阿里云
访问控制

权限策略管理

文档版本：20191112

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. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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:** 重置操作将丢失用户配置数据。
	该类警示信息可能会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:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	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:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`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。	`switch {active|stand}`

目录

1 权限策略概览

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RAM操作资源。
- 资源创建者（RAM用户）默认对所创建资源没有任何权限。
  - 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见**权限策略语法和结构**。

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。详情请参见*#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。

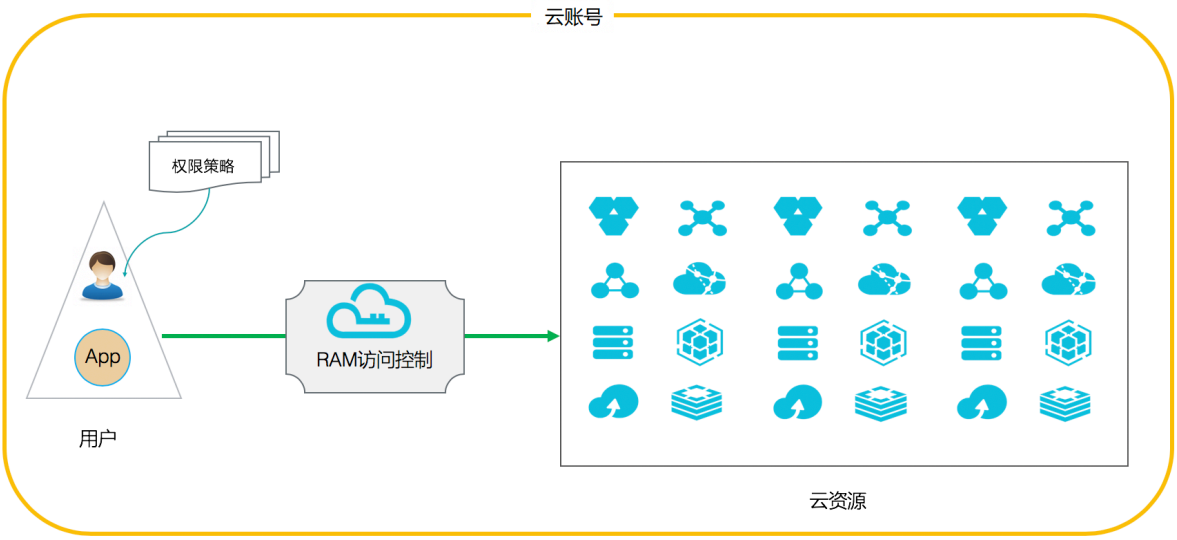
- 绑定的权限策略可以是系统策略也可以是自定义策略。
- 如果绑定的权限策略被更新，更新后的权限策略自动生效，无需重新绑定权限策略。

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

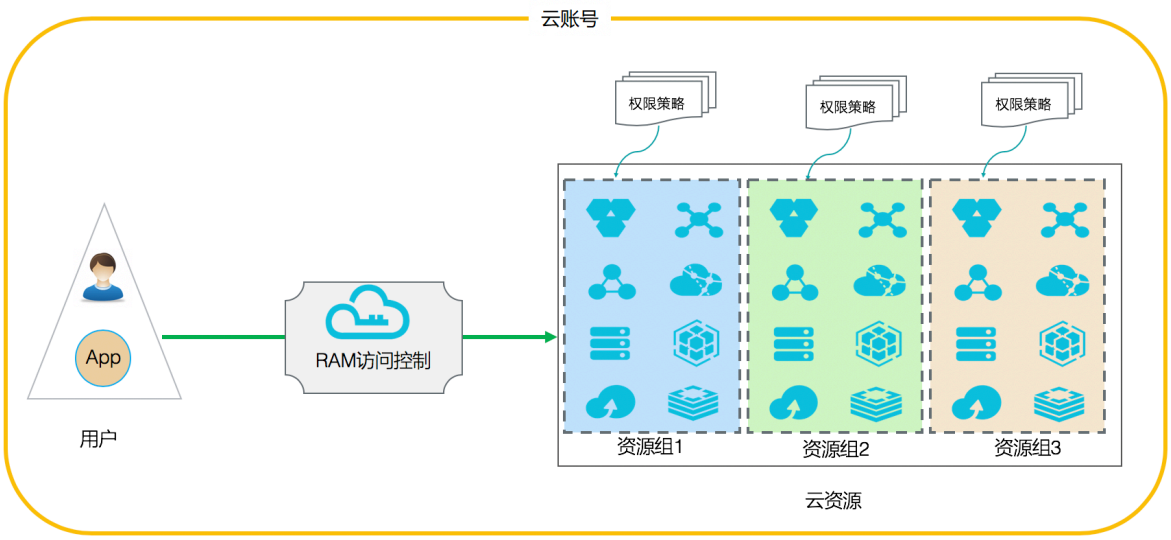
云账号内授权：对一个RAM身份主体添加权限策略时，该策略的可授权范围是云账号内的所有资源，这是最常见的一种权限模型。



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. 云账号登录*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。

相关文档

#unique_10

#unique_11

#unique_12

#unique_13

4 自定义策略

4.1 创建自定义策略

如果系统策略无法满足您的需求，您可以通过创建自定义策略实现精细化权限管理。

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，请参见权限策略语法和结构。

操作步骤

1. 云账号登录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. 输入策略名称和备注。
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，请参考权限策略语法和结构编辑策略内容。
6. 单击确定。

相关文档
#unique_16

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。

操作步骤

1. 云账号登录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能修改，自定义策略可以创建、查看和修改。

4. 在策略内容页签下，单击修改策略内容。

> 说明:
> 请参见权限策略语法和结构编辑策略内容。

5. 单击确定。

> 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。

相关文档
#unique_18

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. 云账号登录*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。

相关文档
#unique_20
#unique_21
#unique_22

#unique_23

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。详情请参见管理权限策略引用记录。**

操作步骤

1. **云账号登录*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. **从策略类型下拉列表中选择自定义策略。**
4. **在权限策略名称列表下，找到目标权限策略，单击删除。**
5. **单击确认。**

相关文档

#unique_26

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. 云账号登录*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。

相关文档

#unique_27

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见**#unique_30。

  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。

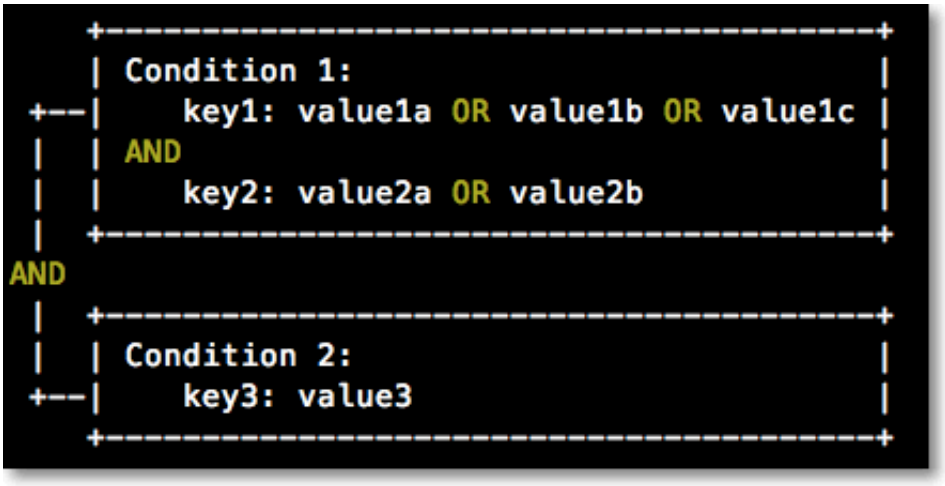
  格式： `acs:<service-name>:<region>:<account-id>:<relative-id>`。

  - `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：`123456789012****`，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。



  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 - StringNotEquals - StringEqualsIgnoreCase - StringNotEqualsIgnoreCase - StringLike - StringNotLike

条件操作类型	支持类型
数字类型（Numeric）	- NumericEquals - NumericNotEquals - NumericLessThan - NumericLessThanEquals - NumericGreaterThan - NumericGreaterThanEquals
日期类型（Date and time）	- DateEquals - DateNotEquals - DateLessThan - DateLessThanEquals - DateGreaterThan - DateGreaterThanEquals
布尔类型（Boolean）	Bool
IP 地址类型（IP address）	- IpAddress - 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。 **说明:** `acs:SourceIp`的取值如果是单个IP地址，需要写明具体的IP地址（例如10.0.0.1），不能使用IP地址段（例如10.0.0.1/32）。

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。

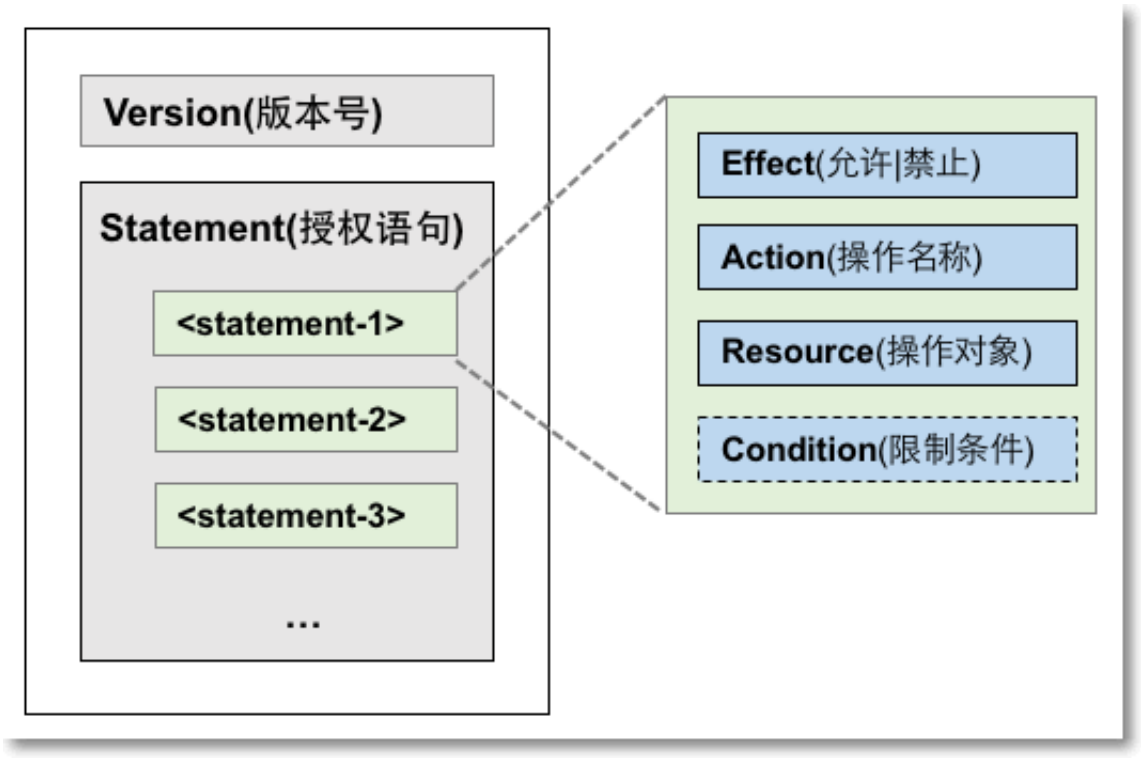
- 权限策略字符
  - 权限策略中所包含的JSON字符：{ } [ ] " , :。
  - 描述语法使用的特殊字符：= < > ( ) |。

- **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的语法标准请参见*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用户身份访问或以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。

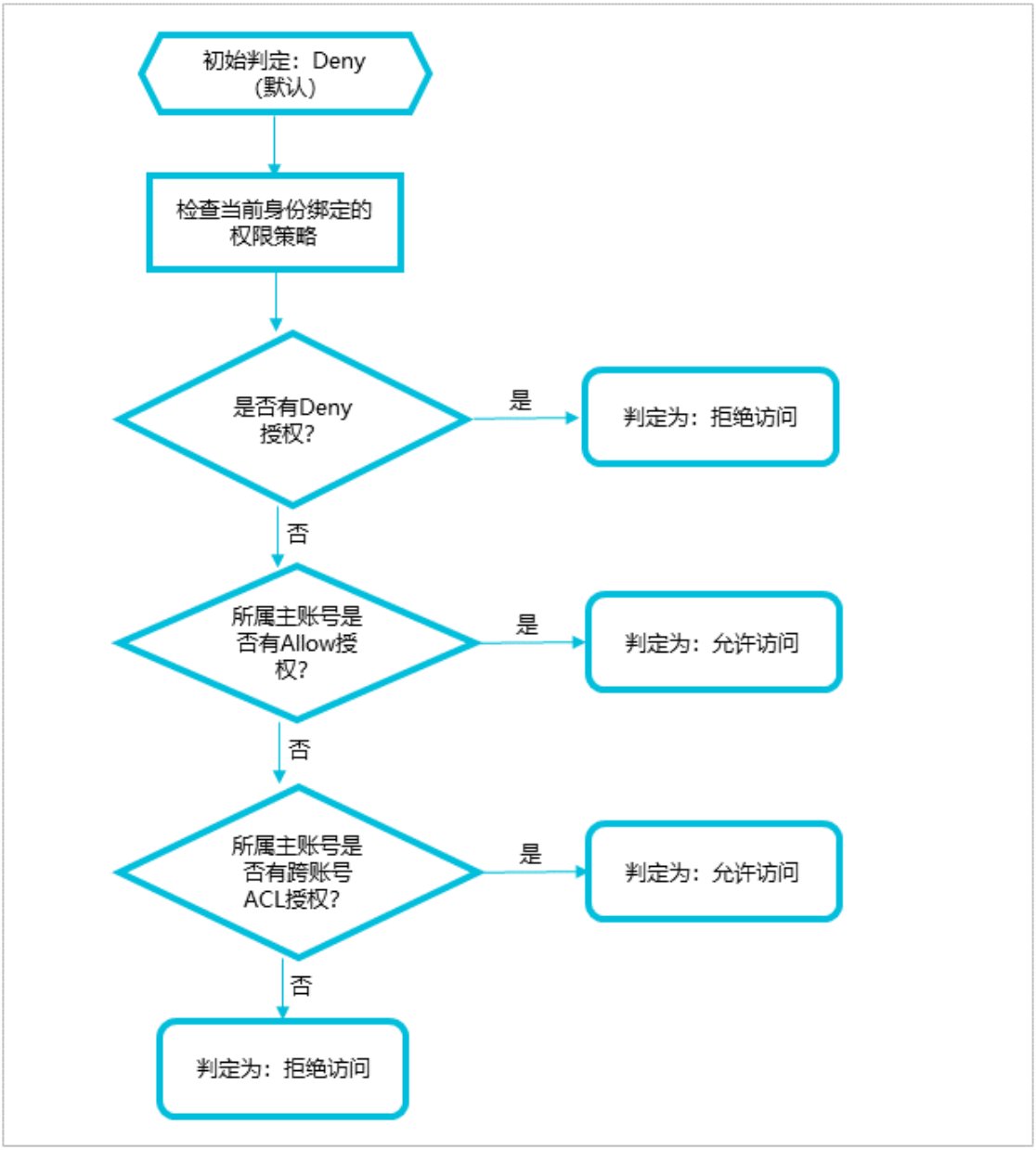
访问类型	权限检查规则
以主账号身份访问	主账号是资源所有者，默认可以访问该账号下的所有资源。 说明: 少数阿里云产品（例如：日志服务）支持跨云账号进行访问控制列表（ACL）授权，如果通过ACL授权检查，则允许访问相应资源。

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。 · RAM用户所属的主账号对资源有访问权限。 · RAM用户所属的主账号有跨账号ACL授权。 说明: 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。 具体权限检查规则请参见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。 RAM角色令牌相关信息，请参见#unique_32。 · 主账号对RAM角色有显式的授权。 · RAM角色所属的主账号对资源有访问权限。 · RAM角色所属的主账号有跨账号ACL授权 说明: 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。 具体权限检查规则请参见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。

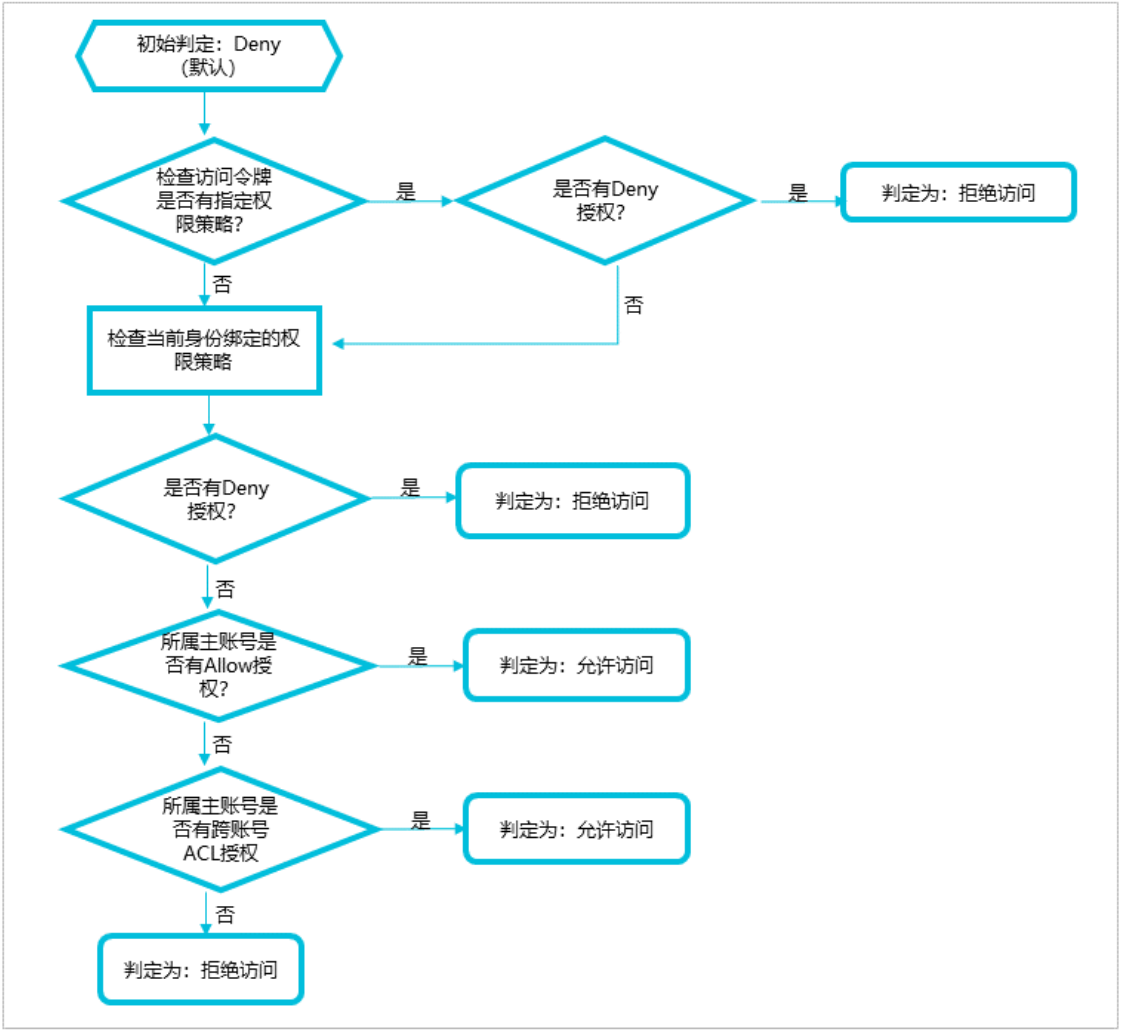
说明:
权限策略支持Allow（允许）和Deny（禁止）两种授权类型，当同时出现Allow和Deny授权时，遵循Deny优先原则。



1. 检查RAM用户所绑定权限策略：
   - 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API *#unique_33*，其中请求参数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：

- **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 权限策略示例库

7.1 重启ECS实例

本文为您提供重启ECS实例的参考示例。

以下策略表示：仅被授予此策略的RAM用户启用MFA并使用MFA登录时，才具有重启ECS实例的权限。您可以通过设置`Condition`下`acs:MFAPresent`的值为`true`来实现。

```
{
  "Statement": [
    {
      "Action": "ecs:RestartInstance",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "acs:MFAPresent": "true"
        }
      }
    }
  ],
  "Version": "1"
}
```

说明：

`Condition`（限制条件）只针对当前权限策略描述的操作有效。您可以修改`acs:MFAPresent`的值为`true`或`false`。

7.2 通过指定的IP地址访问阿里云

本文为您提供限制RAM用户登录IP地址的参考示例。

下述策略表示：被授予此策略的RAM用户只能通过192.168.0.0/16这个IP地址访问ECS。您可以通过设置`Condition`下`acs:SourceIp`的值为`192.168.0.0/16`来实现。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "192.168.0.0/16"
        }
      }
    }
  ],
```

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

说明:

Condition（限制条件）只针对当前权限策略描述的操作有效。您可以修改IP：192.168.0.0/16为企业的专用网络IP地址。

7.3 在指定的时间段访问阿里云

本文为您提供限制RAM用户登录时间段的参考示例。

下述策略表示：被授予此策略的RAM用户只能在特定时间段（北京时间2019年8月12日17：00之前）访问ECS。您可以通过设置Condition下acs:CurrentTime的值为2019-08-12T17:00:00+08:00来实现。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
          "DateLessThan": {
              "acs:CurrentTime": "2019-08-12T17:00:00+08:00"
          }
      }
    }
  ],
  "Version": "1"
}
```

说明:

Condition（限制条件）只针对当前权限策略描述的操作有效。您可以修改时间2019-08-12T17:00:00+08:00为企业允许访问的时间。

7.4 通过指定的访问方式访问阿里云

本文为您提供限制RAM用户访问方式的参考示例。

下述策略表示：被授予此策略的RAM用户只能通过HTTPS方式访问ECS。您可以通过设置Condition下acs:SecureTransport的值为true来实现。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": "*",
```

```
      "Condition": {
        "Bool": {
          "acs:SecureTransport": "true"
        }
      }
    }
  ],
  "Version": "1"
}
```

说明:

Condition（限制条件）只针对当前权限策略描述的操作有效。您可以修改acs:SecureTransport的值为true或false。

7.5 自主管理多因素认证

本文为您提供自主管理多因素认证（MFA）的参考示例。

下述策略表示：RAM用户alice可以自主管理MFA，包括绑定MFA和解绑MFA。

```
{
    "Statement": [
        {
            "Action": [
                "ram:GetUserMFAInfo",
                "ram:BindMFADevice",
                "ram:UnbindMFADevice"
            ],
            "Resource": "acs:ram:*:*:user/alice",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ram:CreateVirtualMFADevice",
                "ram:DeleteVirtualMFADevice"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ],
    "Version": "1"
}
```

说明:

如果您想通过RAM控制台设置允许RAM用户自主管理MFA的操作，请参见#unique_40。

7.6 自主管理访问密钥

本文为您提供自主管理访问密钥（AccessKey）的参考示例。

下述策略表示：RAM用户`alice`可以自主管理AccessKey，包括创建AccessKey、删除AccessKey以及更新AccessKey的状态等。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
      "ram:CreateAccessKey",
      "ram:ListAccessKeys",
      "ram:UpdateAccessKey",
      "ram:DeleteAccessKey"
      ],
      "Resource": "acs:ram:*:*:user/alice",
      "Effect": "Allow"
    }
  ]
}
```

说明:

如果您想通过RAM控制台设置允许RAM用户自主管理AccessKey的操作，请参见*#unique_40*。

7.7 管理指定的ECS实例

本文为您提供管理指定的ECS实例的参考示例。

以下策略表示：您可以查看所有ECS实例及资源，但只能操作其中一个实例`i-001`。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": "acs:ecs:*:*:instance/i-001"
    },
    {
      "Action": "ecs:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

说明:

`Describe*`在权限策略中是必须的，否则用户在控制台将无法看到任何实例，但使用API、CLI或SDK直接对实例进行操作是可以的。

7.8 查看指定地域的ECS实例

本文为您提供查看指定地域ECS实例的参考示例。

以下策略表示：仅允许您查看青岛的ECS实例，但不允许查看磁盘及快照。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ecs:Describe*",
      "Resource": "acs:ecs:cn-qingdao:*:instance/*"
    }
  ],
  "Version": "1"
}
```

说明：

查看ECS资源列表的授权粒度可以到地域+资源类型的级别，如果您想授权RAM用户或RAM角色查看其他地域的ECS实例，您可以将Resource中的cn-qingdao替换为其他地域ID。关于地域ID，详情请参见#unique_44。

7.9 管理云账号下的ECS安全组

本文为您提供管理云账号下ECS安全组的参考示例。

下述策略表示：您拥有管理云账号下ECS安全组的权限。

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

7.10 管理云账号下除费用信息外的所有资源

本文为您提供管理云账号下除费用信息外的所有资源的参考示例。

以下策略表示：您可以管理云账号下除费用信息外的所有云资源。

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*"
```

```
        },
        {
            "Action": [
                "bss:*",
                "efc:*"
            ],
            "Effect": "Deny",
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

7.11 查看云账号下除费用信息外的所有云资源

本文为您提供查看云账号下除费用信息外的所有云资源的参考示例。

以下策略表示：您可以查看云账号下除费用信息外的所有云资源。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "*:Describe*",
                "*:List*",
                "*:Get*",
                "*:BatchGet*",
                "*:Query*",
                "*:BatchQuery*",
                "actiontrail:LookupEvents",
                "dm:Desc*",
                "dm:SenderStatistics*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
    {
            "Action": [
                "bss:*",
                "efc:*"
            ],
            "Effect": "Deny",
            "Resource": "*"
        }

    ]
}
```

7.12 跨云服务授权

本文为您提供跨云服务授权的参考示例。

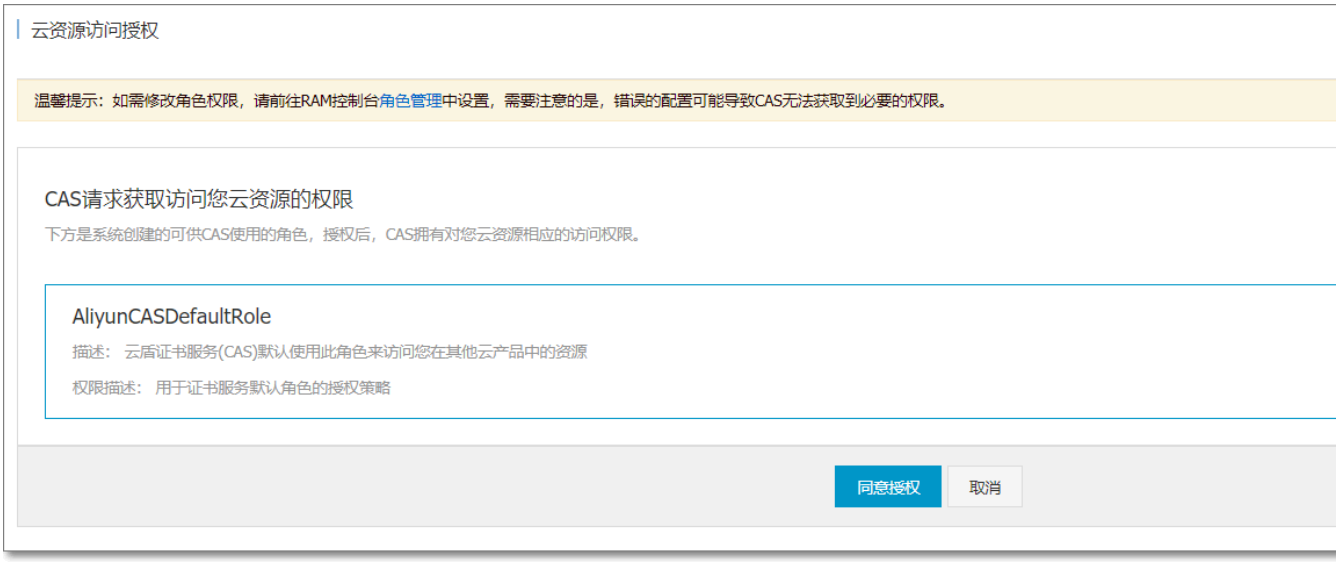
跨云服务授权指一个云服务A去访问另一个云服务B中的资源。本文为您提供跨云服务通用授权和精确授权的参考示例。

- **通用授权：云账号下被授权的RAM用户可以对所有的跨云服务进行授权。**

```
{
    "Statement": [
        {
            "Action": [
                "ram:GetPolicy",
                "ram:CreateRole",
                "ram:AttachPolicyToRole"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        }
    ],
    "Version": "1"
}
```

- **精确授权：云账号下被授权的RAM用户只能针对云盾证书服务（CAS）进行跨云服务授权。**

> **说明：**
> **精确授权的权限策略是在通用权限策略的基础上限制到RAM角色和权限策略名称，在本示例中RAM角色为：** `AliyunCASDefaultRole`，**云盾证书服务（CAS）的系统策略为** `AliyunCASRolePolicy`。




```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:GetPolicy",
                "ram:AttachPolicyToRole"
            ],
            "Resource": [
                "acs:ram:*:*:policy/AliyunCASRolePolicy",
                "acs:ram:*:*:role/AliyunCASDefaultRole"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateRole"
            ],
            "Resource": "acs:ram:*:*:role/*"
        }
    ],
    "Version": "1"
}
```

7.13 创建快照

本文为您提供创建快照的参考示例。

以下策略表示：通过授予ECS实例的管理员权限和指定云盘的权限，即可正常创建快照。在本示例中，ECS实例ID为`inst-01`，云盘ID为`dist-01`。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
        "acs:ecs:*:*:instance/inst-01"
      ]
    },
    {
      "Action": "ecs:CreateSnapshot",
      "Effect": "Allow",
      "Resource": [
        "acs:ecs:*:*:disk/dist-01",
        "acs:ecs:*:*:snapshot/*"
      ]
    },
    {
      "Action": [
        "ecs:Describe*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

7.14 管理OSS存储空间

本文为您提供管理OSS存储空间的参考示例。

以下策略表示：您可以管理一个名为`myphotos`的存储空间。

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

```
        {
            "Effect": "Allow",
            "Action": "oss:*",
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ]
        }
    ]
}
```

7.15 列出并读取一个存储空间中的资源

本文为您提供列出并读取一个存储空间中资源的参考示例。

- **以下策略表示：您可以通过OSS SDK或OSS命令行工具列出并读取一个存储空间`myphotos`中的资源。**

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "oss:ListObjects",
            "Resource": "acs:oss:*:*:myphotos"
        },
        {
            "Effect": "Allow",
            "Action": "oss:GetObject",
            "Resource": "acs:oss:*:*:myphotos/*"
        }
    ]
}
```

- **以下策略表示：您可以通过OSS控制台列出并读取一个存储空间`myphotos`中的资源。**

说明：

为了操作体验的优化，用户登录OSS控制台时，OSS控制台会额外调用`ListBuckets`、`GetBucketAcl`和`GetObjectAcl`，以确定存储空间属性是公开还是私有。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
                      "oss:GetBucketStat",
                      "oss:GetBucketInfo",
                      "oss:GetBucketTagging",
                      "oss:GetBucketAcl"
                      ],
            "Resource": "acs:oss:*:*:*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "oss:ListObjects",
                "oss:GetBucketAcl"
            ],
            "Resource": "acs:oss:*:*:myphotos"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject",
                "oss:GetObjectAcl"
            ],
            "Resource": "acs:oss:*:*:myphotos/*"
        }
    ]
}
```

7.16 通过指定的IP地址访问OSS

本文为您提供指定的IP地址访问OSS的参考示例。

- **以下策略表示：在`Allow`授权中增加IP限制，允许通过`192.168.0.0/16`和`172.12.0.0/16`两个IP地址来读取`myphotos`中的信息。**

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
                      "oss:GetBucketStat",
                      "oss:GetBucketInfo",
                      "oss:GetBucketTagging",
                      "oss:GetBucketAcl"
                      ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ],
            "Condition":{
                "IpAddress": {
                    "acs:SourceIp": ["192.168.0.0/16", "172.12.0.0/
16"]
                }
            }
        }
    ]
```

```
}
```

- **以下策略表示：在Deny授权中增加IP限制，如果源IP地址不是192.168.0.0/16，则禁止对OSS执行任何操作。**

说明：

权限策略的鉴权规则是Deny优先，所以访问者从192.168.0.0/16以外的IP地址访问myphotos中的内容时，OSS会提示没有权限。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
                      "oss:GetBucketStat",
                      "oss:GetBucketInfo",
                      "oss:GetBucketTagging",
                      "oss:GetBucketAcl"
                      ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "oss:*",
            "Resource": [
                "acs:oss:*:*:*"
            ],
            "Condition":{
                "NotIpAddress": {
                    "acs:SourceIp": ["192.168.0.0/16"]
                }
            }
        }
    ]
```

```
}
```

7.17 读取OSS指定文件的内容

本文为您提供读取OSS指定文件内容的参考示例。

假设用于存放照片的存储空间名为：`myphotos`**。该存储空间下有一些目录代表照片的拍摄地，每个拍摄地下又有年份子目录。**

```
myphotos[Bucket]
   ├── beijing
   │   ├── 2014
   │   └── 2015
   ├── hangzhou
   │   ├── 2013
   │   ├── 2014
   │   └── 2015
   └── qingdao
       ├── 2014
       └── 2015
```

以下策略表示：被授予此策略的RAM用户可以读取`myphotos/hangzhou/2015/`**目录下文件的内容，但不能列出文件。**

说明:

RAM用户知道文件的完整路径，此时可以使用完整的文件路径直接读取文件内容。通常这样的权限应授予应用程序。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        }
    ]
}
```

7.18 使用OSS命令行工具访问并列出指定的文件

本文为您提供使用OSS命令行工具访问并列出指定文件的参考示例。

以下策略表示：被授予此策略的RAM用户可以使用OSS命令行工具访问`myphotos/hangzhou/2015/`**目录并列出该目录下的文件。**

说明:

RAM用户不清楚目录中有哪些文件，可以使用OSS命令行工具或API直接获取目录信息。通常这样的权限应授予软件开发者。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos"
            ],
            "Condition":{
                "StringLike":{
                    "oss:Prefix":"hangzhou/2015/*"
                }
            }
        }
    ]
}
```

7.19 通过OSS控制台访问指定的目录

本文为您提供通过OSS控制台访问指定目录的参考示例。

以下策略表示：被授予此策略的RAM用户可以使用可视化的OSS控制台（类似Windows文件管理器）访问`myphotos/hangzhou/2015/`目录。

说明:

RAM用户可以从根目录开始，一层一层的进入要访问的目录，此场景是最易用的场景。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
                      "oss:GetBucketStat",
                      "oss:GetBucketInfo",
                      "oss:GetBucketTagging",
                      "oss:GetBucketAcl"
```

```
                    ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject",
                "oss:GetObjectAcl"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos"
            ],
            "Condition": {
                "StringLike": {
                    "oss:Delimiter": "/",
                    "oss:Prefix": [
                        "",
                        "hangzhou/",
                        "hangzhou/2015/*"
                    ]
                }
            }
        }
    ]
}
```