Alibaba Cloud
Resource Access Management

クイックスタート

Document Version20190802

目次

1 概要..... 1
2 RAM ユーザーのセキュリティポリシーの設定.....2
3 RAM ユーザーの作成..... 3
4 RAM ユーザーグループの作成..... 4
5 カスタマイズポリシーの作成.....5
6 RAM ユーザーへの権限付与..... 6
7 RAM ユーザーログイン..... 7

1 概要

このドキュメントでは、 Resource Access Management （RAM）を開始するために実行するべきタスクを説明します。

1. （オプション）MFA の設定
2. RAM 構成の初期設定
3. RAM ユーザーの作成
4. （オプション）RAM ユーザグループの作成
5. （オプション）カスタムポリシーの作成
6. RAM ユーザーへの権限付与
7. Web コンソールへの RAM ユーザーのログイン

2 RAM ユーザーのセキュリティポリシーの設定

このトピックでは、Alibaba Cloud アカウント配下の RAM ユーザーのセキュリティポリシーを設定して、RAM ユーザーの権限を管理しやすくする方法について説明します。

1. RAM コンソールにログインします。
2. [アイデンティティ] > [設定] を選択します。
3. [セキュリティ設定] タブで、[RAM ユーザーセキュリティ設定の更新] をクリックし、関連するパラメーターを設定します。
   - MFA ログイン状態を 7 日間保持する：RAM ユーザーの多要素認証 (MFA) ログインステータスを保持するかどうかを指定します。 デフォルト値は [拒否済み] です。 [許可] を選択した場合、MFA ログインステータスは 7 日間保持されます。
   - パスワードの管理：RAM ユーザーが自分のパスワードを変更できるかどうかを指定します。
   - AccessKey の管理：RAM ユーザーが自分の AccessKey を管理できるかどうかを指定します。
   - MFA デバイスの管理：RAM ユーザーが MFAデ バイスを有効または無効にできるかどうかを指定します。
   - ログインセッションの有効期間：ログインセッションの有効期間。 単位は時間です。
   - ログインアドレスマスク：ログインに使用できない IP アドレスを指定します。 このパラメーターはデフォルトでは指定されていません。 つまり、すべての IP アドレスをログインに使用できます。 このパラメーターを指定した場合、パスワードやシングルサインオン (SSO) を使用してコンソールにログインすることはできません。 ただし、Access Key を使用して API を呼び出すことができます。 ログインマスクの設定方法については、「Alibaba Cloud アカウントのログインマスクの設定」をご参照ください。
4. [OK] をクリックします。

> 注：
> セキュリティポリシーの設定は、Alibaba Cloud アカウント配下のすべての RAM ユーザーに適用されます。

3 RAM ユーザーの作成

RAM ユーザーは、メンテナンス作業員、またはアプリケーションなどを対応している Alibaba Cloud で作成されたエンティティです。 RAM ユーザーを作成し、それに必要な Alibaba Cloud リソースにアクセスするための適切な権限を付与することができます。

1. RAM コンソールにログインします。
2. ID > ユーザー をクリックします。
3. ユーザーの作成をクリックして、ログイン名と表示名を入力します。

   注 :
   ユーザーの追加をクリックして、一度に複数の RAM ユーザーを作成できます。
4. アクセスモードを選択します。 利用可能なアクセスモードは、コンソールパスワードログインとプログラムによるアクセスです。

   - コンソールパスワードログイン を選択した場合、ログインに関する基本的なセキュリティ設定を完了させる必要があります。これには、パスワードを自動的に生成するかどうか、またはログインパスワードをカスタマイズするかどうかの決定、ユーザーに対し次回のログインのためにパスワードのリセットを要求するかどうかの設定、および MFA (multi-factor authentication) を有効化するかどうかの設定が含まれます。
   - プログラムによるアクセスを選択した場合、RAM ユーザ用のアクセスキーが自動的に作成されます。 ユーザーは API を呼び出すか開発ツールを使用することで Alibaba Cloud リソースにアクセスできます。

   注 :
   Alibaba Cloud アカウントのセキュリティ上の原因で、ユーザーにアクセスモードを 1 つだけ設定することをお勧めします。
5. OK をクリックします。

- 必要に応じて、RAM ユーザーを 1 つまたは複数の RAM ユーザーグループに追加し、ユーザーに対して権限を付与できます。 詳細は、グループへの RAM ユーザーの追加 をご参照ください.
- ユーザーにアクセス権限を付与するために、RAM ユーザーに 1 つまたは複数のポリシーをアタッチすることもできます。 詳細は、RAM ユーザーへの権限付与 をご参照ください.

4 RAM ユーザーグループの作成

本ドキュメントでは、RAM ユーザーグループを作成する方法について説明します。 Alibaba Cloud アカウントに複数の RAM ユーザーがある場合、RAM ユーザーグループを作成し、これらの RAM ユーザーを分類、整理し、ユーザーと権限の管理を簡単にすることができます。

1. RAM コンソールにログインします。
2. ID > グループ をクリックします。
3. グループの作成をクリックして、グループ名、表示名、および説明を入力します。
4. OK をクリックします。

RAM ユーザーグループに 1 つまたは複数のポリシーを添付できます。 詳細は、RAM ユーザーグループへの権限付与 をご参照ください.

5 カスタマイズポリシーの作成

本ドキュメントでは、カスタマイズポリシーを作成する方法について説明します。 カスタマイズポリシーはシステムポリシーよりも正確な制御を提供します。

カスタマイズポリシーを作成する前に、ポリシーの基本構造と構文についてお読みいただくことを推奨します。 詳細は、ポリシー構造と構文 をご参照ください.

1. RAM コンソールにログインします。
2. 権限 > ポリシー をクリックします。
3. ポリシーの作成 をクリックします。
4. ポリシーの名前と説明を入力します。
5. 構成モードを設定します。
   - 構成モードを 視覚化 に設定した場合は、文の追加 をクリックしプロンプトに従って権限の Effect、Action、および Resource を設定します。
   - 構成モードを Script に設定した場合は、ポリシーの構造と文法に従ってポリシーを編集します。
6. OK をクリックします。

6 RAM ユーザーへの権限付与

このトピックでは、RAM ユーザーに権限を付与する方法について説明します。 RAM ユーザーは、関連する権限を取得した後、Alibaba Cloud リソースにアクセスできるようになります。

1. RAM コンソール にログインします。
2. [権限] > [権限付与] を選択します。
3. [権限の付与] をクリックします。
4. [プリンシパル] フィールドに、ユーザー名またはユーザー ID を入力し、対象の RAM ユーザーをクリックします。

   注：
   キーワードを入力して、特定のユーザー名を検索することもできます。
5. [ポリシー名] 列で、対象のポリシーを選択し、[OK] をクリックします。

   注：
   選択を解除するには、[X] をクリックします。

7 RAM ユーザーログイン

このトピックでは、RAM ユーザーがコンソールにログインするための URL と方法を説明します。

ログイン URL

RAM ユーザーのログイン URL は、Alibaba Cloud アカウントのログイン URL とは異なります。

RAM ユーザーのログイン URLは、RAM ユーザーログイン URL です。

注：
RAM コンソールの [概要] ページで、RAM ユーザーログイン URL を取得することもできます。

ログイン方法

[RAM ユーザーログイン] ページで、以下のいずれかの方法でコンソールにログインできます。

- UPN 形式：<$username>@<$AccountAlias>.onaliyun.com (例： `username @ company - alias . onaliyun . com`)

  注：
  <$username> は RAM ユーザーのユーザー名、<$AccountAlias>.onaliyun.com はデフォルトのドメイン名です。

- <$username>@<$AccountAlias> (例： `username @ company - alias`)

  注：
  <$username> は RAM ユーザーのユーザー名、<$AccountAlias> はアカウントのエイリアスです。