Alibaba Cloud
Resource Access Management

権限付与ユースケース

Document Version20190805

目次

1 RAM ユーザーに関してよくある質問

RAM ユーザーとして Alibaba Cloud コンソールにログインするにはどうすればよいですか。

https://signin-intl.aliyun.com/login.htm にアクセスするか、または RAM コンソールの概要ページの右側にある RAM ユーザーのログイン URL にアクセスしてください。

ログイン用のユーザー名は、次のいずれかの形式になります。<$username>@<$AccountAlias> および <$username>@<$AccountAlias>.onaliyun.com。 ドメインエイリアスを作成した場合は、 <$username>@<$DomainAlias> 形式のドメインエイリアスをログインに使用することもできます。

> 注 :
> RAM コンソールの概要ページの右側にある RAM ユーザーログイン URL にアクセスして Alibaba Cloud コンソールにログインすると、システムは自動的にデフォルトドメイン名を提供します。 ユーザー名を入力するだけです。

デフォルトのドメイン名、アカウントエイリアス、ドメインエイリアスは何ですか。 それらをどのように使用し管理しますか。

デフォルトドメイン名、アカウントエイリアスおよびドメインエイリアスについては、「用語」をご参照ください。

アカウントのデフォルトドメイン名、アカウントエイリアス、およびドメインエイリアスを表示および管理するには、 アカウントを利用するか、 RAM 権限を持つ RAM ユーザーとして RAM コンソールにログインします。[ID] > [設定] > [詳細な設定] > [ドメインエイリアス]の順にクリックします。

RAM ユーザーが Alibaba Cloud プロダクトを購入するのに必要な許可は何ですか？

- 従量課金プロダクトの場合、プロダクトインスタンスを作成する権限、または同様の権限が必要です。
- サブスクリプションプロダクトの場合、プロダクトインスタンスを作成する権限と支払いを行う権限 (AliyunBSSOrderAccess ポリシー) が必要です。

- 他のリソースを使用または作成して購入しなければならないプロダクトの場合は、対応するリソースを読み取りまたは作成するための許可が必要です。 次の例では、ECS インスタンスを作成するために必要な権限について説明します。

  次のポリシーでは、RAM ユーザーはコンソール、API、またはインスタンス起動テンプレートを使用して ECS インスタンスを作成できます。

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Action ": [
        " ecs : DescribeLa  unchTempla  tes ",
        " ecs : CreateInst  ance ",
         ecs : RunInstanc  es
        " ecs : DescribeIn  stances ",
        " ecs : DescribeIm  ages ",
        " ecs : DescribeSe  curityGrou  ps "
      ],
      " Resource ": "*",
      " Effect ": " Allow "
    },
    {
      " Action ": [
        " vpc : DescribeVp  cs ",
        " vpc : DescribeVS  witches "
      ],
      " Resource ": "*",
      " Effect ": " Allow "
    }
  ]
}
```

  ユーザーが ECS インスタンスを作成しているときにユーザーが他のリソースを使用または作成できるようにするには、リソースの種類に応じて次の権限をユーザーに付与します。 RAM コンソールにログインして、[ポリシー]をクリックします。 表示されたページで、カスタムポリシーを作成し、必要に応じてユーザーに権限を付与します。

操作	ポリシーアクション
スナップショットを使用した ECS インスタンスの作成	`ecs : DescribeSn  apshots`
VPC の作成と使用	`vpc : CreateVpc` `vpc : CreateVSwi  tch`
セキュリティグループの作成と使用	`ecs : CreateSecu  rityGroup` `ecs : AuthorizeS  ecurityGro  up`

操作	ポリシーアクション

インスタンス RAM の役割指定	`ecs : DescribeIn stanceRamR ole`
	
	`ram : ListRoles`
	
	`ram : PassRole`

鍵ペアの使用	`ecs : CreateKeyP air`
	
	`ecs : DescribeKe yPairs`

専用ホスト (DDH) 上に ECS インスタンスを作成します。	`ecs : AllocateDe dicatedHos ts`

ユーザーに許可を与えた後、ユーザーがシステムにアクセスしたときに、そのユーザーに許可がないことを示すメッセージが表示されるのはなぜですか。

- ユーザーに付加されているポリシーが正しいかどうかを確認します。
- 対応するリソースまたは操作のためにユーザーに付加されているカスタムポリシー (ユーザーのポリシーおよびユーザーのグループのポリシーを含む)で、`" Effect ": " Deny "` が設定されているかをチェックします。

  たとえば、ユーザーが AliyunECSReadOnlyAccess ポリシー (ECS にアクセスするための読み取り専用のアクセス許可を含む) と次のポリシーの両方を持っているとします。

  ```
  {
    " Statement ": [
      {
        " Action ": " ecs :*",
        " Effect ": " Deny ",
        " Resource ": "*"
      }
    ],
    " Version ": " 1 "
  }
  ```

  RAM 内の "拒否を優先する" 原則によると、ユーザーは ECS リソースを表示できません。

ユーザーが対応する許可なしに操作を実行できるのはなぜですか。

たとえば、ユーザーが必要なカスタムポリシー、または ECS の FullAccess または ReadOnly システムポリシーを持たず、ECS インスタンスを表示できる場合、次の操作を実行します。

1. ユーザーのグループポリシーに、ユーザーが対応する操作を実行できるようにする権限が含まれているかどうかを確認します。
2. ユーザーに関連付けられている他のポリシーに対応する権限が含まれているかどうかを確認してください。

たとえば、CloudMonitor のシステムポリシーが AliyunCloudMonitorFullAccess で、以下の権限を含むとします。`" ecs : DescribeIn  stances "` (ECS インスタンスの表示)、`" rds : DescribeDB  Instances "` (RDS インスタンスの表示) および `" slb : DescribeLo  adBalancer "` (SLB インスタンスの表示)。AliyunCloudMonitorFullAccess ポリシーをユーザーに添付した場合、そのユーザーには ECS、RDS および SLB インスタンスに関する情報を表示する権限があります。

更新管理のみを目的としてユーザーに許可を与えるにはどうすればよいですか。

統一された更新管理ポリシーは現在利用できません。 特定のプロダクトに応じてポリシーをカスタマイズする必要があります。 ユーザーにプロダクトの購入許可と支払い許可を与えることができます。

たとえば、ECS の更新管理をユーザーに実行させる場合は、 RAM ユーザーがAlibaba Cloud プロダクトを購入するために必要な権限をご参照ください。 必要な権限と AliyunBSSOrderAccess ポリシーをユーザーに付与します。

RAM ログインページ

日本サイトと国際サイトの RAM ログインページは下記のように、共通 URL を利用しているため、どのサイト(言語)を表示するかはブラウザが保持している cookie 情報に依存します。

https://signin-intl.aliyun.com/[UID]/login.htm

もし、cookie を保持していない場合、ログインページのヘッダー/フッターはデフォルトで国際サイトの表示となります。 一度日本サイトのアカウントでログインしたことがある場合、cookie の有効期限切れ、または削除されるまで日本サイトのログインページが表示されます。

2 STS に関するよくある質問

STS を使用するとエラーが発生する理由はなんですか。

次のエラーメッセージが表示された場合は、 AliyunSTSAssumeRoleAccess ポリシーが許可されているユーザーに関連付けられていないことを意味しています。

```
Error message : You are not authorized to do this
action . You should be authorized by RAM
```

AliyunSTSAssumeRoleAccess ポリシーを許可されているユーザーに添付してから、引き続き STS を使用します。

STS トークンにはどのような権限がありますか。

STS トークンの許可は、AssumeRole API が呼び出されたときにポリシーセットに含まれる指定されたロールの権限です。

AssumeRole API を呼び出すときにポリシーパラメータを設定しない場合、返された STS トークンは指定されたロールのすべての権限を持ちます。

STS トークンの有効期間はどれだけですか。

STS トークンの有効期間は 900 秒から 3600 秒です。 デフォルト値は 3600 秒です。
AssumeRole API を呼び出すときに DurationSeconds パラメーターを設定して、STS トークンの有効期間を制限できます。

STS API を呼び出すことができる回数に上限はありますか。

STS は最大毎秒 100 のクエリ (QPS) をサポートします。 通話要求が 100 QPS を超えると、エラーが報告されます。

複数の STS トークンが異なる時点で取得されている場合、新旧のトークンは同時に有効ですか。

新しい STS トークンと古い STS トークンはどちらも有効期限が切れるまで有効です。

3 RDS インスタンスをグループにタグ付けして権限を付与した後に、1 人または複数の RAM ユーザーの関連する権限がなくなった場合はどうすればいいですか。

この問題を解決するには、次の手順に従うことを推奨します。

1. タグが正しいインスタンスに添付されているかどうかを確認します。
2. ポリシーがインスタンスで正しいタグキーと値を使用しているかどうかを確認します。

   注：
   RDS インスタンスのタグキーと値に大文字を含めることはできません。 大文字を入力すると、タグキーと値を保存するときに自動的に小文字に変換されます。
3. RDS コンソールにログインしている RAM ユーザーにターゲットポリシーを適用したかどうかを確認します。
4. コンソールに表示されているリージョンが対象リージョンであるか確認します。
5. ターゲットタグの値を選択したかどうかを確認します。 ターゲット値を選択した後にのみ、システムは対応するリソースをフィルタリングできます。
6. RDS コンソールにログインしたら、RAM ユーザーにエラーメッセージウィンドウを閉じるように依頼します。

   注：
   多くの場合、エラーメッセージ "この操作を実行する権限がありません" が表示されます。コンソールにはデフォルトですべてのリソースが表示されますが、ユーザーにはすべてのリソースを表示する権限がないために発生します。