阿里云
访问控制

最佳实践

文档版本：20190813

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:** 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:** 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:** 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 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

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。详情请参见账号注册。

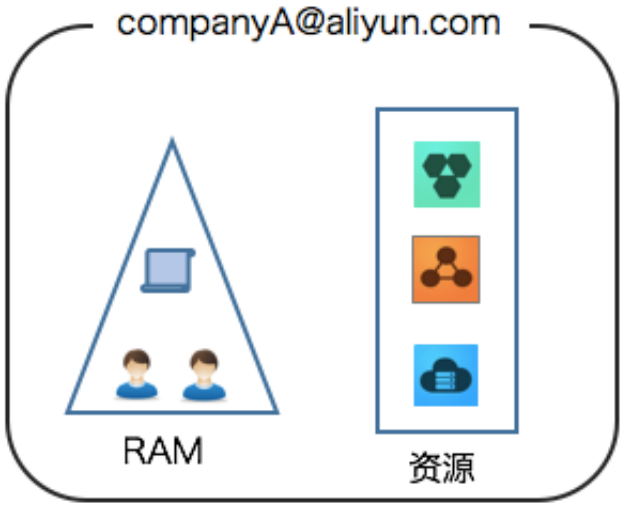
背景信息

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，他们的组织结构更加复杂，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。

  详情请参见创建RAM用户。

- 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。

  详情请参见创建RAM用户。

- 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。

  详情请参见创建用户组。

- 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。如果允许子用户更改登录密码，那么应该要求他们创建强密码并且定期轮换登录密码或访问密钥。

  详情请参见设置RAM用户安全策略。

- 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

  详情请参见为云账号设置多因素认证。

- 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。

  详情请参见用户SSO概览。

- 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。

  详情请参见为RAM用户创建访问密钥。

- 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。

  详情请参见为RAM用户授权。

- 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。

  详情请参见什么是STS。

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RAM对多运维人员的权限管控。

2 通过RAM限制用户的登录IP地址

RAM可以限制用户只能通过指定的IP地址访问企业的云资源，从而增强访问安全性。

前提条件

- 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。详情请参见账号注册。
- 请确保您已经开通RAM服务并登录RAM控制台。如还未开通，请先开通RAM服务。详情请参见开通方法。
- 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。详情请参见权限策略基本元素和权限策略语法和结构。

背景信息

企业A购买了很多阿里云资源来开展业务，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。为了确保其业务和数据安全，企业希望RAM用户只能通过企业专用网络的IP地址访问阿里云，而不是在任意地点都可以访问阿里云。

解决方案

您可以根据需要创建自定义策略并为RAM用户添加相应的权限，从而保证RAM用户只能通过指定的IP地址访问阿里云。

1. 创建RAM用户。
2. 创建自定义策略。
3. 为RAM用户授权。

创建自定义策略

1. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
2. 单击新建权限策略。
3. 填写策略名称和备注。

4. 配置模式选择脚本配置，拷贝下述策略示例到策略内容区域下并根据实际情况进行修改。

下述策略表示：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。

5. 单击确认。

3 通过RAM限制用户的登录时间段

RAM可以限制用户只能在指定的时间段访问企业的云资源，从而增强访问安全性。

前提条件

- 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。详情请参见账号注册。
- 请确保您已经开通RAM服务并登录RAM控制台。如还未开通，请先开通RAM服务。详情请参见开通方法。
- 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。详情请参见权限策略基本元素和权限策略语法和结构。

背景信息

企业A购买了很多阿里云资源来开展业务，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。为了确保其业务和数据安全，企业希望RAM用户只能在工作时间访问阿里云，而不是在任意时间都可以访问阿里云。

解决方案

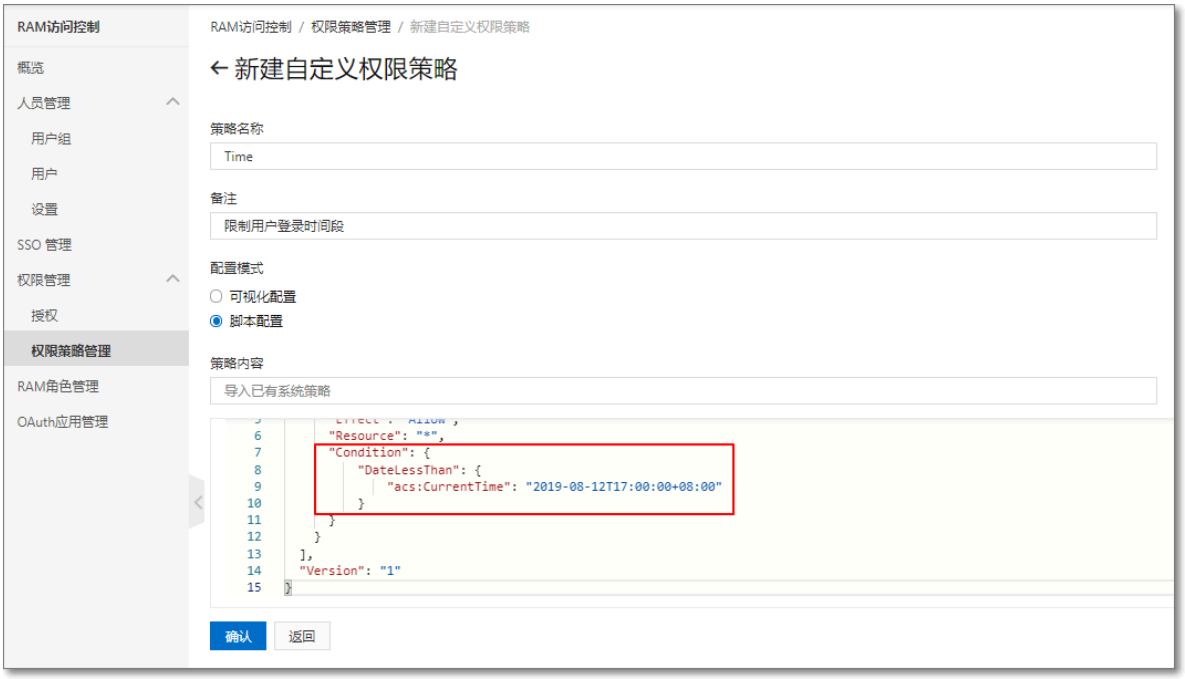
您可以根据需要创建自定义策略并为RAM用户添加相应的权限，从而保证RAM用户只能在指定的时间段访问阿里云。

1. 创建RAM用户。
2. 创建自定义策略。
3. 为RAM用户授权。

创建自定义策略

1. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
2. 单击新建权限策略。
3. 填写策略名称和备注。

4. 配置模式选择脚本配置，拷贝下述策略示例到策略内容区域下并根据实际情况进行修改。



下述策略表示：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。

5. 单击确认。

4 通过RAM限制用户的访问方式

RAM可以限制用户只能通过指定的访问方式访问企业的云资源，从而增强访问安全性。

前提条件

- 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。详情请参见账号注册。
- 请确保您已经开通RAM服务并登录RAM控制台。如还未开通，请先开通RAM服务。详情请参见开通方法。
- 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。详情请参见权限策略基本元素和权限策略语法和结构。

背景信息

企业A购买了很多阿里云资源来开展业务，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。为了确保其业务和数据安全，企业希望RAM用户只能通过HTTPS方式访问阿里云。

解决方案

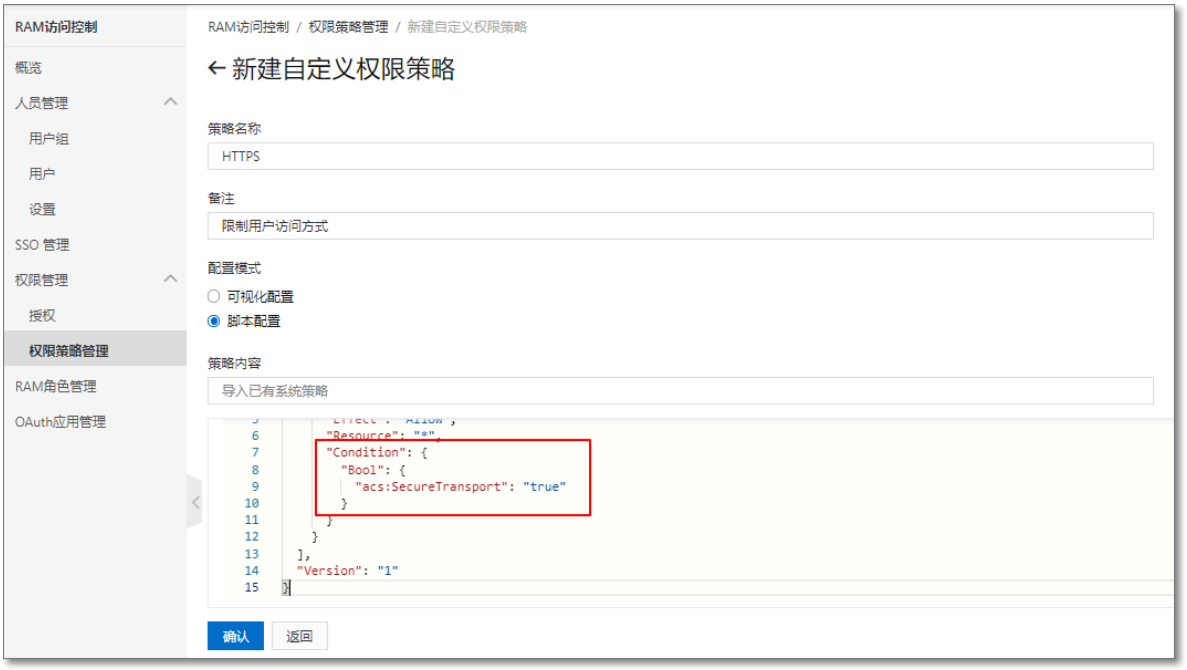
您可以根据需要创建自定义策略并为RAM用户添加相应的权限，从而保证RAM用户只能通过HTTPS方式访问阿里云。

1. 创建RAM用户。
2. 创建自定义策略。
3. 为RAM用户授权。

创建自定义策略

1. 在左侧导航栏的权限管理菜单下，单击权限策略管理。
2. 单击新建权限策略。
3. 填写策略名称和备注。

4. 配置模式选择脚本配置，拷贝下述策略示例到策略内容区域下并根据实际情况进行修改。



下述策略表示：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为true或false。

5. 单击确认。

5 RAM对多运维人员的权限管控

当您的企业涉及多种运维需求时，通过RAM进行运维划分，对不同的运维人员授予不同的权限，方便管理和控制。

前提条件

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。详情请参见账号注册。

背景信息

某公司购买了大量的阿里云产品，并将应用系统部署在云上，因此涉及多种运维需求：

- 不同的运维负责人需要运维不同的阿里云产品。
- 不同的运维人员需要不同的访问、操作、管理云资源的权限。

运维划分解决方案

根据云产品进行运维划分，设置如下运维负责人并授予特定的权限策略。

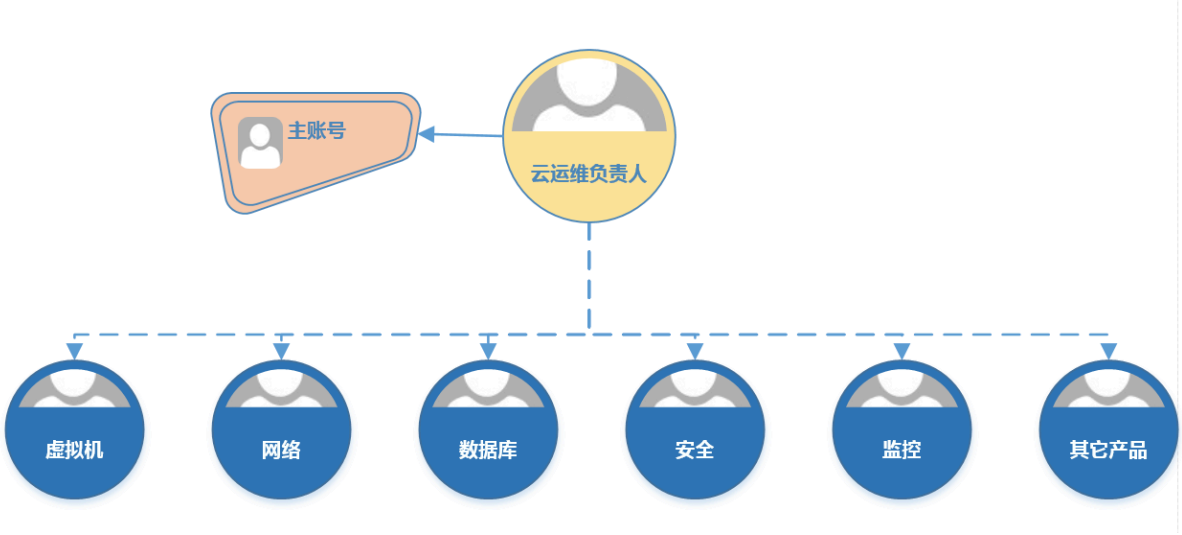


表 5-1: 权限策略

运维负责人	权限策略名称	权限策略说明
云运维负责人	AdministratorAccess	管理所有阿里云资源的权限
虚拟机运维负责人	AliyunECSFullAccess	管理云服务器服务（ECS）的权限
	AliyunESSFullAccess	管理弹性伸缩服务（ESS）的权限
	AliyunSLBFullAccess	管理负载均衡服务（SLB）的权限
	AliyunNASFullAccess	管理文件存储服务（NAS）的权限

运维负责人	权限策略名称	权限策略说明
	AliyunOSSFullAccess	管理对象存储服务（OSS）权限
	AliyunOTSFullAccess	管理表格存储服务（OTS）的权限
网络运维负责人	AliyunCDNFullAccess	管理CDN的权限
	AliyunCENFullAccess	管理云企业网（CEN）的权限
	AliyunCommonBandwidthPackageFullAccess	管理共享带宽的权限
	AliyunEIPFullAccess	管理弹性公网IP（EIP）的权限
	AliyunExpressConnectFullAccess	管理高速通道（ExpressConnect）的权限
	AliyunNATGatewayFullAccess	管理NAT网关（NATGateway）的权限
	AliyunSCDNFullAccess	管理安全加速（SCDN）的权限
	AliyunSmartAccessGatewayFullAccess	管理智能接入网关（SmartAccessGateway）的权限
	AliyunVPCFullAccess	管理专有网络（VPC）的权限
	AliyunVPNGatewayFullAccess	管理VPN网关（VPNGateway）的权限
数据库运维负责人	AliyunRDSFullAccess	管理云数据库服务（RDS）的权限
	AliyunDTSFullAccess	管理数据传输服务（DTS）的权限
安全运维负责人	AliyunYundunFullAccess	管理云盾所有产品（Yundun）的权限
监控运维负责人	AliyunActionTrailFullAccess	管理操作审计（ActionTrail）的权限
	AliyunARMSFullAccess	管理业务实时监控服务（ARMS）的权限
	AliyunCloudMonitorFullAccess	管理云监控（CloudMonitor）的权限
	ReadOnlyAccess（可选）	只读访问所有阿里云资源的权限（可选）
	AliyunSupportFullAccess	管理工单系统的权限

示例：将用户配置为数据库运维负责人

此示例将RAM用户`alice@secloud.onaliyun.com`配置为数据库运维负责人，从而允许该用户管理云数据库服务（RDS）和数据传输服务（DTS）。

1. 登录RAM控制台。
2. 创建RAM用户为`alice@secloud.onaliyun.com`。
3. 找到创建好的RAM用户，单击添加权限 。
4. 从左侧权限策略名称列中勾选`AliyunRDSFullAccess`和`AliyunDTSFullAccess`，单击确定。

> 说明:
> 如需将用户配置为其他运维负责人，请参考上述权限策略表格，为相关负责人授予相应的权限。

更多信息

如需了解详细运维案例，请参见阿里云RAM运维最佳实践。

6 用户管理与分权

当企业有多种云资源时，使用RAM的身份管理与权限管理功能，实现用户分权及资源统一管理。

前提条件

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。详情请参见账号注册。

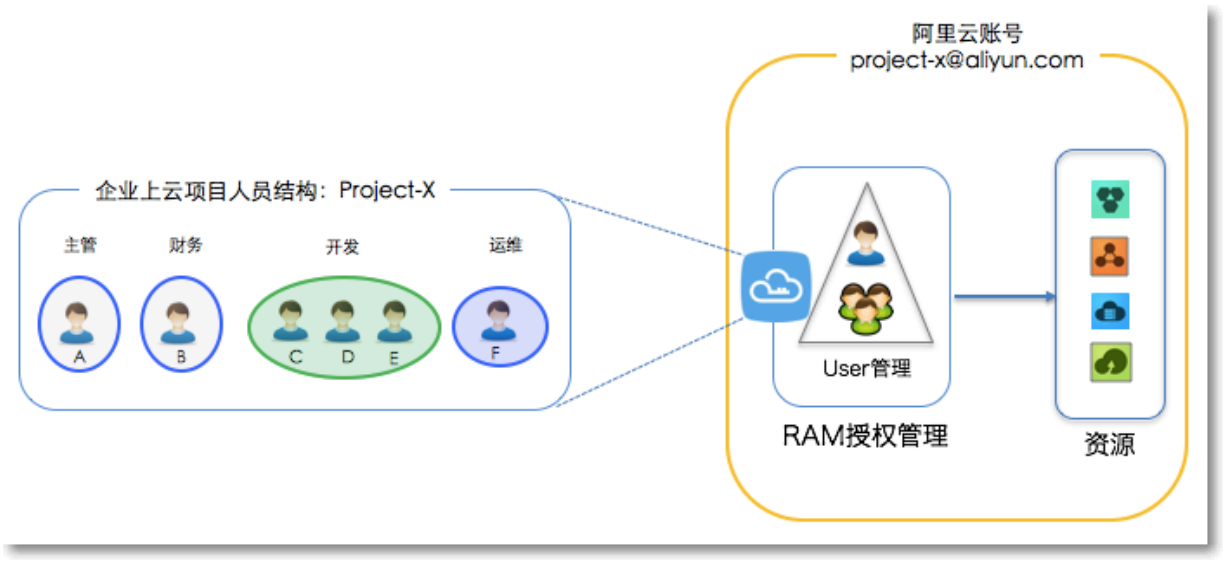
背景信息

企业A的某个项目（Project-X）上云，购买了多种阿里云资源，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。项目里有多个员工需要操作这些云资源，由于每个员工的工作职责不同，需要的权限也不一样。

企业A希望能够达到以下要求：

- 企业A不希望多员工共享同一个云账号，共享云账号可能导致密码或访问密钥泄露。
- 企业A希望能给员工创建独立账号（操作员账号）并独立分配权限，做到责权一致。
- 企业A希望用户账号只能在授权的前提下操作资源，所有用户账号的所有操作行为可审计。
- 企业A希望随时可以撤销用户账号身上的权限，也可以随时删除其创建的用户账号。
- 企业A不需要对用户账号进行独立的计量计费，所有发生的费用统一计入云账号账单。

解决方案



- 为云账号设置多因素认证，避免因云账号密码泄露导致风险。详情请参见为云账号设置多因素认证。
- 为不同员工（应用系统）创建RAM用户，并按需设置登录密码或创建访问密钥。详情请参见创建RAM用户。

- 如果有多个员工的职责相同，建议创建用户组，并将用户添加到用户组。详情请参见创建用户组。
- 为RAM用户或用户组添加一条或多条系统策略。详情请参见为RAM用户授权或为用户组授权。如果需要更细粒度的授权，可以创建自定义策略并为RAM用户或用户组进行授权。详情请参见创建自定义策略。
- 为不需要权限的RAM用户或用户组移除权限。详情请参见为RAM用户移除权限或为用户组移除权限。

7 移动设备应用使用临时安全令牌访问阿里云

本文介绍移动设备应用如何使用RAM角色的临时安全令牌（STS token）访问阿里云相关资源。

前提条件

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。详情请参见账号注册。

背景信息

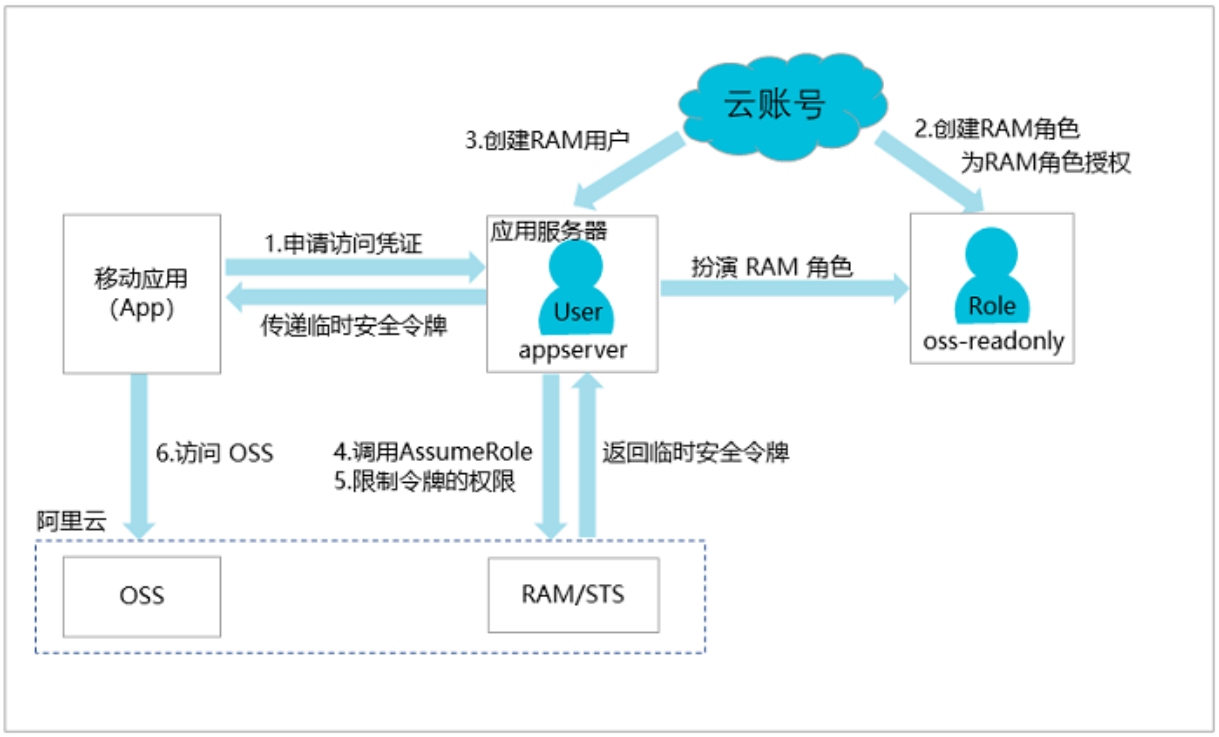
企业A开发了一款移动应用（App），并购买了对象存储（OSS）服务。App需要直连OSS上传或下载数据，但是App运行在用户自己的移动设备上，这些设备不受企业A的控制。

企业A有如下要求：

- 直传数据：企业A不希望所有App都通过企业的服务端应用服务器（Application Server）来进行数据中转，而希望能够直连OSS上传或下载数据。
- 安全管控：企业A不希望将访问密钥（AccessKey）保存到移动设备中，因为移动设备是归属于用户控制，属于不可信的运行环境。
- 风险控制：企业A希望将风险控制到最小，每个App直连OSS时都必须拥有最小的访问权限且访问时效需要很短。

解决方案

当移动应用（App）直连OSS上传或下载数据时，App需要向应用服务器申请访问凭证。应用服务器以RAM用户身份扮演RAM角色，调用STS API `AssumeRole`接口获取临时安全令牌，并将临时安全令牌传递给App，App使用临时安全令牌访问OSS。



1. App向应用服务器申请访问凭证。
2. 云账号A创建一个RAM角色，并为RAM角色授予合适的权限。

   操作流程请参见创建RAM角色并授权。
3. 云账号A为应用服务器创建一个RAM用户，并允许应用服务器以RAM用户身份扮演该RAM角色。

   操作流程请参见创建RAM用户并允许扮演RAM角色。
4. 应用服务器通过调用STS API AssumeRole接口获取RAM角色的临时安全令牌。

   操作流程请参见应用服务器获取临时安全令牌。
5. 应用服务器可以进一步限制临时安全令牌的权限，以更精细地控制每个App的权限。

   操作流程请参见限制临时安全令牌的权限。
6. 当App需要直连OSS上传或下载数据时，可以使用临时安全令牌访问OSS进行数据直传。

   操作流程请参见App使用临时安全令牌并访问OSS。

创建RAM角色并授权

假设云账号A的账号ID为：`123456789012****`。

1. 云账号A创建可信实体为阿里云账号的RAM角色：`oss-readonly`。

   说明:

创建RAM角色时选择当前云账号作为受信云账号，即只允许云账号A下的RAM用户来扮演该RAM角色。

关于如何创建RAM角色，详情请参见创建可信实体为阿里云账号的RAM角色。

RAM角色创建成功后，在角色基本信息页面可以查看到该RAM角色的ARN和信任策略。

- RAM角色的ARN：`acs:ram::123456789012****:role/oss-readonly`。
- RAM角色的信任策略如下：

说明：

以下策略表示只允许云账号A下的RAM用户来扮演RAM角色。

```
{
"Statement": [
{
 "Action": "sts:AssumeRole",
 "Effect": "Allow",
 "Principal": {
   "RAM": [
     "acs:ram::123456789012****:root"
   ]
 }
}
],
"Version": "1"
}
```

2. 为RAM角色授权。为RAM角色：`oss-readonly` 授予OSS的只读访问权限：`AliyunOSSReadOnlyAccess` 。

   关于如何为RAM角色授权，详情请参见为RAM角色授权。

创建RAM用户并允许扮演RAM角色

1. 云账号A为应用服务器创建RAM用户：`appserver`。

   关于如何创建RAM用户，详情请参见创建RAM用户。

2. 为创建好的RAM用户授予 `AliyunSTSAssumeRoleAccess` 权限，即允许RAM用户扮演RAM角色。

   关于如何为RAM用户授权，详情请参见为RAM用户授权。

应用服务器获取临时安全令牌

1. 应用服务器使用RAM用户的访问密钥调用STS API `AssumeRole`接口。

说明：

必须配置应用服务器的访问密钥，而非云账号A的访问密钥。

使用阿里云CLI调用AssumeRole的示例如下：

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::123456789012****:role/
oss-readonly --RoleSessionName client-001
 {
     "AssumedRoleUser": {
         "AssumedRoleId": "391578752573****:client-001",
         "Arn": "acs:ram::123456789012****:role/oss-readonly/client-
001"
     },
     "Credentials": {
         "AccessKeySecret": "93ci2umK1QKNEja6WGqi1Ba7Q2Fv9P
wxZqtVF2Vy****",
         "SecurityToken": "********",
         "Expiration": "2016-01-13T15:02:37Z",
         "AccessKeyId": "STS.F13GjskXTjk38dBY6YxJt****"
     },
     "RequestId": "E1779AAB-E7AF-47D6-A9A4-53128708B6CE"
 }
```

说明：

若没有指定Policy参数，返回的临时安全令牌将拥有RAM角色：oss-readonly 的所有权限。

2. STS服务将临时安全令牌返回给应用服务器。返回的临时安全令牌中包含：AccessKeyId、AccessKeySecret和SecurityToken。

说明：

SecurityToken过期时间较短。如果需要一个较长的过期时间，应用服务器需要重新颁发临时安全令牌，例如：每隔1800秒颁发一次。

限制临时安全令牌的权限

如果需要进一步限制临时安全令牌的权限，可以通过配置Policy参数来实现。

以下示例表示：只允许访问sample-bucket/2015/01/01/*.jpg。

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::123456789012****:role/
oss-readonly --RoleSessionName client-002 --Policy "{\"Version\":\"1
\", \"Statement\": [{\"Effect\":\"Allow\", \"Action\":\"oss:GetObject
\", \"Resource\":\"acs:oss:*:*:sample-bucket/2015/01/01/*.jpg\"}]}"
{
   "AssumedRoleUser": {
       "AssumedRoleId": "391578752573****:client-002",
       "Arn": "acs:ram::123456789012****:role/oss-readonly/client-002"
   },
   "Credentials": {
       "AccessKeySecret": "28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7x
****",
       "SecurityToken": "********",
       "Expiration": "2016-01-13T15:03:39Z",
```

```
        "AccessKeyId": "STS.FJ6EMcS1JLZgAcBJSTDG1****"
    },
    "RequestId": "98835D9B-86E5-4BB5-A6DF-9D3156ABA567"
}
```

说明:

临时安全令牌的默认过期时间为3600秒。通过DurationSeconds参数可以限制其过期时间，最长不超过3600秒。

App使用临时安全令牌并访问OSS

1. **应用服务器将临时安全令牌传递给App。**
2. **App使用临时安全令牌访问OSS。**

   下面是阿里云CLI使用临时安全令牌访问OSS的示例:

```
配置临时安全令牌语法: aliyuncli oss Config --host  --accessid  --
accesskey  --sts_token
$ aliyuncli oss Config --host oss.aliyuncs.com --accessid STS.
FJ6EMcS1JLZgAcBJSTDG1**** --accesskey 28Co5Vyx2XhtTqj3RJgdud4ntyzrSN
dUvNygAj7x**** --sts_token CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm
8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU78Fkszx
hnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4
NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEa
egoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDwoNb3NzOkdldE9i
amVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoq
Oio6c2FtcGxlLWJ1Y2tldC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4
NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4NTRyCWVj
cy1hZG1pbnjgxt7Cj/bo****
访问 OSS
$ aliyuncli oss Get oss://sample-bucket/2015/01/01/grass.jpg grass.
jpg
```

更多参考

关于移动应用直传场景，请参见以下文档:

- **快速搭建移动应用直传服务**
- **权限控制**
- **快速搭建移动应用上传回调服务**
- **STS临时授权访问**

8 跨云账号的资源授权

当一个企业希望将部分业务授权给另一个企业时，可以使用RAM角色进行跨云账号授权来管理资源的授权及访问。

前提条件

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。详情请参见账号注册。

背景信息

企业A购买了多种阿里云资源来开展业务，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。企业A希望将部分业务授权给企业B。

企业A有如下要求：

- 企业A希望能专注于业务系统，仅作为资源Owner。企业A希望可以授权账号B来操作部分业务，例如：云资源运维、监控以及管理等。
- 企业A希望当企业B的员工加入或离职时，无需做任何权限变更。企业B可以进一步将企业A的资源访问权限分配给企业B的RAM用户（员工或应用），并可以精细控制其员工或应用对资源的访问和操作权限。
- 企业A希望如果双方合同终止，企业A随时可以撤销企业B的授权。

解决方案

企业A需要授权企业B的员工对ECS进行操作。假设企业A和企业B下分别有一个云账号A和云账号B。

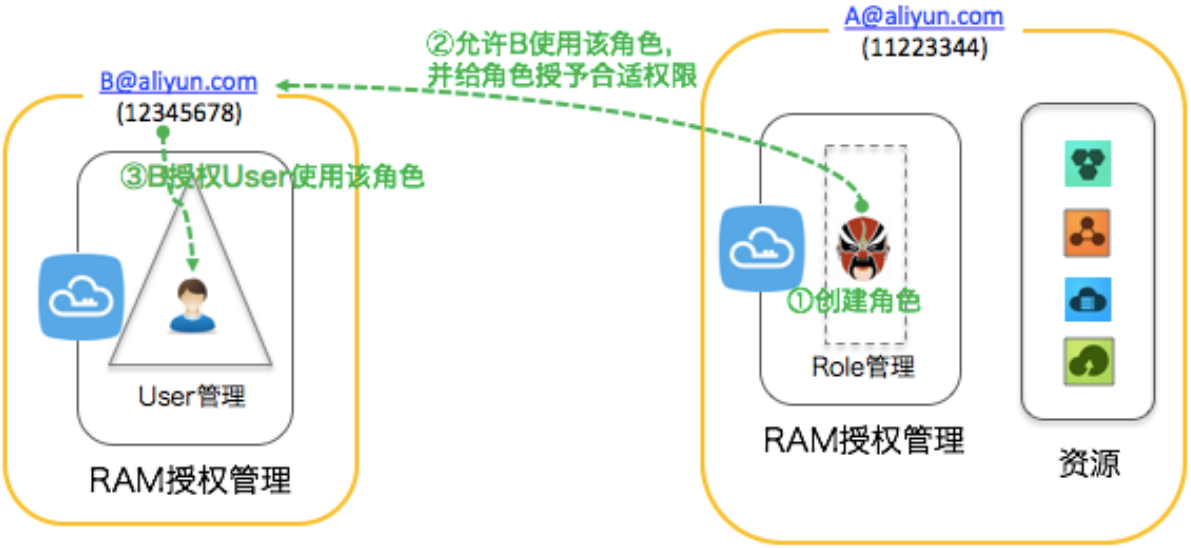
- 企业A的云账号ID为：`123456789012****`，账号别名为：`company-a`。
- 企业B的云账号ID为：`134567890123****`，账号别名为：`company-b`。
- 云账号A创建一个RAM角色，并为RAM角色授予合适的权限，允许云账号B使用该角色。

  操作流程请参见跨云账号授权。
- 如果云账号B下的某个员工（RAM用户）需要使用该RAM角色，那么云账号B可以自主进行授权控制。云账号B下的RAM用户将扮演RAM角色来操作云账号A的资源。

  操作流程请参见跨云账号访问资源。
- 如果企业A与企业B的合作终止，企业A只需要撤销云账号B对RAM角色的使用。此时云账号B下的所有RAM用户对RAM角色的使用权限将被自动撤销。

  操作流程请参见撤销跨云账号授权 。

跨云账号授权



1. 云账号A创建可信实体为阿里云账号的RAM角色`ecs-admin`。

   说明:
   创建RAM角色时选择其他云账号：`134567890123****`作为受信云账号，即允许云账号B下的RAM用户来扮演该RAM角色。

   关于如何创建RAM角色，详情请参见创建可信实体为阿里云账号的RAM角色。

   RAM角色创建成功后，在角色基本信息页面中可以查看到该RAM角色的ARN和信任策略。

   - RAM角色的ARN： `acs:ram::123456789012****:role/ecs-admin`。
   - RAM角色的信任策略如下：

     说明:
     以下策略表示允许云账号B下的RAM用户来扮演该RAM角色。

     ```
     {
     "Statement": [
     {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::134567890123****:root"
        ]
      }
     }
     ],
     "Version": "1"
     ```

```
}
```

2. 云账号A为RAM角色ecs-admin添加AliyunECSFullAccess权限。

   关于如何为RAM角色授权，请参见为RAM角色授权。

3. 云账号B为其员工创建RAM用户：Alice。

   关于如何创建RAM用户，请参见创建RAM用户。

4. 云账号B为创建好的RAM用户设置登录密码：123456****并添加AliyunSTSAssumeRoleAccess权限，即允许RAM用户扮演RAM角色。

   关于如何为RAM用户授权，请参见为RAM用户授权。

跨云账号访问资源

对云账号B的RAM用户Alice进行授权后，RAM用户通过切换角色便可以访问云账号A下的ECS资源。

1. 云账号B的RAM用户登录RAM控制台。

   > **说明:**
   > RAM用户登录时需要输入账号别名：company-b，RAM用户名称：Alice和RAM用户密码：123456****。

   关于RAM用户如何登录控制台，请参见RAM用户登录控制台。

2. RAM用户登录成功后，将鼠标悬停在右上角头像的位置，单击切换身份。

   > **说明:**
   > 切换角色时需要输入账号别名：company-a和RAM角色名称：ecs-admin。

   关于如何切换角色，详情请参见使用RAM角色。

撤销跨云账号授权

云账号A可以撤销云账号B对RAM角色ecs-admin的使用。

1. 云账号A登录RAM控制台。
2. 在左侧导航栏，单击RAM角色管理。
3. 单击RAM角色名称ecs-admin。
4. 在信任策略管理页签下，单击修改信任策略，删除整行策略内容"acs:ram::134567890123****:root"。

   > **说明:**

云账号A也可以通过删除RAM角色ecs-admin来撤销云账号B的权限。但在删除RAM角色前，请先为RAM角色移除权限。详情请参见为RAM角色移除权限。

9 对云上应用进行动态身份管理与授权

当企业购买阿里云产品后，通过访问控制（RAM），应用程序可以获取RAM角色的临时安全令牌从而访问阿里云。

前提条件

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。详情请参见账号注册。

背景信息

企业购买了ECS实例，并且打算在ECS中部署企业的应用程序。这些应用程序需要使用访问密钥（AccessKey）访问其它云服务API。

有两种做法：

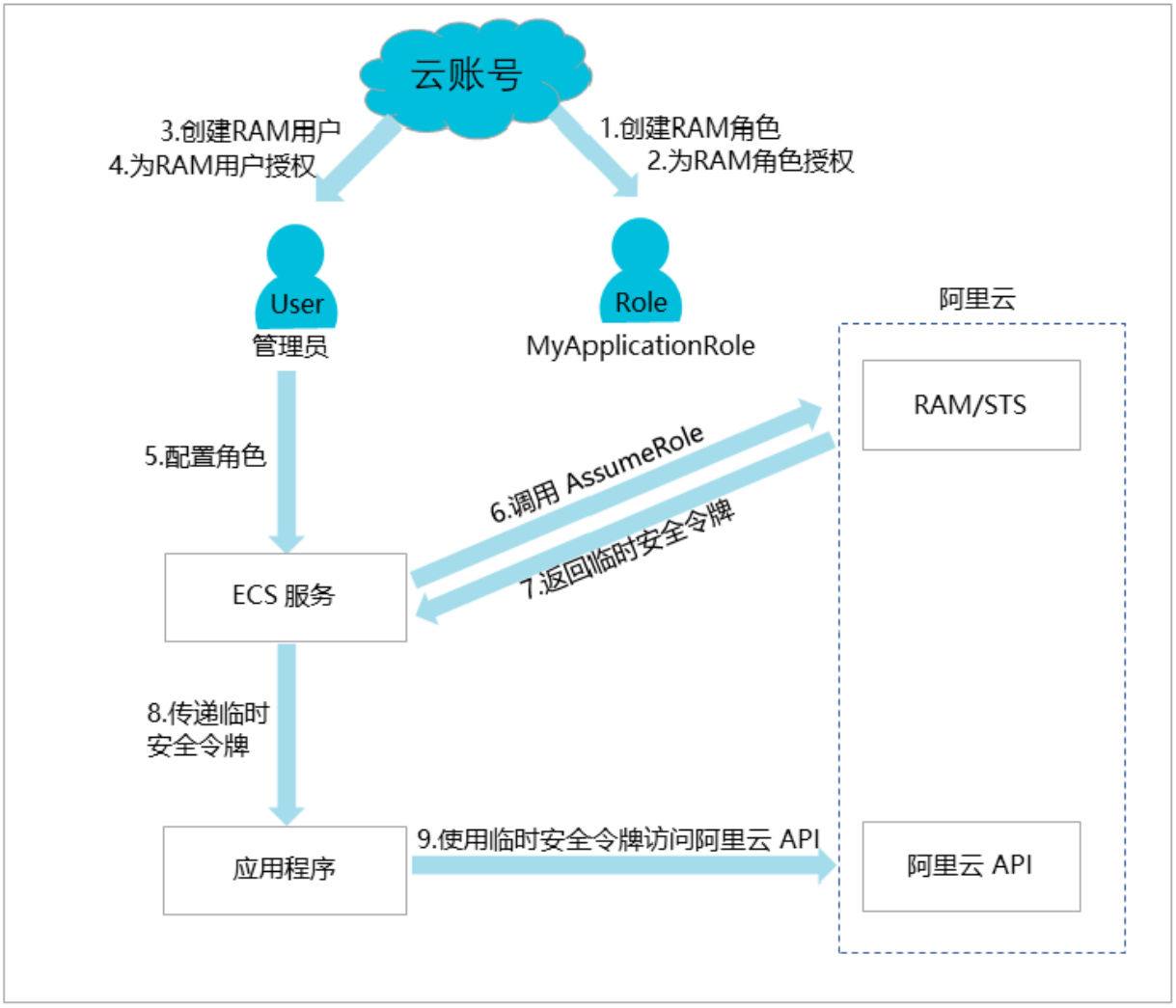
- 将访问密钥直接嵌入在代码里。
- 将访问密钥保存在应用程序的配置文件中。

这样会带来两个问题：

- 保密性问题：如果访问密钥以明文形式存在于ECS实例中，可能会随着快照、镜像及镜像创建出来的实例泄露。
- 难运维问题：由于访问密钥存在于实例中，如果要更换访问密钥（例如：周期性轮转或切换用户身份），那么需要对每个实例和镜像进行更新并重新部署，这会增加对实例和镜像管理的复杂性。

解决方案

ECS服务结合RAM提供的访问控制能力，允许给每一个ECS实例配置一个拥有合适权限的RAM角色身份。应用程序通过获取该RAM角色的临时安全令牌来访问云API。



操作流程

1. 云账号创建一个RAM角色：`MyApplicationRole`。

   说明：
   创建RAM角色时受信实体选择阿里云服务，受信服务选择云服务器ECS，即允许允许云服务ECS扮演该RAM角色来访问阿里云资源。

   关于如何创建RAM角色，请参见创建可信实体为阿里云服务的RAM角色。

2. 为RAM角色授予合适的权限。

   关于如何为RAM角色授权，请参见为RAM角色授权。

   说明：
   如果临时安全令牌权限不足时，您可以根据需要为RAM角色添加相应的权限。权限更新后立即生效，无需重新启动ECS实例。

3. 云账号创建一个RAM用户。

   关于如何创建RAM用户，请参见创建RAM用户。

4. 为RAM用户授予合适的权限。

   - 若管理员和操作员是同一人，需要授予RAM用户管理员权限：`AdministratorAccess`。
   - 若管理员与操作员职责分离，需要授予RAM用户`PassRole`权限将管理员和操作员区分为不同的RAM用户。

     在RAM控制台创建自定义策略，然后将这个自定义策略授权给RAM用户。策略内容如下：

     ```
     {
        "Statement": [
         {
           "Effect": "Allow",
           "Action": "ram:PassRole",
           "Resource": "acs:ram:*:*:role/MyApplicationRole"//替换
     MyApplicationRole为自己的RAM角色名称
         }
       ],
       "Version": "1"
     }
     ```

     说明：

     - 只有被授权的RAM用户才能为ECS实例配置RAM角色，避免RAM角色权限被滥用。
     - 如果RAM用户没有管理员权限，仅有管理ECS的权限。在创建ECS实例并配置RAM角色时，ECS服务会强制检查当前RAM用户是否拥有指定RAM角色的`ram:PassRole`权限，否则将无法成功创建ECS实例。

   关于如何为RAM用户授权，请参见为RAM用户授权。

5. 启动ECS实例时，配置创建好的RAM角色。

6. ECS服务调用STS API AssumeRole去获取该RAM角色的临时安全令牌。

   说明：

   STS服务会验证ECS服务身份及RAM角色的授权类型，验证通过后颁发临时安全令牌。

   关于如何通过调用STS API使用RAM角色，请参见通过API使用实例RAM角色。

7. STS服务将临时安全令牌返回给ECS服务。

8. ECS将通过实例元数据将临时安全令牌传递给ECS实例中的应用程序。

   - 若在Linux系统中，通过实例元数据可以获取临时安全令牌及过期时间等信息。 请参见借助于实例RAM角色访问其他云产品。

     请求示例：

     ```
     $ curl http://100.100.100.200/latest/meta-data/ram/security-credentials/MyApplicationRole
     ```

     返回示例：

     ```
     [root@local ~]# curl http://100.100.100.200/latest/meta-data/ram/security-credentials/MyApplicationRole
     {
     "AccessKeyId" : "STS.J8XXXXXXXXX4",
     "AccessKeySecret" : "9PjfXXXXXXXXBf2XAW",
     "Expiration" : "2017-06-09T09:17:19Z",
     "SecurityToken" : "CAIXXXXXXXXXXwmBkleCTkyI+",
     "LastUpdated" : "2017-06-09T03:17:18Z",
     "Code" : "Success"
     }cess"
     }
     ```

   - 若应用程序使用了阿里云SDK，无需在SDK中配置任何访问密钥相关的信息，阿里云SDK将会自动从ECS实例元数据中获取临时安全令牌。 请参见配置RamRole实现ECS实例的无AK访问。

     > 说明：
     > 临时安全令牌过期时间通常为1小时，有效期内应用程序都能正常访问阿里云API，过期之前ECS服务会自动刷新临时安全令牌。

9. 应用程序使用临时安全令牌访问阿里云API。

后续步骤

除了ECS服务之外，阿里云其它计算类服务（例如：函数计算、MaxCompute）也提供了类似的RAM角色访问能力，以帮助用户解决云上应用的动态身份管理与授权的问题。

10 RAM资源分组与授权

若您的公司购买了多种阿里云资源，您可以通过创建资源组进行云资源分组，从而实现独立管理资源组内成员、权限和资源。

前提条件

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。详情请参见账号注册。

背景信息

某游戏公司A正在开发3个游戏项目，每个游戏项目都会用到多种云资源。公司A只有1个阿里云账号，该云账号下有超过100个ECS实例。

公司A有如下要求：

- 项目独立管理：每个管理员各自能够独立管理项目人员及其访问权限。
- 按项目分账：财务部门希望能够根据项目进行出账，以解决财务成本分摊的问题。
- 共享底层网络：客户希望云资源的底层网络默认共享。

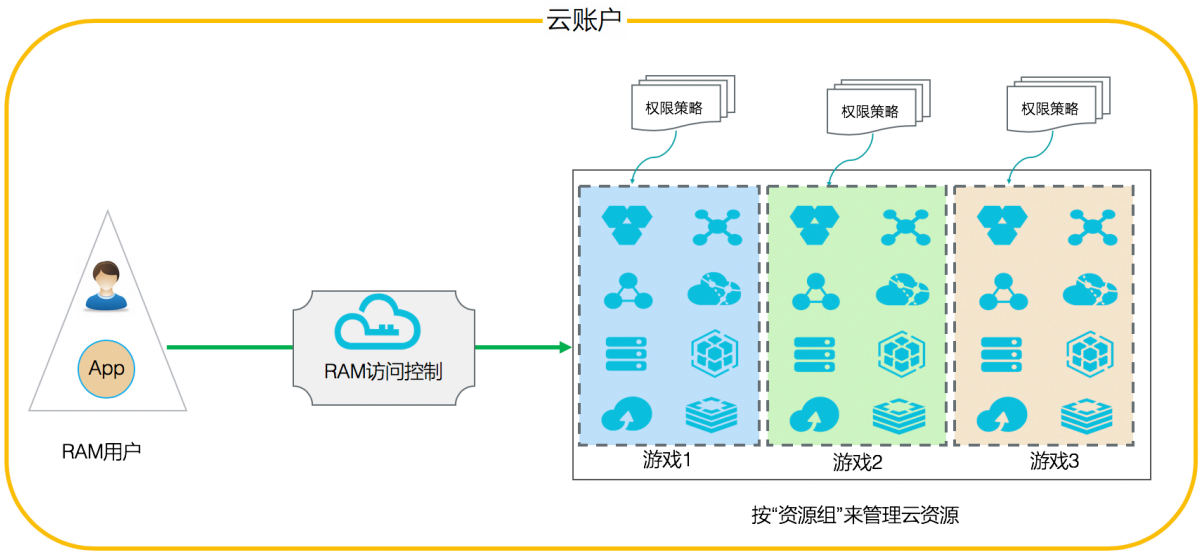
公司A有如下解决方案：

- 多账号方案
  - 可以满足项目独立管理：公司A注册3个账号（对应3个项目），每个账号有对应项目管理员可以独立管理成员及其访问权限。
  - 可以满足按项目分账：每个账号有默认账单，可以利用阿里云提供的多账号合并记账能力来解决统一账单和发票问题。
  - 无法满足共享底层网络：账号之间是有安全边界的，不同账号之间的资源是100%隔离的，网络之间默认不通。虽然可以通过VPC-Peering来打通跨账号的VPC网络，但会带来较高的管理成本。
- 单账号给资源打标签方案
  - 无法满足项目独立管理：给资源打标签可以模拟项目分组，但无法解决项目管理员独立管理项目成员及其访问权限的问题。
  - 可以满足按项目分账：按照项目组给资源打上对应标签，根据标签实现分账。
  - 可以满足共享底层网络：公司A只用1个账号，根据项目打不同的项目标签，结合RAM提供的基于标签的条件授权能力，可以将一组资源授权给某些RAM用户，不存在打通网络所需的额外管理成本。

- 资源组管理方案
  - 可以满足项目独立管理：每个资源组有对应的管理员，资源组管理员可以独立管理成员及其访问权限。
  - 可以满足按项目分账：账单管理功能支持按资源组进行分账，解决财务成本分摊的问题。
  - 可以满足共享底层网络：资源组属于账号内部的分组功能，同一账号下的不同资源组可以共享同一个VPC网络，节约管理成本。

解决方案

资源组是在阿里云账号下进行资源分组管理的一种机制，公司A只需使用1个账号，创建3个资源组（对应3个项目）。



1. 创建3个RAM用户：`alice@secloud.onaliyun.com`、`bob@secloud.onaliyun.com`和`charlie@secloud.onaliyun.com`。

   详情请参考：创建RAM用户。

   > 说明：
   > 下面的操作均以RAM用户Alice为例，介绍如何将其设为项目的管理员。

2. 登录资源管理控制台。
3. 单击左侧导航栏的资源组管理，单击新建资源组。
4. 输入标识和显示名后，单击确定。

   > 说明：
   > 创建3个资源组，分别命名为：Game1、Game2、Game3。

5. 找到创建好的资源组，单击管理权限。
6. 在权限管理页签下，单击新增授权。
7. 在被授权主体区域下，输入Alice，单击其名称。
8. 在权限策略名称列表下，单击`AdministratorAccess`。
9. 单击确定。

说明:

如何将Bob或Charlie设置为资源组管理员，请参考上述步骤。

下一步

由于Alice、Bob和Charlie分别是Game1、Game2、Game3的资源组管理员，将有以下权限：

- 登录ECS控制台，可以看到相应资源组，并可以创建和管理ECS实例。
- 登录资源管理控制台，可以添加其它RAM用户并授予相应的资源访问权限。

11 利用标签对ECS实例进行分组授权

本文介绍了如何利用标签对ECS实例进行分组并授权，以满足RAM用户只能查看和操作被授权资源的需求。

前提条件

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。详情请参见账号注册。

背景信息

假设您的账号购买了10个ECS实例，其中5个想要授权给dev团队，另外5个授权给ops团队。企业希望每个团队只能查看被授权的实例，未被授权的不允许查看。

分组授权的前提条件

请确保已拥有RAM账号并可以登录RAM控制台。

分组授权解决方案

创建两个用户组，通过打标签将ECS实例分成2个组并授权给对应的用户组。

- 其中5个实例打上一对标签，标签键是team，标签值是dev。
- 另外5个实例打上另一对标签，标签键是team，标签值是ops。

分组授权的操作步骤

1. 登录ECS控制台，选择一个实例，在操作菜单下选择更多 > 实例设置 > 编辑标签。
2. 单击新建标签，输入标签键和标签值，单击确定。

   说明:

   将所有机器分别打上对应的标签。
3. 登录RAM控制台创建两个用户组： dev和ops。

   详情请参见创建用户组。
4. 创建不同的RAM账号，并添加到相应的用户组下。

   详情请参见创建RAM用户。
5. 创建两个自定义策略，分别授权给两个用户组。

   详情请参见为用户组授权。

   说明:

授权后RAM用户已继承对应用户组的相关权限。

例如：给dev组授权的自定义策略名称是policyForDevTeam，策略内容如下：

```
{
    "Statement": [
    {
        "Action": "ecs:*",
        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ecs:tag/team": "dev"
            }
        }
    },
    {
        "Action": "ecs:DescribeTag*",
        "Effect": "Allow",
        "Resource": "*"
    }
    ],
    "Version": "1"
}
```

在上述权限策略中：

- 带有Condition的"Action": "ecs:*"部分用于过滤标签为"team": "dev"的资源。
- "Action": "ecs:DescribeTag*"用于展示所有标签。当RAM用户在操作 ECS控制台时，系统展示出所有标签供RAM用户选择，只有当RAM用户选择了标签值后，系统才能根据选中的标签值过滤相应资源。

说明：

根据上述自定义策略，创建另一个policyForOpsTeam权限策略并授权给ops用户组。

显示被授权实例

1. RAM用户登录ECS控制台。

说明：

登录控制台后，系统默认跳转到ECS概览页，此时RAM用户看到的实例数为0，如需查看相关实例，请切换到实例页签下。

2. 单击实例，单击搜索栏旁的标签。

说明：

请确保控制台展示的当前地域是期望地域。

3. 鼠标悬停在标签键上，在标签键下拉列表的右侧会展示出对应的标签值，点击对应的标签值，系统可以过滤出相应资源。

> 说明:
> 选中标签值之后，系统才可以过滤出相应资源。

更多信息

利用标签对安全组、云盘、快照或镜像进行分组授权的方法与上述对实例分组授权的方法相同。

> 说明:
> 镜像中只有自定义镜像支持打标签。

12 利用标签对RDS实例进行分组授权

本文介绍了如何利用标签对RDS实例进行分组并授权，以满足RAM用户只能查看和操作被授权资源的需求。

前提条件

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。详情请参见账号注册。

背景信息

假设您的账号购买了10个RDS实例，其中5个想要授权给dev团队，另外5个授权给ops团队。企业希望每个团队只能查看被授权的实例，未被授权的不允许查看。

利用标签对RDS分组授权的操作步骤

具体操作步骤请参见利用标签对ECS实例进行分组授权。

RDS相关自定义策略：

```
{
  "Statement": [
    {
      "Action": "rds:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:ResourceTag/team": "dev"
        }
      }
    },
    {
       "Action": "rds:DescribeTag*",
       "Effect": "Allow",
       "Resource": "*"
     }
  ],
  "Version": "1"
}
```

权限策略内容分为两部分：

- 其中带有Condition的"Action": "rds:*"部分用于过滤标签为"team": "dev"的资源。Condition部分的关键字为rds:ResourceTag。
- "Action": "rds:DescribeTag*"用于展示所有标签。当RAM用户在操作RDS控制台时，系统展示出所有标签供RAM用户选择，只有当RAM用户选择了标签值后，系统才能根据选中的标签值过滤相应资源。

更多信息

利用标签对RDS实例分组授权后，如果遇到RAM用户登录控制台报无权限的问题，请参见利用标签对RDS实例分组授权的常见问题。

13 使用RAM对ECS进行权限管理

本文介绍了通过RAM的权限管理功能，创建相应的权限策略，从而对云服务器（ECS）进行权限管理，以满足RAM用户操作ECS的多种需求。

前提条件

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。详情请参见账号注册。

基本信息

使用RAM对ECS进行权限管理前，需先了解几个常用的权限策略。

权限策略	描述
AliyunECSFullAccess	为RAM用户授予ECS的完全管理权限。
AliyunECSReadOnlyAccess	为RAM用户授予ECS的只读访问权限。

说明:

查看ECS的权限定义，请参见ECS产品文档中的鉴权规则。

将自定义策略授权给RAM用户

1. 根据下述ECS授权样例创建相应的自定义策略。

   详情请参见创建自定义策略。
2. 找到创建好的权限策略，单击其权限策略名称。
3. 单击引用记录 > 新增授权。
4. 被授权主体处输入需要授权的用户名称或ID。
5. 单击确定。

说明:

您也可以直接对用户或用户组授予创建好的权限策略，详情请参见为RAM用户授权和为用户组授权。

ECS授权样例

- 示例1：授权RAM用户管理2台指定的ECS实例。

  假设您的账号购买了多个实例，而作为RAM管理员，您希望仅授权其中的2个实例给某个RAM用户。实例ID分别为：i-001，i-002。

```
{
```

```
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
                  "acs:ecs:*:*:instance/i-001",
                  "acs:ecs:*:*:instance/i-002"
                  ]
    },
    {
      "Action": "ecs:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

说明:

- **授予该权限策略的RAM用户可以查看所有的实例及资源，但只能操作其中2个实例。**
- `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，使用API、CLI或SDK直接对两个实例进行操作是可以的。**

- **示例2：仅授权RAM用户查看青岛的ECS实例，但不允许查看磁盘及快照信息。**

  查看ECS资源列表的授权粒度可以到Region+资源类型的级别。

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

- **示例3：授权RAM用户创建快照权限。**

  若RAM用户已拥有ECS实例管理员权限， 但仍不能创建磁盘快照，再次授予RAM用户指定磁盘的权限即可正常使用。ECS实例ID：inst-01，磁盘ID：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"
}
```

14 使用RAM对OSS进行权限管理

本文介绍了通过RAM的权限管理功能，创建相应的权限策略，从而对对象存储（OSS）进行权限管理，以满足RAM用户操作OSS的多种需求。

前提条件

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。详情请参见账号注册。

基本信息

使用RAM对OSS进行权限管理前，需先了解几个常用的权限策略。

权限策略	描述
AliyunOSSFullAccess	为RAM用户授予OSS的完全管理权限。
AliyunOSSReadOnlyAccess	为RAM用户授予OSS的只读访问权限。

说明:

查看OSS的权限定义，请参见OSS产品文档中的权限控制概述。

将自定义策略授权给RAM用户

1. 根据下述OSS授权样例创建相应的自定义策略。

   详情请参见创建自定义策略。
2. 找到创建好的权限策略，单击其权限策略名称。
3. 单击引用记录 > 新增授权。
4. 被授权主体处输入需要授权的用户名称或ID。
5. 单击确定。

说明:

您也可以直接对用户或用户组授予创建好的权限策略，详情请参见为RAM用户授权和为用户组授权。

OSS授权样例

- 示例1：授权RAM用户完全管理某个Bucket的权限。

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

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

- 示例2：授权RAM用户列出并读取一个Bucket中的资源。
  - 授权RAM用户通过OSS SDK或OSS命令行工具列出并读取一个Bucket中的资源。Bucket名称为：`myphotos`。

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

  - 授权RAM用户能够通过OSS控制台进行操作。

> **说明：**
> 用户登录OSS控制台时，为了操作体验的优化，OSS控制台会额外调用`ListBuckets`操作，以及`GetBucketAcl`和`GetObjectAcl`，以确定bucket属性是公开还是私有。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
                      "oss:GetBucketStat",
                      "oss:GetBucketInfo",
                      "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/*"
        }
    ]
}
```

- **示例3：授权RAM用户通过特定的IP地址访问OSS。**
  - **在`Allow`授权中增加IP限制：允许通过`192.168.0.0/16`, `172.12.0.0/16`两个IP段读取`myphotos`中的信息。**

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

  - **在`Deny`授权中增加IP限制：如果源IP不在`192.168.0.0/16`中，则禁止对OSS执行任何操作。**

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
```

```
                        "oss:GetBucketStat",
                        "oss:GetBucketInfo",
                        "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"]
                }
            }
        }
    ]
}
```

说明:

因为Policy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服务会提示没有权限。

- **示例4：OSS目录级别的授权。**

  假设用于存放照片的`Bucket: myphotos`。这个Bucket下有一些目录，代表照片的拍摄地，每个拍摄地目录下又有年份子目录。

```
myphotos[Bucket]
   ├── beijing
   │    ├── 2014
   │    └── 2015
   ├── hangzhou
   │    ├── 2013
   │    ├── 2014
   │    └── 2015 //授予此目录只读权限
   └── qingdao
        ├── 2014
```

```
    └── 2015
```

若要授权RAM用户访问myphotos/hangzhou/2015/目录的只读权限。目录级别的授权属于授权的高级功能，根据使用场景不同，授权策略的复杂程度也不同，以下几种场景可供参考。

- 场景1：授予RAM用户读取文件内容的权限，不需要列出文件的权限。

  RAM用户知道文件的完整路径，可以使用完整的文件路径直接去读取文件内容，通常会将这样的权限授予应用程序。

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

- 场景2：授权RAM用户使用OSS命令行工具访问目录myphotos/hangzhou/2015/并列出目录中文件的权限。

  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，通常会将这样的权限授予软件开发者。

  此场景需要新增ListObjects的权限。

```
{
    "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/*"
                }
```

```
            }
        }
    ]
}
```

- **场景3：授予RAM用户使用OSS控制台访问目录。**

  RAM用户使用可视化的OSS客户端访问目录`myphotos/hangzhou/2015/`，可视化的客户端类似Windows文件管理器，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。

  此场景需要新增以下权限：

  ■ 列出所有`Bucket`的权限

  ■ 列出`myphotos`下目录的权限。

  ■ 列出`myphotos/hangzhou`下的目录的权限。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                      "oss:ListBuckets",
                      "oss:GetBucketStat",
                      "oss:GetBucketInfo",
                      "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/*"
                    ]
```

```
                    }
                }
            }
        ]
}
```

15 使用RAM对RDS进行权限管理

本文介绍了通过RAM的权限管理功能，创建相应的权限策略，从而对云数据库（RDS）进行权限管理，以满足RAM用户操作RDS的多种需求。

前提条件

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。详情请参见账号注册。

基本信息

使用RAM对RDS进行权限管理前，需先了解几个常用的权限策略。

权限策略	描述
AliyunRDSFullAccess	为RAM用户授予RDS的完全管理权限。
AliyunRDSReadOnlyAccess	为RAM用户授予RDS的只读访问权限。

说明:

查看RDS的权限定义，请参考RDS产品文档中的RAM资源授权。

将自定义策略授权给RAM用户

1. 根据下述 RDS授权样例创建相应的自定义策略。

   详情请参考：创建自定义策略。
2. 找到创建好的权限策略，单击其权限策略名称。
3. 单击引用记录 > 新增授权。
4. 被授权主体处输入需要授权的用户名称或ID。
5. 单击确定。

说明:

您也可以直接对用户或用户组授予创建好的权限策略，详情请参见为RAM用户授权和为用户组授权。

RDS授权样例

- 示例1：授权RAM用户管理2台指定的RDS实例。

  假设您的账号购买了多个实例，而作为RAM管理员，您希望仅授权其中的2个实例给某个RAM用户。实例ID分别为：i-001，i-002。

```
{
```

```
  "Statement": [
    {
      "Action": "rds:*",
      "Effect": "Allow",
      "Resource": [
                  "acs:rds:*:*:dbinstance/i-001",
                  "acs:rds:*:*:dbinstance/i-002"
                  ]
    },
    {
      "Action": "rds:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

说明:

- **授予该权限策略的RAM用户可以查看所有的实例及资源，但只能操作其中2个实例。**
- **`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，使用API、CLI或SDK直接对两个实例进行操作是可以的。**

- **示例2：授权RAM用户访问DMS管理数据库内容。**
  - **授权RAM用户登录指定RDS：**

```
{
  "Statement": [
    {
      "Action": "dms:LoginDatabase",
      "Effect": "Allow",
      "Resource": "acs:rds:*:*:dbinstance/rds783a0639ks5k7****"
    }
  ],
  "Version": "1"
}
```

说明:

请将`rds783a0639ks5k7****`替换为您要授权的RDS实例ID。

  - **授权RAM用户登录所有RDS：**

```
{
  "Statement": [
    {
      "Action": "dms:LoginDatabase",
      "Effect": "Allow",
      "Resource": "acs:rds:*:*:*"
    }
  ],
  "Version": "1"
}
```

16 使用RAM对SLB进行权限管理

本文介绍了通过RAM的权限管理功能，创建相应的权限策略，从而对负载均衡（SLB）进行权限管理，以满足RAM用户操作SLB的多种需求。

前提条件

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。详情请参见账号注册。

基本信息

使用RAM对SLB进行权限管理前，需先了解几个常用的权限策略。

权限策略	描述
AliyunSLBFullAccess	为RAM用户授予SLB的完全管理权限。
AliyunSLBReadOnlyAccess	为RAM用户授予SLB的只读访问权限。

说明:

查看SLB的权限定义，请参见SLB产品文档中的RAM鉴权。

将自定义策略授权给RAM用户

1. 根据下述SLB 授权样例创建相应的自定义策略。

   详情请参见创建自定义策略。
2. 找到创建好的权限策略，单击其权限策略名称。
3. 单击引用记录 > 新增授权。
4. 被授权主体处输入需要授权的用户名称或ID。
5. 单击确定。

说明:

您也可以直接对用户或用户组授予创建好的权限策略，详情请参见为RAM用户授权和为用户组授权。

SLB 授权样例

- 示例1：授权 RAM 用户管理2台指定的SLB实例。

  假设您的账号购买了多个实例，而作为RAM管理员，您希望仅授权其中的2个实例给某个RAM用户。实例ID分别为：i-001，i-002。

```
{
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
                  "acs:slb:*:*:loadbalancer/i-001",
                  "acs:slb:*:*:loadbalancer/i-002"
                  ]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

说明:

- 授予该权限策略的RAM用户可以查看所有的实例及资源，但只能操作其中2个实例。
- `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，使用API、CLI或 SDK直接对两个实例进行操作是可以的。

· 示例2：将ECS实例加入SLB-001负载均衡器。实例ID：i-001。

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

说明:

即使RAM用户按照示例1被授予管理某个SLB的权限，该用户在SLB实例中添加/移除ECS服务器或设置权重时仍然提示没有权限，原因是在负载均衡器中关于ECS服务器操作时没有授予以下两个权限：

- SLB的资源权限。
- ECS服务器的权限。

- **示例3：允许在特定SLB实例上执行任意ECS相关的操作。**

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
                  "acs:slb:*:*:loadbalancer/i-001",
                  "acs:slb:*:*:loadbalancer/i-002"
                  ]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": "acs:ecs:*:*:*"
    }
  ],
  "Version": "1"
}
```

说明:

上述授权策略，允许RAM用户在i-001和i-002这两个负载均衡器实例上执行所有管理操作，并允许在这两个实例上执行与ECS资源相关的所有操作，例如向实例中添加ECS服务器，以及设置ECS服务器的权重等。

17 使用RAM对CDN进行权限管理

本文介绍了通过RAM的权限管理功能，创建相应的权限策略，从而对内容分发（CDN）进行权限管理，以满足RAM用户操作CDN的多种需求。

前提条件

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。详情请参见账号注册。

基本信息

使用RAM对CDN进行权限管理前，需先了解几个常用的权限策略。

权限策略	描述
AliyunCDNFullAccess	为RAM用户授予CDN的完全管理权限。
AliyunCDNReadOnlyAccess	为RAM用户授予CDN的只读访问权限。

说明:

查看CDN的权限定义，请参见CDN产品文档中的CDN API鉴权规则。

将自定义策略授权给RAM用户

授权RAM用户执行CDN只读、刷新缓存及预热，详情请参见创建自定义策略。

1. 创建自定义策略。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "cdn:Describe*",
        "cdn:PushObjectCache",
        "cdn:RefreshObjectCaches"
      ],
      "Resource": "acs:cdn:*:*:*",
      "Effect": "Allow"
    }
  ]
}
```

2. 找到创建好的权限策略，单击其权限策略名称。
3. 单击引用记录 > 新增授权。
4. 被授权主体处输入需要授权的用户名称或ID。

5. 单击确定。

> **说明:**
> 您也可以直接对用户或用户组授予创建好的权限策略，详情请参见为RAM用户授权和为用户组授权。

18 通过ActionTrail查看RAM的操作记录

ActionTrail可以记录主账号或RAM用户进行的操作，通过ActionTrail可以查看所有用户对资源实例进行操作的记录。

前提条件

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。详情请参见账号注册。

通过ActionTrail控制台查看事件

1. 登录ActionTrail控制台。
2. 在历史事件查询页签下，使用过滤器进行搜索。
3. 输入相关的用户名，选择事件类型和时间后，单击搜索。

> 说明:
> 您也可以通过事件名称、资源类型、资源名称以及AccessKeyId等进行搜索。

4. 单击需要查看的事件，单击查看事件。

ActionTrail记录的操作

ActionTrail可以记录RAM的如下操作信息：

- 主账号或RAM用户的登录信息，详情请参见ConsoleSignin。
- RAM控制台的操作，例如：

```
{
    "apiVersion":"2015-05-01",
    "eventId":"2cc52dee-d8d2-40c2-8de0-3a2cf1df****",
    "eventName":"DeleteGroup",
    "eventSource":"ram.aliyuncs.com",
    "eventTime":"2015-11-03T13:41:49Z",
    "eventType":"ApiCall",
    "eventVersion":"1",
    "requestId":"9AE24F49-C52C-4F0F-BCF9-9A4B8C22B147",
    "requestParameters":{
        "GroupName":"grp1",
    },
    "serviceName":"Ram",
    "sourceIpAddress":"42.120.XX.XX",
    "userAgent":"AliyunConsole",
    "userIdentity":{
        "type":"ram-user",
        "principalId":"27418064654829****",
        "accountId":"123456789012****",
        "userName":"Alice",
        "sessionContext":{
            "sessionAttributes":{
                "creationDate":"2015-11-03T13:41:48Z",
                "mfaAuthenticated":"true"
            }
```

```
        }
    }
}
```

- **RAM/STS的所有创建、变更、删除类API调用信息，例如：**

```
{
    "apiVersion": "2015-05-01",
    "eventId": "234ef3c7-8938-4bd7-bb80-11754b7b****",
    "eventName": "CreateGroup",
    "eventSource": "ram.aliyuncs.com",
    "eventTime": "2016-01-04T08:58:50Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "4****",
    "requestId": "1485748C-DB62-4693-AB7E-4BA3F3A970E1",
    "requestParameters": {
        "Comments": "this is a test group",
        "GroupName": "grp1"
    },
    "serviceName": "Ram",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "principalId": "27418064654829****",
        "accountId": "4****",
        "accessKeyId": "f6Iz********EI4d",
        "userName": "Alice"
    }
}
```

更多信息

关于操作记录的详细信息，请参见操作事件(Event)结构定义。

19 使用RAM授权ActionTrail操作资源

本文介绍了通过RAM的权限管理能力，通过创建用户并授予相应的权限，以满足RAM用户操作ActionTrail 的资源。

前提条件

- 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。详情请参见账号注册。
- 使用RAM对ActionTrail进行授权前，请先了解ActionTrail相关API接口及其描述方式，详情请参考：RAM鉴权。
- 使用RAM对ActionTrail进行授权前，请先了解权限策略语法和结构。

使用RAM授权ActionTrail操作资源

1. 创建RAM用户。
2. 为RAM用户授权。
   - 若要为 RAM 用户添加一条或多条系统策略，可根据下述ActionTrail相关系统策略授予RAM用户相应权限。
   - 如果需要更细粒度的授权，可根据下述授权样例创建相应的自定义策略并授予相应 RAM 用户。 详情请参见创建自定义策略。

ActionTrail相关系统策略

ActionTrail常见的系统策略如下所示：

系统策略名称	说明
AliyunActionTrailFullAccess	ActionTrail完全管理权限。
AliyunActionTrailReadOnlyAccess	ActionTrail只读权限。

授权样例

- 示例1：授予RAM用户只读权限。

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*"
    }]
}
```

- **示例2：仅允许RAM用户从指定的IP地址发起的只读操作。**

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*",
        "Condition":{
            "IpAddress": {
                "acs:SourceIp": "42.120.XX.X/24"
            }
        }
    }]
}
```