ALIBABA CLOUD

阿里云

访问控制

权限策略管理

文档版本：20220517

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	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。
注意	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。
说明	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	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。详情请参见为RAM用户授权、为用户组授权和为RAM角色授权。

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。

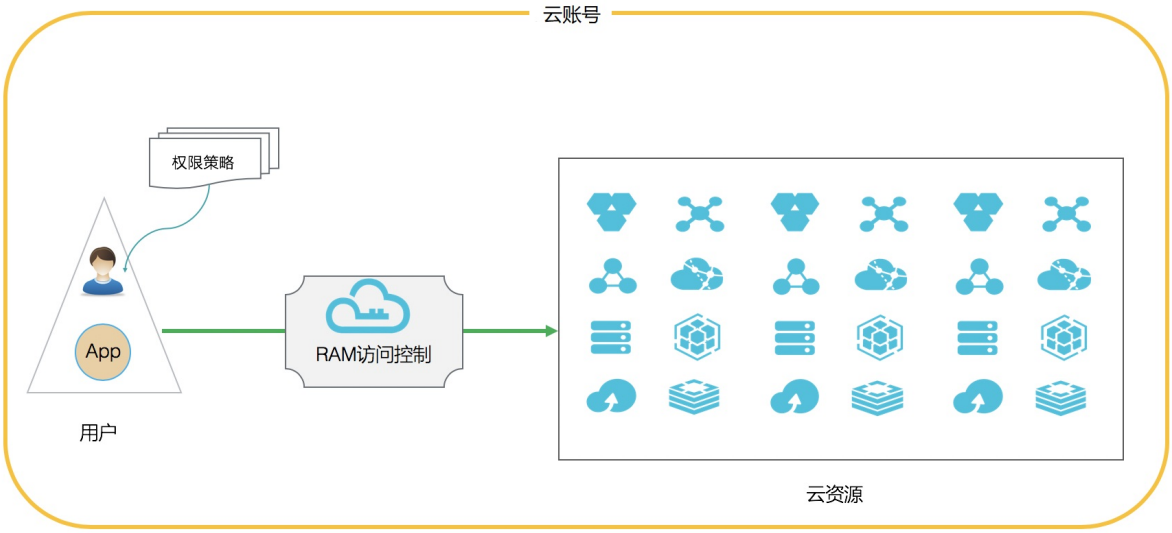
- 绑定的权限策略可以是系统策略也可以是自定义策略。
- 如果绑定的权限策略被更新，更新后的权限策略自动生效，无需重新绑定权限策略。

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

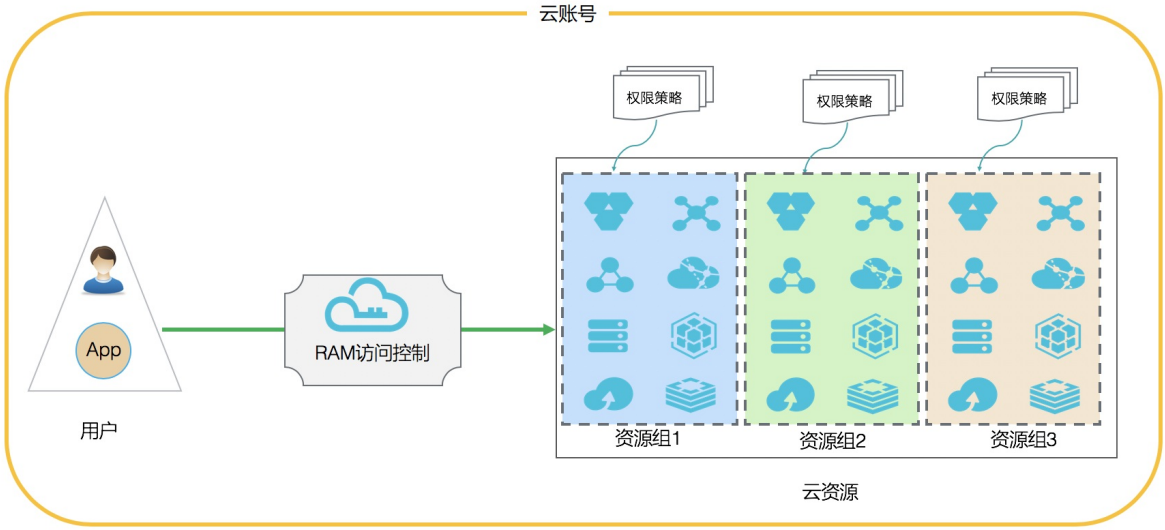
云账号内授权：对一个RAM身份主体添加权限策略时，该策略的可授权范围是云账号内的所有资源，这是最常见的一种权限模型。



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。



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的基本信息，包括权限策略名称、备注和策略类型等。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，从**策略类型**列表中，选择策略类型。
4. 在搜索框中，输入目标权限策略名称或备注进行模糊搜索，然后单击目标权限策略名称。
5. 在**基本信息**区域，查看**策略名称**、**备注**和**策略类型**等信息。

相关文档

- GetPolicy
- ListPoliciesForUser
- ListPoliciesForGroup
- ListPoliciesForRole

4.自定义权限策略

4.1. 创建自定义权限策略

如果系统权限策略不能满足您的需求，您可以通过创建自定义权限策略实现精细化权限管理。

创建方式

- 通过可视化编辑模式创建自定义权限策略

  RAM提供所见即所得的可视化编辑界面，您只需选择效果、云服务、操作、资源和条件，就可以生成自定义权限策略。同时，提供的智能校验功能，帮助您提高权限策略的正确性和有效性。该方式操作简单，易于上手。

- 通过脚本编辑模式创建自定义权限策略

  RAM提供JSON脚本编辑界面，您需要按照权限策略语法和结构编写自定义权限策略。该方式使用灵活，适用于对权限策略语法比较熟悉的用户。

- 通过导入模板创建自定义权限策略

  基于长期的业务实践，RAM提供了常见场景的权限策略模板。例如：系统管理员、财务人员、网络管理员等。您只需要导入合适的权限策略模板，然后基于模板进行简单修改，就能一键轻松创建自定义策略。

- 通过导入系统策略创建自定义权限策略

  您可以通过导入一个系统策略模板，然后基于规范化的系统策略模板修改适合实际业务的内容，更加方便快捷地创建自定义权限策略。

通过可视化编辑模式创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**可视化编辑**页签。
5. 配置权限策略，然后单击**下一步：编辑基本信息**。
   i. 在**效果**区域，选择**允许**或**拒绝**。
   ii. 在**服务**区域，选择云服务。

   > **说明** 支持可视化编辑模式的云服务以控制台界面显示为准。

   iii. 在**操作**区域，选择**全部操作**或**指定操作**。

   系统会根据您上一步选择的云服务，自动筛选出可以配置的操作。如果您选择了**指定操作**，您需要继续选择具体的操作。

   iv. 在**资源**区域，选择**全部资源**或**指定资源**。

   系统会根据您上一步选择的操作，自动筛选出可以配置的资源类型。如果您选择了**指定资源**，您需要继续单击**添加资源**，配置具体的资源ARN。您可以使用**匹配全部**功能，快速选择对应配置项的全部资源。

   > **说明** 为了权限策略的正常生效，对操作关联的必要资源ARN标识了**必要**，强烈建议您配置该资源ARN。

v. （可选）在**条件**区域，单击**添加条件**，配置条件。

条件包括阿里云通用条件和服务级条件，系统会根据您前面配置的云服务和操作，自动筛选出可以配置的条件列表。您只需要选择对应条件键配置具体内容。

vi. 单击**添加语句**，重复上述步骤，配置多条权限策略语句。

6. 输入权限策略**名称**和**备注**。
7. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
8. 单击**确定**。

通过脚本编辑模式创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**脚本编辑**页签。
5. 输入权限策略内容，然后单击**下一步：编辑基本信息**。

   关于权限策略语法结构的详情，请参见权限策略语法和结构。
6. 输入权限策略**名称**和**备注**。
7. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
8. 单击**确定**。

通过导入模板创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击页面右上角的**导入策略模板**。
5. 在**导入策略模板**对话框，导入权限策略模板。
   i. 选择权限策略模板。

   > **说明** 支持的权限策略模板列表，请以控制台显示为准。

   ii. （可选）部分模板需要根据实际业务配置模板参数。
   iii. 选择新导入的权限策略模板的覆盖规则。
      - 覆盖（默认）：新导入的权限策略模板内容完全覆盖已有的内容。
      - 追加：新导入的权限策略模板内容添加到已有内容的末尾。
   iv. 单击**导入**。
6. 在可视化编辑或脚本编辑模式下，查看和修改已导入的权限策略内容，然后单击**下一步：编辑基本信息**。

   导入的权限策略模板默认以可视化模式展示，方便您查看和修改。 您也可以选择脚本编辑模式进行修改。
7. 输入权限策略**名称**和**备注**。
8. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：
     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：
     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。
9. 单击**确定**。

通过导入系统策略创建自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击页面右上角的**导入系统策略**。
5. 在**导入系统策略**对话框，导入系统策略。

i. 选择系统策略。

ii. 选择新导入的系统策略的覆盖规则。

- 覆盖：新导入的系统策略内容完全覆盖已有的内容。
- 追加（默认）：新导入的系统策略内容添加到已有内容的末尾。

iii. 单击**导入**。

6. 在可视化编辑或脚本编辑模式下，查看和修改已导入的系统策略内容，然后单击**下一步：编辑基本信息**。

   导入的系统策略默认以可视化模式展示，方便您查看和修改。 您也可以选择脚本编辑模式进行修改。

7. 输入权限策略**名称**和**备注**。
8. 检查并优化权限策略内容。
   - 基础权限策略优化

     系统会对您添加的权限策略语句自动进行基础优化。基础权限策略优化会完成以下任务：

     - 删除不必要的条件。
     - 删除不必要的数组。

   - （可选）高级权限策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对权限策略内容进行高级优化。高级权限策略优化功能会完成以下任务：

     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。

9. 单击**确定**。

相关文档

- CreatePolicy

4.2. 删除自定义权限策略

当权限发生变化或不再需要某个自定义权限策略时，您可以删除自定义权限策略。

前提条件

删除权限策略前，应保证当前权限策略未被引用（即未授予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。更多信息，请参见管理权限策略引用记录。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击目标自定义权限策略**操作**列的**删除**。
4. 在**删除自定义策略**对话框，单击**确定**。

相关文档

- DeletePolicy

4.3. 修改自定义权限策略内容和备注

您可以根据需要修改自定义权限策略内容和备注，不能修改权限策略名称。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击目标权限策略名称。
4. 在**基本信息**区域，单击**备注**右侧的编辑图标，修改备注。
5. 在**策略内容**页签，单击**修改策略内容**。
6. 通过可视化编辑模式或脚本编辑模式修改权限策略内容，然后单击**下一步：编辑基本信息**。

   具体操作，请参见创建自定义权限策略。
7. 修改**备注**，然后单击**确定**。

执行结果

权限策略内容修改完成后，系统会自动生成一个新的权限策略版本，该新版本将变为当前版本。

相关文档

- CreatePolicyVersion

4.4. 管理自定义权限策略版本

本文为您介绍如何管理自定义权限策略版本，包括查看版本、设置当前版本和删除版本。

背景信息

自定义权限策略的版本管理机制如下：

- 一个自定义权限策略最多可以有5个版本。
- 当自定义权限策略版本达到5个，在控制台再次修改自定义权限策略时，可以用最新版本替换最早的非当前版本，也可以手动删除不需要的版本。
- 对于一个存在多版本的自定义权限策略，只有一个版本是活跃的，即当前版本。
- 当前版本只能查看，不能删除。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击目标自定义权限策略名称。
4. 单击**版本管理**页签，您可以查看、设置和删除权限策略版本。
   - 查看版本：单击**操作**列的**查看**，查看权限策略名称、版本号和内容。
   - 设置当前版本：单击**操作**列的**设为当前版本**，可以将任一版本设为当前版本。
   - 删除版本：找到不需要的非当前版本，单击**操作**列的**删除**，然后单击**确定**，删除不需要的版本。

相关文档

- SetDefaultPolicyVersion
- GetPolicyVersion
- ListPolicyVersions
- DeletePolicyVersion

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、新增和删除引用记录。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击目标权限策略名称。
4. 单击**引用记录**页签，管理权限策略引用记录。
   - 查看引用记录：查看该条权限策略被引用的信息，包括**权限应用范围**、**被授权主体**、**主体类型**和**授权时间**。
   - 新增引用记录（新增授权）：单击**新增授权**，根据界面提示，将该条权限策略授权给RAM用户、用户组或RAM角色，即新增一条引用记录。
   - 删除引用记录（移除授权）：单击目标引用记录**操作**列的**移除授权**，然后单击**确定**，为RAM用户、用户组或RAM角色移除授权，即删除一条引用记录。

相关文档

- ListEntitiesForPolicy

6.权限策略语言

6.1. 权限策略基本元素

RAM中使用权限策略描述授权的具体内容，权限策略由效果（Effect）、操作（Action）、资源（Resource）和条件（Condition）四个基本元素组成。

元素名称	描述
效果（Effect）	授权效果包括两种：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。
条件（Condition）	条件是指授权生效的条件。

效果（Effect）

- 取值：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）

- 取值：云服务所定义的API操作名称。支持多值。

  > **说明** 多数情况下操作与云服务的API一一对应，但也有例外。更多信息，请参见各云服务的帮助文档。

- 格式：`<ram-code>:<action-name>`。
  - `ram-code`：云服务的RAM代码。更多信息，请参见支持RAM的云服务的**RAM代码**列。
  - `action-name`：相关的API操作接口名称。
- 样例：`"Action": ["oss:ListBuckets", "ecs:Describe*", "rds:Describe*"]`。

资源（Resource）

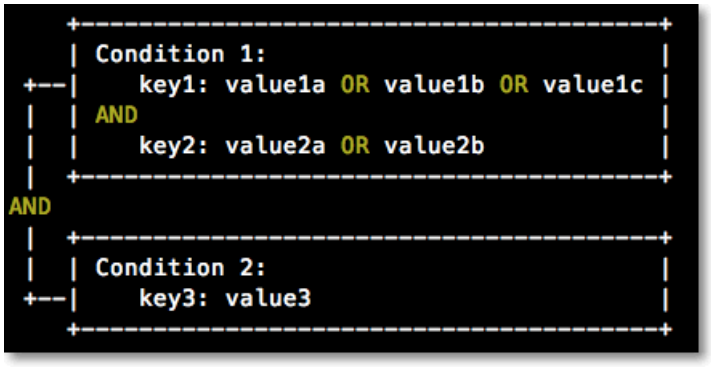
- 取值：资源ARN（Aliyun Resource Name）。支持多值。
- 格式：遵循阿里云ARN统一规范，为`acs:<ram-code>:<region>:<account-id>:<relative-id>`。
  - `acs`：Alibaba Cloud Service的首字母缩写，表示阿里云的公共云平台。
  - `ram-code`：云服务RAM代码。更多信息，请参见支持RAM的云服务的**RAM代码**列。
  - `region`：地域信息。对于全局资源（无需指定地域就可以访问的资源），该字段置空。更多信息，请参见地域和可用区。
  - `account-id`：阿里云账号ID。例如：`123456789012****`。

- `relative-id`：与服务相关的资源描述部分，其语义由具体云服务指定。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/*"]`。

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（Number）、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
数字类型（Number）	○ NumericEquals ○ NumericNotEquals ○ NumericLessThan ○ NumericLessThanEquals ○ NumericGreaterThan ○ NumericGreaterThanEquals

条件操作类型	支持类型
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，不能使用该IP地址的IP地址段形式xx.xx.xx.xx/32。例如：10.0.0.1不能写成10.0.0.1/32。
`acs:MFAPresent`	Boolean	用户登录时是否使用了多因素认证。
`acs:PrincipalARN`	String	仅限资源目录管控策略中使用，用于表示操作执行者的身份。例如：`acs:ram:*:*:role/*resourcedirectory*`。 **说明** 目前，只支持指定RAM角色的ARN，且必须为小写英文字母。（您可以在RAM控制台的角色详情页面查看RAM角色的ARN）。

- 阿里云服务级别条件关键字命名格式：`<ram-code>:<condition-key>`。

服务级别条件关键字	云服务名称	类型	描述
`ecs:tag/<tag-key>`	ECS	String	ECS资源的标签关键字，可自定义。 说明 <tag-key>为标签键，请在使用时替换为实际值。
`rds:ResourceTag/<tag-key>`	RDS	String	RDS资源的标签关键字，可自定义。 说明 <tag-key>为标签键，请在使用时替换为实际值。
`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。

相关文档

- 权限策略语法和结构
- 权限策略示例库概览

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。

前提条件

运用策略语法前，您应了解策略字符及其使用规则。

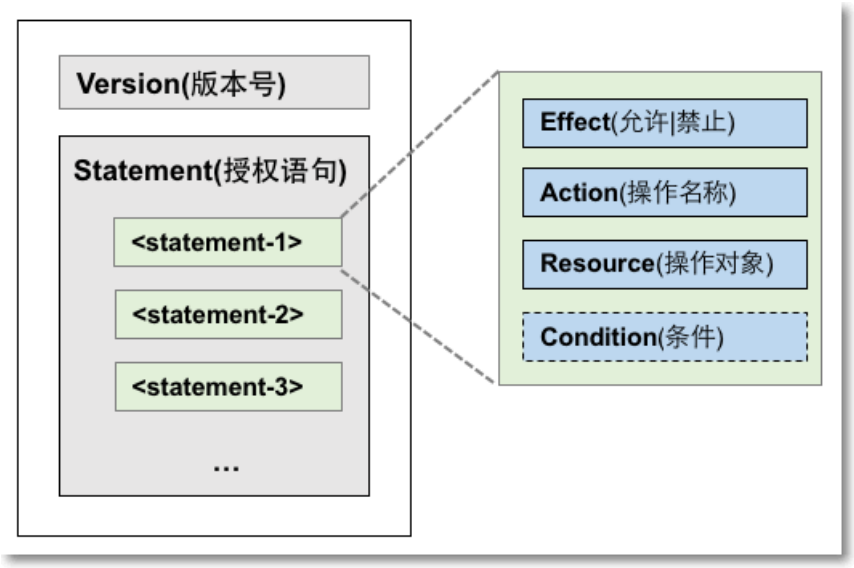
- 权限策略字符如下：
  - 权限策略中所包含的JSON字符：`{ } [ ] " , :`。
  - 描述语法使用的特殊字符：`= < > ( ) |`。
- 字符使用规则如下：
  - 当一个元素允许多值时，可以使用下述两种方式表达，效果相同。
    - 使用半角逗号（,）和省略号（...）进行表达。例如：`[ <action_string>, <action_string>, ...]`。
    - 使用单值进行表达。例如：`"Action": [<action_string>]` 和 `"Action": <action_string>`。

- 元素带有半角问号（?）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果（Effect）、操作（Action）、资源（Resource）以及条件（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" :
    ("*" | [<action_string>, <action_string>, ...])
<resource_block> = "Resource" :
    ("*" | [<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" | "Date and time" | "IP address")
```

权限策略语法说明：

- 版本：当前支持的权限策略版本，固定为1，不允许修改。
- 授权语句：一个权限策略可以有多条授权语句。
  - 每条授权语句的效果为：`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条件（Condition）。

    > **说明** 一个条件块支持多个条件的组合，每个条件的操作类型可以不同。

- 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：
  - 当元素取值为字符串类型（String）、数字类型（Number）、日期类型（Date and time）、布尔类型（Boolean）和IP地址类型（IP address）时，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

权限策略支持JSON格式。当您创建或更新权限策略时，系统会检查JSON格式的正确性。您也可以使用第三方JSON格式验证器和编辑器自行检查JSON格式的正确性。关于JSON语法标准，请参见RFC 7159。

相关文档

- 权限策略基本元素
- 权限策略示例库概览

6.3. 权限策略判定流程

当RAM身份（RAM用户或RAM角色）通过阿里云控制台、API或CLI发起资源访问请求时，都需要执行权限策略的判定流程，根据判定结果决定是否允许访问。本文为您介绍阿里云的权限策略判定流程。

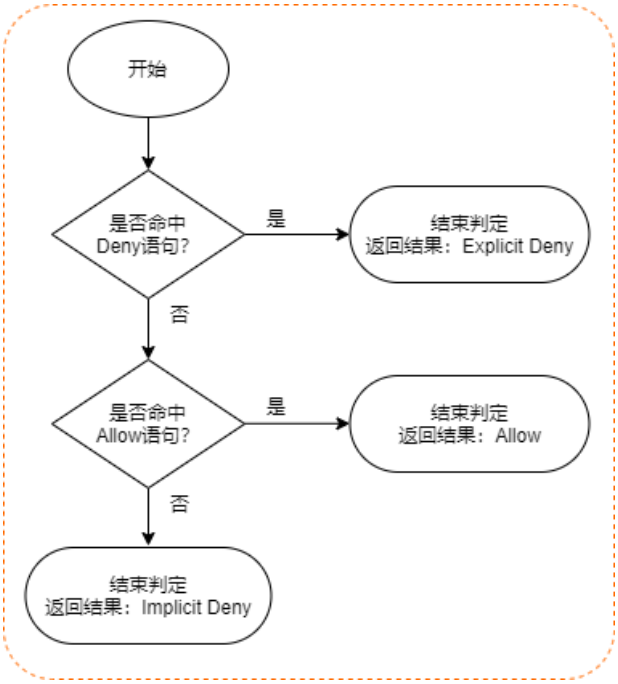
概述

阿里云支持多种类型的权限策略。一次完整的权限策略判定流程包含以下步骤：

1. 判定程序收集访问请求涉及的所有类型的权限策略，包括：资源目录的管控策略（Control Policy）、RAM角色的会话策略（Session Policy）、基于身份的策略（Identity-based Policy）和基于资源的策略（Resource-based Policy）。
2. 判定程序会按照最小单元判定流程依次对每一种权限策略执行判定，根据判定结果决定是否继续进行下一步判定，直到判定结束并获得最终的判定结果。

最小单元判定流程

每种类型的权限策略都会按照下图所示的流程进行权限判定，这个流程称为最小单元判定流程。



最小单元判定流程如下：

1. 权限判定遵循Deny优先原则，优先检查访问请求是否命中Deny语句。
   - 是：判定结束，返回判定结果为Explicit Deny（显式拒绝）。
   - 否：继续下一步判定。
2. 检查访问请求是否命中Allow语句。
   - 是：判定结束，返回判定结果为Allow（允许）。
   - 否：判定结束，返回判定结果为Implicit Deny（隐式拒绝）。

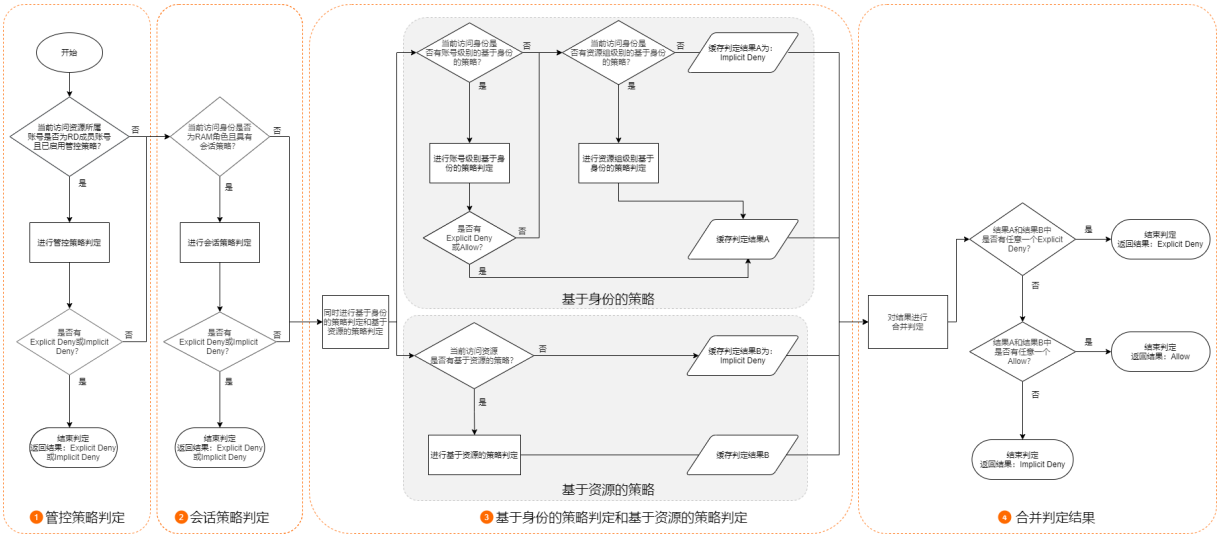
判定结果说明如下表所示。

判定结果	说明
Allow（允许）	如果访问请求命中了权限策略中的Allow语句，且没有命中Deny语句，那么本次判定结果是Allow（允许）。
Explicit Deny（显式拒绝）	一旦访问请求命中了权限策略中的Deny语句，那么本次判定结果是Explicit Deny（显式拒绝）。即使此时访问请求同时命中了Allow语句，但遵循Deny优先原则，Deny语句优先级高于Allow语句，判定结果仍为显式拒绝。
Implicit Deny（隐式拒绝）	如果访问请求既没有命中权限策略中的Allow语句，也没有命中Deny语句，那么本次判定结果是Implicit Deny（隐式拒绝）。RAM身份默认没有执行任何操作的权限，没有被显式允许执行的操作都会被隐式拒绝。

完整判定流程

完整的判定流程会按照下图所示的顺序依次对每一种权限策略进行判定，并获得最终判定结果。

> **说明** 阿里云的绝大多数云服务都按照阿里云账号维度进行隔离，只能在单个阿里云账号内部执行操作，但也有个别云服务（例如：对象存储OSS）允许直接进行跨账号访问。无论哪种情况，阿里云都遵循同样的权限判定流程。



完整判定流程如下：

1. **管控策略判定**

管控策略（Control Policy）是资源目录中对成员账号访问定义的权限边界。如果请求访问的资源所属账号是资源目录的成员账号，并且管控策略已开启，判定程序会按照最小单元判定流程执行管控策略判定。否则，判定程序会跳过此步。

根据管控策略的判定结果，作出下一步判定。具体如下：

- 管控策略的判定结果是Explicit Deny（显式拒绝）或Implicit Deny（隐式拒绝）：判定结束，管控策略的判定结果就是最终的判定结果。
- 管控策略的判定结果是Allow（允许）：继续进行下一步判定。

2. **会话策略判定**

会话策略（Session Policy）是在以编程方式扮演RAM角色（调用AssumeRole API）的过程中创建临时会话时，在参数中传递的策略，用于进一步限制会话的权限。如果发起访问请求的身份是RAM角色，并且拥有会话策略，判定程序会按照最小单元判定流程执行会话策略判定。否则，判定程序会跳过此步。

根据会话策略的判定结果，作出下一步判定。具体如下：

- 会话策略的判定结果是Explicit Deny（显式拒绝）或Implicit Deny（隐式拒绝）：判定结束，会话策略的判定结果就是最终的判定结果。
- 会话策略的判定结果是Allow（允许）：继续进行下一步判定。

3. **基于身份的策略判定和基于资源的策略判定**

同时进行基于身份的策略（Identity-based Policy）判定和基于资源的策略（Resource-based Policy）判定，并将两者的判定结果缓存。

- **基于身份的策略判定**

  对于RAM用户，基于身份的策略包括直接授权的策略和从RAM用户组中继承的策略。对于RAM角色，基于身份的策略为直接授权的策略。基于身份的策略因授权范围不同，又分为账号级别和资源组级别，账号级别的策略优先级高于资源组级别的策略。

  判定流程如下：

  a. 检查发起访问请求的RAM身份是否拥有账号级别的基于身份的策略。
     - 是：判定程序按照最小单元判定流程执行账号级别的身份策略判定。判定结果说明如下：
       - 如果判定结果是Explicit Deny（显式拒绝）或Allow（允许）：基于身份策略的判定结束，将结果缓存到判定结果A。
       - 如果判定结果是Implicit Deny（隐式拒绝）：继续进行下一步判定。
     - 否：继续进行下一步判定。

  b. 检查发起访问请求的RAM身份是否拥有资源组级别的基于身份的策略。
     - 是：判定程序按照最小单元判定流程执行资源组级别的身份策略判定，并将结果缓存到判定结果A。
     - 否：直接保存判定结果A为Implicit Deny（隐式拒绝）。

- **基于资源的策略判定**

  检查请求访问的资源是否拥有基于资源的策略。

  - 是：判定程序按照最小单元判定流程执行基于资源的策略判定，并将结果缓存到判定结果B。
  - 否：直接保存判定结果B为Implicit Deny（隐式拒绝）。

> **说明** 目前阿里云提供了两种基于资源的策略：OSS存储空间策略（Bucket Policy）和RAM角色的信任策略（Trust Policy）。如果请求访问的不是以上两种资源，则不会进行基于资源的策略判定，而直接将基于身份的策略判定结果作为最终结果。

4. **合并判定结果**

   将基于身份策略的判定结果A和基于资源策略的判定结果B进行合并。合并逻辑如下：

   - 如果判定结果A和判定结果B中存在任意一个Explicit Deny（显式拒绝）：合并后的最终判定结果为Explicit Deny（显式拒绝），判定结束。
   - 如果判定结果A和判定结果B中存在任意一个Allow（允许）：合并后的最终判定结果为Allow（允许），判定结束。
   - 如果判定结果A和B中既无Explicit Deny（显式拒绝）也无Allow（允许）：合并后的最终判定结果为Implicit Deny（隐式拒绝），判定结束。

   > **说明**
   > - 合并判定结果的逻辑由资源所属的云服务决定，也可能存在上述以外的情况。例如：扮演RAM角色时的权限策略判定流程。
   > - OSS的权限判定，在合并判定结果之后还需要继续进行Bucket或Object ACL相关判定。OSS的完整权限判定流程，请参见OSS鉴权详解。

如果最终判定结果是Allow（允许），访问会被允许。不管最终判定结果是Explicit Deny（显式拒绝）还是Implicit Deny（隐式拒绝），访问均会被拒绝。

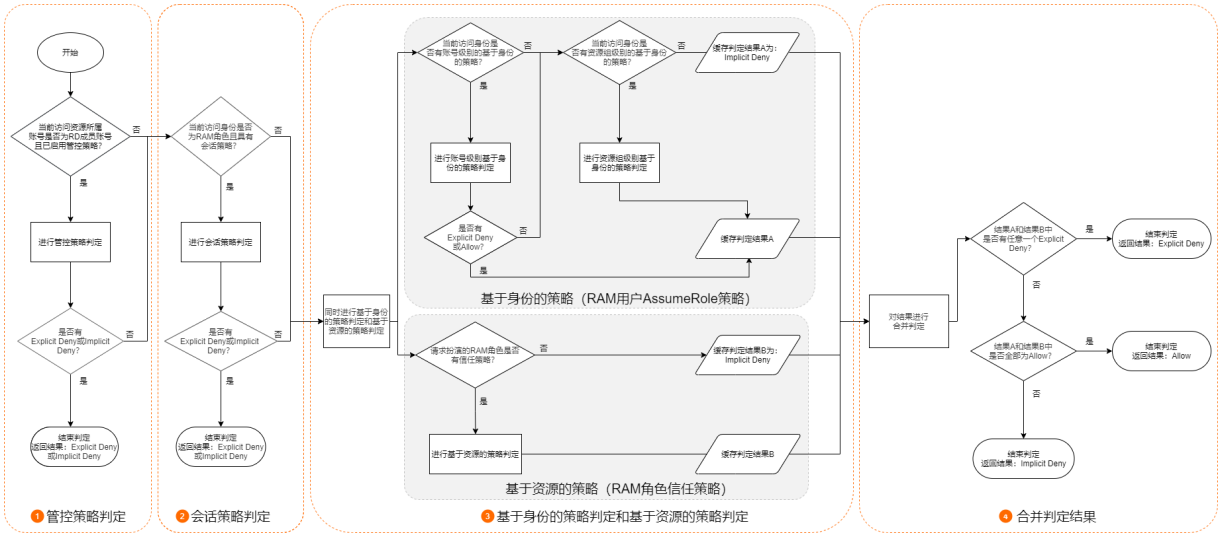
6.4. 扮演RAM角色时的权限策略判定流程

当可信实体通过阿里云控制台、API或CLI扮演RAM角色时，需要执行权限策略的判定流程，根据判定结果决定是否允许扮演RAM角色（AssumeRole）。本文为您介绍扮演RAM角色时的权限策略判定流程。

> **说明** 扮演RAM角色时的权限策略判定流程，遵从阿里云通用的权限策略判定流程，仅在合并判定结果时不同。如果您了解通用的权限策略判定流程，您只需关注本文所述的合并判定结果章节。

创建RAM角色时需要为RAM角色添加信任策略，该信任策略用于指定允许扮演RAM角色的可信实体，是一种基于资源的策略。当可信实体扮演某个RAM角色时，又需要拥有扮演RAM角色的相应权限，这是可信实体的基于身份的策略。

当可信实体扮演RAM角色时，判定程序会按照下图所示的顺序依次进行权限策略判定，此时可信实体是访问身份，被扮演的RAM角色是访问资源。



RAM角色扮演请求涉及多种类型的权限策略，每种权限策略内部的判定都遵从最小单元判定流程，完整的判定流程如下：

1. **管控策略判定**

   管控策略（Control Policy）是资源目录中对成员账号访问定义的权限边界。如果请求扮演的RAM角色所属账号是资源目录的成员账号，并且管控策略已开启，判定程序会按照最小单元判定流程执行管控策略判定。否则，判定程序会跳过此步。

   根据管控策略的判定结果，作出下一步判定。具体如下：

   - 管控策略的判定结果是Explicit Deny（显式拒绝）或Implicit Deny（隐式拒绝）：判定结束，管控策略的判定结果就是最终的判定结果。
   - 管控策略的判定结果是Allow（允许）：继续进行下一步判定。

2. **会话策略判定**

   会话策略（Session Policy）是在以编程方式扮演RAM角色（调用AssumeRole API）的过程中创建临时会话时，在参数中传递的策略，用于进一步限制会话的权限。如果发起访问请求的身份是RAM角色，并且拥有会话策略，判定程序会按照最小单元判定流程执行会话策略判定。否则，判定程序会跳过此步。

   > **说明** 进行角色SSO时，没有会话策略，因此判定程序会跳过此步。

   根据会话策略的判定结果，作出下一步判定。具体如下：

   - 会话策略的判定结果是Explicit Deny（显式拒绝）或Implicit Deny（隐式拒绝）：判定结束，会话策略的判定结果就是最终的判定结果。
   - 会话策略的判定结果是Allow（允许）：继续进行下一步判定。

3. **基于身份的策略判定和基于资源的策略判定**

   同时进行基于身份的策略（Identity-based Policy）判定和基于资源的策略（Resource-based Policy）判定，并将两者的判定结果缓存。

   - **基于身份的策略判定**

     对于RAM用户，基于身份的策略包括直接授权的策略和从RAM用户组中继承的策略。对于RAM角色，基于身份的策略为直接授权的策略。基于身份的策略因授权范围不同，又分为账号级别和资源组级别，账号级别的策略优先级高于资源组级别的策略。

> **说明** 进行角色SSO时，由于用户还未登录成功，所以没有基于身份的策略，判定程序会跳过此步，直接以基于资源的策略判定结果作为最终结果。

判定流程如下：

a. 检查发起请求的RAM身份是否拥有账号级别的基于身份的策略。
   - 是：判定程序按照最小单元判定流程执行账号级别的身份策略判定。判定结果说明如下：
     - 如果判定结果是Explicit Deny（显式拒绝）或Allow（允许）：基于身份策略的判定结束，将结果缓存到判定结果A。
     - 如果判定结果是Implicit Deny（隐式拒绝）：继续进行下一步判定。
   - 否：继续进行下一步判定。

b. 检查发起请求的RAM身份是否拥有资源组级别的基于身份的策略。
   - 是：判定程序按照最小单元判定流程执行资源组级别的身份策略判定，并将结果缓存到判定结果A。
   - 否：直接保存判定结果A为Implicit Deny（隐式拒绝）。

- **基于资源的策略判定**

  检查请求扮演的RAM角色是否拥有信任策略。
  - 是：判定程序按照最小单元判定流程执行基于资源的策略判定，并将结果缓存到判定结果B。
  - 否：直接保存判定结果B为Implicit Deny（隐式拒绝）。

4. **合并判定结果**

   将基于身份策略的判定结果A和基于资源策略的判定结果B进行合并。合并逻辑与通用的权限策略判定流程不同，只有当基于身份的策略判定（判定结果A）和基于资源的策略判定（判定结果B）全部是Allow（允许）时，扮演RAM角色的请求才会被允许，其他情况均会被拒绝。

   具体如下：

   - 如果判定结果A和判定结果B中存在任意一个Explicit Deny（显式拒绝）：合并后的最终判定结果为Explicit Deny（显式拒绝），判定结束。
   - 如果判定结果A和判定结果B全部是Allow（允许）：合并后的最终判定结果为Allow（允许），判定结束。
   - 除上述两种外的其他情况：合并后的最终判定结果为Implicit Deny（隐式拒绝），判定结束。

7.权限策略示例库

7.1. 权限策略示例库概览

本文为您提供常见权限策略的示例库。

- 重启ECS实例
- 通过指定的IP地址访问阿里云
- 在指定的时间段访问阿里云
- 通过指定的访问方式访问阿里云
- 指定RAM用户自主管理多因素认证
- 指定RAM用户自主管理访问密钥
- 管理指定的ECS实例
- 查看指定地域的ECS实例
- 管理阿里云账号下的ECS安全组
- 管理阿里云账号下除费用信息外的所有资源
- 查看阿里云账号下除费用信息外的所有资源
- 跨云服务授权
- 创建快照
- 管理OSS存储空间
- 列出并读取一个存储空间中的资源
- 通过指定的IP地址访问OSS
- 读取OSS指定文件的内容
- 使用OSS命令行工具访问并列出指定的文件
- 通过OSS控制台访问指定的目录

7.2. 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:RebootInstance",
      "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`。

7.3. 通过指定的IP地址访问阿里云

本文为您提供RAM用户通过指定IP地址访问阿里云的策略样例。

RAM用户只能通过192.168.0.0/16和172.16.215.218这两个IP地址访问ECS。

您可以通过设置 `Condition` 下 `acs:SourceIp` 的值来实现。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp":[
          "192.168.0.0/16",
          "172.16.215.218"
         ]
        }
      }
    }
  ],
  "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。
> - 请将 `acs:SourceIp` 的值修改为您实际环境的真实IP地址。

7.4. 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。

7.5. 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`。

7.6. 指定RAM用户自主管理多因素认证

本文为您提供指定RAM用户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"
}
```

该权限策略适用于：仅允许阿里云账号下指定RAM用户自主管理多因素认证（MFA），其他RAM用户不需要自主管理多因素认证（MFA）的场景。

如果允许阿里云账号下所有RAM用户都自主管理多因素认证（MFA），请登录RAM控制台，修改RAM用户安全设置，将**自主管理多因素设备**设置为**允许**。具体操作，请参见设置RAM用户安全策略。

7.7. 指定RAM用户自主管理访问密钥

本文为您提供指定RAM用户自主管理访问密钥（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"
    }
  ]
}
```

该权限策略适用于：仅允许阿里云账号下指定RAM用户自主管理AccessKey，其他RAM用户不需要自主管理AccessKey的场景。

如果允许阿里云账号下所有RAM用户都自主管理AccessKey，请登录RAM控制台，修改RAM用户安全设置，将**自主管理AccessKey**设置为**允许**。具体操作，请参见设置RAM用户安全策略。

7.8. 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。

7.9. 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，详情请参见地域和可用区。

7.10. 管理阿里云账号下的ECS安全组

本文为您提供管理阿里云账号下ECS安全组的参考示例。

下述策略表示：您拥有管理阿里云账号下ECS安全组的权限。

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

7.11. 管理阿里云账号下除费用信息外的所有资源

本文为您提供管理阿里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：您可以管理阿里云账号下除费用信息外的所有资源。

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

7.12. 查看阿里云账号下除费用信息外的所有资源

本文为您提供查看阿里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：您可以查看阿里云账号下除费用信息外的所有资源。

```
{
    "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": "*"
        }
    ]
}
```

7.13. 跨云服务授权

跨云服务授权是指允许云服务A访问云服务B中的资源。本文将为您提供跨云服务授权的权限策略示例。

您可以通过通用授权或精确授权两种方式完成授权操作：

- 通用授权

  阿里云账号下被授权的RAM用户可以对所有的云服务进行跨云服务授权。

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

- 精确授权

  阿里云账号下被授权的RAM用户只能对指定云服务进行跨云服务授权。

  > **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RAM角色和权限策略名称。本示例中RAM角色为 `aliyuncasdefaultrole` ，SSL证书服务的系统策略为 `AliyunCASRolePolicy` 。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ram:AttachPolicyToRole",
                "ram:CreateRole"
            ],
            "Resource": [
                "acs:ram:*:system:policy/AliyunCASRolePolicy",
                "acs:ram:*:*:role/aliyuncasdefaultrole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

7.14. 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"
}
```

7.15. 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/*"
            ]
        }
    ]
}
```

7.16. 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/*"
        }
    ]
}
```

7.17. 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"]
                }
            }
        }
    ]
}
```

7.18. 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/*"
            ]
        }
    ]
}
```

7.19. 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/*"
                }
            }
        }
    ]
}
```

7.20. 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/*"
                    ]
                }
            }
        }
    ]
}
```

7.21. 管理资源组

本文为您提供管理资源组的权限策略示例。

以下策略表示：您可以在资源管理中创建资源组、删除资源组、查看和修改资源组基本信息。

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

说明 如果您想在资源组中进行更多的操作，例如：管理资源组中的资源、为资源组授权和跨资源组转移资源等，您需要添加其他的权限策略。更多信息，请参见资源组鉴权列表。