# 阿里云
# 访问控制

## 权限策略管理

文档版本：20190917

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
|  | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 |  **禁止:**<br>重置操作将丢失用户配置数据。 |
|  | 该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。 |  **警告:**<br>重启操作将导致业务中断，恢复业务所需时间约10分钟。 |
|  | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 |  **说明:**<br>您也可以通过按Ctrl + A选中全部文件。 |
| > | 多级菜单递进。 | 设置 > 网络 > 设置网络类型 |
| **粗体** | 表示按键、菜单、页面名称等UI元素。 | 单击 **确定**。 |
| `courier` 字体 | 命令。 | 执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。 |
| *## * | 表示参数、变量。 | `bae log list --instanceid` *`Instance_ID`* |
| []或者[a\|b] | 表示可选项，至多选择一个。 | `ipconfig` *`[-all\|-t]`* |
| {}或者{a\|b} | 表示必选项，至多选择一个。 | `swich` *`{stand \| slave}`* |

# 目录

# 1 权限策略概述

权限指在某种条件下允许或拒绝对某些资源执行某些操作，权限策略是一组访问权限的集合。

### 权限（Permission）

阿里云使用权限来描述用户、用户组、角色对具体资源的访问能力，下面为您介绍云账号、RAM 用户、资源创建者所拥有的权限：

- 云账号（资源属主）控制所有权限。
  - 每个资源有且仅有一个资源属主，该资源属主必须是云账号，对资源拥有完全控制权限。
  - 资源属主不一定是资源创建者。例如：一个 RAM 用户被授予创建资源的权限，该用户创建的资源归属于云账号，该用户是资源创建者但不是资源属主。
- RAM 用户（操作员）默认无任何权限。
  - RAM 用户代表的是操作员，其所有操作都需被云账号显式授权。
  - 新建的 RAM 用户默认没有任何操作权限，只有在被授权之后，才能通过控制台和 API 操作资源。
- 资源创建者（RAM 用户）默认对所创建资源的没有任何权限。
  - RAM 用户被授予创建资源的权限，用户将可以创建资源。
  - RAM 用户默认对所创建资源的没有任何权限，除非资源属主对 RAM 用户有显式的授权。

### 权限策略（Policy）

权限策略是用语法结构描述的一组权限的集合，可以精确地描述被授权的资源集、操作集以及授权条件。权限策略是描述权限集的一种简单语言规范，RAM 支持的语言规范请参考：#unique_4。

在 RAM 中，权限策略是一种资源实体，RAM 支持以下两种权限策略：

- 阿里云管理的系统策略：统一由阿里云创建，用户只能使用不能修改，策略的版本更新由阿里云维护。
- 客户管理的自定义策略：用户可以自主创建、更新和删除，策略的版本更新由客户自己维护。

通过为 RAM 用户、用户组或 RAM 角色绑定权限策略，可以获得权限策略中指定的访问权限。详情请参考：#unique_5、#unique_6和#unique_7。

### 为 RAM 主体绑定权限策略

为 RAM 主体授权，指为用户、用户组或角色绑定一个或多个权限策略。

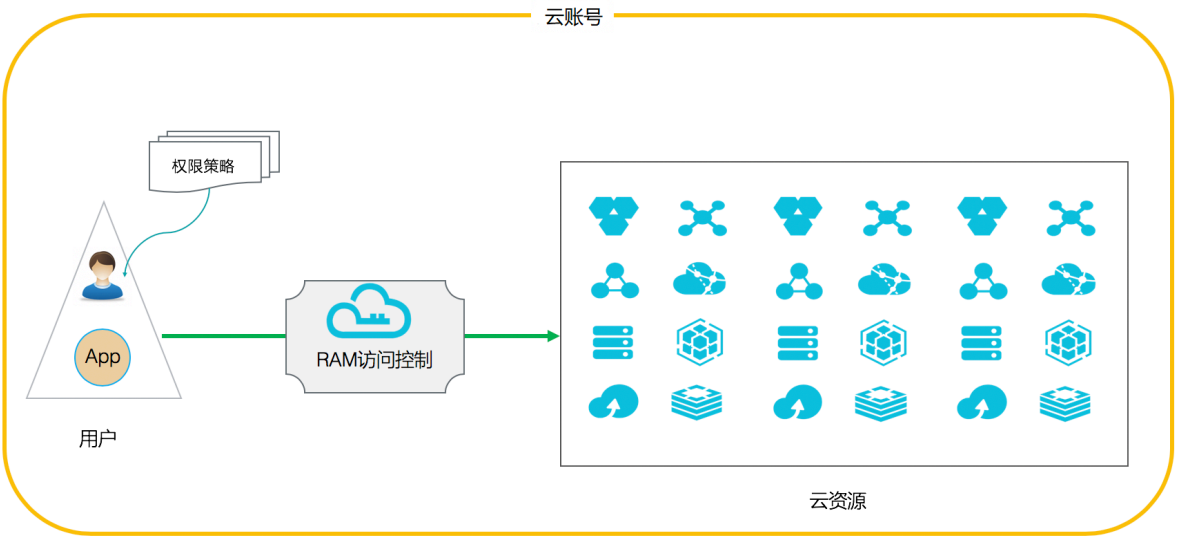
- 绑定的权限策略可以是系统策略也可以是自定义策略。
- 如果绑定的权限策略被更新，更新后的权限策略自动生效，无需重新绑定权限策略。

# 2 权限策略模型

阿里云提供了云账号内授权和资源组内授权两级授权能力，您可以根据需要选择合理的授权模型。

## 云账号内授权模型

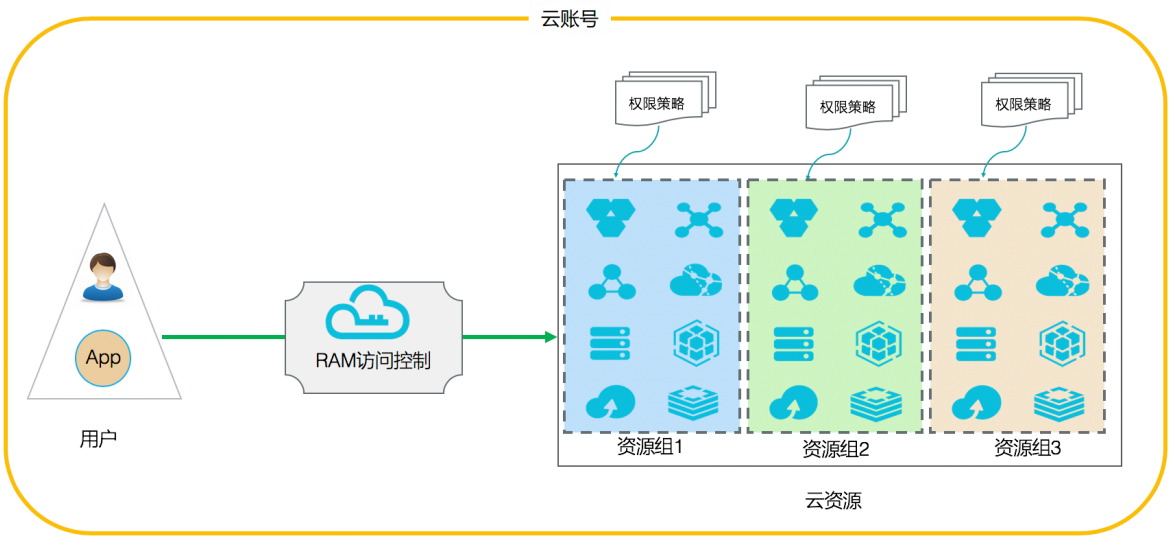
云账号内授权：对一个 RAM 身份主体添加权限策略时，该策略的可授权范围是云账号内的所有资源，这是最常见的一种权限模型。




## 资源组内授权模型

资源组内授权：在某个资源组内对一个 RAM 身份主体添加权限策略时，该策略的可授权范围仅仅是该资源组内的资源。

管理员：在资源组内拥有`AdministratorAccess`系统策略的用户，资源组创建者默认为管理员。资源组管理员可以在资源组的成员管理中添加其他的 RAM 用户并在资源组内进行授权。


云账号
权限策略
权限策略
权限策略
App
用户
RAM访问控制
资源组1
资源组2
资源组3
云资源

# 3 查看权限策略基本信息

本文为您介绍如何查看权限策略基本信息，包括权限策略名称、备注、策略类型和被引用次数等信息。

**操作步骤**

1. 登录 RAM 控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 在搜索框中，输入策略名称或备注。
4. 策略类型选择系统策略或自定义策略，可以查看权限策略。

> **说明:**
> 系统策略用户只能查看不能修改，自定义策略用户可以自行创建、查看和修改。

# 4 自定义策略

## 4.1 创建自定义策略

自定义策略可以更大程度的满足您的细粒度的要求，从而实现更灵活的权限管理。

**前提条件**

创建自定义策略前，需要先了解权限策略语言的基本结构和语法，请参考：#unique_12。

**操作步骤**

1. 登录 RAM 控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 单击新建权限策略。
4. 填写策略名称和备注。
5. 配置模式选择可视化配置或脚本配置。
   - 若选择可视化配置：单击添加授权语句，根据界面提示，对权限效力、操作名称和资源等进行配置。
   - 若选择脚本配置，请参考#unique_12编辑策略内容。
6. 单击确认。

## 4.2 修改自定义策略内容

当用户的权限发生变更时，您可以根据需要修改策略内容。

**背景信息**

当需要新增或撤销权限时，可能存在以下需求：

- 希望一段时间后，老的权限策略还能继续使用。
- 修改策略内容后，如果权限策略修改有误，需要使用修改前的权限策略。

**操作步骤**

1. 登录 RAM 控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 在权限策略名称列表下，单击目标权限策略名称。

说明:

RAM 支持两种权限策略，其中系统策略只能查看不支持修改，自定义策略支持创建、查看和修改。

4. 在策略内容页签下，单击修改策略内容。

说明:

可以参考#unique_12编辑策略内容。

5. 单击确认。

说明:

修改完成后，系统会自动生成一个新的版本，此版本将变为默认版本。

## 4.3 管理自定义策略版本

本文为您介绍如何管理自定义策略版本，包括查看权限版本、设置当前版本和删除权限版本。

**背景信息**

权限策略具备版本管理机制：

- 可以为一个权限策略保留多个版本。
- 如果版本数量超出限制，需要手动删除不需要的版本。
- 对于一个存在多版本的权限策略，只有一个版本是活跃的，即当前版本（默认版本）。
- 当前版本（默认版本）只能查看，不能删除。

**操作步骤**

1. 登录 RAM 控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 在权限策略名称列表下，单击目标权限策略名称。
4. 在版本管理页签下，您可以查看、设置和删除权限策略版本。
   - 查看权限版本：单击查看可以查看权限策略的版本号和策略内容。
   - 设置默认版本：找到目标版本，单击操作列表下的设为当前版本，可以将选定版本设为默认版本。
   - 删除权限版本：找到不需要的非默认版本，单击操作列表下的删除，单击确认，可以删除不需要的版本。

## 4.4 删除自定义策略

当权限发生变化或不再需要某个自定义策略时，可以删除自定义策略。

**前提条件**

- 删除权限策略前，应保证当前权限策略不存在多版本，只有一个默认版本。若该权限策略存在多个版本，您需要先删除除默认版本之外的所有版本。
- 删除权限策略前，应保证当前权限策略未被引用（即授予 RAM 用户、用户组或 RAM 角色）。若该权限策略已被引用，您需要在该权限策略的引用记录中移除授权。请参考：#unique_16。

**操作步骤**

1. 登录 RAM 控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 在权限策略名称列表下，找到目标权限策略，单击删除。
4. 单击确认。

# 5 管理权限策略引用记录

本文为您介绍如何管理权限策略引用记录，包括查看权限策略引用记录和删除权限策略引用记录。

## 操作步骤

1. 登录 RAM 控制台。
2. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
3. 在权限策略名称列表下，单击目标权限策略名称。
4. 在引用记录页签下，您可以查看或删除引用记录。
   - 查看引用记录：您可以查看被授权主体和主体类型等信息。
   - 删除引用记录（移除权限）：单击操作列表下的移除授权，单击确认可以移除引用记录。

# 6 权限策略语言

## 6.1 权限策略基本元素

权限策略基本元素是权限策略的基本组成部分，RAM 中使用权限策略来描述授权的具体内容，掌握权限策略基本元素的基本知识可以更好的使用权限策略。

### 基本元素

| 元素名称 | 描述 |
| --- | --- |
| 效力（Effect） | 授权效力包括两种：允许（Allow）和拒绝（Deny）。 |
| 操作（Action） | 操作是指对具体资源的操作。 |
| 资源（Resource） | 资源是指被授权的具体对象。 |
| 限制条件（Condition） | 限制条件是指授权生效的限制条件。 |

### 使用规则

- 效力（Effect）

  取值为：允许（Allow）或拒绝（Deny）。

  > 说明:
  > 当权限策略中既有允许（Allow）又有拒绝（Deny）的授权语句时，遵循 Deny 优先的原则。

  样例：`"Effect": "Allow"`。

- 操作（Action）

  操作支持多值，取值为：云服务所定义的 API 操作名称。

  > 说明:
  > 多数情况下 操作与云产品的 API 一一对应，但也有例外。各产品支持的操作列表请参考：#unique_20。

  格式：`<service-name>:<action-name>`。

  - `service-name`：阿里云产品名称。
  - `action-name: service`：相关的 API 操作接口名称。

  样例：`"Action": ["oss:ListBuckets", "ecs:Describe*", "rds:Describe*"]`

- **资源（Resource）**

  **资源是指被授权的具体对象。**

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

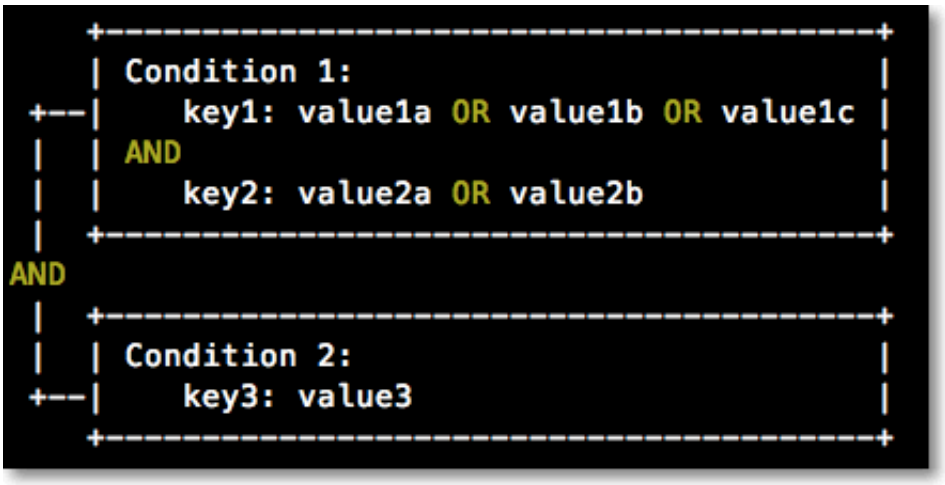
  - `acs`：**Alibaba Cloud Service 的首字母缩写，表示阿里云的公有云平台。**
  - `service-name`：**阿里云产品名称。**
  - `region`：**地域信息。如果不支持该项，可以使用通配符**`*`**来代替。**
  - `account-id`：**账号 ID。例如：**`1234567890123***`，**可以用**`*`**代替。**
  - `relative-id`：**与服务相关的资源描述部分，其语义由具体服务指定。这部分的格式支持树状结构（类似文件路径）。以 OSS 为例，表示一个 OSS 对象的格式为：**`relative-id = “mybucket/dir1/object1.jpg”`。

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

· 限制条件（Condition）

条件块（Condition Block）由一个或多个条件子句构成。一个条件子句由条件操作类型、条件关键字和条件值组成。

图 6-1: 条件块判断逻辑




逻辑说明

- 条件满足：一个条件关键字可以指定一个或多个值，在条件检查时，如果条件关键字的值与指定值中的某一个相同，即可判定条件满足。
- 条件子句满足：同一条件操作类型的条件子句下，若有多个条件关键字，所有条件关键字必须同时满足，才能判定该条件子句满足。
- 条件块满足：条件块下的所有条件子句同时满足的情况下，才能判定该条件块满足。

条件操作类型

条件操作类型包括：字符串类型（String）、数字类型（Numeric）、日期类型（Date and time）、布尔类型（Boolean）和 IP 地址类型（IP address）。

| 条件操作类型 | 支持类型 |
| --- | --- |
| 字符串类型（String） | - StringEquals<br>- StringNotEquals<br>- StringEqualsIgnoreCase<br>- StringNotEqualsIgnoreCase<br>- StringLike<br>- StringNotLike |

| 条件操作类型 | 支持类型 |
| --- | --- |
| 数字类型（Numeric） | - NumericEquals<br>- NumericNotEquals<br>- NumericLessThan<br>- NumericLessThanEquals<br>- NumericGreaterThan<br>- NumericGreaterThanEquals |
| 日期类型（Date and time） | - DateEquals<br>- DateNotEquals<br>- DateLessThan<br>- DateLessThanEquals<br>- DateGreaterThan<br>- DateGreaterThanEquals |
| 布尔类型（Boolean） | Bool |
| IP 地址类型（IP address） | - IpAddress<br>- NotIpAddress |

**条件关键字**

- **阿里云通用条件关键字命名格式：**

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

| 通用条件关键字 | 类型 | 描述 |
| --- | --- | --- |
| `acs:CurrentTime` | Date and time | Web Server 接收到请求的时间。以 ISO 8601 格式表示，例如：`2012-11-11T23:59:59Z`。 |
| `acs:SecureTransport` | Boolean | 发送请求是否使用了安全信道。例如：HTTPS。 |
| `acs:SourceIp` | IP address | 发送请求时的客户端 IP 地址。 |

| 通用条件关键字 | 类型 | 描述 |
| --- | --- | --- |
| acs:MFAPresent | Boolean | 用户登录时是否使用了多因素认证。 |

- 阿里云产品级别条件关键字命名格式：

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

| 产品级别条件关键字 | 产品名称 | 类型 | 描述 |
| --- | --- | --- | --- |
| ecs:tag/<tag-key> | ECS | String | ECS 资源的标签关键字，可自定义。 |
| rds:ResourceTag/<tag-key> | RDS | String | RDS 资源的标签关键字，可自定义。 |
| oss:Delimiter | OSS | String | OSS 对 Object 名字进行分组的分隔符。 |
| oss:Prefix | OSS | String | OSS Object 名称的前缀。 |

## 6.2 权限策略语法和结构

本文介绍 RAM 中权限策略的语法和结构，帮助您正确理解权限策略语法，以完成创建或更新权限策略。

### 运用权限策略语法的前提条件

运用权限策略语法前，首先应了解权限策略字符及其使用规则。

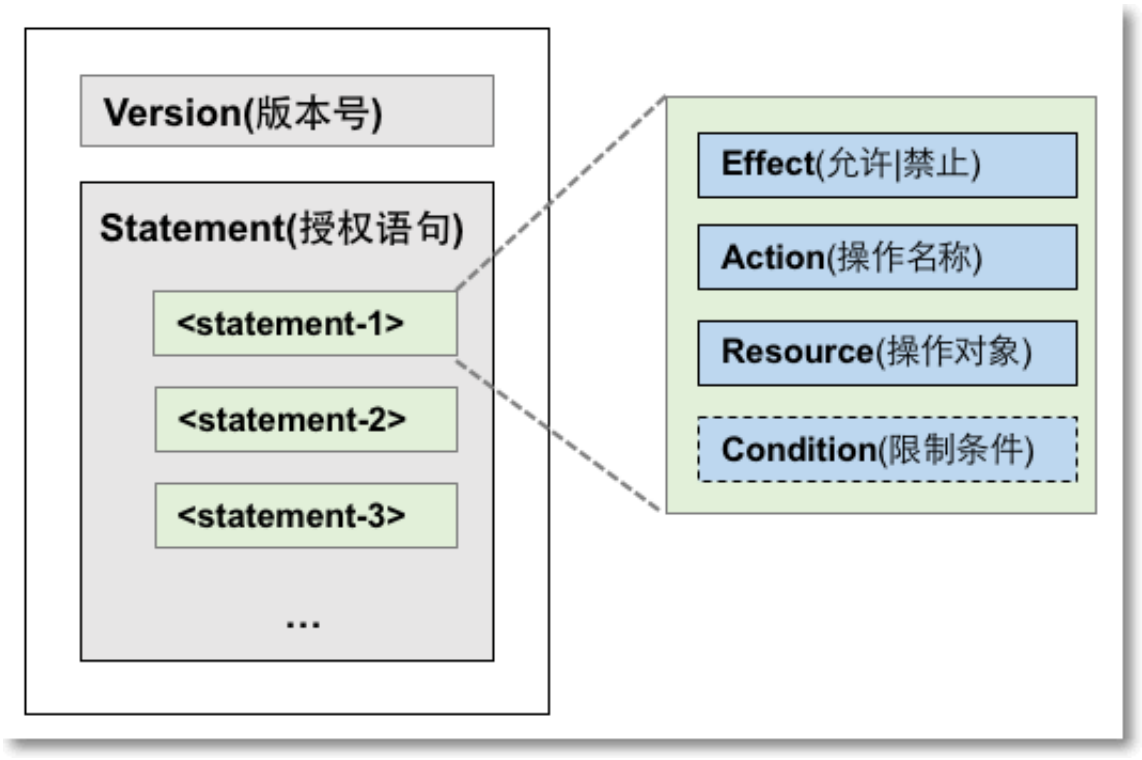
- 权限策略字符
  - 权限策略中所包含的 JSON 字符：`{ } [ ] " , :`。
  - 描述语法使用的特殊字符：`= < > ( ) |`。

- 字符使用规则
  - 当一个元素允许多值时，可以使用下述两种方式表达，效果相同。
    - 使用逗号和省略号进行表达。例如：`[ <action_string>, <action_string>, ...]`。
    - 使用单值进行表达。例如：`"Action": [<action_string>]` 和 `"Action": <action_string>`。
  - 元素带有问号表示此元素是一个可选元素。例如：`<condition_block?>`。
  - 多值之间用竖线 `|` 隔开，表示取值只能选取这些值中的某一个。例如：`("Allow" | "Deny")`。
  - 使用双引号的元素，表示此元素是文本串。例如：`<version_block> = "Version" : ("1")`。

### 权限策略结构

权限策略结构包括：

- 版本号。
- 授权语句列表。每条授权语句包括授权效力（Effect）、操作（Action）、资源（Resource）以及限制条件（Condition，可选项）。



### 权限策略语法

```
policy  = {
     <version_block>,
     <statement_block>
}
<version_block> = "Version" : ("1")
<statement_block> = "Statement" : [ <statement>, <statement>, ... ]
<statement> = {
    <effect_block>,
    <action_block>,
    <resource_block>,
    <condition_block?>
}
<effect_block> = "Effect" : ("Allow" | "Deny")
<action_block> = ("Action" | "NotAction") :
    ("*" | [<action_string>, <action_string>, ...])
<resource_block> = ("Resource" | "NotResource") :
    ("*" | [<resource_string>, <resource_string>, ...])
<condition_block> = "Condition" : <condition_map>
<condition_map> = {
  <condition_type_string> : {
      <condition_key_string> : <condition_value_list>,
      <condition_key_string> : <condition_value_list>,
      ...
  },
  <condition_type_string> : {
      <condition_key_string> : <condition_value_list>,
      <condition_key_string> : <condition_value_list>,
      ...
  }, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("String" | "Number" | "Boolean")
```

**权限策略语法说明：**

- **版本：当前支持的权限策略版本为 1。**
- **授权语句：一个权限策略可以有多条授权语句。**
  - **每条授权语句的效力为：`Allow`或`Deny`。**

    **说明：**

    **一条授权语句中，操作（Action）和资源（Resource）都支持多值。**
  - **每条授权语句都支持独立的限制条件（Condition）。**

    **说明：**

    **一个条件块可以支持多种条件操作类型，以及多种条件的逻辑组合。**
- **Deny 优先原则：一个用户可以被授予多个权限策略，当这些权限策略同时包含`Allow`和`Deny`时，遵循 Deny 优先原则。**

- 元素取值：
  - 当元素取值为数字（Number）或布尔值（Boolean）时，与字符串类似，需要使用双引号。
  - 当元素取值为字符串值（String）时，支持使用*和?进行模糊匹配。
    - *代表 0 个或多个任意的英文字母。 例如：ecs:Describe* 表示 ECS 的所有以Describe开头的操作。
    - ?代表 1 个任意的英文字母。

权限策略格式检查

RAM 仅支持 JSON 格式。当创建或更新权限策略时，RAM 会首先检查 JSON 格式的正确性。

- 关于 JSON 的语法标准请参考：RFC 7159。
- 您也可以使用一些在线的 JSON 格式验证器和编辑器来校验 JSON 文本的有效性。

## 6.3 权限策略检查规则

本文为您介绍了几种不同的权限策略检查规则，掌握权限策略检查规则可以更好的理解权限策略。

权限策略检查规则

在 RAM 中访问阿里云资源分为三种类型：以主账号身份访问、以 RAM 用户身份访问、以 RAM 角色身份访问。

针对上述不同的访问类型，系统的权限检查规则如下表所示。

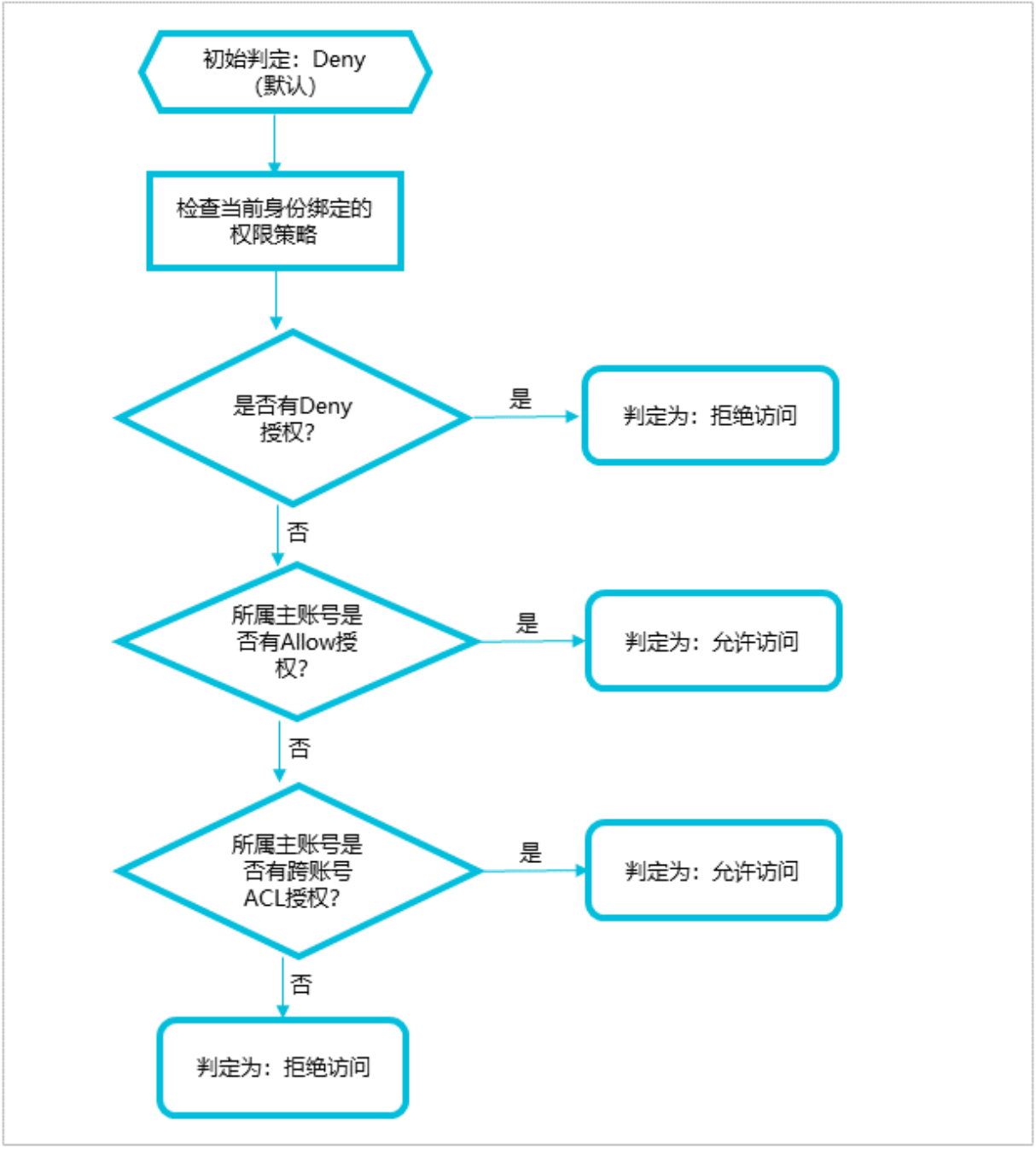
| 访问类型 | 权限检查规则 |
| --- | --- |
| 以主账号身份访问 | 主账号是资源所有者，默认可以访问该账号下的所有资源。<br>  说明:<br>少数阿里云产品（例如：日志服务）支持跨云账号进行访问控制列表（ACL）授权，如果通过 ACL 授权检查，则允许访问相应资源。 |

| 访问类型 | 权限检查规则 |
| --- | --- |
| 以 RAM 用户身份访问 | · 主账号对 RAM 用户有显式的授权。<br>· RAM 用户所属的主账号对资源有访问权限。<br><br>说明:<br>RAM 用户访问资源时，默认没有任何权限，以上条件需同时满足 RAM 用户才能访问相应资源。<br><br>具体权限检查规则请参考：RAM 用户的权限策略检查规则。 |
| 以 RAM 角色身份访问 | · RAM 角色令牌有相应的权限策略。<br>RAM 角色令牌相关信息，请参考：STS 简介。<br>· 主账号对 RAM 角色有显式的授权。<br>· RAM 角色所属的主账号对资源有访问权限。<br><br>说明:<br>RAM 角色访问资源时，默认没有任何权限，以上条件需同时满足 RAM 角色才能访问相应资源。<br><br>具体权限检查规则请参考：RAM 角色的权限策略检查规则。 |

### RAM 用户的权限策略检查规则

RAM 用户默认没有任何权限，主账号对 RAM 用户进行显示授权后，RAM 用户可以访问相应的资源。

说明:
权限策略支持 Allow（允许）和 Deny（禁止）两种授权类型，当同时出现 Allow 和 Deny 授权时，遵循 Deny 优先原则。




1. 检查 RAM 用户所绑定权限策略是否有授权：
   - 如果有 Deny 授权，判定为：拒绝访问。
   - 否则，需要进行下一步检查。
2. 检查 RAM 用户所属的主账号是否有访问权限：
   - 如果有 Allow 授权，判定为：允许访问。
   - 否则，需要进行下一步检查。

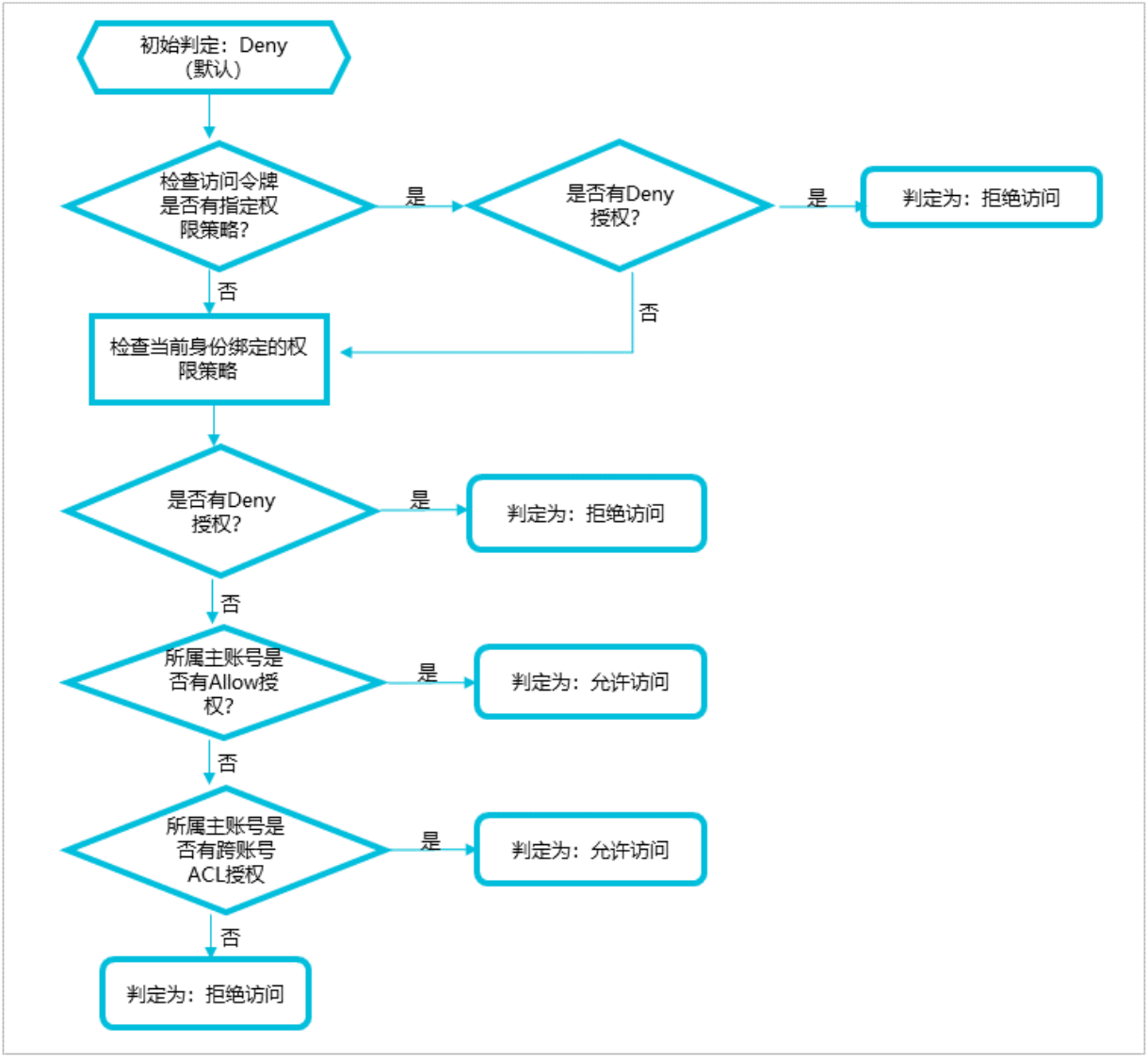
3. 检查 RAM 用户所属的主账号是否有跨账号 ACL 授权：

   · 如果有 ACL 授权，判定为：允许访问。

   · 否则，判定为：拒绝访问。

### RAM 角色的权限策略检查规则

RAM 角色可以使用角色访问令牌访问阿里云资源，调用 #unique_24，请求参数Policy可以控制访问阿里云资源的权限。




1. 检查访问令牌是否有指定权限策略：

   · 如果有指定权限策略，需要查看是否有 Deny 授权：

     - 如果有 Deny 授权，判定为：拒绝访问。
     - 否则，需要检查 RAM 角色所绑定的权限策略。

   · 如果没有指定权限策略，需要检查 RAM 角色所绑定的权限策略。

2. 检查 RAM 角色所绑定的权限策略是否有授权：
   - 如果有 Deny 授权，判定为：拒绝访问。
   - 否则，需要进行下一步检查。
3. 检查 RAM 角色所属的主账号是否有访问权限：
   - 如果有 Allow 授权，判定为：允许访问。
   - 否则，需要进行下一步检查。
4. 检查 RAM 角色所属的主账号是否有跨账号 ACL 授权：
   - 如果有 ACL 授权，判定为：允许访问。
   - 否则，判定为：拒绝访问。

# 7 最佳实践

## 7.1 RAM企业上云安全实践

本文为您介绍当企业上云之后，通过RAM进行安全管控，帮助您实现简单管理账号、统一分配权限、集中管控资源，建立安全完善的资源控制体系。

### 前提条件

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

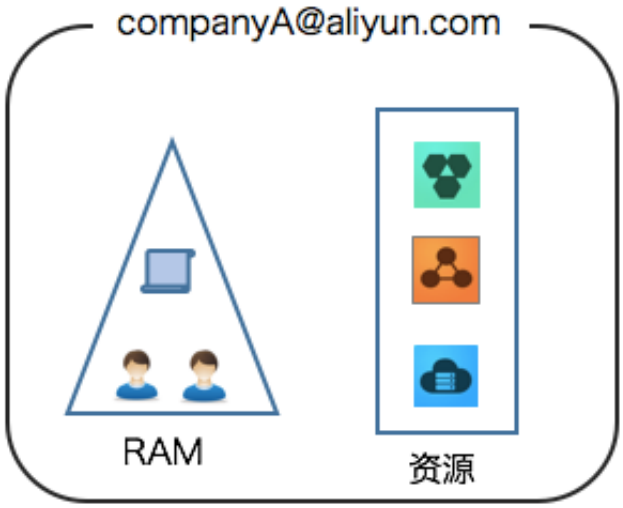
### 背景信息

某些公司使用RAM初期，对RAM的优势不够了解，也对云资源的安全管理要求不高。但是当初创企业成长为大型公司或大型企业客户迁移上云，组织结构更加复杂，对云资源的安全管理需求也更加强烈，需要建立安全完善的资源控制体系。

- 存在多用户协同操作，RAM用户分工不同，各司其职。
- 云账号不想与其他RAM用户共享云账号密钥，密钥泄露风险较大。
- RAM用户对资源的访问方式多种多样，资源泄露风险高。
- 某些RAM用户离开组织时，需要收回其对资源的访问权限。

### 解决方案

使用RAM，您可以创建、管理RAM用户，并可以控制这些RAM用户对资源的操作权限。当您的企业存在多用户协同操作资源时，使用RAM可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，管理更加方便，权限更加明确，信息更加安全。




安全管理实施方案

- 创建独立的RAM用户

  企业只需使用一个云账号。通过RAM为名下的不同操作员创建独立的RAM用户，进行分权管理，不使用云账号进行日常运维管理。

  详情请参见#unique_27。

- 将控制台用户与API用户分离

  不建议给一个RAM用户同时创建用于控制台操作的登录密码和用于API操作的访问密钥。

  - 对于应用程序账号，只需要通过OpenAPI访问云资源，只需要给它创建访问密钥即可。
  - 对于员工账号，只需要通过控制台操作云资源，只需要设置登录密码即可。

  详情请参见#unique_27。

- 创建用户并进行分组

  当云账号下有多个RAM用户时，可以通过创建用户组对职责相同的RAM用户进行分类并授权。

  详情请参见#unique_28。

- 给不同用户组分配最小权限

  您可以使用系统策略为用户或用户组绑定合理的权限策略，如果您需要更精细粒度的权限策略，也可以选择使用自定义策略。通过为用户或用户组授予最小权限，可以更好的限制用户对资源的操作权限。

  详情请参见创建自定义策略。

- 为用户登录配置强密码策略

  您可以通过RAM控制台设置密码策略，如密码长度、密码中必须包含元素、密码有效期等。如果允许RAM用户更改登录密码，那么应该要求RAM用户创建强密码并且定期轮换登录密码或访问密钥。

  详情请参见#unique_29。

- 为云账号开启多因素认证

  开启多因素认证（Multi-factor authentication，MFA）可以提高账号的安全性，在用户名和密码之外再增加一层安全保护。启用MFA后，用户登录阿里云时，系统将要求输入两层安全要素：

  1. 第一安全要素：用户名和密码
  2. 第二安全要素：多因素认证设备生成的验证码

  详情请参见#unique_30。

- 为用户开启SSO单点登录功能

  开启SSO单点登录后，企业内部账号进行统一的身份认证，实现使用企业本地账号登录阿里云才能访问相应资源。

  详情请参见#unique_31。

- 不要为云账号创建访问密钥

  由于云账号对名下资源有完全控制权限，AccessKey与登录密码具有同样的权力，AccessKey用于程序访问，登录密码用于控制台登录。为了避免因访问密钥泄露带来的信息泄露，不建议您创建云账号访问密钥并使用该密钥进行日常工作。

  您可以通过为RAM用户创建访问密钥，使用RAM用户进行日常工作。

  详情请参见#unique_32。

- 使用策略限制条件来增强安全性

  要求用户必须使用安全信道（例如：SSL）、在指定时间范围或在指定源IP条件下才能操作指定的云资源。

  详情请参见权限策略基本元素。

- 集中控制云资源

  阿里云默认云账号是资源的拥有者，掌握完全控制权。RAM用户对资源只有使用权，没有所有权。这一特性可以方便您对用户创建的实例或数据进行集中控制。

  - 当用户离开组织：只需要将对应的账号移除，即可撤销所有权限。
  - 当用户加入组织：只需创建新的账号，设置登录密码或访问密钥并为 RAM 用户授权。

  详情请参见#unique_33。

- 使用STS给用户授权临时权限

  STS （Security Token Service）是RAM的一个扩展授权服务，使用STS访问令牌可以给用户授予临时权限，您可以根据需要来定义访问令牌的权限和自动过期时间，可以让授权更加可控。

  详情请参见#unique_34。

操作结果

遵循最佳安全实践原则，企业上云之后，综合利用这些保护机制，建立安全完善的资源控制体系，可以更有效的保护账号及资产的安全。

更多信息

企业上云以后通过RAM进行运维划分，根据不同的职责，划分不同的运维人员，方便管理和控制。详情请参见#unique_35。