けられているプリンシパルの 。`Principal`—ARNs
- `Action`—AWS RAMアクセス許可で定義されている標準アクション。

リソースベースのポリシーは、共有リソースにアタッチされます。これらのポリシーによって、指定されたプリンシパルは、リソースに対して許可されるアクションを実行できます。

AWS管理のアクセス許可

AWS RAMは次のデフォルトの AWS 管理対象アクセス権限を提供します。

トピック

AWS App Mesh

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可AWS App Mesh を提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
[appmesh:Mesh]	名前: AWSRAMDefaultPermissionAppMesh	許可	• `appmesh:CreateVirtualNode`

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
	ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAppMesh		• appmesh:CreateVirtualRouter • appmesh:CreateRoute • appmesh:CreateVirtualService • appmesh:UpdateVirtualNode • appmesh:UpdateVirtualRouter • appmesh:UpdateRoute • appmesh:UpdateVirtualService • appmesh:ListVirtualNodes • appmesh:ListVirtualRouters • appmesh:ListRoutes • appmesh:ListVirtualServices • appmesh:DescribeVirtualNode • appmesh:DescribeVirtualRouter • appmesh:DescribeRoute • appmesh:DescribeVirtualService • appmesh:DeleteVirtualNode • appmesh:DeleteVirtualRouter • appmesh:DeleteRoute • appmesh:DeleteVirtualService

Amazon Aurora

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可Amazon Auroraを提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
rds:Cluster	名前: AWSRAMDefaultPermissionRDSCluster ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionRDSCluster	許可	• rds:RestoreDbClusterToPointInTime • rds:DescribeDbClusters

AWS Certificate Manager Private Certificate Authority

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可ACM Private CAを提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
acm-pca:CertificateAuthority	名前: AWSRAMDefaultPermissionCertificateAuthority	許可	• acm-pca:IssueCertificate

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
	ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCertificateAuthority		• acm-pca:DescribeCertificateAuthority • acm-pca:GetCertificate • acm-pca:GetCertificateAuthorityCertifi • acm-pca:ListPermissions • acm-pca:ListTags

AWS CodeBuild

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可AWS CodeBuild を提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
コードビルド: プロジェクト	名前: AWSRAMDefaultPermissionCodeBuildProject ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCodeBuildProject	許可	• codebuild:BatchGetBuilds • codebuild:BatchGetProjects • codebuild:ListBuildsForProject
codebuild:ReportGroup	名前: AWSRAMDefaultPermissionCodeBuildReportGroup ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCodeBuildReportGroup	許可	• codebuild:BatchGetReports • codebuild:BatchGetReportGroups • codebuild:ListReportsForReportGrou • codebuild:DescribeTestCases

Amazon EC2

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可Amazon EC2を提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
ec2: CapacityReservation	名前: AWSRAMDefaultPermissionCapacityReservation ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCapacityReservation	許可	• ec2:RunInstance • ec2:DescribeCapacityReservations
ec2:DedicatedHost	名前: AWSRAMDefaultPermissionDedicatedHost	許可	• ec2:RunInstances • ec2:StartInstances • ec2:DescribeHosts • ec2:ModifyInstancePlacement

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
	ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionDedicatedHost		

Amazon EC2Image Builder

は、共有可能な AWS RAM Image Builder リソースに対して、次のデフォルトの AWS 管理アクセス許可Amazon EC2を提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
イメージビルダー: コンポーネント	名前: AWSRAMDefaultPermissionImageBuilderComponent ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionImageBuilderComponent	許可	• imagebuilder:GetComponent • imagebuilder:ListComponents
イメージビルダー: イメージ	名前: AWSRAMDefaultPermissionImageBuilderImage ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionImageBuilderImage	許可	• imagebuilder:GetImage • imagebuilder:ListImages
イメージビルダー: ImageRecipe	名前: AWSRAMDefaultPermissionImageBuilderImageRecipe ARN: arn:aws:ram::aws:permission/imagebuilder:AWSRAMDefaultPermissionImageBuilderImageRecipe	許可	• imagebuilder:GetImageRecipe • imagebuilder:ListImageRecipes

AWSグルー

は、共有可能な AWS RAM Glue リソースに対して、次のデフォルトの AWS 管理アクセス許可AWSを提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
glue:Catalog	名前: AWSRAMDefaultPermissionGlueCatalog ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionGlueCatalog	許可	• glue:GetTable • glue:GetTableVersion • glue:GetTableVersions • glue:GetPartition • glue:GetPartitions • glue:BatchGetPartition • glue:GetDatabase • glue:GetTables • glue:GetDatabases

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
			• glue:SearchTables
グルー: データベース	名前: AWSRAMDefaultPermissionGlueDatabase ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionGlueDatabase	許可	• glue:GetTable • glue:GetTableVersion • glue:GetTableVersions • glue:GetPartition • glue:GetPartitions • glue:BatchGetPartition • glue:GetDatabase • glue:GetDatabases • glue:GetTables • glue:SearchTables
glue:Table (グルー: テーブル)	名前: AWSRAMDefaultPermissionGlueTable ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionGlueTable	許可	• glue:GetTable • glue:GetTableVersion • glue:GetTableVersions • glue:GetPartition • glue:GetPartitions • glue:BatchGetPartition • glue:SearchTables

AWS License Manager

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可AWS License Managerを提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
ライセンスマネージャー:LicenseConfiguration	名前: AWSRAMDefaultPermissionLicenseConfiguration ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionLicenseConfiguration	許可	• license-manager:GetLicenseConfiguration • license-manager:ListLicenseConfigurations • license-manager:ListAssociationsForLicense • license-manager:ListUsageForLicenseConfigu

AWS Outposts

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可AWS Outpostsを提供します。

> Note
>
> Outposts の共有サブネットとローカルゲートウェイルートテーブルに対するデフォルトの AWS 管理アクセス許可については、「サブネットと (p.)ローカルゲートウェイのルートテーブル」を参照してください。 (p.)

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
outposts:Outpost	名前: AWSRAMDefaultPermissionOutpostsOutpost ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionOutpostsOutpost	許可	• outposts:GetOutpost • outposts:GetOutpostInstanceTypes • outposts:ListOutposts

AWS リソースグループ

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可AWS リソースグループを提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
resource-groups:Group	名前: AWSRAMDefaultPermissionResourceGroup ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionResourceGroup	許可	• resource-groups:GetGroup • resource-groups:GetGroupConfiguration • resource-groups:ListGroupResources

Amazon Route 53

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可Amazon Route 53を提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
route53resolver:Resolver	名前: AWSRAMDefaultPermissionResolverRule ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionResolverRule	許可	• route53resolver:GetResolverRule • route53resolver:AssociateResolverR • route53resolver:DisassociateResolv • route53resolver:ListResolverRules • route53resolver:ListResolverRuleAs
route53resolver:Resolver	名前: AWSRAMDefaultPermissionResolverQueryLogConfig ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionResolverQueryLogConfig	許可	• route53resolver:AssociateResolverQ • route53resolver:DisassociateResolv • route53resolver:ListResolverQueryL

Amazon VPC

は、共有可能なAWS RAMリソースに対して、次のデフォルトの AWS 管理アクセス許可Amazon VPCを提供します。

[リソースタイプ]	アクセス許可名と ARN	Effect	アクション
ec2:PrefixList	名前: AWSRAMDefaultPermissionPrefixList ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionPrefixList	許可	• ec2:DescribeManagedPrefixLists • ec2:GetManagedPrefixListEntries
ec2:Subnet	名前: AWSRAMDefaultPermissionSubnet ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet	許可	• ec2:RunInstances • ec2:CreateNetworkInterface • ec2:DescribeSubnets
ec2:TrafficMirrorTarget	名前: AWSRAMDefaultPermissionTrafficMirror ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionTrafficMirror	許可	• ec2:DescribeTrafficMirrorTargets • ec2:CreateTrafficMirrorSession • ec2:DeleteTrafficMirrorSession • ec2:DescribeTrafficMirrorSessions
ec2:[TransitGateway]	名前: AWSRAMDefaultPermissionTransitGateway ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionTransitGateway	許可	• ec2:DescribeTransitGateways • ec2:CreateTransitGatewayVpcAttachm • ec2:ModifyTransitGatewayVpcAttachm • ec2:DeleteTransitGatewayVpcAttachm
ec2:LocalGatewayRouteTable	名前: AWSRAMDefaultPermissionLocalGateway ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionLocalGateway	許可	• ec2:CreateLocalGatewayRouteTableVp • ec2:DeleteLocalGatewayRouteTableVp • ec2:DescribeLocalGatewayRouteTable • ec2:DescribeLocalGatewayRouteTable • ec2:DescribeLocalGatewayRouteTable • ec2:DescribeLocalGatewayVirtualInt • ec2:DescribeLocalGatewayVirtualInt • ec2:DescribeLocalGateways • ec2:SearchTransitGatewayRoutes

AWS RAM のログ記録とモニタリング

モニタリングは、AWS RAM および 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役割を果たします。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS には、AWS RAM リソースをモニタリングし、潜在的なインシデントに対応するための複数のツールが用意されています。

Amazon CloudWatch Events

AWSリソースの変更を示すシステムイベントをほぼリアルタイムのストリームとして配信します。CloudWatch イベント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 の他のAWS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、を参照してください CloudWatchイベントによるモニタリング (p. 34)。

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 呼び出しおよび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、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、を参照してください AWS CloudTrail による AWS RAM API コールのログ記録 (p. 34)。

CloudWatchイベントによるモニタリング

Amazon CloudWatch Events を使用して、AWS RAM の特定のイベントに対する自動通知を設定できます。AWS RAM サービスからのイベントは、ほぼリアルタイムに CloudWatch イベント に配信されます。イベントをモニタリングし、リソースの共有 に対する変更を示すイベントに応答してターゲットを呼び出すように、CloudWatch イベント を設定できます。リソースの共有 への変更によって、リソースの共有の所有者と リソースの共有 に対するアクセス許可が付与された プリンシパル の両方に、イベントがトリガーされます。

イベントパターンを作成するとき、ソースは `aws.ram` です。

詳細については、Amazon CloudWatch Events ユーザーガイド を参照してください。

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

AWS RAM は、AWS RAM のユーザーやロール、または AWS のサービスによって実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。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。キャプチャされたコールには、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。証跡を作成する場合は、CloudTrail のイベントなど、Amazon S3 バケットへの AWS RAM 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 [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、AWS RAM に対して行われたリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエストの実行日時、その他の詳細を判別します。

CloudTrail の詳細については、「AWS CloudTrail User Guide」を参照してください。

CloudTrail での AWS RAM 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。AWS RAM でアクティビティが発生すると、そのアクティビティは AWS の他のサービスのイベントと共に CloudTrail イベントとして [イ

ベント履歴] に記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS RAMのイベントなど、AWS アカウントのイベントの継続的な記録については、証跡を作成します。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、コンソールで作成した証跡がすべての AWS リージョンに適用されます。証跡では、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がログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、より詳細な分析と CloudTrail ログで収集されたデータに基づいた行動のためにその他の AWS サービスを設定できます。詳細については、以下を参照してください。

- 証跡の作成に関する概要
- CloudTrail でサポートされるサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンから CloudTrail ログファイルを受け取ると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ます。これらのアクションは AWS RAM API リファレンス で説明されています。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、リクエストの生成者に関する情報が含まれます。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、ルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたかどうか。
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか.
- リクエストが、別の AWS サービスによって送信されたかどうか。

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

AWS RAM ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できる設定です。CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなど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 コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例は、`CreateResourceShare` アクションに対する 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"
}
```


AWS Resource Access Manager での耐障害性

AWSグローバルインフラストラクチャはAWS、リージョンとアベイラビリティーゾーンを中心として構築されます。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立· 隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断することなく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。アベイラビリティーゾーンは、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、および拡張性が優れています。

AWSのリージョンやアベイラビリティーゾーンの詳細については、AWSグローバルインフラストラクチャを参照してください。

AWS RAM でのインフラストラクチャセキュリティ

マネージド型サービスとしての AWS RAMは、 に説明されているAWSグローバルネットワークセキュリティの手順で保護されていますAmazon Web Services。セキュリティプロセスの概要ホワイトペーパー。

AWS が公開している API コールを使用して、ネットワーク経由で AWS RAM にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

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

AWS RAM ユーザーガイドのドキュメント履歴

以下の表は、AWS RAM のドキュメントの主な更新をまとめたものです。

変更	説明	日付
Outposts およびローカルゲートウェイルートテーブルの共有のサポート	Outposts とローカルゲートウェイルートテーブルを共有するために使用します。AWS RAM詳細については、「AWS Outposts (p. 7)」および「Amazon VPC (p. 8)」を参照してください。	2020 年 10 月 15 日
クエリログの共有のサポート	クエリログを共有するにはAWS RAM、 を使用します。Route 53 詳細については、を参照してください Amazon Route 53 (p. 7)。	2020 年 9 月 7 日
ACM Private CAプライベート認証機関 (CA) の共有のサポート	プライベート AWS RAM を共有するには、 を使用しますACM Private CA。CAs 詳細については、「」を参照してくださいAWS Certificate Manager Private Certificate Authority (p. 4)。	2020 年 8 月 17 日
AWSGlue データカタログ、データベース、およびテーブルの共有のサポート	AWS RAMを使用して AWS Glue データカタログ、データベース、テーブルを共有します。詳細については、を参照してください AWSグルー (p. 6)。	2020 年 7 月 07 日
マネージドプレフィックスリストの共有のサポート	マネージドプレフィックスリストを共有するために使用します。AWS RAM詳細については、を参照してください Amazon EC2 (p. 5)。	2020 年 6 月 29 日
AWS Outpostsお客様が所有するIPv4住所の共有のサポート	お客様が所有するAWS RAMアドレスを共有するために使用します。AWS OutpostsIPv4詳細については、を参照してください Amazon EC2 (p. 5)。	2020 年 4 月 22 日
AWS App Meshメッシュの共有のサポート	メッシュを共有するために使用します。AWS RAM詳細については、を参照してください AWS App Mesh (p. 3)。	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	AWS RAMを使用してAWS CodeBuildプロジェクトとレポートグループを共有します。詳細	2019 年 12 月 13 日

変更	説明	日付
	については、を参照してください AWS CodeBuild (p. 4)。	
追加のリソースの共有のサポート	を使用して、AWS RAM専用ホスト、Amazon EC2リソースグループ、AWS リソースグループImage Builder のコンポーネント、イメージ、イメージレシピを共有します。Amazon EC2詳細については、を参照してください 共有可能なリソース (p. 3)。	2019 年 12 月 02 日
オンデマンドキャパシティー予約の共有のサポート	を使用してオンデマンドキャパシティー予約を共有します。AWS RAM詳細については、を参照してください Amazon EC2 (p. 5)。	2019 年 7 月 29 日
Aurora DB クラスターの共有のサポート	Aurora DB クラスターを共有するには、 を使用します。AWS RAM詳細については、を参照してください Amazon Aurora (p. 3)。	2019 年 7 月 02 日
Traffic Mirroringターゲットの共有のサポート	ターゲットを共有するにはAWS RAM、 を使用します。Traffic Mirroring詳細については、を参照してください Amazon EC2 (p. 5)。	2019 年 6 月 25 日
ライセンス設定の共有のサポート	を使用してAWS RAMAWS ライセンス設定を共有します。License Manager詳細については、を参照してください AWS ライセンスマネージャー (p. 6)。	2018 年 12 月 05 日
サブネットの共有のサポート	AWS RAM を使用して Amazon VPC サブネットを共有します。詳細については、を参照してください Amazon EC2 (p. 5)。	2018 年 11 月 27 日
中継ゲートウェイの共有のサポート	AWS RAM を使用して Amazon VPC 中継ゲートウェイを共有します。詳細については、を参照してください AWS ライセンスマネージャー (p. 6)。	2018 年 11 月 26 日
転送ルールの共有のサポート	AWS RAM を使用して Route 53 転送ルールを共有します。詳細については、を参照してください Amazon Route 53 (p. 7)。	2018 年 11 月 20 日
初回リリース	このリリースで AWS Resource Access Manager が導入されました。	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。」