Alibaba Cloud
Resource Access Management

はじめに

Document Version20190220

目次

1 RAM の概要

Resource Access Management (RAM) は、ユーザー ID の管理とアクセス制御のための Alibaba Cloud サービスです。 RAM を 使用すると、ユーザーアカウント (従業員、システム、アプリケーションなど) を作成および管理し、Alibaba Cloud アカウントのリソースに対してそのユーザーアカウントが所有する操作権限を制御できます。 企業の複数のユーザーが共同でリソースを操作する必要がある場合、 RAM により、Alibaba Cloud アカウントのアクセスキーを他のユーザーと共有する必要がなくなります。 ユーザーには作業に必要な最小限の権限を付与できるため、企業のセキュリティリスクが軽減されます。

ID 管理とアクセス制御

RAM を使用すると、Alibaba Cloud アカウントで複数のユーザー ID を作成および管理できます。また、異なる権限付与ポリシーを異なる ID や ID グループに割り当てて、 異なるリソースアクセス権限を異なるユーザーに付与することができます。

ID 管理

RAM ユーザー ID は、コンソールまたは Open API を使用して Alibaba Cloud リソースに対する操作を実行するユーザー、システム、またはアプリケーションを示します。 さまざまな適用シナリオにおける ID 管理に対応するために、RAM には RAM-User と RAM-Role の 2 つのユーザー ID タイプが用意されています。

- RAM-User は、固定の ID と ID 認証アクセスキーを持つ実際の ID であり、 一般的には、特定のユーザーまたはアプリケーションに対応します。
- RAM-Role は仮想 ID であり、固定の ID は持っていますが、ID 認証情報アクセスキーを持ちません。

RAM-Role を使用するには、実際の ID に関連付ける必要があります。 RAM-Role は複数の実際の ID と関連付けることができます。例：現在の Alibaba Cloud アカウントの RAM-User、別の Alibaba Cloud アカウントの RAM-User、Alibaba Cloud サービス (例: EMR、MTS)、外部の実際の ID (例: ローカルエンタープライズアカウント) の RAM-Userなど。

権限付与

RAM を使用すると、Alibaba Cloud アカウントで複数の権限付与ポリシーを作成および管理できます。 基本的には、各権限付与ポリシーは権限のコレクションであり、 管理者が、1 つ以上の権限付与ポリシーを RAM ユーザー (RAM-User、RAM-Role など) に割り当てることができます。

RAM の権限付与ポリシー言語によって、権限付与ポリシーの内容を詳細に記述します。 ポリシーによって権限を API 操作とリソース ID に付与し、複数の制限 (例: ソース IP、アクセス時間、MFA) を指定できます。

Alibaba Cloud アカウントと RAM ユーザー

- 所有権の観点に基づくと、Alibaba Cloud アカウントとそのアカウントの RAM ユーザーは親子関係にあります。
  - Alibaba Cloud アカウントは、Alibaba Cloud リソースの所有権とリソース消費の請求を確認するための基本エンティティです。
  - RAM ユーザーは、特定の Alibaba Cloud アカウントの RAM インスタンスにのみ存在します。 RAM ユーザーはリソースを所有しません。付与された権限でユーザーが作成したリソースは親アカウントに属します。 また、RAM ユーザーに課金されることもありません。許可された操作によって発生した費用はすべて、親アカウントに請求されます。
- 権限の面では、Alibaba Cloud アカウントとそのアカウントの RAM ユーザーの間には、(Linux のように) root とユーザーの関係があります。
  - root はリソースに対するすべての操作と制御の権限を持ちます。
  - RAM ユーザーは root によって付与された権限しか持ちません。 さらに、root はユーザーに付与した権限をいつでも取り消すことができます。

RAM を使用してエンタープライズレベルのクラウドリソース管理

RAM は、次のエンタープライズシナリオに適用されます：

- エンタープライズは、各オペレータ（またはアプリケーション）のアカウントと権限を簡単に管理する必要があります。
- 企業は、各オペレーター（またはアプリケーション）の費用と料金を別々に計算したくありません。

具体的な要件は次のとおりです：

図 1-1 : エンタープライズシナリオ

- A 社には Alibaba Cloud アカウントが 1 つだけ必要です（図では companyA@aliyun.com ）。
- すべてのリソースはこの Alibaba Cloud アカウントに属します。 リソース所有者として、このアカウントはすべてのリソースを完全に制御し、 すべての請求の支払いを担当します。

- A は RAM を使用して、アカウント（リソースの O&M 制御操作を実行する従業員）のオペレータ用の独立したユーザーアカウントを作成し、承認管理を実行できます。
- ユーザーアカウントにはリソースがありません。 デフォルトでは、作成するリソースに対するアクセス許可はなく、アクセス許可の承認後にのみリソースに対する操作を実行できます。
- ユーザーアカウントの操作によって発生した料金は、プライマリアカウントに請求されます。ユーザーアカウントの個別請求はサポートされていません。

ラーニングパス

RAMの専門家になるために必要な知識は、*RAM* ラーニングパス を参考してください。

2 機能

RAM は、ユーザーのID管理とリソースアクセス管理に役立ちます。 各機能の詳細は次の通りです：

RAM ユーザーとそのアクセスキーの管理

Alibaba Cloud アカウントには、RAMユーザーとそのアクセスキーを作成、管理、RAMユーザーの MFA デバイスを有効、無効にすることができます。

RAMユーザーへのアクセス権限付与

ユーザー、ユーザーグループまたはロールに1つ以上の認証ポリシーをつけることができ、指定されたリソースへの必要な操作権限を付与することができます。

ユーザーへのクラウドリソースアクセス制限

ユーザーにはセキュリティチャネル（SSLなど）を通じて、指定された時間帯、或いは指定された送信元IPアドレスで指定されたクラウドリソースにアクセスさせることが可能です。

外部アカウントIDのロール権限管理

RAMロールを外部IDシステム（ローカルエンタープライズドメインアカウント、アプリアカウントなど）に関連付けることができます。 このようにして、外部IDで直接にRAMロールにログオンし、Alibaba Cloudコンソールまたは APIにアクセスできます。

クラウドリソースの集中管理

RAMユーザーによって作成されたインスタンスとデータを集中管理することができます。 よって、ユーザーが組織から離れても、そのユーザーが作成したインスタンスとデータに対する完全制御は変わりません。

請求書の統合

アカウントには、すべてのRAMユーザーが実行したリソース操作によって発生したすべての費用が請求書にまとめて送られます。

3 適用シナリオ

RAMは、企業におけるアカウント管理および権限の割り当て、多企業間のリソース管理および権限の付与、臨時クライアントエンドポイントで実行されるアプリケーションに対する一時的な認証などのシナリオに適用されます。

企業におけるサブアカウント管理および権限の割り当て

企業Aは多種類のクラウドリソース（ECSインスタンス、RDSインスタンス、SLBインスタンス、またはOSSバケットなど）を購入したとします、 A の従業員はそのリソースに対して、購入、O&M、オンライン適用などの操作を実行する必要があります。 従業員によって役割が異なるため、さまざまな権限が必要です。

要件

- セキュリティ確保のため、A は Alibaba Cloud アカウントのアクセスキーを従業員に公開するのではなく、 それぞれの従業員に、RAMユーザーアカウントを作成し、さまざまな権限を付与すると考えています。
- ユーザーアカウントでは、付与されている権限の範囲でのみリソース操作を行うことができます。また、ユーザーアカウントには課金されません。費用はすべて A に請求されます。
- もちろんA は、いつでもユーザーアカウントの権限を取り消し、削除することが可能です。

多企業間のリソース管理および権限の付与

企業AとBがあります。Aは業務用で多種類のクラウドリソース（ECSインスタンス、RDSインスタンス、SLBインスタンス、またはOSSバケットなど）をたくさん購入したとします。

要件

- 企業Aは業務システムに専念するために、クラウドリソースのO&M、モニタリングの管理を企業Bに任せ、権限を付与しました。
- そしてB は、O&M タスクを従業員に委任します。 B は、A のクラウドリソースを操作する従業員の権限に対して細かく制御できます。
- AとBはO&M委任契約を終了した場合、A は、Bの権限を必要に応じて取り消すことができます。

臨時クライアントエンドポイントで実行されるアプリケーションに対する一時的な権限の付与

企業Aは開発したモバイルアプリケーションのために、OSSを購入したとします。 そのモバイルアプリケーションのダウンロードおよびアップロードはOSSで実行する必要があります。

要件

- 企業Aには、AppServer を使用したデータ転送を許可しないアプリケーションもあります。よって、このアプリケーションのダウンロードおよびアップロードはOSSで実行すると考えています。
- モバイルアプリはユーザーのデバイスで実行されるため、A では制御できません。セキュリティ確保のため、アクセスキーをアプリに保存することはできません。
- 企業Aはセキュリティにおけるリスクを最小限に抑えるため、各アプリケーションにOSSに接続するための必要最小限の権限と制限されたアクセス時間（30分など）を持つアクセストークンを与えます。

4 基本概念

このドキュメントでは、サービスの理解を深めるため、RAM の関連概念について説明します。

ID管理の概念

Alibaba Cloud アカウント

Alibaba Cloud アカウント (プライマリアカウント) は、Alibaba Cloud リソースの所有権とリソース消費の請求を確認するための基本エンティティです。 Alibaba Cloud サービスを使用するには、先に Alibaba Cloud アカウントに登録しておく必要があります。 Alibaba Cloud アカウントには、そのアカウントのリソースすべての料金が請求され、そのリソースに対する完全な権限が付与されています。

デフォルトでは、リソースにアクセスできるのはリソースオーナーだけです。 他のユーザーがリソースにアクセスするには、オーナーから明示的に権限が付与されていなければなりません。 したがって、権限管理の観点から見た場合、Alibaba Cloud アカウントは、オペレーティングシステムの root または管理者アカウントと似ており、root アカウント、 プライマリアカウント とも呼ばれます。

Alibaba Cloud アカウントのエイリアス

RAM では、各 Alibaba Cloud アカウントにグローバルに一意なエイリアスを設定できます。 エイリアスは主に RAM ユーザーのログオンに使用され、正常にログオンすると表示されます。

たとえば、Alibaba Cloud アカウント admin@abc.com に対してエイリアス abc.com が設定されている場合、RAM ユーザー Alice が Alibaba Cloud コンソールに正常にログオンすると、表示名は alice@abc.com になります。 alice@abc.com.

ID 資格情報

ID 資格情報は、ユーザーの実際の ID を認証するときに使用され、 通常は、ユーザーのログオンパスワードまたはアクセスキーを指します。 機密情報であるため、だれにも知られないようにする必要があります。

- ログオン名/パスワードログオン名とパスワードを使用すると、Alibaba Cloud コンソールへのアクセス、注文内容または請求書の確認、リソースの購入、リソース操作の実行を行うことができます。
- アクセスキーアクセスキーを使用すると、リソース操作を実行するための API リクエストを作成 (またはクラウドサービス SDK を使用) できます。

- 多要素認証多要素認証 (MFA) は、 ユーザー名とパスワードのほかに追加のセキュリティ保護を提供できる、シンプルながらも効果的なベストプラクティスです。 MFA を有効にすると、ユーザーは Alibaba Cloud Web サイトにログオンするとき、ユーザー名とパスワード (1 番目のセキュリティ要素) を入力した後に、MFA デバイスによって提供される毎回変わる認証コード (2 番目のセキュリティ要素) を入力する必要があります。 このすべての要素が連携することで、アカウントのセキュリティ保護がさらに強化されます。

RAM ユーザー

RAM では、(企業の従業員、システム、アプリケーションに対応する) 複数の RAM ユーザーを Alibaba Cloud アカウントで作成できます。 RAM ユーザーはリソースを所有せず、個別に課金されることはありません。 ユーザーの管理と支払いは Alibaba Cloud アカウントごとに行われます。 RAM ユーザーは Alibaba Cloud アカウントに属しており、このアカウントでのみ表示できます。 また、独立した Alibaba Cloud アカウントではありません。 Alibaba Cloud アカウントから権限付与された後にのみ、Alibaba Cloud アカウントの下で、コンソールにログオンすることや、API を使用してリソースで操作を実行することができます。

RAMは、RAM-UserとRAM-Roleの2種類のIDをサポートします。

- RAM-Userは、IDが固定されたIDであり、 一般に特定の人物やアプリケーションに対応します。
- RAMロールは、固定アイデンティティクレデンシャルを持たない仮想アイデンティティです。RAMロールは、実際のIDに関連付けて使用可能にする必要があります。

RAM ロール

伝統的なロール（テキストブックのロール）は一連のアクセス許可の集まりで、RAMのポリシーと 似たものです。 ユーザーにロールが割り当てられている場合、ユーザーには一連のアクセス許可が与えられ、ユーザーは認可されたリソースにアクセスすることが可能です。

RAMのロールはテキストブックのロールとは異なります。 RAMロールは仮想ユーザー（またはシャドウアカウント）で、 RAMユーザーの一種です。 このタイプの仮想ユーザーは固定IDを持ち、アクセス許可のセットを割り当てることもできます（ポリシー）が、ユーザーには固定ID認証キー（ログオンパスワードまたはアクセスキー）が無い状態です。 RAMロールと通常のRAMユーザーの違いは、使用方法にあります。 RAMロールは権限付与されたエンティティユーザーによってプレイする必要があります。 プレイが成功したら、エンティティユーザーはRAMロールの一時的なセキュリティトークンを取得できます。 一時的なセキュリティトークンを使用して、ロールアイデンティティとして認可されたリソースにアクセスすることが可能です。

RAMロールとテキストブックロールの違いは次のとおりです。

- （類似点） RAMロールとテキストブックロールは両方とも権限セットにバインドできます。
- （相違点） RAM-Role は仮想 ID またはシャドウアカウントであり、 独立した ID を持ちます。 RAMロールには権限をバインドし、このロールのユーザーのリスト (ロールプレイヤー) を指定する必要があります。 RAMロールは、主に、 IDフェデレーションの問題を解決するときに使用されます。 テキストブックロールは、一般的には権限セットのみを示します。これは ID ではなく、主に権限付与の管理を簡素化する目的で使用されます。

  RAMロールのロール 想定と切り替え
- ログオン ID からロール ID への切り替え (SwitchRole)：このロールに既に関連付けられている実際のユーザー (RAM-User など) は、コンソールにログオンした後に、 ロールへの切り替えが可能です。 ロールへの切り替えは、一度に 1 ロールずつ行う必要があります。 ログオン ID からロール IDに切り替えると、 使用できるのはそのロール ID にバインドされている権限だけになり、 ログオン ID にバインドされている権限は使用できなくなります。 ログオン ID の権限を使用する必要がある場合は、ロール ID からログオン ID に戻す必要があります。
- ロールを引き受けるプログラムの呼び出し (AssumeRole)：RAMロールに関連付けられている実際のユーザー (RAMユーザーなど) は、 アクセスキーを使って STS サービスの AssumeRole インターフェイスを呼び出して、この RAMロールの一時的な アクセスキーを入手できます。 一時的なアクセスキーには有効期間と制限付きアクセス権限があります (ロールにバインドされている権限セットを超えることはありません)。 一般的に、一時的なアクセスキーは、一時的な権限付与の問題を解決するときに使用されます。

RAM関連の概念

リソース

リソースは、クラウドサービスからユーザーに提供されるオブジェクトを抽象化したもので、ユーザーとのやり取りに使用されます。OSS バケットやオブジェクト、ECS インスタンスなどがあります。

各リソースには、グローバル Alibaba Cloud Resource Name (ARN) が定義されています。 形式は次のとおりです。

```
acs:<service-name>:<region>:<account-id>:<resource-relative-id>
```

形式の説明:

- acs: Alibaba Cloud Service の略語です。Alibaba Cloud パブリッククラウドプラットフォームを示します。

- service-name: Alibaba Cloud が提供するオープンサービスの名前です (ecs、oss、odps など)。
- region: リージョン情報です。 このオプションに対応していない場合は、代わりにワイルドカード “*” を使用します。
- account-id: アカウント ID です 例: `1234567890123456`。
- resource-relative-id: サービス関連のリソースです。 その意味は特定のサービスによって指定されます。 たとえば OSS の場合、 `acs:oss::1234567890123456:sample_bucket/file1.txt` は、 パブリッククラウドプラットフォームの OSS リソースであることを示します。ここで、`sample_bucket/file1.txt`は OSS オブジェクト名で、`1234567890123456` はオブジェクトオーナーです。

権限

権限を使用すると、特定のクラウドリソースに対する特定のユーザー操作を許可または禁止できます。

操作は、主に、リソース制御操作とリソース使用操作の 2 つのカテゴリに分類できます。

- リソース制御操作とは、ECS インスタンスの作成、停止、再起動、OSS バケットの作成、変更、削除など、クラウドリソースのライフサイクル管理や O&M 管理の操作を指します。 リソース制御操作は、一般的に、組織のリソース購入者や O&M 担当者を対象としています。
- リソース使用操作とは、ECS インスタンスオペレーティングシステムでのユーザー操作、OSS バケットデータのアップロード/ダウンロードなど、 リソースのコア機能の使用を指します。 リソース使用操作は、組織の R&D 担当者やアプリケーションシステムを対象としています。

> 注：
> エラスティックコンピューティングプロダクトやデータベースプロダクトの場合、リソース制御操作は RAM を使用して管理できますが、 リソース使用操作は各プロダクトインスタンスで管理できます。 (例：ECS インスタンスの OS 権限制御、MySQL データベースの権限制御など)。 OSS、Table Store などのストレージタイプのプロダクトについては、 リソース制御操作とリソース使用操作の両方を RAM で管理できます。

ポリシー

ポリシーとは、権限セットを記述するシンプルな言語仕様のタイプです。 RAM がサポートする言語仕様については、ポリシー構文の構造 を参照してくださいポリシーの構文構造。 RAM は、システムアクセスポリシーとカスタマイズアクセスポリシーの 2 種類の権限付与ポリシーに対応しています。

- Alibaba Cloud によって管理されているシステムアクセスポリシーは、使用できますが、変更することはできません。 システムアクセスポリシーのバージョンは自動的に更新されます。
- お客様が管理するカスタマイズアクセスポリシーについては、作成したり削除したりできます。 また、ポリシーのバージョンは、お客様自身で管理する必要があります。