Alibaba Cloud
Resource Access Management

ユーザーガイド

Document Version20190906

目次

1 権限管理

1.1 ポリシーの概要

Alibaba Cloud では権限を使用して、特定のリソースにアクセスするための RAM ID (RAM ユーザー、ユーザーグループ、ロールなど) の許可アクションを記述します。 権限は、特定の条件下で一部のリソースに対して操作を実行できるかどうかを決定します。 ポリシーは一連のアクセス権限です。

権限

- アカウント (リソース所有者) がすべての権限を制御します。
  - 各リソースの所有者は 1 人だけです。 所有者がアカウントである必要があり、完全なリソース管理権限を持っています。
  - リソースの所有者がリソースの作成者ではない場合もあります。 たとえば、RAM ユーザーにリソースの作成権限がある場合、この RAM ユーザーが作成したリソースは RAM ユーザーのアカウントに属します。 RAM ユーザーはリソース作成者ですが、リソース所有者ではありません。
- RAM ユーザーにはデフォルトでは権限がありません。
  - RAM ユーザーは操作員であり、操作を実行する前に明示的な権限を付与されている必要があります。
  - 新しい RAM ユーザーはデフォルトで操作権限を持たず、権限が付与されるまではコンソールまたは API を介しリソースに対して操作を実行することはできません。
- リソース作成者 (RAM ユーザー) には、作成されたリソースに対する権限が自動的に付与されることはありません。
  - ユーザーにリソース作成権限が付与されている場合、RAM ユーザーはリソースを作成できます。
  - ただし、リソースの所有者がユーザーに明示的に権限を付与しない限り、RAM ユーザーには作成されたリソースに対する権限が自動的に付与されることはありません。

ポリシー

ポリシーは、 #unique_3に記載されている一連の権限です。 許可されているリソースセット、操作セット、およびユーザーに付与できる権限の条件を正確に記述できます。 ポリシーが添付さ

れていると、ユーザーまたはユーザーグループは、そのポリシーで指定されているアクセス権限を取得できます。 ポリシーに Allow 文と Deny 文の両方がある場合は、Deny が優先されます。

RAM では、ポリシーはユーザーが作成、更新、削除、および閲覧できるリソースエンティティです。 RAM は、以下の 2 種類のポリシーをサポートしています。

- システムポリシー：システムポリシーは Alibaba Cloud が提供する共通の権限のグループです。 権限には、読み取り専用権限、または一般に使用されているさまざまなプロダクトに対する完全な権限が含まれます。 ユーザーはシステムポリシーを変更できません。 ポリシーは Alibaba Cloud によって自動的にアップグレードされます。
- カスタマイズポリシー：システムポリシーが要件を満たしていない場合は、必要に応じてカスタマイズポリシーを作成できます。 たとえば、特定の ECS インスタンスに対する操作権限を制御する場合、またはリソース操作リクエストを指定の IP アドレスから発信する場合は、カスタマイズポリシーを使用する必要があります。

RAM ID への権限付与

RAM ID への権限付与は、RAM ユーザー、ユーザーグループ、またはロールに 1 つ以上のポリシーを添付することです。

- 添付されたポリシーはシステムポリシーまたはカスタマイズポリシーのどちらかです。
- 添付されたポリシーの更新時はポリシーへの更新が自動的に有効になるため、再度ポリシーを添付する必要はありません。

1.2 ポリシー言語

1.2.1 ポリシー要素

本ドキュメントでは、Alibaba Cloud リソースアクセスマネージメント（RAM）で権限を定義するために使用されるポリシーの要素について説明します。

要素

要素名	説明
Effect	ステートメントの結果が許可か、拒否のいずれになるかを指定します。 有効値： 許可 | 拒否
Action	操作対象となるリソースを指定します。
Resource	権限付与されるオブジェクトを指定します。

要素名	説明
Condition	ポリシーが有効になる時刻を指定します。

ポリシー要素の使い方

- Effect

   注：
  リクエストに適用されるポリシーに許可 `Allow` と拒否 `Deny` ステートメントが同時に含まれている場合、 `Deny` が `Allow` よりも優先されます。

  例：`" Effect ": " Allow "`

- Action

   注：
  ほとんどの場合、各 Alibaba Cloud サービスには独自の API アクションセットがあります。 詳細は、#unique_6 をご参照ください。

  形式：`< service - name >:< action - name >`

  - `service - name` ：Alibaba Cloud サービスの名前
  - `action - name : service` ：関連する API の名前

  例：`" Action ": [" oss : ListBucket s ", " ecs : Describe *", " rds : Describe *"]`

- Resource

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

  - `acs` ：Alibaba Cloud Service のイニシャル
  - `service - name` ：Alibaba Cloud サービスの名前
  - `region` ：リージョン情報。 この要素がサポートされない場合は、アスタリスク（`*`）を使用します。
  - `account - id` ：Alibaba Cloud のアカウント ID。例：`1234567890 12 ****`。 ID が不要、または利用できない場合、アスタリスクで置き換えることができます (`*`)。
  - `relative - id` ：サービス関連のリソース説明。 その意味は、特定のAlibaba Cloudサービスによって指定されます。 `relative - id` 要素はファイルパスに似て

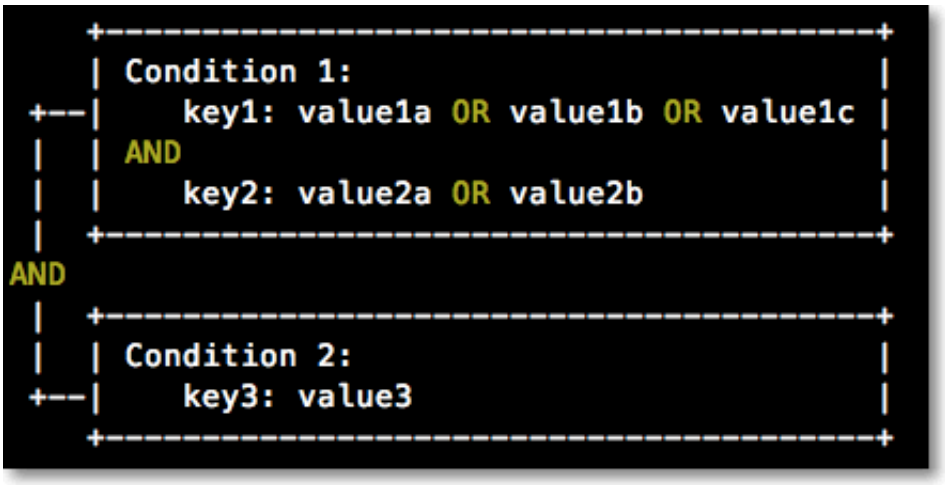
います。たとえば、`relative - id = " mybucket / dir1 / object1 . jpg "` という記述は OSS オブジェクトを示します。

例：`" Resource ": [" acs : ecs :*:*: instance / inst - 001 ", " acs : ecs :*:*: instance / inst - 002 ", " acs : oss :*:*: mybucket ", " acs : oss :*:*: mybucket /*"]`

- Condition

コンディションブロック（Condition Block）には複数の条件を含めることができ、各条件には複数のキーと値のペアを含めることができます。

図 1-1 : コンディションブロック



- 特に指定がない限り、すべてのキーは複数の値を持つことができます。 条件が評価されるときに、condition キーワードのランタイム値が対応する値のいずれかと一致すると、その条件は満たされます。
- 条件は、同じ操作タイプの複数の条件がすべて満たされた場合にのみ成立します。
- コンディションブロックが成立するのは、そのすべての条件が満たされる場合に限ります。

操作タイプ

以下のタイプの操作がサポートされています：文字列、数値、日付と時刻、ブール値、および IP アドレス。

操作タイプ	サポートされているタイプ
String	- StringEquals - StringNotEquals - StringEqualsIgnoreCase - StringNotEqualsIgnoreCase - StringLike - StringNotLike

操作タイプ	サポートされているタイプ
Numeric	- NumericEquals - NumericNotEquals - NumericLessThan - NumericLessThanEquals - NumericGreaterThan - NumericGreaterThanEquals
日付と時刻	- DateEquals - DateNotEquals - DateLessThan - DateLessThanEquals - DateGreaterThan - DateGreaterThanEquals
Boolean	Bool
IP アドレス	- IpAddress - NotIpAddress

条件キー

- 共通コンディションキーの形式は次のとおりです。

```
acs :< condition - key >
```

条件キー	データ型	説明
`acs : CurrentTim e`	日付と時刻	Web サーバーがリクエストを受信する日付と時刻。 このキーは ISO 8601 形式で定義されています。例： `2012 - 11 - 11T23 : 59 : 59Z` 。
`acs : SecureTran sport`	Boolean	HTTPS などセキュアチャネルを使用してリクエストを送信するかどうかを示します。
`acs : SourceIp`	IP アドレス	リクエストを送信するクライアントの IP アドレス。

条件キー	データ型	説明
acs : MFAPresent	Boolean	ユーザーログイン時にマルチファクター認証（MFA）を使用するかどうか示します。

- Alibaba Cloud サービス関連の条件キーの形式は次のとおりです。

```
< service - name >:< condition - key >
```

条件キー	Alibaba Cloud サービス	データ型	説明
ecs : tag /< tag - key >	ECS	String	ECS の tag-key のペア。 このキーは、カスタマイズすることができます。
rds : ResourceTag /< tag - key >	RDS	String	RDS の tag-key のペア。 このキーは、カスタマイズすることができます。
oss : Delimiter	OSS	String	OSS がオブジェクト名をグループ化するときに使用する区切り文字。
oss : Prefix	OSS	String	OSS オブジェクト名のプレフィックス。

1.2.2 ポリシー構造と構文

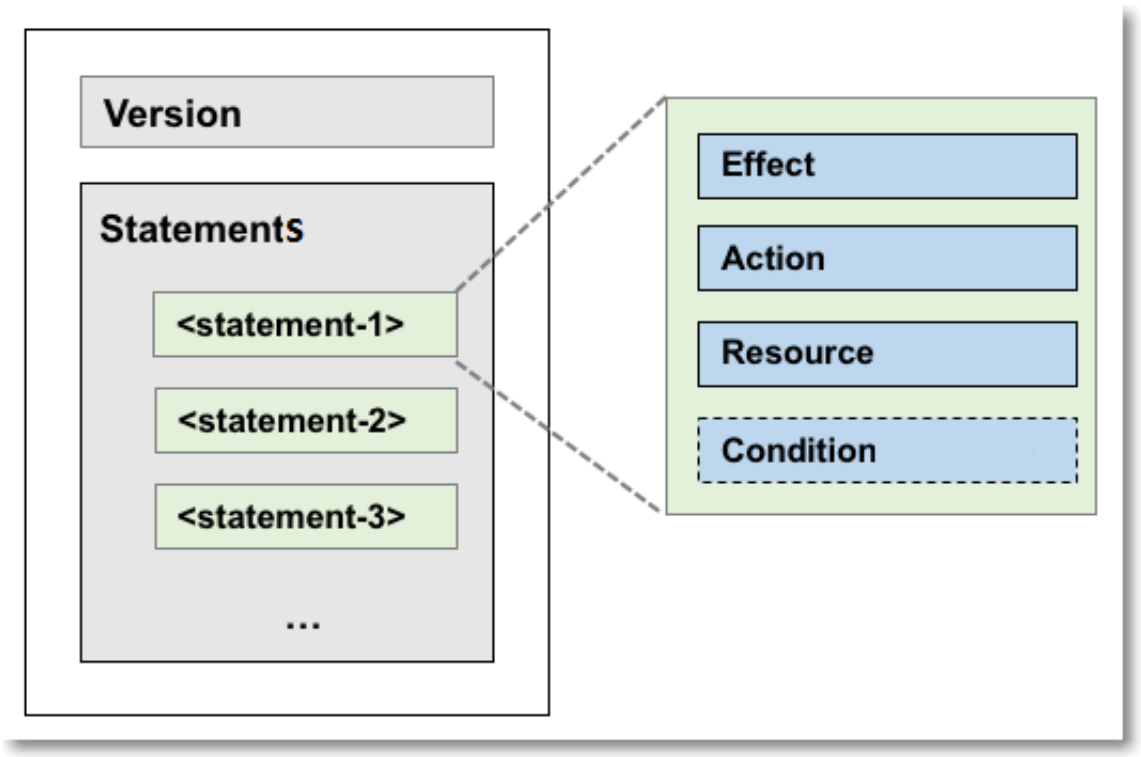
このトピックでは、Alibaba Cloud RAM で使用されるポリシーの構造、構文、およびルールについて説明します。

ポリシー構造

ポリシー構造には、バージョン番号および文の一覧が含まれます。

各文には、Effect、Action、Resource、および Condition という要素が含まれます。 条件要素は省略可能です。

図 1-2 : ポリシー構造



ポリシー構文を使用するにあたっての注意点

ポリシーの構文を使用する前に、その文字とルールを理解する必要があります。

- ポリシー文字 :
  - ポリシー内の JSON 文字には `{ } [ ] " , :` が含まれます。
  - ポリシーの構文の記述に使用される特殊文字には、`= < > ( ) |` が含まれます。
- ポリシー文字を使用する場合のルール :
  - 要素に複数の値が必要な場合は、各値を区切るための区切り文字としてコンマ (,) が使用され、その他の値の記述には省略記号 (...) が使用されます。 たとえば、`[ < action_str ing >, < action_str ing >, ...]` などです。

> 注 :

> 複数の値をサポートする要素は単一の値もサポートします。つまり、" Action ": [< action_str ing >] および " Action ": < action_str ing > の 2 つの記述は同等です。

- 構文内に疑問符 (?) が付いている要素は、それが省略可能な要素であることを示します (例 : < condition_ block ?>)。
- 構文で複数の値が縦線で区切られている場合は、(|) どちらか 1 つの値だけが選択可能です (例 : (" Allow " | " Deny "))。
- 二重引用符 ("") で囲まれた要素はテキスト文字列です (例 : < version_bl ock > = " Version " : (" 1 "))。

ポリシー構文

ポリシーの構文の例は以下のとおりです。

```
 policy   = {
     < version_bl  ock >,
     < statement_  block >
}
< version_bl  ock > = " Version " : (" 1 ")
< statement_  block > = " Statement " : [ < statement >, < statement
 >, ... ]
< statement > = {
    < effect_blo  ck >,
    < action_blo  ck >,
    < resource_b  lock >,
    < condition_  block ?>
}
< effect_blo  ck > = " Effect " : (" Allow " | " Deny ")
< action_blo  ck > = (" Action " | " NotAction ") :
    ("*" | [< action_str  ing >, < action_str  ing >, ...])
< resource_b  lock > = (" Resource " | " NotResourc  e ") :
    ("*" | [< resource_s  tring >, < resource_s  tring >, ...])
< condition_  block > = " Condition " : < condition_  map >
< condition_  map > = {
  < condition_  type_strin  g > : {
      < condition_  key_string > : < condition_  value_list >,
      < condition_  key_string > : < condition_  value_list >,
      ...
  },
  < condition_  type_strin  g > : {
      < condition_  key_string > : < condition_  value_list >,
      < condition_  key_string > : < condition_  value_list >,
      ...
  }, ...
}
< condition_  value_list > = [< condition_  value >, < condition_
 value >, ...]
< condition_  value > = (" String " | " Number " | " Boolean ")
```

説明 :

・ バージョン : 現在のポリシーバージョンは 1 です。

- 文 : ポリシーには複数の文を記述できます。
  - 各文は `Allow` または `Deny` のどちらかにすることができます。

     注 :
    文では、Action 要素と Resource 要素の両方に複数の値を指定できます。
  - 各文は独自の条件をサポートします。

     注 :
    条件ブロックには、操作タイプが異なる複数の条件とそれらの条件の論理的な組み合わせを含めることができます。
- Deny が有効になります。ユーザーに複数のポリシーを付与できます。 これらのポリシーに `Allow` 文と `Deny` 文が両方記述されている場合は、 `Deny` が優先 (`Allow` 文は `Deny` 文に上書き) されます。
- 要素値 :
  - 要素値が数値またはブール値の場合は、文字列などの二重引用符 ("") を使用して囲む必要があります。
  - 要素の値が文字列の場合は、あいまい一致にアスタリスク (*) などの文字および疑問符 (?) を使用できます。

    ■ アスタリスク (*) は、任意の数 (ゼロを含む) の許容文字数を示します。

     注 :
    たとえば `ecs : Describe *` は、Describe で始まるすべての ECS アクションを示します。

    ■ 疑問符 (?) は、使用可能な 1 つの文字を示します。

ポリシー形式のチェック

RAM ポリシーは JSON 形式で表現する必要があります。 ポリシーを作成または更新すると、RAM はまず JSON 形式が正しいかどうかをチェックします。

- JSON 構文標準の詳細は、「RFC 7159」をご参照ください。
- JSON の検証ソフトやエディターなどのツールを使用して、JSON構文標準を満たすためのポリシーを検証するよう推奨します。

2 ユーザーガイド

2.1 概要

『RAM ユーザーガイド』には、RAM プロダクトの主要機能と適用シナリオが詳しく記載されています。

主要機能

ID

- #unique_10
- #unique_11
- #unique_12

権限付与

- #unique_13
- #unique_14
- #unique_15

典型的な適用シナリオ

- #unique_16
- #unique_17
- #unique_18

2.2 セキュリティ設定

セキュリティ設定により、RAM ユーザーのログインパスワード、およびアクセスモードの設定が行えます。

ログインパスワード設定

1. RAM コンソールで、[ID] > [設定] の順にクリックします。
2. [セキュリティ設定] タブページで、[パスワードルールの編集] をクリックします。
3. [パスワードの長さ]、[パスワードの必須要素]、[パスワード有効期間] および [パスワードの再試行制限ポリシー] などのルールを定義し、[OK] をクリックします。

注：

設定完了後、これらの設定はすべての RAM ユーザーに適用されます。

ユーザーセキュリティ設定

1. RAM コンソールで、[ID] > [設定] の順にクリックします。
2. [セキュリティ設定] タブページで、[RAM ユーザーセキュリティ設定の更新] をクリックします。
3. 必須設定を変更して、[OK] をクリックします。

2.3 ドメイン名管理

各アカウントにはデフォルトドメインがあります。 アカウントにドメインエイリアスを設定することもできます。 具体的には、ドメイン名管理機能を介してログイン名サフィックスをカスタマイズできます。 その後、RAM ユーザーはデフォルトのドメイン名またはドメインエイリアスを使用してコンソールにログインできます。

RAM ユーザーがコンソールにログインするにあたっての注意点

RAM ユーザーは、RAM コンソールの ユーザー ページのログインユーザー名などユーザープリンシパル名 (UPN) 形式のログインアカウントでログインする必要があります。

RAM ユーザーは、RAM ユーザーのログインページで以下のうちどちらかのログイン方法を選択できます。

- <$username>@<$AccountAlias>.onaliyun.com
- <$username>@<$AccountAlias>

RAM ユーザーログインエントリ

RAM ユーザーと Alibaba Cloud アカウントのログインエントリは異なります。

RAM ユーザーのログインエントリ : https://signin.alibabacloud.com/login.htm。

注 :
ログインリンクは RAM コンソールにログイン後 概要 のページからご利用いただくことも可能です。

ドメイン名管理

デフォルトドメイン名

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] > [詳細] をクリックしてデフォルトドメイン名を閲覧または変更します。
   - デフォルトドメインの形式は <$AccountAlias>.onaliyun.com です。
   - アカウントエイリアスを設定していない場合は、デフォルトでアカウント ID が使用されます。 この場合、ドメインエイリアス の形式は <$AccountID>.onaliyun.com です。

ドメインエイリアス

デフォルトのドメイン名に加えて、自分のアカウントにドメインエイリアスを設定することもできます。

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] > [詳細] をクリックしてドメインエイリアスを閲覧します。
3. [ドメインエイリアスを作成] をクリックします。
4. ドメイン名を入力します。
5. [OK] をクリックします。
6. [ドメインの所有権の確認] をクリックします。

> 注 :
> ドメインエイリアスが作成されたら、確認コードをコピーしてドメイン購入プラットフォームに DNS TXT レコードを貼り付けます。 設定が完了したら、ドメインの所有権を確認します。

次のステップ

ドメインエイリアスを作成してシングルサインオン (SSO) を設定する方法については、「フェデレーション SSO の概要 (Federated SSO overview)」をご参照ください。

ドメインエイリアスの管理方法の詳細は、「アカウントの SAML を (Configure the SAML of an account)」をご参照ください。

2.4 権限付与管理

2.4.1 ポリシーの例

本ドキュメントでは、ポリシーを作成する方法、関連する基本要素、ポリシー構造、およびポリシー構文の詳細について説明します。

以下に、2 つのステートメントを含むポリシーの例を示します。

- 最初のステートメントは、中国 (杭州) リージョンのすべての ECS リソースを表示する (`ecs : Describe *`) 権限を付与します。
- 2 番目のステートメントは、OSS バケット mybucket 内のオブジェクトにアクセスする 2 つの読み取り専用権限 (`oss : ListObject  s` および `oss : GetObject`) を付与し、ソース IP アドレスが `192 . 168 . 0 . 0 / 16` または `172 . 12 . 0 . 0 / 16` のリソースへのアクセスだけを許可するステートメントです。

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": " ecs : Describe *",
            " Resource ": " acs : ecs : cn - hangzhou :*:*"
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: mybucket ",
                " acs : oss :*:*: mybucket /*"
            ],
            " Condition ":{
                " IpAddress ": {
                    " acs : SourceIp ": [" 192 . 168 . 0 . 0 / 16 ", "
 172 . 12 . 0 . 0 / 16 "]
                }
            }
        }
    ]
}
```

2.4.2 RAM での権限付与

本ドキュメントでは、Alibaba Cloud アカウントで 1 つまたは複数のポリシーを RAM ID（つまり、RAM ユーザー、RAM ユーザーグループ、または RAM ロール）にアタッチする方法について説明します。

シナリオ

- RAM ユーザーに権限を付与することは、主に Alibaba Cloud アカウントのユーザーに権限を付与して、ユーザーが必要なリソースにアクセスできるようにすることを意味します。
- RAM ユーザーグループへの権限付与は、主に Alibaba Cloud アカウントのグループへの権限付与を意味します。 ユーザーグループに権限を付与すると、そのグループ内のすべてのユーザーが同じ権限を共有されます。
- RAM ロールへの権限の付与は、主に、スタンドアロンの操作およびアプリケーションへの権限の付与、たとえば、モバイルデバイスアプリケーションの一時的な権限付与、クロスアカウ

ントリソースの権限付与、クラウドアプリケーションの動的な ID および権限管理、クラウドサービス間の操作の権限などです。

RAM に権限を付与する前に

RAM コンソール にログインします。

RAM ユーザーへの権限付与

1. RAM コンソールにログインし、ID > ユーザー をクリックします。
2. ユーザー名 / 表示名 列で、権限付与するユーザーを特定し、権限の追加をクリックします。
3. 左側の ポリシー名 列で、対象のポリシーを選択して OK をクリックします。

> 注 :
> ポリシーを削除するには、右側のエリアからポリシーを選択して、 X をクリックします。

ユーザーグループへの権限付与

1. RAM コンソールにログインし、ID > グループ をクリックします。
2. グループ名/表示名 列で権限を付与するユーザーグループを見つけて 権限の追加 をクリックします。
3. 左側の ポリシー名 列で、対象のポリシーを選択して OK をクリックします。

> 注 :
> ポリシーを削除するには、右側のエリアからポリシーを選択して、 X をクリックします。

RAM ロールへの権限付与

RAM ロールを作成する場合は、信頼できるエンティティを Alibaba Cloud アカウント (現行 Alibaba Cloud アカウントまたは他の Alibaba Cloud アカウント) 、Alibaba Cloud サービス、または IdP として選択できます。 対応する信頼できるアカウント ID を入力して、信頼できるサービスを選択するか、必要に応じて信頼できる ID プロバイダー（IdP）を選択する必要があります。

- Alibaba Cloud アカウント と 現行 Alibaba Cloud アカウント を選択した場合、現行アカウントの RAM ユーザーは RAM ロールを引き受け可能なため、必要なクラウドリソースへのアクセスが許可されます。
- Alibaba Cloud アカウント と その他の Alibaba Cloud アカウントを選択した場合、他の指定済みのアカウントの RAM ユーザーは RAM ロールを引き受け可能なため、必要なクラウドリソースへのアクセスが許可されます。

- Alibaba Cloud サービスを選択した場合、信頼できるクラウドサービスは RAM ロールを引き受け可能なため、必要なクラウドリソースへのアクセスが許可されます。
- IdP を選択した場合、信頼できる IdP のユーザーは RAM ロールを引き受け可能です（つまり、必要なクラウドリソースへのアクセスが許可されます）。

1. RAM コンソールにログインして、RAM ロール をクリックします。
2. ロール名 列で対象の RAM ロールを見つけて 権限の追加 をクリックします。
3. 左側の ポリシー名 列で、対象のポリシーを選択して OK をクリックします。

> 注：
> ポリシーを削除するには、右側のエリアからポリシーを選択して、 X をクリックします。

2.5 RAM ユーザーの設定

このページでは、RAM ユーザー同期ツールを使用して Microsoft Active Directory (AD) または LDAP ディレクトリから RAM にユーザーを同期する方法について説明します。

前提条件

- Alibaba Cloud にトライアルを申し込み済み。
- RAM ユーザー同期ツールのインストール先のサーバーは Windows サーバーであること。

RAM ユーザー同期ツールの設定

RAM ユーザー同期ツールをインストールしてから、以下のステップを実行してツールを設定します。

1. ローカル IdP サービスアドレスを設定します。
2. IdP ディレクトリデータを読み取るために、同期ツールのユーザーアカウント (ユーザー名とパスワード) を設定します。

> 重要：
> ユーザーに AD の読み取り権限を付与する必要があります。

3. Alibaba Cloud RAM API を呼び出すために、同期ツール用の AccessKey を設定します。

> 重要：
> 関連する RAM API 権限を取得した RAM ユーザーの AccessKey を使用することを推奨します。

2.6 ID

2.6.1 ユーザー

RAMユーザーは、ユーザーやアプリケーションなどのIDと関連付けるためのRAMで使用されるIDです。 新しいユーザーまたはアプリケーションがクラウドリソースにアクセスできるようにするには、 RAMユーザーに権限を作成して付与することが必要です。 一般的な手順は次のとおりです。

1. プライマリアカウント（またはRAM操作権限を持つRAMユーザー）を使用して、RAMコンソールにログインします。
2. RAMユーザーを作成し、ユーザーを複数のグループに追加します。
3. 複数の権限付与ポリシーをユーザー（またはユーザーが所属するグループ）に追加します。
4. ユーザーの権限を作成します。 ユーザーがコンソールを使用して操作を行う場合は、ユーザーのログインパスワードを設定する必要があります。 ユーザーがAPIを呼び出し操作を行う必要がある場合は、そのユーザーのためにAPI AccessKeyを作成する必要があります。
5. ユーザーが特別な権限（ECSインスタンスを停止するなど）を使用する必要がある場合は、そのユーザーのためにMFAを設定し、ユーザーにMFAパスワードを使用してAlibaba Cloudコンソールにログインするよう要求できます。
6. ログインURL、ユーザー名、およびログインパスワードをユーザーに提供します。

RAM設定

- RAMコンソールで
- パスワードポリシーの設定
- セキュリティポリシーの設定

RAMコンソールで

1. エンタープライズ別名を設定するには、設定 > ユーザーの別名の設定 > ユーザーの別名の編集.
2. エンタープライズ別名を入力してOKをクリックします。

パスワードポリシーの設定

手順は次のとおりです。

1. RAMコンソールで、設定 > パスワードの強度の設定.

2. ページの指示に従って、パスワードの長さ、文字列のフォーマット、有効期限、再入力回数ポリシーなどを設定し、変更の保存をクリックして設定を有効にします。

> 注：
> パスワードポリシーが有効になると、 これ以降作成されるあらゆるRAMユーザーはパスワードの強度設定に従わなければなりません。

セキュリティポリシーの設定

1. RAMコンソールで、設定 > サブユーザーのセキュリティ設定.
2. サブユーザーのセキュリティ設定では、セキュリティポリシーを設定し、
3. 変更の保存をクリックしてください。

RAMユーザーの作成

操作手順は下記の通りです。

1. RAMコンソールで、 ユーザー > 新規ユーザー.
2. ダイアログボックスにユーザー情報を入力してOKをクリックします。

RAMユーザー作成後、必要に応じて次の操作を実行できます：

- ログインパスワードの設定
- AccessKey の作成
- 仮想MFAデバイスの有効化

ログインパスワードの設定

RAMユーザーをRAMコンソールにアクセスできるようにするには、ユーザーのログインパスワードを設定します。 手順は次のとおりです。

1. RAMコンソールの左側のユーザーをクリックします [ユーザー管理] ページで、ログイン名を選択します。 ログイン名、または管理をクリックします
2. ユーザーの詳細ページで、コンソールへのログインの有効化をクリックします。

図 2-1 : ログインパスワードの設定

3. ポップアップウィンドウで、ユーザーの初期パスワードを設定できます。 ログイン時の強制的なパスワード変更を指定できます。

AccessKey の作成

APIを呼び出す必要のあるユーザーにAccessKeyを作成するには、次を参照してください：

1. RAMコンソールで、ユーザーをクリックします。 [ユーザーの詳細]ページを開き、ログイン名を選択します。 ログイン名または管理をクリックします。
2. ユーザーの詳細ページで、 AccessKeyの作成をクリックします。
3. ダイアログボックスに新しいAccessKey情報を確認し、AK情報を保存をクリックします。

> 注 :
>
> - 新しいAccessKeyは作成の段階にのみ表示されます。 セキュリティ上の理由から、RAMはAccessKeyクエリインターフェイスを提供しません。 よって、AccessKeyは安全な場所に保管してください。
> - AccessKeyを公開したり、紛失した場合は、新しく作成する必要があります。

仮想MFAデバイスの有効化

マルチファクタ認証（MFA）は、シンプルで効果的なベストプラクティスであり、更なるセキュリティ保護を提供できます。 MFAを有効にし、 ユーザーがAlibaba Cloudにログインするには、まずユーザー名とパスワードの入力を要求されます（第1セキュリティーファクター）、 そしてVMFAによって提供される可変検証コード（第2セキュリティーファクター）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。

仮想MFA（VMFA）デバイスは、6桁の確認コードを生成するアプリケーションです。 これは、時間ベースのワンタイムパスワードアルゴリズム（TOTP）標準 （RFC 6238）に準拠しています。 このアプリケーションはスマートフォンを含むモバイルハードウェアデバイス上で実行でき、簡単にアクセスできます。

RAMユーザーの仮想MFAデバイスを有効にするには、次の手順に従ってください :

1. RAMコンソールにログインし、左側のメニュでユーザーをクリックしてください [ユーザー管理]ページで、ログイン名を選択します。 ログイン名または管理をクリックします。
2. ユーザーの詳細ページで、 VMFAデバイスの有効化をクリックします。

図 2-2 : MFAの設定

RAMユーザーのログイン

ログイン画面

RAMユーザーはAlibaba Cloudアカウントとは異なるため、ログインポータルが異なります。 RAMユーザーはAlibaba Cloudアカウントのログインページからログインできません。

RAMユーザーのログインページ：https://signin.aliyun.com/login.htm（ログインページをダッシュボードにて確認できます。）

ログイン情報

RAM ユーザーとしてログオンするには、エンタープライズエイリアス、サブユーザー名、パスワードが必要です。

エンタープライズエイリアスはRAM初期設定で設定したものです。 エンタープライズエイリアスを設定していない場合は、デフォルト設定としてクラウドアカウントID名を使いします。（次のパスで確認できます。アカウント管理 > セキュリティ設定.

注：
デフォルト設定では、RAMユーザには一切のアクセス権限がありません。 権限のないRAMユーザーはコンソールにログインできますが、操作は実行できません。 RAMユーザーに権限を与える方法の詳細については、 #unique_14を参照してください。

RAMユーザーの削除

注：
RAM ユーザーを削除する前によく考えてください。 ユーザーが特定のサービスを実行している場合、このユーザーを削除するとサービスが失敗になる可能性があります。

RAMユーザーを削除するには、次の手順を参照してください：

1. RAMコンソールにログインし、左側のメニューでユーザーをクリックして、ユーザー管理ページを開きます。
2. 目標RAMユーザーを選定し、操作列での削除をクリックします。

   図 2-3 : RAMユーザーを削除します。

3. ユーザーの削除のダイアログボックスで、関連付けの強制削除チェックボックスをチェックし、OKをクリックします。

   図 2-4 : 削除操作を確認します。

2.6.2 グループ

Alibaba Cloud アカウントで多数の RAM ユーザー を作成した場合は、ユーザーとその権限を管理しやすくするために、グループ単位でユーザーを管理することをお勧めします。 同じ責任を持つユーザーをグループに追加し、#unique_14します。 そのメリットは次の通り：

- 特定ユーザーの責任が変更された場合、他のユーザーに影響せず、適切なグループに移動することができます。
- グループの権限が変更された場合、そのグループの権限付与ポリシーを調整するだけですべてのユーザーに適用できます。

本ドキュメントでは次の各項目について説明します：

- グループの作成
- グループメンバーの管理
- グループ名の変更
- グループの削除
- グループに権限を付与

グループの作成

操作手順は次の通り：

1. RAMコンソールの ホームページで、[グループ管理] > [新規グループ].
2. グループ名を入力してOKをクリックします。

グループメンバーの管理

操作手順は次の通り：

1. RAMコンソールのホームページで、グループ管理をクリックします。
2. グループ管理ページで、操作列の管理をクリックすることで、グループメンバーを管理できます。

- グループメンバの追加：

  1. グループリストで管理したいグループを検索し（グループ名でファジークエリ可能）、[操作]列でグループメンバーの編集をクリックします。
  2. 左側のボックスでグループに追加したいユーザーを選定し（キーワードで検索可能）、右矢印をクリックすることで右側のボックスに移動できます。ユーザーを元に戻すには左矢印をクリックしてください。
  3. OKをクリックします。

・ グループメンバーの削除：

1. グループリストで管理したいグループを検索し（グループ名でファジークエリ可能）、グループ名をクリックします。
2. グループメンバー管理セクションで、グループから削除をクリックすることでユーザーをグループから削除できます。

グループ名の変更

操作手順は次の通り：

1. RAMコンソールのホームページで、グループ管理をクリックします。
2. グループリストでグループ名を変更したいグループを検索し（グループ名でファジークエリ可能）、グループ名または管理をクリックしてグループの詳細ページを開きます。
3. 基本情報の編集をクリックします。
4. グループ名を入力してOKをクリックします。

グループの削除

操作手順は次の通り：

1. RAMコンソールのホームページで、グループ管理をクリックします。
2. グループリストで削除したいグループを検索し（グループ名でファジークエリ可能）、グループ名または操作列での削除をクリックします。

> 注：
> グループにグループメンバーが存在する場合や、権限付与ポリシーがバインドされている場合は、 関連付けの強制削除のチェックボックスにチェックを付けないと削除できません。

グループに権限を付与

グループに権限を付与するには、#unique_14を参照してください。

2.6.3 RAM ロール

RAM ロールは、仮想ユーザーを象徴する RAM ID です。 RAM ロールには長期のパスワードや AccessKey はなく、信頼できるエンティティがコンソールまたは API を介して使用することができます。

> 注：
> 特に指定しない限り、本ドキュメントでの「ロール」は「RAM ロール」を指します。

関連する概念

次の図に、RAM ロールに関連する概念間の関係を示します。

図 2-5 : RAM ロールに関連する概念

表 2-1 : RAM ロール概念の説明

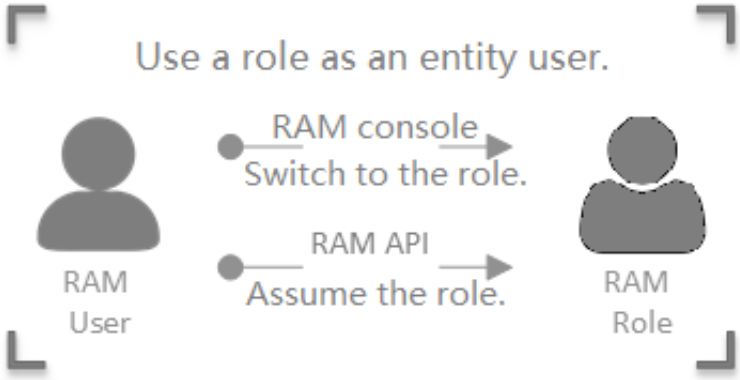
概念	説明
ARN	Alibaba Cloud リソース名（ARN）は、ロールのグローバルリソース ID です。 ロールを指定する場合に使用します。 ・ ARN は Alibaba Cloud ARN の命名規則に準拠します。 例：Alibaba Cloud アカウントの下にあるロールの DevOps の ARN は `acs : ram :: 1234567890 123456 : role / samplerole` です。 ・ ロールを作成後、ロール名をクリックし [基本情報] のエリアでそのロールの ARN を見つけます。
信頼できるエンティティ	信頼できるエンティティとは、ロールの引き受けが可能な信頼できるエンティティユーザーの ID です。 ・ ロールをの作成時に信頼できるエンティティを指定する必要があります。 信頼できるエンティティだけがロールを引き受けることができます。 ・ 信頼できるエンティティは、信頼できる Alibaba Cloud アカウントまたは Alibaba Cloud サービスであることが可能です。

概念	説明
ポリシー	ロールは一連のポリシーに関連付けることができます。 ロールをどのポリシーにも関連付けないままにすることは可能ですが、そのロールはリソースにはアクセスできません。
ロールの引き受け	ロールの引き受けは、エンティティユーザーがロールのセキュリティトークンを取得するための方法です。 エンティティユーザーは、`AssumeRole` API を呼び出すことでロールのセキュリティトークンを取得し、そのトークンを使用して Alibaba Cloud サービス API にアクセスできます。
ID の切り替え	ID の切り替えは、エンティティユーザーが RAM コンソールでログイン ID からロール ID に切り替えることができるメソッドです。 ・ RAM コンソールにログイン後、エンティティユーザーは引き受け可能なロールに切り替えることができます。 切り替え後、ユーザーはそのロール ID を使用して Alibaba CLoud リソースを操作できます。 ・ そのロール ID が必要なくなったら、ユーザーは自身のログイン ID に戻ることができます。
ロールトークン	ロールトークンは、ロール ID の一時的な AccessKey です。 RAM ロールには特定の ID 認証キーがありません。 エンティティユーザーは、ロールを使用する場合そのロールを引き受けてロールトークンを取得する必要があります。 その後、ユーザーはロールトークンを使用して Alibaba Cloud サービス API を呼び出すことができます。

説明

RAM ロールは、信頼されたエンティティユーザーによって引き受けられた後にのみ使用できます。

図 2-6 : RAM ロールの使用



RAM ロールとテキストブックロール（Textbook-Role）の違い：

- 仮想ユーザーとして、RAM ロールは特定の ID を持ち、一連のポリシーを付与できます。 ただし、RAM ロールには特定の ID 認証キー（ログインパスワードまたはアクセスキー）はありません。
- テキストブックロール（または伝統的な定義済みロール）は、RAM 内のポリシーと同様に、権限セットを示します。 そのようなロールがユーザーに付与されている場合、そのユーザーは一連の権限を持ち、許可されたリソースにアクセスできます。

エンティティユーザーと仮想ユーザーの違い：

- エンティティユーザーには、特定のログインパスワードまたはアクセスキーがあります。 アカウント、RAM ユーザーアカウント、および Alibaba Cloud サービスアカウントは、すべてがエンティティユーザーです
- 仮想ユーザーには特定の認証キーがありません。 RAM ロールはエンティティユーザーにより引き受ける必要があります。

RAM ロールタイプ

RAM ロールは、信頼できるエンティティのタイプにより以下のように分類されます。

- ユーザロール：RAM ユーザーが引き受けられるロール。 RAM ユーザーは、自分の Alibaba Cloud アカウントまたは他のアカウントに属している可能性があります。 このようなロールにより、クロスアカウントアクセスと一時的な権限付与に対するソリューションが提供されます。
- サービスロール ：Alibaba Cloud サービスが引き受けられるロール。 そのようなロールは、Alibaba Cloud サービスにリソースに対する操作する権限を付与するときに使用されます。

RAM ロールを作成します。

RAM コンソールで RAM ロールを作成するには、次の手順を実行します。

1. ロールタイプを選択します。
2. 信頼できるエンティティを選択します。
3. ロール名を入力します。
4. ロールにポリシーをアタッチします。

ユーザー用に RAM ロールを作成

1. RAM コンソール にログインします。
2. 左側のナビゲーションウィンドウで、[ロール] をクリックします。

3. 表示されたページで、ロールの作成 をクリックします。
4. ユーザーロールを選択します。
5. 信頼できる Alibaba Cloud アカウントを選択して、次へ をクリックします。
   - ご自身の Alibaba Cloud アカウントで RAM ユーザーのロールを作成するには、現行 Alibaba Cloud アカウント を選択します。
   - 別の Alibaba Cloud アカウントで RAM ユーザーのロールを作成するには、その他の Alibaba Cloud アカウント を選択してアカウント ID を入力します。
6. ロール名 にロールの名前を入力します。 説明 フィールドに説明を入力することもできます。次に、作成 をクリックします。

   注：
   - RAM ロールを作成後、権限付与 をクリックしてロールに権限を付与できます。 詳細は、#unique_31 をご参照ください.
   - RAMロールを作成後、ロール名 列でロール名をクリックするか、または操作列で管理をクリックしてロールの詳細を表示できます。

Alibaba Cloud サービス用の RAM ロールを作成

1. RAM コンソール にログインします。
2. 左側のナビゲーションウィンドウで、ロール をクリックします。
3. 表示されたページで、ロールの作成 をクリックします。
4. サービスロール をクリックして、信頼できる Alibaba Cloud サービスを選択します。 利用可能なサービスは次のとおりです。
   - メディアトランスコーディングサービス（MTS）：ロールを作成し、MTS を信頼済みサービスとして構成し、MTS タスクのデータソースとして OSS バケットを設定すると、MTS

を使用してロールを引き受け、Object Storage Service（OSS）データにアクセスできます。

- アーカイブストレージ：OSS バケットをアーカイブストレージのデータソースとして設定すると、ロールを作成し、アーカイブストレージを信頼できるサービスとして設定し、アーカイブストレージを使用してロールを引き受けて OSS データにアクセスできます。
- Log Service： ロールを作成し、Log Service を信頼できるサービスとして構成し、Log Service で収集したログを OSS にインポートするときに、そのロールを引き受け、データを OSS に書き込むことができます。
- API Gateway： ロールを作成し、ApiGateway を信頼できるサービスとして設定し、API Gateway のバックエンドサービスとして機能サービスを設定する場合に API Gateway を使用してロールを引き受け、機能サービスを呼び出すことができます。
- Elastic Compute Service（ECS）：ロールを作成し、このロールを使用して ECS に他の Alibaba Cloud サービス内のリソースへのアクセスを許可することができます。

 注：

信頼できるサービスの詳細は、RAM コンソールをご参照ください。

5. ロール名 フィールドにロールの名前を入力します。 説明 フィールドに説明を入力することもできます。 次に、作成 をクリックします。

 注：

- ロールを作成後、権限付与 をクリックしてこのロールに権限を付与します。 詳細は、#unique_31 をご参照ください.
- RAM ロールを作成後、ロール名 列でロール名をクリックするか、操作 列で 管理 をクリックしてロールの詳細を表示できます。

RAM ロールの使用

Alibaba Cloud サービス用に作成されたロールは、信頼できる Alibaba Cloud サービスによってのみ引き受けることができ、ユーザー用に作成されたロールは、RAM ユーザーによって引き受けることができます。

1. RAM ユーザーを作成して AccessKey を作成するか、ユーザーのパスワードを設定します。
2. システムポリシー AliyunSTSAssumeRoleAccess をアタッチして RAM ユーザーに権限を付与します。

 注：

アカウントのセキュリティを維持するために、信頼できる Alibaba Cloud アカウントはロール自体を引き受けることを許可されていません。 代わりに、Alibaba Cloud アカウントの RAM ユーザーがロールを引き受ける必要があります。

RAM ユーザーは、RAM コンソールまたは API を介してロールを引き受けることができます。

- RAM コンソールで RAM ロールを引き受けます。

  エンティティユーザーが RAM ロールを引き受ける場合は、エンティティユーザーは RAM コンソールにログインしてロールを切り替える必要があります。

  1. RAM ユーザーとして RAM コンソールにログインします。
  2. 右上のアカウントアイコンの上にポインタを移動し、ロールの切り替え をクリックします。
  3. 表示された ロールの切り替え ダイアログボックスでアカウントのエイリアスとロール名を入力後、切り替え をクリックします。

     注：

     - ロールを切り替えすると、新しい RAM ロールを持つ RAM ユーザーとしてコンソールにログインできます。 この場合、現在のロールと ID、およびログイン ID の両方がコンソールの右上角に表示されます。
     - ロールを切り替えた後実行できるのはこのロールに許可されている操作だけです。 コンソールにログインすると、元の ID のアクセス権限は隠されます。
  4. 切り替えられたログインユーザー をクリックしログイン ID に戻ります。

     注：
     ログイン ID に切り替えると、元の権限を取得し、ロールに関連付けられている権限を失います。

- API を呼び出して RAM ロールを引き受けます。

  RAM ユーザーに AssumeRole アクセス許可が付与された後、ユーザーは AccessKey を使用してセキュリティトークンサービス（STS）の `AssumeRole` API を呼び出して、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。 次に、ユーザーはトークンを使用して Alibaba Cloud リソース API にアクセスします。

  `AssumeRole` API を呼び出す方法の詳細は、 #unique_32 をご参照ください。

RAM ロールが適用可能なシナリオ

- #unique_33

- #unique_34

2.7 権限付与

2.7.1 ポリシーの概要

ポリシーを作成し、それらを RAM ID（RAM ユーザー、RAM ユーザーグループ、RAM ロール）または Alibaba Cloud リソースにアタッチすることで、Alibaba Cloud でアクセスを管理できます。 ポリシーは、ID またはリソースに関連付けられている場合、それらの権限を定義します。 ポリシー内の権限によって、RAM ユーザーまたは RAM ロールのリクエストを許可するか拒否するかが決まります。

権限

- アカウント (リソース所有者) がすべての権限をコントロールします。
  - 各リソースの所有者は 1 人だけです。 所有者が Alibaba Cloud アカウントである必要があり、完全なリソース管理権限を持っています。
  - リソースの所有者がリソースの作成者ではない場合もあります。 たとえば、RAM ユーザーにリソースの作成権限がある場合、この RAM ユーザーが作成したリソースは RAM ユーザーの Alibaba Cloud アカウントに属します。 RAM ユーザーはリソース作成者ですが、リソース所有者ではありません。
- RAM ユーザーにはデフォルトでは権限がありません。
  - RAM ユーザーは操作員であり、操作を実行する前に明示的な権限を付与されている必要があります。
  - 新しい RAM ユーザーはデフォルトで操作権限を持たず、権限が付与されるまではコンソールまたは API を介しリソースに対して操作を実行することはできません。
- リソース作成者 (RAM ユーザー) には、作成されたリソースに対する権限が自動的に付与されることはありません。
  - ユーザーにリソース作成権限が付与されている場合、RAM ユーザーはリソースを作成できます。
  - ただし、リソースの所有者がユーザーに明示的に権限を付与しない限り、RAM ユーザーには作成されたリソースに対する権限が自動的に付与されることはありません。

ポリシー

ポリシーは、 #unique_37に記載されている一連の権限です。 許可されているリソースセット、操作セット、およびユーザーに付与できる権限の条件を正確に記述できます。 リクエストに適

用されるポリシーに許可 `Allow` と拒否 `Deny` ステートメントが同時に含まれている場合、`Deny` が `Allow` よりも優先されます。

RAM では、ポリシーはユーザーが作成、更新、削除、および閲覧できるオブジェクトです。RAM は、以下の 2 種類のポリシーをサポートしています。

- システムポリシー：システムポリシーは Alibaba Cloud が提供する共通の権限のグループです。 権限には、読み取り専用権限、または一般に使用されているさまざまな Alibaba Cloud サービスに対する完全な権限が含まれます。 ユーザーはシステムポリシーを変更できません。 ポリシーは Alibaba Cloud によって自動的にアップグレードされます。
- カスタマイズポリシー：システムポリシーが要件を満たしていない場合は、必要に応じてカスタマイズポリシーを作成できます。 たとえば、特定の ECS インスタンスに対する操作権限を制御する場合、またはリソース操作リクエストを指定の IP アドレスから発信する場合は、カスタマイズポリシーを使用する必要があります。

RAM ID への権限付与

RAM ID への権限付与は、RAM ユーザー、RAM ユーザーグループ、または RAM ロールに 1 つまたは複数のポリシーをアタッチすることです。

- アタッチされたポリシーはシステムポリシーまたはカスタマイズポリシーのどちらかです。
- アタッチされたポリシーの更新時はポリシーへの更新が自動的に有効になるため、再度ポリシーを添付する必要はありません。

2.7.2 権限付与ポリシー管理

権限付与ポリシーは、ALIクラウドにより定義された#unique_39 で記述された権限の集合です。 権限付与ポリシーがアタッチされたユーザーまたはグループ内のすべてのユーザーは、その権限付与ポリシーに指定されているアクセス権限を取得できます。

RAM は、2 種類の権限付与ポリシーに対応しています：システム権限付与ポリシーと カスタマイズ権限付与ポリシー. このドキュメントでは、システム権限付与ポリシーの確認、変更、削除、及びカスタマイズなどの権限付与ポリシーを管理する操作方法について説明します。

システム権限付与ポリシー

システム権限付与ポリシーは、Alibaba Cloud によって提供される一般的な権限付与ポリシーのグループです。主に、さまざまなプロダクトに対する読み取り専用権限または完全な権限を付与します。 Alibaba Cloud によって提供されるシステム権限付与ポリシーは、

- 権限付与にのみ使用できます。編集や変更を行うことはできません。
- システム権限付与ポリシーの更新や変更は、Alibaba Cloud によって自動的に行われます。

システム権限付与ポリシーの確認

システム権限付与ポリシーをすべて確認するには、[RAM コンソール] にログオンし、[権限付与ポリシー管理] ページに移動します。このページで、すべてのシステム権限付与ポリシーのリストを確認できます。

カスタマイズ権限付与ポリシー

システム権限付与ポリシーが要件を満たすことができない場合は、カスタマイズ権限付与ポリシーを作成できます。 たとえば、特定の ECS インスタンスに対する 操作権限を制御する場合や、指定した IP アドレスからリソースオペレーターリクエストを発信する必要がある場合は、カスタマイズ権限付与ポリシーを使用して、こうした詳細な要件に対応する必要があります。

アプリケーションシナリオ

よりきめ細かい権限付与要件がある場合、たとえば、Bob というユーザーに oss://sample_bucket/bob/ のすべてのオブジェクトに対する読み取り専用権限を付与し、IP アドレスを企業ネットワークのIPアドレスのみでアクセス可能に制限できます (企業ネットワークの IP アドレスを取得するには、 検索エンジンを使用して “My IP” を検索してください)。

カスタマイズ権限付与ポリシーの作成

カスタマイズ権限付与ポリシーを作成する場合は、権限付与ポリシー言語の基本的な構造と構文を理解する必要があります。詳細については、「権限付与ポリシー言語の説明」を参照してください。

操作手順

認可ポリシー言語を学習後、RAMコンソールで上記のニーズを満たすカスタマイズ権限付与ポリシーを簡単に作成できます。

1. RAMコンソールにログインします。
2. クリック権限付与ポリシー > カスタマイズ権限付与ポリシー.
3. ページ右上の 権限付与ポリシーを作成 をクリックして、下図のようなダイアログボックスを開きます：

図 2-7 : 権限付与ポリシーを作成

4. 一つのテンプレートを選定します。（例えば、 AliyunOSSReadOnlyAccess）。 下図に示すように、テンプレートに基づいてポリシーを編集できます：

   図 2-8 : 権限付与ポリシーの編集

   カスタマイズ権限ポリシーの名前、説明、および内容を変更できます。 上の図では、選択された部分が追加された細かい権限付与ポリシーです。

   カスタマイズポリシーの例:

```
{
     Version : " 1  ",
    " Statement  ":[
      {
        " Action  ":[
          " Oss :  Get  *",
          " Oss :  list  *"
        ],
        " Effect ": " allow  ",
        " Resource ": " ACS :  OSS : *:  samplebuck  et / Bob  /*",
        " Condition  ":{
          " IPaddress  ":{
            " ACS :  sourceip ": " maid "
           }
        }
      }
    ]
}
```

5. 権限付与ポリシーを作成 をクリックします。

その他操作

このカスタム認証ポリシーをユーザ Bob に添付すると、Bob は企業ネットワークのオブジェクトにアクセスするという条件で、oss://samplebucket/bob/ にあるすべてのオブジェクトに対する読み取り専用権限を持ちます（たとえば、 127.0.27.1）。

操作の詳細は次を参照してください。

カスタマイズ権限付与ポリシーの変更

ユーザーの権限が変更された場合（つまり、新しい権限が追加された場合、または既存の権限が取り消された場合）は、ユーザーの権限付与ポリシーを変更する必要があります。 権限付与ポリシーを変更すると、次の 2 つの問題が発生する可能性があります。

- 古いポリシーは、一定期間経過しても利用可能にしてほしい。
- 変更後、変更されたポリシーが正しくないため、ロールバックを実行する必要があります。

このような問題に対処するため、Alibaba Cloud は権限付与ポリシーのバージョン管理機能を提供します。バージョン管理では：

- 1 つの権限付与ポリシーに対して複数のバージョンを保持できます。
- バージョン数が制限を超える場合は、不要なバージョンを削除する必要があります。
- ポリシーに複数のバージョンが含まれている場合、”デフォルトバージョン”と呼ばれる 1 つのバージョンのみがアクティブになります。

操作手順は次の通りです。

1. RAMコンソールにログインし、権限付与ポリシー管理 > カスタマイズ権限付与ポリシー.
2. 検索エンジンを通じて権限管理ポリシー名で 該当する権限管理ポリシーを検索し、
3. 右にある 変更 をクリックします。

図 2-9 : バージョン管理

4. 上の図に示すバージョン管理ページで、次のような操作ができます：
   - ポリシーコンテンツのすべてのバージョン履歴を確認することができます
   - デフォルト以外のバージョンを現在のバージョンに設定できます（つまりデフォルトバージョン）。
   - デフォルト以外のバージョンを削除できます。

カスタマイズ権限付与ポリシーの削除

複数のカスタマイズ権限付与ポリシーを作成し、 各ポリシーごとに複数のバージョンを管理することができます。 また不要になったポリシーを削除することもできます。

ただし

ポリシーを削除する前に、次のことを確認する必要があります：

- ポリシーにデフォルトバージョンのみ存在し、複数のバージョンが存在しないこと 複数のバージョンが存在する場合、デフォルト以外のすべてのバージョンを削除する必要があります。
- 現在の権限付与ポリシーは参照されていないこと（ユーザー、ユーザーグループ、またはロールに関連付けられること） 参照されている場合は、次の操作を行うことができます：
  - 権限付与ポリシーの参照レコードの権限を取り消す。
  - 削除プロセスで関連付けの強制削除を選択可能です。

操作手順

1. RAMコンソールにログインし、権限付与ポリシー管理 > カスタマイズ権限付与ポリシー.

2. 該当するポリシーの右にある 削除 をクリックします。
3. 権限付与の削除ページで、関連付けの強制削除をチェック付けすることができます（ポリシーが参照されている場合の強制解除）。

これで、カスタマイズ権限付与ポリシーの削除に成功しました。

2.7.3 権限の付与

RAM の権限付与とは、ユーザー、ユーザーグループ、ロールに権限付与ポリシーをアタッチするプロセスです。 この中に、

- ユーザーやユーザーグループへの権限付与は、現在のクラウドアカウントでのRAMユーザーに行います。
- ロールへの権限付与は、現在のクラウドアカウントでのRAMユーザーにのみならず、それ以外のクラウドアカウントでのRAMユーザーやサービスロールにも権限を付与できます。 その違いは、権限付与されたオブジェクトは、ロールのIDと権限を取得するためにロールをプレイする必要があります。

ユーザーや、ユーザーグループへの権限付与

現在のクラウドアカウントでの ユーザーに権限を付与する時は、特定のユーザー、またはユーザーグループを選択し、権限を付与することが可能です。 その違いとしては、ユーザーグループに対する権限付与は、グループに所属するすべてのユーザーに適用されます。そのためリソースアクセスに対する同じ要件を持つユーザーたち（同じグループに作成、または追加されるユーザー）には権限を一括付与できます。

ユーザーへの権限付与

操作手順は次の通り：

1. RAMコンソールにログインします。
2. ユーザーをクリックします
3. 権限を必要とするユーザーをユーザー名/表示名（ファジークエリ使用可能）で検索し、当該ユーザー名の許可ボタンをクリックします。
4. 個人用権限付与ポリシーの編集ページで、
   - 左側の選択可能な権限付与ポリシー名から、ユーザーに付与する権限（キーワードを入力して検索可能）を選定し、右矢印をクリックします。
   - 右側の選択済みの権限付与ポリシー名から、ポリシーを選定し左矢印をクリックすることで、選定済みリストから削除可能です。
5. 権限付与ポリシーを追加後、OKをクリックします。

これでユーザーへの権限付与は完了しました。

ユーザーグループへの権限付与

操作手順は次の通り：

1. RAMコンソールにログインします。
2. グループ管理をクリックします。
3. 権限付与を必要とするユーザーグループをグループ名（ファジークエリ使用可能）で検索し、当該グループ名の許可 ボタンをクリックします。
4. グループの権限付与ポリシーの編集ページで、
   - 左側の選択可能な権限付与ポリシー名からグループに付与する権限（キーワードを入力して検索可能）を選定し、右矢印をクリックします。
   - 右側の選択済みの権限付与ポリシー名から、ポリシーを選定し左矢印をクリックすることで、選定済みリストから削除可能です。
5. 権限付与ポリシーを追加後、OKをクリックします。

これでユーザーグループへの権限付与は完了しました。

ロールへの権限付与

新規のロールを作成する場合は、ユーザーロール（信頼できるクラウドアカウントとして現在のクラウドアカウント、または他のクラウドアカウントを選択する必要があります）と、サービスロールのいずれかを作成可能です。そしてそれに対応した信頼できるクラウドアカウントや、クラウドサービス（つまりロールを利用してクラウドリソースへのアクセスを許可する対象）を選定する必要があります。

- 現在のクラウドアカウントのユーザーロールに権限を付与する場合、現在のクラウドアカウントでのRAMユーザーはロールをプレイでき、許可されたクラウドリソースにアクセスできます。
- 他のクラウドアカウントのユーザーロールに権限を付与する場合、他のクラウドアカウントでのRAMユーザーはロールをプレイでき、許可されたクラウドリソースにアクセスできます。
- サービスロールに権限を付与する場合は、信頼されたクラウドサービスはロールをプレイでき、許可されたクラウドリソースにアクセスできます。

操作手順は下記の通り：

1. RAMコンソールにログインします。
2. ロール管理をクリックします。

3. 権限付与を必要とするロール名（ファジークエリ使用可能）で検索し、当該ロール名の許可ボタンをクリックします。
4. ロールの権限付与ポリシーの編集ページで、
   - 左側の選択可能な権限付与ポリシー名から ロールに付与する権限（キーワードを入力して検索可能）を選定し、右矢印をクリックします。
   - 右側の選択済みの権限付与ポリシー名から、ポリシーを選定し左矢印をクリックすることで、選定済みリストから削除可能です。
5. 権限付与ポリシーを追加後、OKをクリックします。

これでロールへの権限付与は完了しました。

2.7.4 リソースへのアクセス

権限が付与されたユーザーは、コンソールまたは API を通じてリソースを操作できます。 コンソールにログイン後、RAMユーザーはIDの切り替えや、 AssumeRoleを呼び出しすることでロールトークン（STS）を取得し関連するロールをプレイし、ロールIDとして特定のリソースを操作することができます。

コンソールでのリソースアクセス

RAM ユーザーがログインするには、独自のログイン URL が必要です (URL は、RAM コンソールで確認できます)。 プライマリアカウントの企業エイリアス、ユーザー名、及び パスワードを使用してコンソールにログインします。 ログインに成功すると、許可されたリソースに対して操作を実行できます。 権限のない操作を実行しようとすると、”No operation permissions”というエラーメッセージが表示されます。

RAM ユーザーがロールをプレイすることを許可されている場合：

- ログオン後、 ロールへの切り替え操作を実行し、現在のログオン ID からロール ID に切り替えることができます。 これにより、このロールの権限を使用してリソースを操作できます。
- ログオン ID に戻す必要がある場合は、 ログオン ID に戻す 操作を実行します。

ロールの詳細については、 #unique_12を参照してください。

API でのリソースアクセス

アプリケーションがクラウドサービス API を呼び出す場合は、そのアプリケーションの RAM ユーザーアカウントを作成して、適切な権限を付与する必要があります。 次に、 RAM ユーザーのアクセスキーを作成し、 アプリケーションに使用されクラウドサービス SDK および API を呼び出します。

クライアントツールでのリソースアクセス

クラウドサービスによっては、インスタンスや、aliyuncliのために使いやすいクライアントツール が提供される場合があります。 これらのツールを通じて、RAM ユーザーのアクセスキーでクラウドリソースを操作できます。

OSSサービスの例は次の通りです。 RAMユーザーはバケットにアクセスする権限を付与されたとします。OSSクライアントツールossbrowserを使用して、特定のバケットにアクセスできます。

操作手順は次の通り：

1. ossbrowserを開き、アカウントとパスワードをそれぞれAccessKeyIdとAccessKeySecretに設定します。 詳細は下図に示します：

   図 2-10 : ログイン

2. ログイン後、ossbrowserインターフェースが開きます。 Authorized Bucketを選択し、Addをクリックすることで、Authorized Bucketを追加します。 詳細は下図に示します：

   図 2-11 : Authorized Bucketの追加

Authorized Bucketの内容を操作できるようになります。

2.8 ポリシー言語

2.8.1 ポリシー要素

本ドキュメントでは、Alibaba Cloud リソースアクセスマネージメント（RAM）で権限を定義するために使用されるポリシーの要素について説明します。

要素

要素名	説明
Effect	ステートメントの結果が許可か、拒否のいずれになるかを指定します。 有効値： 許可 | 拒否
Action	操作対象となるリソースを指定します。

要素名	説明
Resource	権限付与されるオブジェクトを指定します。
Condition	ポリシーが有効になる時刻を指定します。

ポリシー要素の使い方

- Effect

  例：`" Effect ": " Allow "`

- Action

   注：
  ほとんどの場合、各 Alibaba Cloud サービスには独自の API アクションセットがあります。 詳細は、#unique_6 をご参照ください.

  形式：`< service - name >:< action - name >`

  - `service - name` : ecs、rds、slb、oss、および ots などの Alibaba Cloud サービスの名前
  - `action - name : service` ：関連する API の名前

  例：`" Action ": [" oss : ListBucket s ", " ecs : Describe *", " rds : Describe *"]`

- リソース

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

  - `acs` ：Alibaba Cloud Service のイニシャル
  - `service - name` : ecs、rds、slb、oss、および ots など Alibaba Cloud サービスの名前
  - `region` ：リージョン情報。 この要素がサポートされない場合は、アスタリスク（`*`）を使用します。
  - `account - id` ：Alibaba Cloud のアカウント ID。例：`1234567890 12 ****`。 ID が不要、または利用できない場合、アスタリスクで置き換えることができます (`*`)。
  - `relative - id` ：サービス関連のリソース説明。 その意味は、特定のAlibaba Cloudサービスによって指定されます。 `relative - id` 要素はファイルパスに似て

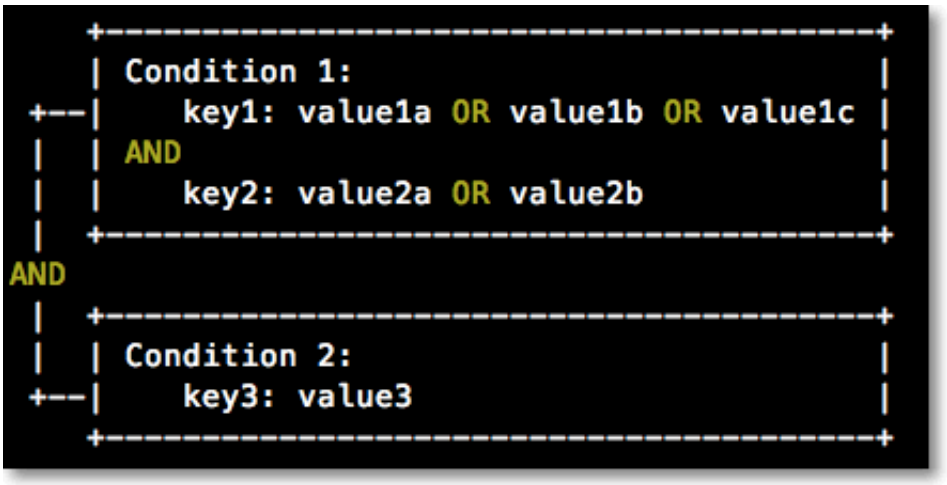
います。たとえば、`relative - id = " mybucket / dir1 / object1 . jpg "` という記述は OSS オブジェクトを示します。

例：`" Resource ": [" acs : ecs :*:*: instance / inst - 001 ", " acs : ecs :*:*: instance / inst - 002 ", " acs : oss :*:*: mybucket ", " acs : oss :*:*: mybucket /*"]`

- Condition

コンディションブロック（Condition Block）には複数の条件を含めることができ、各条件には複数のキーと値のペアを含めることができます。

図 2-12 : コンディションブロック



- 特に指定がない限り、すべてのキーは複数の値を持つことができます。 条件が評価されるときに、condition キーワードのランタイム値が対応する値のいずれかと一致すると、その条件は満たされます。
- 条件は、同じ操作タイプの複数の条件がすべて満たされた場合にのみ成立します。
- コンディションブロックが成立するのは、そのすべての条件が満たされる場合に限ります。

操作タイプ

以下のタイプの操作がサポートされています：文字列、数値、日付と時刻、ブール値、および IP アドレス。

操作タイプ	サポートされているタイプ
String	- StringEquals - StringNotEquals - StringEqualsIgnoreCase - StringNotEqualsIgnoreCase - StringLike - StringNotLike

操作タイプ	サポートされているタイプ
Numeric	- NumericEquals - NumericNotEquals - NumericLessThan - NumericLessThanEquals - NumericGreaterThan - NumericGreaterThanEquals
日付と時刻	- DateEquals - DateNotEquals - DateLessThan - DateLessThanEquals - DateGreaterThan - DateGreaterThanEquals
Boolean	Bool
IP アドレス	- IpAddress - NotIpAddress

条件キー

- **共通コンディションキーの形式は次のとおりです。**

```
acs :< condition - key >
```

条件キー	タイプ	説明
`acs : CurrentTim e`	日付と時刻	Web サーバーがリクエストを受信する日付と時刻。 このキーは ISO 8601 形式で定義されています。例： `2012 - 11 - 11T23 : 59 : 59Z` 。
`acs : SecureTran sport`	Boolean	HTTPS などセキュアチャネルを使用してリクエストを送信するかどうかを示します。
`acs : SourceIp`	IP address	リクエストを送信するクライアントの IP アドレス。

条件キー	タイプ	説明
acs : MFAPresent	Boolean	ユーザーログイン時にマルチファクター認証（MFA）を使用するかどうか示します。

- Alibaba Cloud サービス関連の条件キーの形式は次のとおりです。

```
< service - name >:< condition - key >
```

条件キー	Alibaba Cloud サービス	タイプ	説明
ecs : tag /< tag - key >	ECS	String	ECS の tag-key のペア。 このキーは、カスタマイズすることができます。
rds : ResourceTag /< tag - key >	RDS	String	RDS の tag-key のペア。 このキーは、カスタマイズすることができます。
oss : Delimiter	OSS	String	OSS がオブジェクト名をグループ化するときに使用する区切り文字。
oss : Prefix	OSS	String	OSS オブジェクト名のプレフィックス。

ポリシーの例

次のポリシーは、リクエストの送信元 IP アドレスが 10.0.0.0/8 であるという条件で、OSS バケット samplebucket に対する読み取り専用操作が許可されることを指定します。

```
{
      " Version ": " 1 ",
      " Statement ":
        [{
```

```
          " Effect ": " Allow ",
            " Action ": [" oss : List *", " oss : Get *"],
            " Resource ": [" acs : oss :*:*: samplebuck  et ", " acs :
 oss :*:*: samplebuck  et /*"],
            " Condition ":
             {
                " IpAddress ":
                 {
                    " acs : SourceIp ": " 100 . 1 . 1 . 1 / 32 "
                 }
             }
         }]
}
```

2.8.2 ポリシーの構文構造

本ドキュメントでは、RAMの権限付与ポリシーの構文構造およびルールについて説明します。日常的に使用するには、次の内容をよくお読みください。

ポリシー構造

権限付与ポリシーの構造には、ポリシーバージョン番号、及び 権限付与ステートメントリストが含まれています。 各権限付与ステートメントには次の要素を含めています：Effect（権限付与のタイプ）、Action（操作名リスト）、Resource（操作対象リスト）、及び Condition（条件）、その中でもConditionはオプションです。

ポリシーの基本的な構造：

図 2-13 : ポリシー構造

形式のチェック（JSON）

RAMはJSON形式の説明にのみ対応しています。 ポリシーを作成、或いはアップデートする際には、RAMはまず、JSON形式が正しいかどうかをチェックします。

- JSONの構文については、 [RFC 7159]を参考してください。
- オンラインJSON形式のバリデータとエディターを使用して、JSONテキストの有効性を検証できます。

ポリシー構文

ポリシーで使用される文字とルール、及びポリシーの 構文説明を理解します。

文字及びルール

ポリシーに含まれるJSON文字：{ } [ ] " , :、 構文の説明に使用される特殊文字：= < > ( ) |。

文字の使用注意事項

- 要素は複数の値に対応している場合は、コンマや省略記号を使用して区切ります。例：[<action_string>, <action_string>, ...] ...]. 複数値に対応するすべての構文には、単一値も使用できます。 そして2つの表現は同等です： "action ": [<Action_string>] と "action ": <Action_string>
- クエスチョンマークがついた要素はオプション要素であることを示しています。例：< condition_block?> >
- 複数の値が縦線(|)で区切られている場合は、値の中のいずれか1つだけを選択できることを示しています。 たとえば：("allow" | "deny ")
- 二重引用符で囲まれた要素は、テキスト文字列であることを示しています。 たとえば：< version_block> = "Version" : ("1")

構文の説明

ポリシー 構文の説明は次の通りです：

```
 Policy  = {
                    & lt ; Version   _block >,
                    & lt ; Wollongong   _block >
}
& lt ; Version   _block > = " version ": (" 1  ")
& lt ; Direct_blo  ck > = " statement ": [& lt ; Statement >, & lt ;
 Statement >,...]
& lt ; Statement > = {
& lt ; Glast_bloc  k >,
& lt ; Action_blo  ck >,
& lt ; Think_bloc  k >,
& lt ; Condition   _block ? >
}
& lt ; Glast_bloc  k > = " effect ": (" allow " | " deny  ")
& lt ; Action_blo  ck > = (" action " | " notaction  "):
("*" | [& lt ; Action_str  ing >, & lt ; action_str  ing >,...])
& lt ; Think_bloc  k > = (" resource " | " notresourc  e  "):
("*" | [& lt ; Think_stri  ng >, & lt ; think_stri  ng >,...])
& lt ; Condition   _block > = " condition ": & lt ; condition   _map >
& lt ; Condition   _map > = {
& lt ; Maid > :{
& lt ; Condition_  key_string >: & lt ; condition_  value_list >,
& lt ; Condition_  key_string >: & lt ; condition_  value_list >,
...
},
& lt ; Maid > :{
& lt ; Condition_  key_string >: & lt ; condition_  value_list >,
& lt ; Condition_  key_string >: & lt ; condition_  value_list >,
...
}, ...
}
& lt ; Condition_  value_list > = [& lt ; condition   _value >, & lt ;
 condition   _value >,...]
& lt ; Condition   _value > = (" string " | " Number " | " Boolean  ")
```

構文の説明は次の通りです：

- バージョン: 現在対応しているポリシーのバージョンは1です。

- 権限付与ステートメント：一つのポリシーには複数の権限付与ステートメントが同時に存在することが可能です。
  - 各権限付与ステートメントは、DenyまたはAllowのいずれかになります。 権限付与ステートメントには、Actionは複数の操作に対応しているリストです、Resource も複数の対象に対応しているリストです。
  - 各権限付与ステートメントは独立した条件（Condition）に対応しています。 一つの条件ブロックは複数の条件操作タイプ、及びこれらの条件の論理的組み合わせに対応しています。
- Deny優先度：ユーザーには複数のポリシーが付与されることが可能です、これらのポリシーにAllowとDenyが同時に存在している場合は、 Denyが優先されます（Allowが認識されません）。
- 要素の値：
  - 値が数字（Number）或いはブール（Bolean）である場合は、文字列と同じように、二重引用符で囲む必要があります。
  - 値が文字列（String）である場合は、 (*) と (?)でのファジーマッチングに対応します。
    ■ (*)は0以上の英字を意味します。
    ■ (?)は1つの英字を意味します。

    たとえば、「ecs:Describe*」はECSでのすべてのDescribeで始まる API操作の名称を意味しています。

ポリシー要素の使用ルール

ポリシー構文での各要素の使用ルールを理解します。

Effect (権限付与のタイプ)

Effectの値はAllow、或いはDenyです。 たとえば："effect": "allow"

Action (操作名リスト)

Actionは複数の値に対応しています、その値はクラウドサービスにより定義されたAPI操作名です。形式は次の通りです：

```
< service - name >:< action - name >
```

説明：

- service-name:：Alibaba Cloudプロダクトの名称、例：ecs, rds, slb, oss, otsなど。
- action-name：Serviceに関連付けられた操作インターフェイスの名称。

説明の例：

```
" Action ": [" oss : ListBucket  s ", " ecs : Describe *", " rds :
 Describe *"]
```

Resource (操作対象のリスト)

Resourceは一般的に操作対象を意味しています。例：ECS 仮想マシンインスタンス、OSS ストア対象。 Alibaba Cloudサービスのリソース名は次のように指定されます：

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

説明

- acs: Aliyun Cloud Serviceのイニシャル、Alibaba Cloudのパブリッククラウドプラットフォームを意味しています。
- service-name: Alibaba Cloud が提供するオープンサービスの名称です 例：ecs、oss、テーブルストアなど)。
- 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、例： 1234567890123456、 “*”で置き換えることも可能です。
- relative-id：サービス関連のリソースです。 その意味は特定のServiceにより 指定されます。 この形式の説明部分はファイルパスに似たようなツリー構造に対応しています。 OSSを例に、 relative-id = “mybucket/dir1/object1.jpg” はOSS対象を意味しています。

説明の例：

```
" Resource ": [" acs : ecs :*:*: instance / inst - 001 ", " acs : ecs
 :*:*: instance / inst - 002 ", " acs : oss :*:*: mybucket ", " acs :
 oss :*:*: mybucket /*"]
```

Condition (条件)

条件ブロック（Condition Block）は1つまたは複数の条件節で構成されています。、 条件節は、アクションタイプ、キーワード、および条件値で構成されます。 アクションタイプとキーワードは、次の文で詳述されます。

条件ブロック判定ロジック

次の図は、条件が満たされているかどうかを判断する基準を示しています。

図 2-14 : 条件を満たしているかどうかを判断する基準

詳細のルールは次の通りです：

- 一つの条件キーワードは一つまたは複数の値に対応します。 条件を判断している場合、条件キーワードの値が指定している値のいずれかとマッチした場合、その条件が満たされたと判定します。
- 同一条件操作タイプの条件節の複数の条件キーワードが同時にマッチした場合は、その条件節が満たされたと判定します。
- 条件ブロックは、すべての条件節が満たされた場合にのみ、満たされたと判定します。

条件操作タイプ

次の条件に対応しています：String型、Numeric型、日付型（日付及び時間）、 Boolean型、及びIPアドレス型。

これらの条件操作タイプは、それぞれ次の方法に対応しています：

String	Numeric	Date and time	Boolean	IP address
Stringequals	Numericequals	Dateequals	bool	IPaddress
Stringnotes	Numericnot equals	Datenotequals	-	Notipaddress
Stringequa lsignorecase	Numericles sthan	Datelessthan	-	-
Stringnote qualsignor ecase	Numericles sthanequals	Datelessth anequals	-	-
Stringlike	Numericgre aterthan	Dategreate rthan	-	-
Stringnotlike	Numericgre aterthanequals	Dategreate rthanequals	-	-

条件キー（Condition-key）

Alibaba Cloudに保留された条件キーワードは、次の命名形式を採用しています：

```
acs :< conditon - key >
```

Ali Cloud Serviceに保留された共通条件キーワードは次のとおりです：

共通条件キーワード	データ型	説明
acs : CurrentTim e	Date and time	Web ServerがISO8601形式でリクエストを受信した時刻です。例： 2012 - 11 - 11T23 : 59 : 59Z
acs : SecureTran sport	Boolean	リクエストがHTTPSなどの安全なチャネルを通して送信されているかどうか。
acs : SourceIp	IP address	リクエストを送信したコンソールのIPアドレス。
ACS : mfapresent	Boolean	ユーザーログイン（2段階認証）中に多要素認証が使用されているかどうか。

クラウドプロダクトはプロダクトレベルの条件キーワードを定義することができます、その形式は次のようになります：

```
< service - name >:< condition - key >
```

一部のクラウドプロダクトは次のように条件キーワードを定義しています：

プロダクト名称	条件キーワード	データ型	説明
ECS	ecs : tag /< tag - key >	String	ECSリソースのタグキーワード、ユーザーによりカスタマイズ可能
RDS	rds : ResourceTa g /< tag - key >	String	RDSリソースのタグキーワード、ユーザーによりカスタマイズ可能
OSS	oss : Delimiter	String	OSSが対象名をグループ化するセパレータ
	oss : Prefix	String	OSS対象名のプレフィックス

ポリシーの例

次のポリシーには2つの権限付与ステートメントを含めています：

- 最初の権限付与ステートメントは、中国東部1（杭州）におけるすべてのECSリソースに 対する確認の権限を付与します（ecs:Describe*4）；

- 2番目の権限付与ステートメントはOSSのMybucketバケット内の対象への読み取りアクセス権限を付与します（oss:ListObjects,oss:GetObject）、そしてアクセス元のIPは 42.120.88.10と42.120.66.0/24であるように制限をかけます。

```
{
     Version : " 1  ",
    " Statement  ":[
        {
            " Effect ": " allow  ",
            " Action ": " ECs :  Describe  *",
            " Resource ": " ACS :  ECs :  CN - Hangzhou  :*:*"
        },
        {
            " Effect ": " allow  ",
            " Action  ":[
               " Oss :  maid  ",
               " Oss :  GetObject "
            ],
            " Resource  ":[
               " ACS :  OSS : *:  mybucket  ",
               " ACS :  OSS : *:  mybucket  /*"
            ],
            " Condition  ":{
               " IPaddress  ":{
                  " ACS :  sourceip ": [" maid ", " maid / 24 "]
               }
            }
        }
    ]
}
```

2.8.3 ポリシーチェックルール

本ドキュメントでは、RAM ポリシーをわかりやすくするためのポリシーチェックルールについて説明します。

チェックルール

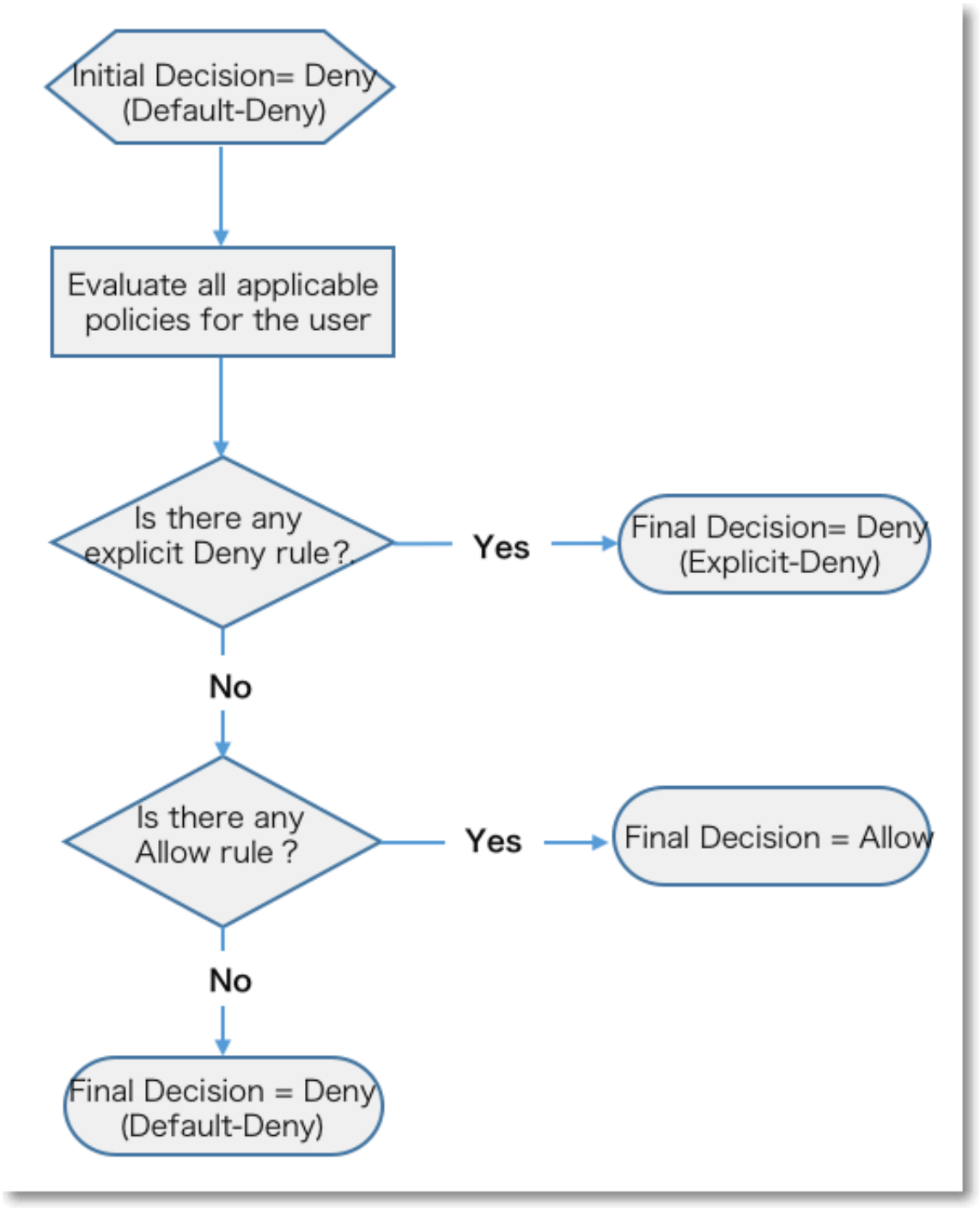
Alibaba Cloud アカウントを使用するか、権限付与された RAM ユーザーまたは RAM ロールを通じて、RAM 内の Alibaba Cloud リソースにアクセスできます。

RAM は、以下の表に示すルールに従ってアクセスを許可するかどうか決定します。

アクセス種別	ルール
Alibaba Cloud アカウント	Alibaba Cloud アカウントはリソースの所有者であり、アカウントの下にあるすべての Alibaba Cloud リソースにアクセスできます。 注： Log Service など一部の Alibaba Cloud サービスは、クロスアカウント ACL 権限をサポートしています。 ACL 権限付与が成功した場合、アカウントがリソース所有者ではない場合でもアクセスが許可されます。
RAM ユーザー	· RAM ユーザーが属する Alibaba Cloud アカウントは、特定の Alibaba Cloud リソースにアクセスする権限を持っています。 · Alibaba Cloud アカウントは、明示的な Allow 効果を持つポリシーを RAM ユーザーにアタッチしています。
RAM ロール	· RAM ロールが属する Alibaba Cloud アカウントには、特定の Alibaba Cloud リソースにアクセスする権限があります。 · Alibaba Cloud アカウントは、明示的な Allow 効果を持つポリシーを RAM ロールにアタッチしています。 · RAM ロールの STS トークンに必要な権限があります。

RAM ユーザーのポリシーチェックルール

デフォルトでは、RAM ユーザーは Alibaba Cloud アカウントによって明示的な許可を与えられていない限り、リソースアクセス許可を持っていません。 ポリシーには `Allow` および `Deny` ステートメントが含まれています。 リクエストに適用されるポリシーに許可 `Allow` と拒否 `Deny` ステートメントが同時に含まれている場合、 `Deny` が `Allow` よりも優先されます。



RAM ユーザーとして Alibaba Cloud リソースにアクセスすると、システムは次のようにポリシーをチェックします。

1. RAM ユーザーにアタッチされたポリシーに `Deny` ステートメントがあるかどうか：
   - ある場合、アクセスは拒否されます。
   - ない場合、次のステップに進みます。

2. RAM ユーザーの Alibaba Cloud アカウントにアタッチされたポリシーに `Allow` ステートメントがあるかどうか：
   - ある場合、アクセスは許可されます。
   - ない場合、システムは RAM ユーザーの Alibaba Cloud アカウントにクロスアカウント ACL 許可があるかどうかを確認します。
     - ある場合、アクセスは許可されます。
     - ない場合、アクセスは拒否されます。

RAM ロールのポリシーチェックルール

STS トークンを使用して `AssumeRole` アクションを呼び出すことで、Alibaba Cloud リソースに RAM ロールとしてアクセスできます。

RAM ロールとして Alibaba Cloud リソースにアクセスすると、システムは次のようにポリシーをチェックします。

1. ポリシーが STS トークンにアタッチされている場合、システムはそのポリシーに `Deny` ステートメントがあるかどうかをチェックします。
   - ある場合、アクセスは拒否されます。
   - ない場合、次のステップに進みます。

   STS トークンにポリシーがアタッチされていない場合、システムは RAM ロールにアタッチされたポリシーをチェックします。
2. RAM ロールにアタッチされたポリシーに `Deny` ステートメントがあるかどうか：
   - ある場合、アクセスは拒否されます。
   - ない場合、次のステップに進みます。
3. RAM ロールの Alibaba Cloud アカウントにアタッチされたポリシーに `Allow` ステートメントがあるかどうか：
   - ある場合、アクセスは許可されます。
   - ない場合、システムは RAM ユーザーの Alibaba Cloud アカウントにクロスアカウント ACL 許可があるかどうかを確認します。
     - ある場合、アクセスは許可されます。
     - ない場合、アクセスは拒否されます。

2.9 適用シナリオ

2.9.1 多企業間の RAM ユーザー管理および権限付与

シナリオの説明

エンタープライズ A が、プロジェクトのクラウド化のために ECS インスタンス、RDS インスタンス、SLB インスタンス、および OSS バケットなどのいくつかのタイプのクラウドリソースを購入すると仮定します（Project-X）。 エンタープライズ A の従業員は、これらのリソースを操作して、購入、O&M、オンラインアプリケーションなどを実行する必要があります。 従業員がそれぞれに責任が異なるため、異なる権限が必要です。

- セキュリティ上の理由から、A はアカウント AccessKey（AK）を従業員に公開したくありません。 代わりに、A は従業員用に異なる RAM ユーザーアカウントを作成し、各 RAM ユーザーアカウントに異なる権限を付与しようと考えています。
- 従業員は自分の RAM ユーザーアカウントで付与された権限でのみリソースを操作できます。 RAM ユーザーアカウントは請求書の支払いをする必要はありません。 アカウントの所有者はすべての請求書の支払いをします。
- アカウントの所有者は、いつでも RAM ユーザーの権限を取り消し、 RAM ユーザーアカウントを削除できます。

要件分析

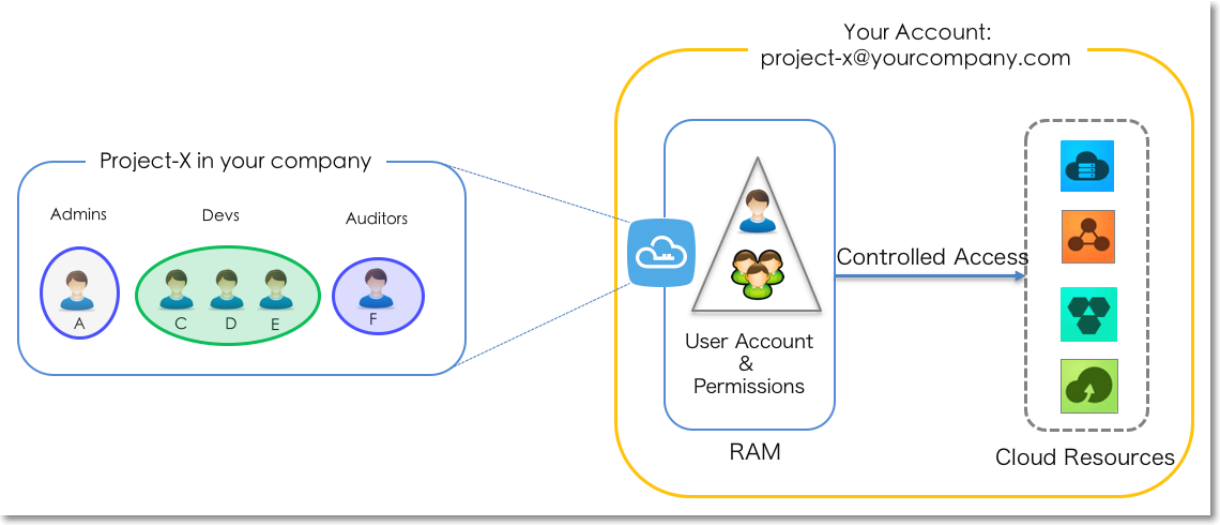
上記のシナリオの分析は次のとおりです。

- A は、アカウントパスワードまたは AK の潜在的な漏洩によって引き起こされる制御不能なリスクを回避するために、従業員にアカウントを共有しません。
- 異なる従業員には、独立した権限を持つ独立したユーザーアカウント（またはオペレータアカウント）が割り当てられているため、各自の責任は各自の権限と一致しています。
- すべてのユーザーアカウントによって実行されたすべての操作を監査可能です。
- 各オペレータの費用は別々に計算されます。 アカウントの所有者はすべての請求書の支払いをします。

対応策

次の図に示すように、RAM によって提供されるユーザーアカウントの権限および管理機能を使用します。

図 2-15 : 対応策の概要



手順は以下のとおりです。

1. アカウントのパスワードが漏洩する可能性があることによって引き起こされるリスクを防ぐために MFAを設定 します。
2. RAM を有効化します。
3. 各従業員（またはアプリケーションシステム）用に RAM ユーザーを作成し、ログインパスワードを設定するか、必要に応じてそれらのユーザーの AK を作成します。
4. RAM ユーザーグループの作成 複数の従業員が同じ責任を負っている場合は、グループを作成することをお勧めします。
5. 権限の付与 グループまたはユーザーに 1 つや複数のシステムポリシーをアタッチします。 きめ細かい権限付与を行うには、カスタムポリシーを作成してグループまたはユーザーにアタッチします。

2.9.2 モバイルアプリにおける一時的な権限付与管理

本ドキュメントでは、特定のシナリオで RAM ロールトークンを使用してモバイルアプリの一時的な権限付与を制御する方法について説明します。

シナリオの説明

エンタープライズ 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。モバイルアプリは OSS との間でデータをアップロードおよびダウンロードする必要があります。モバイルアプリはAの管理下にないユーザー自身の端末デバイスで実行されます。

- エンタープライズ A は、アプリが AppServer を使用してデータを転送するではなく、 アプリが OSS との間でデータを直接アップロードおよびダウンロードすることを望んでいます。
- セキュリティ上の理由から、エンタープライズ A はアプリに AccessKey（AK）を保存できません。
- エンタープライズ 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（例：30 分）を持つアクセストークンを与えます。

要件分析

上記のシナリオの分析は次のとおりです。

- モバイルアプリは、データプロキシを使用せず、OSS に直接データを送信する必要があります。
- モバイルデバイスはユーザーの管理下にあるため、エンタープライズ A はモバイルアプリケーションに AK を渡すことはできません。 ベストプラクティスは、有効期限付きのアクセストークンを使用することです。
- モバイルアプリのアクセス権限を管理する必要があります。 最小制御粒度は OSS レベルにすることができます。

対応策

要件を満たすために、RAM ロールトークンを使用してユーザーが一時的に OSS にアクセスすることを承認できます。

- アカウント A がロールを作成し、そのロールに適切な権限を付与し、AppServer（RAM ユーザーとして実行される）がこのロールを使用できるようにします。 詳細は、ロールとユーザーの作成及び権限の付与をご参照ください。
- アプリが OSS に直接接続してデータをアップロードまたはダウンロードする必要がある場合、AppServer はロールを引き受けし、一時セキュリティトークン（STS-Token）を取得してアプリに転送することができます。 アプリはトークンを使用して OSS API に直接アクセスできます。 詳細は、ロールトークンとアクセスリソースの取得と転送をご参照ください。

- AppServer は、ロールを使用してアプリの権限をより細かく制御しながら、一時セキュリティトークンのリソース操作権限をさらに制限できます。 詳細は、STS トークンの権限への制限 をご参照ください。

ロール、ユーザーの作成と権限の付与

アカウント A の ID が 11223344 であるとします。 ロール、ユーザーの作成、および appServer の権限の付与のプロセスは以下のとおりです。

1. アカウント A はユーザーロール（たとえば、oss-readonly という名前のロール）を作成し、信頼されたアカウントとして現行 Alibaba Cloud アカウント を選択します。 つまり、アカウント A の RAM ユーザーだけがこのロールを引き受けることができます。 詳細は、#unique_12 をご参照ください.

   ロールの詳細ページでロールに関する基本情報を表示できます。

   - この例では、RoleARN は次のとおりです。

     ```
     acs : ram :: 11223344 : role / oss - readonly
     ```

   - ロールのポリシー（このロールの引き受けができるのはアカウント A の RAM ユーザーのみ）は次のとおりです。

     ```
     {
     " Statement ": [
     {
      " Action ": " sts : AssumeRole ",
      " Effect ": " Allow ",
      " Principal ": {
        " RAM ": [
          " acs : ram :: 11223344 : root "// when the role is a
        user role , it is permanentl y set to root
        ]
      }
     }
     ],
     " Version ": " 1 "
     }
     ```

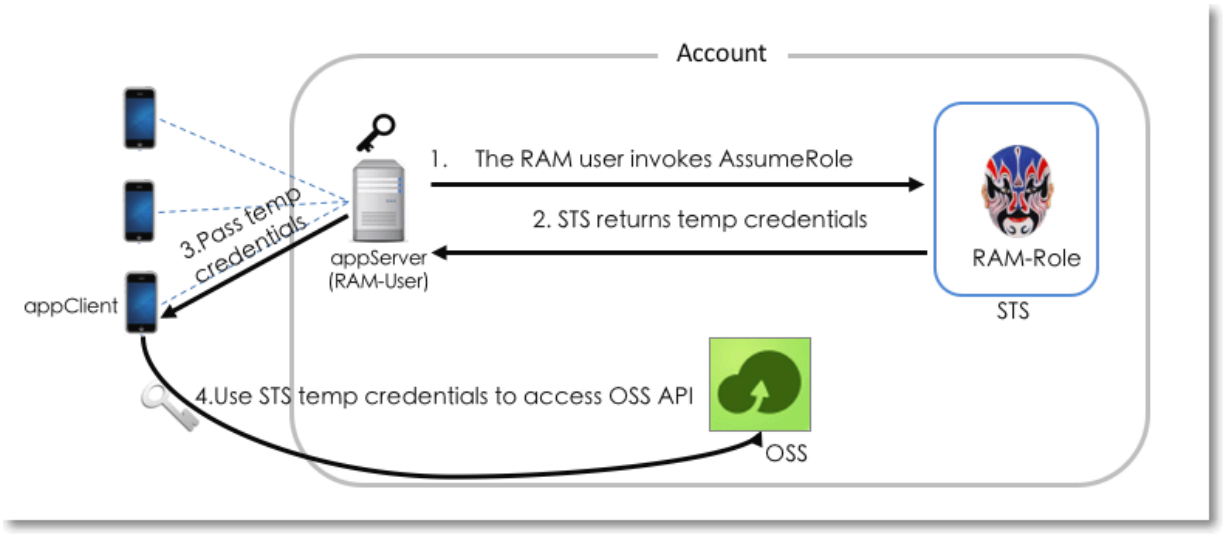
2. アカウント A は、ポリシー AliyunOSSReadOnlyAccess をロール oss-readonly に追加します。
3. アカウントAがAppServer用のRAMユーザー（たとえば、appserverという名前のユーザー）を作成してから、次のようにします。

   - RAM ユーザー用に AK を作成します。 つまり、RAM ユーザー（appserver）は API を呼び出すことができます。
   - AliyunSTSAssumeRoleAccess API を呼び出す許可を与えます。 つまり、RAM ユーザー（appserver）はロールを引き受けることができます。

ロールトークンとアクセスリソースの取得と転送

AppClient がロールトークンを取得、使用して OSS API を呼び出す手順は次のとおりです。

図 2-16 : 手順



手順は以下のとおりです。

1. appServerは、RAM ユーザー (appserver) の AK を使用して STS #unique_52 を呼び出します。 次は、aliyuncli を使用して AssumeRole API を呼び出す方法の例です。

> **注 :**
> アカウント A の AK を使用せず、AppServer の AK を構成する必要があります。

```
$ aliyuncli sts AssumeRole -- RoleArn acs : ram :: 11223344
 : role / oss - readonly -- RoleSessio nName client - 001
 {
     " AssumedRol eUser ": {
         " AssumedRol eId ": " 3915787525 73972854 : client - 001
 ",
         " Arn ": " acs : ram :: 11223344 : role / oss - readonly /
 client - 001 "
     },
     " Credential s ": {
         " AccessKeyS ecret ": " 93ci2umK1Q KNEja6WGqi
 1Ba7Q2Fv9P wxZqtVF2Vy nUvz ",
         " SecurityTo ken ": " CAES6AIIAR KAAUiwSHpk D3GXRMQk9s
 tDr3YSVbyG qanqkS + fPlEEkjZ + dlgFnGdCI2 PV93jksole 8ijH8dHJrH
 RA5JA1YCGs fX5hrzcNM3 7Vr4eVdWFV QhoCw0DXBp Hv // ZcITp +
 ELRr4MHsny GiErnDsXLk I7q / sbuWg6PACZ / jzQfEWQb / f7Y1Gh1TVF
 MuRjEzR2pz a1hUamszOG RCWTZZeEp0 WEFaayISMz kxNTc4NzUy
 NTczOTcyOD U0KgpjbGll bnQtMDAxMK T + lIHBKjoGUn NhTUQ1QkoK
 ATEaRQoFQW xsb3cSGwoM QWN0aW9uRX F1YWxzEgZB Y3Rpb24aAw
 oBKhIfCg5S ZXNvdXJjZU VxdWFscxII UmVzb3VyY2 UaAwoBKkoF
 NDMyNzRSBT I2ODQyWg9B c3N1bWVkUm 9sZVVzZXJg AGoSMzkxNT
 c4NzUyNTcz OTcyODU0cg llY3MtYWRt aW544Mbewo / 26AE =",
         " Expiration ": " 2016 - 01 - 13T15 : 02 : 37Z ",
         " AccessKeyI d ": " STS . F13GjskXTj k38dBY6YxJ tXAZk "
```

```
    },
    " RequestId ": " E1779AAB - E7AF - 47D6 - A9A4 - 53128708B6  CE
"
}
```

STS トークンのアクセス許可を制限する

- **前回 AssumeRole の呼び出し時に Policy パラメーターが指定されていないため、STS トークンは oss-readonly のすべての権限を持っています。**
- **`sample - bucket / 2015 / 01 / 01 /*. jpg` へのアクセスのみを許可するなど、トークンのアクセス許可をさらに制限する必要がある場合は、Policy パラメータを設定して、トークンのアクセス許可をより細かく制限できます。 以下はコマンドの例です。**

```
$  aliyuncli   sts   AssumeRole  -- RoleArn   acs : ram ::
 11223344 : role / oss - readonly  -- RoleSessio  nName   client
 - 002  -- Policy  "{\" Version \":\" 1 \", \" Statement \": [{\"
 Effect \":\" Allow \", \" Action \":\" oss : GetObject \", \"
 Resource \":\" acs : oss :*:*: sample - bucket / 2015 / 01 / 01 /
*. jpg \"}]}"
{
   " AssumedRol  eUser ": {
       " AssumedRol  eId ": " 3915787525  73972854 : client - 002
 ",
       " Arn ": " acs : ram :: 11223344 : role / oss - readonly /
 client - 002 "
   },
   " Credential  s ": {
       " AccessKeyS  ecret ": " 28Co5Vyx2X  htTqj3RJgd
 ud4ntyzrSN  dUvNygAj7x  EMow ",
       " SecurityTo  ken ": " CAESnQMIAR  KAASJgnzMz  lXVyJn4KI
 + FsysaIpTGm  8ns8Y74HVE  j0pOevO8ZW  Xrnnkz4a4r  BEPBAdFkh3
 197GUspruj  siU78Fkszx  hnQPKkQKcy  vPihoXqKvu  ukrQ /
 Uoudk31KAJ  Ez5o2EjlNU  REcxWjRDRS  ISMzkxNTc4  NzUyNTczOT
 cyODU0Kgpj  bGllbnQtMD  AxMKmZxIHB  KjoGUnNhTU  Q1Qn8KATEa
 egoFQWxsb3  cSJwoMQWN0  aW9uRXF1YW  xzEgZBY3Rp  b24aDwoNb3
 NzOkdldE9i  amVjdBJICg  5SZXNvdXJj  ZUVxdWFscx  IIUmVzb3Vy
 Y2UaLAoqYW  NzOm9zczoq  Oio6c2FtcG  xlLWJ1Y2tl  dC8yMDE1Lz
 AxLzAxLyou  anBnSgU0Mz  I3NFIFMjY4  NDJaD0Fzc3  VtZWRSb2xl
 VXNlcmAAah  IzOTE1Nzg3  NTI1NzM5Nz  I4NTRyCWVj  cy1hZG1pbn
 jgxt7Cj / boAQ ==",
       " Expiration ": " 2016 - 01 - 13T15 : 03 : 39Z ",
       " AccessKeyI  d ": " STS . FJ6EMcS1JL  ZgAcBJSTDG  1Z4CE "
   },
   " RequestId ": " 98835D9B - 86E5 - 4BB5 - A6DF - 9D3156ABA5  67
 "
}
```

また、トークンのデフォルトの有効期間は 3,600 秒です。 DurationSeconds パラメーターを使用して、トークンの有効期限を制限することができます（3,600 秒以内）。

2. appServer は資格情報を取得して解析します。
   - appServer は、AssumeRole API が返す資格情報の中から AccessKeyId、AccessKeySecret、および SecurityToken を取得します。
   - トークンの有効期間は比較的短いため、アプリでより長い有効期間が必要な場合、AppServer は新しいトークンを再発行する必要があります（たとえば、AppServe は 1,800 秒ごとにトークンを発行します）。
3. AppServer はトークンを安全に AppClient に送信します。
4. AppClient はトークンを使用してクラウドサービス API（OSS API など）に直接アクセスします。 以下は、aliyuncli がトークン（client-002 に対して発行）を使用して OSS オブジェクトにアクセスするためのコマンドの例です。

```
 Configure   STS - Token   syntax :  aliyuncli   oss   Config  --
 host  -- accessid  -- accesskey  -- sts_token
$  aliyuncli   oss   Config  -- host   oss . aliyuncs . com  --
 accessid   STS . FJ6EMcS1JL  ZgAcBJSTDG  1Z4CE  -- accesskey
 28Co5Vyx2X  htTqj3RJgd  ud4ntyzrSN  dUvNygAj7x  EMow  -- sts_token
   CAESnQMIAR  KAASJgnzMz  lXVyJn4KI + FsysaIpTGm  8ns8Y74HVE
 j0pOevO8ZW  Xrnnkz4a4r  BEPBAdFkh3  197GUspruj  siU78Fkszx
 hnQPKkQKcy  vPihoXqKvu  ukrQ / Uoudk31KAJ  Ez5o2EjlNU  REcxWjRDRS
 ISMzkxNTc4  NzUyNTczOT  cyODU0Kgpj  bGllbnQtMD  AxMKmZxIHB
 KjoGUnNhTU  Q1Qn8KATEa  egoFQWxsb3  cSJwoMQWN0  aW9uRXF1YW
 xzEgZBY3Rp  b24aDwoNb3  NzOkdldE9i  amVjdBJICg  5SZXNvdXJj
 ZUVxdWFscx  IIUmVzb3Vy  Y2UaLAoqYW  NzOm9zczoq  Oio6c2FtcG
 xlLWJ1Y2tl  dC8yMDE1Lz  AxLzAxLyou  anBnSgU0Mz  I3NFIFMjY4
 NDJaD0Fzc3  VtZWRSb2xl  VXNlcmAAah  IzOTE1Nzg3  NTI1NzM5Nz
 I4NTRyCWVj  cy1hZG1pbn  jgxt7Cj / boAQ ==
 Access   OSS   objects
$  aliyuncli   oss   Get   oss :// sample - bucket / 2015 / 01 / 01
 / grass . jpg   grass . jpg
```

参考資料

モバイルアプリケーションでの直接接続の詳細については、以下をご参照ください。

- #unique_53
- 権限コントロール
- モバイルアプリ向けのデータコールバック
- #unique_56

2.9.3 RAMロールを通じてクロスアカウントのリソースへのアクセル管理

本ドキュメントでは、特定シナリオでRAMロールを通じてクロスアカウントのリソースへのアクセス管理について説明します。

シナリオ

AとBはそれぞれ違う企業（チームまたはプロジェクト）を代表します。 Aは業務用で複数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、 OSS バケットなど) を購入したとします。

- 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Bに任せ、権限を付与しました。
- Bは、O&Mタスクをその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の委任契約を打ち切った場合、Aは、Bの権限を必要に応じて取り消すことができます。

要求分析

前述のシナリオに対する分析は次の通りです：

- AlibabaクラウドアカウントAとBの間の権限付与。アカウント A はリソースオーナーで、そのリソースの操作権限を B に付与しようと考えています。
- アカウント B は、そのサブユーザー (従業員またはアプリケーション) に権限を割り当てる必要があります。 Bの従業員は入社または退社しても、Aは権限を変更する必要はありません。
- AとBの間の協力関係が解消された場合、Aは、Bの権限を必要に応じて取り消すことができます。

ソリューション

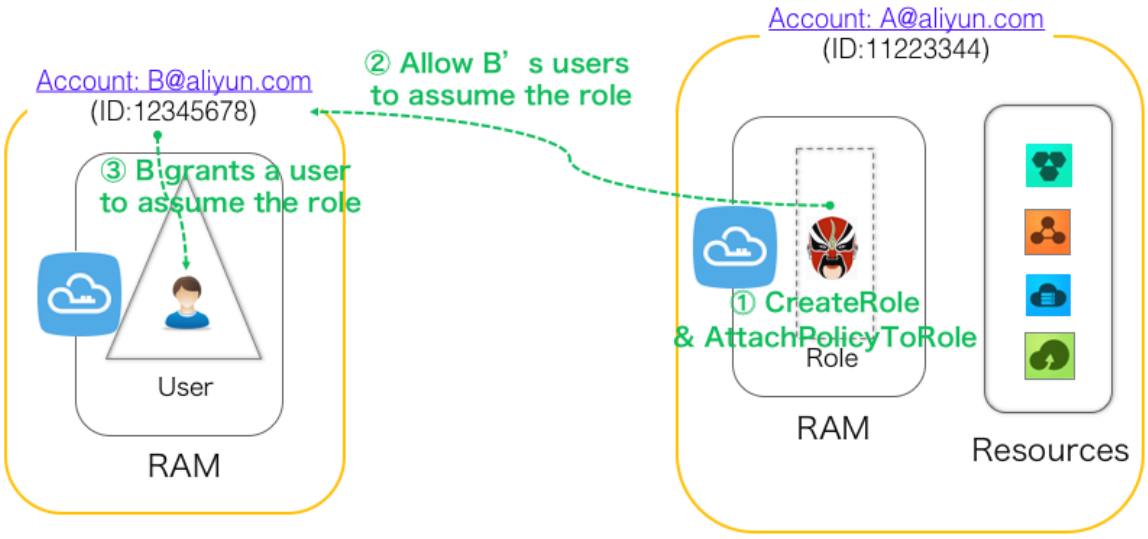
上記の各要求に応えて、RAMロールを通じてクロスアカウントへの権限付与及びリソースへのアクセス。

- AはRAMでロールを作成し、適切な権限を付与します。そしてBにロールの使用を許可します。 操作手順は、クロスアカウントの権限付与を参照してください。
- Bの従業員（RAMユーザー）はこのロールを使用する場合、Bは自主的に権限付与の管理を行えます。 O&M操作の実行時、BのRAMユーザーは 付与されたロールとしてAのリソースを操作できます。操作手順は、クロスアカウントリソースへのアクセスを参照してください。
- AとBはO&Mの委任契約を打ち切った場合、Aは、Bのロールの使用権限を取り消すだけでよいです Bのロールの使用権限が取り消された場合、 すべてのBのRAMユーザーはこのロールを使用できなくなります。 操作手順は、クロスアカウント権限の取り消しを参照してください。

クロスアカウントの権限付与

次の図は、RAMロールを通じてクロスアカウントに対する権限付与の方法を示しています。 A（アカウントID=11223344、エイリアス：company-a）がB（アカウントID=12345678、エイリアス：company-b） の従業員に ECS の操作権限を付与する必要があるとします。

図 2-17 : 操作手順は



次の通りです：

1. Aがユーザーロール（ロール名はecs-adminとします）を作成し、その他Alibabaクラウドアカウント （アカウントB：12345678） を信用できるアカウントにしました。BのRAMユーザーはこのロールの使用を許可されています。 操作手順は、#unique_12を参照してください。

   ロールの作成後、Aはロール詳細ページでロール情報を取得できます。

   - この例では、ロールのグローバル名ARN は：

     ```
     acs : ram :: 11223344 : role / ecs - admin
     ```

   - ロールのポリシー（Bにのみこのロールを使用できます） は次の通りです：

     ```
     " Statement ": [

      " Action ": " sts : AssumeRole ",
      " Effect ": " Allow ",
      " Principal ": {
        " RAM ": [
          " acs : ram :: 12345678 : root "

      }
     ```

```
" Version ": " 1 "
```

2. Aはロールecs-adminに#unique_14(AliyunECSFullAccess)を追加しました。
3. Bはその従業員（ユーザー名はzhangsanとします）のためにRAMユーザーを作成し、
   - ログインパスワードを設定しました。（ログインパスワードは123456とします）。つまりRAMユーザーはコンソールにログイン可能になりました。
   - さらに、STS AssumeRoleインターフェースの権限(AliyunSTSAssumeRoleAccess)が呼び出されています。つまり、RAMユーザーzhangsanにロールの使用や、ロールの切り替えを許可されています。

クロスアカウントリソースへのアクセス

BのRAMユーザーzhangsanはコンソールを通じてAのECSリソースにアクセスします。操作手順は次の通りです：

1. BのRAMユーザー（zhangsan）はコンソールにログインします。

   RAMユーザーはログイン時、エンタープライズ別名（company-b）、RAMユーザー名(zhangsan)、及びRAMユーザーパスワード(123456)を正確に入力する必要があります。
2. BのRAMユーザー(zhangsan)ロールの切り替えを行います。

   コンソールの右上にあるユーザーアイコンにマウスの矢印を移動し、そのメニューからスイッチIDをクリックし、ロール変更ページを開きます。エンタープライズ別名(company-a)、ロール名(ecs-admin)を正確に入力して、ロールをスイッチします。
3. BのRAMユーザー(zhangsan)はAのECSリソースを操作します。

クロスアカウント権限の取り消し

Aは、Bのロールecs-adminの使用を取り消します。操作手順は次の通りです：

1. AはRAMコンソールにログインし、ロール管理ページでロールecs-adminを検索し、ロール名、或いは管理をクリックし、ロールの詳細ページを開きます。
2. 右上の基本情報の編集をクリックします。ダイアログボックスで、ポリシーの内容から `acs : ram :: 12345678 : root` を削除します。（これでBはロールの信用できるクラウドアカウントから削除されました。）

   注：
   また、Aはロール管理ページから、ロールecs-adminを削除することも可能です。削除する前に、ロールに許可ポリシーがないか確認してください。

2.10 RAM操作の記録

2.10.1 ActionTrail を使用した RAM 操作の記録

本ドキュメントでは、ActionTrail を使用して Alibaba Cloud アカウントまたは RAM ユーザーの操作をリソースに記録する方法について説明します。

ActionTrail を使用して RAM 操作を表示

1. ActionTrail コンソール にログインします。
2. 履歴検索 ページで、フィルタ ドロップダウンリストを使用して対象のイベントを検索します。
3. イベントをクリックして、 イベントの表示 をクリックします。

ActionTrail で記録される操作

ActionTrail は以下の RAM 操作を記録できます。

- Alibaba Cloud アカウントまたは RAM ユーザーのログイン情報。 詳細については、#unique_60 をご参照ください.
- RAM コンソールでの操作。 次は、記録された操作イベントの例です。

```
{
    " apiVersion ":" 2015 - 05 - 01 ",
    " eventId ":" 2cc52dee - d8d2 - 40c2 - 8de0 - 3a2cf1df ****",
    " eventName ":" DeleteGrou  p ",
    " eventSourc  e ":" ram . aliyuncs . com ",
    " eventTime ":" 2015 - 11 - 03T13 : 41 : 49Z ",
    " eventType ":" ApiCall ",
    " eventVersi  on ":" 1 ",
    " requestId ":" 9AE24F49 - C52C - 4F0F - BCF9 - 9A4B8C22B1  47
 ",
    " requestPar  ameters ":{
        " GroupName ":" grp1 ",
    },
    " serviceNam  e ":" Ram ",
    " sourceIpAd  dress ":" 42 . 120 . XX . XX ",
    " userAgent ":" AliyunCons  ole ",
    " userIdenti  ty ":{
        " type ":" ram - user ",
        " principalI  d ":" 2741806465  4829 ****",
        " accountId ":" 1234567890  12 ****",
        " userName ":" Alice ",
        " sessionCon  text ":{
            " sessionAtt  ributes ":{
                " creationDa  te ":" 2015 - 11 - 03T13 : 41 : 48Z ",
                " mfaAuthent  icated ":" true "
            }
        }
    }
}
```

- RAM および STS API は、リソースの作成、変更および削除を要求します。 次は記録されたイベントの一例です。

```
{
    " apiVersion ": " 2015 - 05 - 01 ",
    " eventId ": " 234ef3c7 - 8938 - 4bd7 - bb80 - 11754b7b ****",
    " eventName ": " CreateGrou  p ",
    " eventSourc  e ": " ram . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T08 : 58 : 50Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 43274 ",
    " requestId ": " 1485748C - DB62 - 4693 - AB7E - 4BA3F3A970  E1
 ",
    " requestPar  ameters ": {
        " Comments ": " this   is   a   test   group ",
        " GroupName ": " grp1 "
    },
    " serviceNam  e ": " Ram ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " principalI  d ": " 2741806465  4829 ****",
        " accountId ": " 43274 ",
        " accessKeyI  d ": " f6Iz ******** EI4d ",
        " userName ": " Alice "
    }
}
```

次のステップ

操作の記録について詳しくは、#unique_61 をご参照ください。

2.11 Google Authenticatorのインストール方法とユーザーガイド

2.11.1 Google Authenticatorのインストール方法と使用ガイド

Google Authenticator は、TOTP(RFC 6238)プロトコルに対応した2段階認証アプリケーションです。 Googleがモバイルアプリケーションのユーザーを認証するためのものです。

OSを選択してください

- #unique_64
- #unique_65

注：

トークンは時間ベースなので、デバイスの時刻が正確に設定されているか確認してください。

2.11.2 iOS ベースの Google 認証システムのインストールおよび使用ガイド

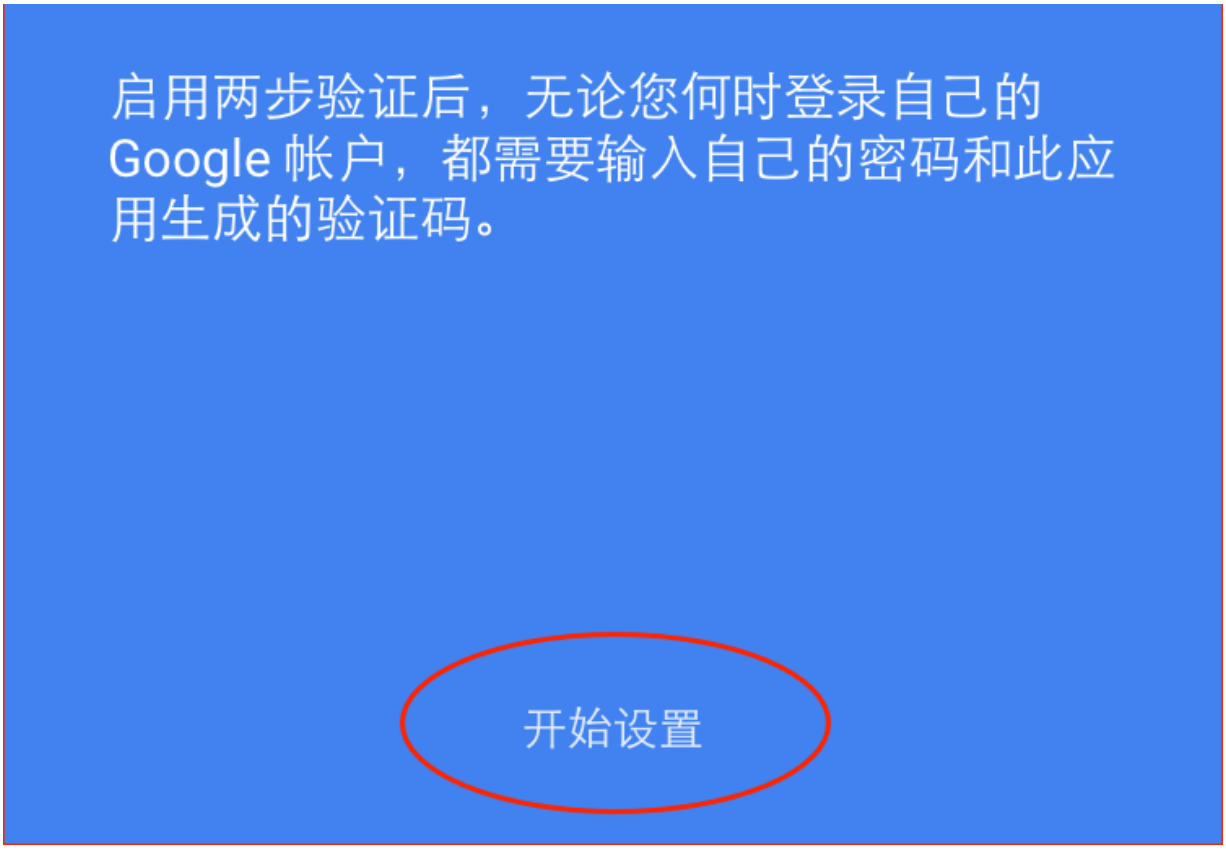
インストール

APPLEのAppストアにて“Google Authenticator”を検索しインストールできます。 或いは、次のQRコードをスキャンしてください

図 2-18 : インストール

設定

Google認証システムを起動し、一番下にある 設定を開始 ボタンをタップします。



バーコードをスキャン をタップし仮想 MFA デバイスの有効化ページで生成されたバーコードをスキャンします。

図 2-19 : バーコードのスキャン

コードをスキャンすると、次の画像が表示されます。このウィンドウには、アカウント名と MFA キーが表示されます。

図 2-20 : 認証

MFA ページで、2 つの MFA コードを連続で入力し、有効化 をクリックすることで、認証システムを

図 2-21 : バインドします。

2.11.3 AndroidのGoogle Authenticatorのインストール方法と使用ガイド

インストール方法

Google Authenticatorは、2段階認証サービスを実装するAndroidアプリケーションです。
このアプリケーションをインストールするには、Google Play StoreやアプリマーケットにてGoogle Authenticatorで検索し、インストールします。

或いは、次のQRコードをスキャンしてください。

図 2-22 : QRコード

設定

Google Authenticatorを起動し、開始をタップします。

図 2-23 : アカウントの追加

”バーコードをスキャン”をタップし、仮想MFAデバイスの有効化ページで生成されたバーコードをスキャンします。

図 2-24 : バーコードのスキャン

バーコードをスキャンすると、次の画面が表示されます。このウィンドウには、アカウント名とMFAキーが表示されます。

図 2-25 : 認証

仮想MFAデバイスの有効化ページで、2つのMFAコードを連続入力し、有効化をクリックすることで、認証システムを

図 2-26 : バインドします。