ALIBABA CLOUD

Alibaba Cloud

访问控制

教程

文档版本：20200915

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.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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

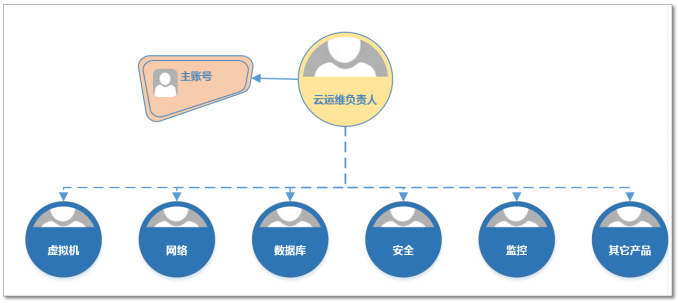
背景信息

某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。



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. 使用阿里云账号登录RAM控制台。
2. 创建RAM用户。
3. 在**用户登录名称/显示名称**列表下，找到目标RAM用户。
4. 单击**添加权限**，被授权主体会自动填入。
5. 从左侧**权限策略名称**列表下，单击 `AliyunRDSFullAccess` 和 `AliyunDTSFullAccess` 。
6. 单击**确定**。
7. 单击**完成**。

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

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
	AliyunECSFullAccess	管理云服务器服务（ECS）的权限

运维负责人	权限策略名称	权限策略说明
虚拟机运维负责人	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
	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

2.通过RAM限制用户的访问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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 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**创建权限策略**。
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**确定**。

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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 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**创建权限策略**。
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. 单击确定。

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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 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**创建权限策略**。
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. 单击确定。

5.通过RAM限制只有启用了MFA的RAM用户才能访问云资源

本文介绍如何通过RAM限制只有启用了多因素认证（MFA）的RAM用户才能访问云资源，比如ECS。

前提条件

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 进行操作前，请确保您已经创建了RAM用户。详情请参见创建RAM用户。
- 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。

步骤1：为RAM用户设置MFA

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**认证管理**页签下，单击**启用虚拟MFA设备**。
5. 在移动端，下载并登录Google Authenticator应用。
6. 在移动端，扫码添加多因素认证设备。
7. 在RAM控制台，输入移动端显示的两组连续的动态验证码，单击**确定启用**，完成绑定。

> **说明** 更多关于MFA的操作，请参见为RAM用户设置多因素认证。

步骤2：创建自定义权限策略

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**创建权限策略**。
3. 输入**策略名称**和**备注**。
4. **配置模式**选择**脚本配置**。
5. 输入策略内容。

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

上述策略表示：只有启用了MFA的RAM用户才能在控制台访问ECS资源。您可以通过设置 `Condition` 下 `acs:MFAPresent` 的值为 `true` 来实现。

您可以根据实际情况修改策略内容，限制访问其他云资源。

6. 单击**确定**。

步骤3：为RAM用户授权

1. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
2. 在**用户登录名称/显示名称**列表下，找到目标RAM用户。
3. 单击**添加权限**，被授权主体会自动填入。
4. 在左侧**权限策略名称**列表下，单击步骤2创建的自定义权限策略。
5. 单击**确定**。
6. 单击**完成**。

6.移动应用使用临时安全令牌访问阿里云

本文介绍移动应用如何使用RAM角色的临时安全令牌（STS token）访问阿里云资源。

前提条件

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

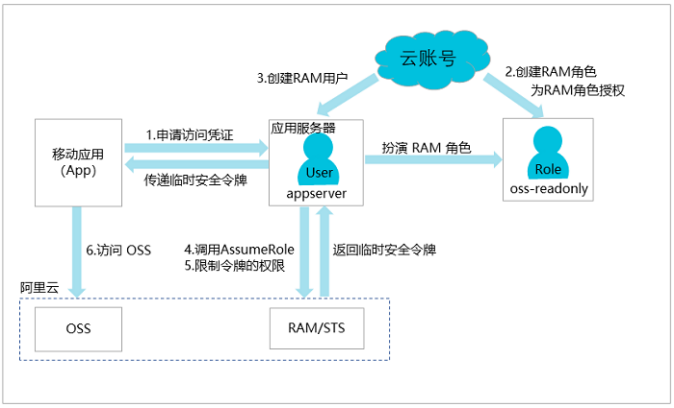
企业A开发了一款移动应用（App），并购买了对象存储（OSS）服务。App需要直连OSS上传或下载数据，但是App运行在用户自己的移动设备上，这些设备不受企业A的控制。

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. 使用阿里云账号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. 使用阿里云账号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

假设阿里云账号A的账号ID为 `123456789012****` 。

1. 使用阿里云账号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，即只允许阿里云账号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为 `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阿里云账号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. 使用阿里云账号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，而非阿里云账号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": "93ci2umK1QKNEja6WGqi1Ba7Q2Fv9PwxZqtVF2Vy****",
        "SecurityToken": "********",
        "Expiration": "2016-01-13T15:02:37Z",
        "AccessKeyId": "STS.F13GjskXTjk38dBY6YxJt****"
    },
    "RequestId": "E1779AAB-E7AF-47D6-A9A4-53128708B6CE"
}
```

   > 说明 上述示例未指定 `Policy` 参数，因此返回的临时安全令牌将拥有RAM角色 `oss-readonly` 的所有权限。您也可以额外限制临时安全令牌的权限，详情请参见限制临时安全令牌的权限。

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

在线上系统，请务必通过使用 `Policy` 参数来根据用户或设备限制不同临时安全令牌的权限，避免越权风险。以下是此参数的使用示例。

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 28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7x**** --sts_token CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU78FkszxhnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEaegoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDwoNb3NzOkdldE9iamVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoqOio6c2FtcGxlLWJ1Y2tldC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4NTRyCWVjcy1hZG1pbnjgxt7Cj/bo****
访问 OSS
$ aliyuncli oss Get oss://sample-bucket/2015/01/01/grass.jpg grass.jpg
```

相关文档

- 快速搭建移动应用直传服务
- 快速搭建移动应用上传回调服务

- STS临时授权访问OSS

7.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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

企业A购买了ECS实例，并计划在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：

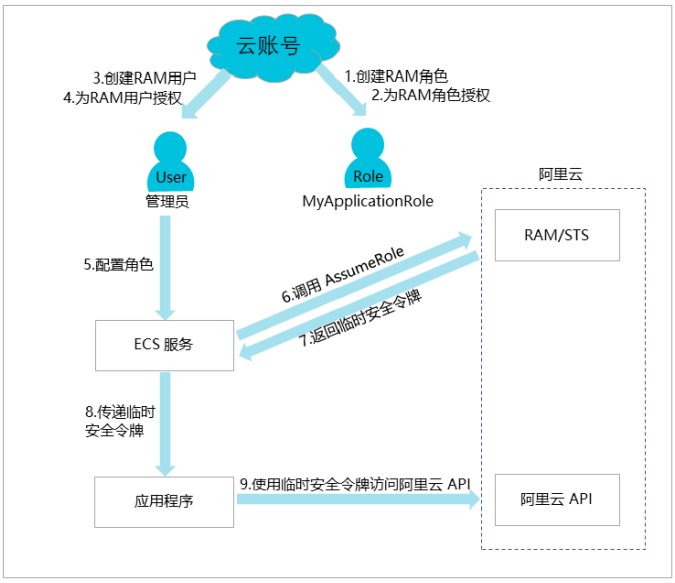
- 将访问密钥直接嵌入在代码里。
- 将访问密钥保存在应用程序的配置文件中。

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，即允许云服务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。请参见使用实例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.J8XXXXXXXXXX4",
     "AccessKeySecret" : "9PjfXXXXXXXXXBf2XAW",
     "Expiration" : "2017-06-09T09:17:19Z",
     "SecurityToken" : "CAIXXXXXXXXXXXwmBkleCTkyI+",
     "LastUpdated" : "2017-06-09T03:17:18Z",
     "Code" : "Success"
     }
     ```

   - 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。

> 说明 除ECS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。

8.跨阿里云账号的资源授权

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角色进行跨阿里云账号授权来管理资源的授权及访问。

前提条件

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用阿里云账号设置账号别名（企业别名），详情请参见管理默认域名 。

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下分别有一个阿里云账号A和阿里云账号B。

- 企业A的阿里云账号ID为 `123456789012****` ，账号别名（企业别名）为 `company-a` 。
- 企业B的阿里云账号ID为 `134567890123****` ，账号别名（企业别名）为 `company-b` 。

1. 阿里云账号A创建一个RAM角色，并为RAM角色授予合适的权限，允许阿里云账号B使用该角色。

   操作流程请参见跨阿里云账号授权。

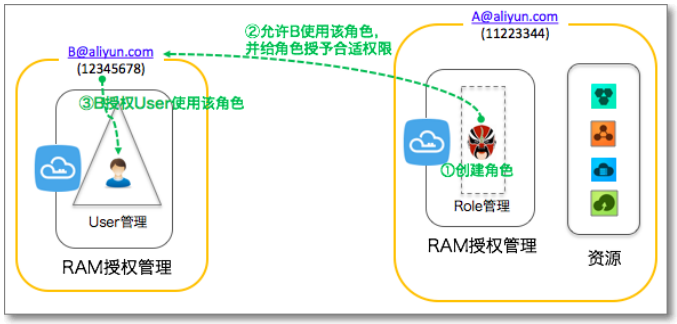
2. 如果阿里云账号B下的某个员工（RAM用户）需要使用该RAM角色，那么阿里云账号B可以自主进行授权控制。阿里云账号B下的RAM用户将扮演RAM角色来操作阿里云账号A的资源。

   操作流程请参见跨阿里云账号访问资源。

3. 如果企业A与企业B的合作终止，企业A只需要撤销阿里云账号B对RAM角色的使用。此时阿里云账号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阿里云账号授权 。

跨阿里云账号授权



1. 阿里云账号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，即允许阿里云账号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为 `acs:ram::123456789012****:role/ecs-admin` 。
   - RAM角色的信任策略如下：

     > 说明 以下策略表示允许阿里云账号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. 阿里云账号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. 阿里云账号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. 阿里云账号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。

跨阿里云账号访问资源

对阿里云账号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阿里云账号A下的ECS资源。

1. 阿里云账号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。

撤销跨阿里云账号授权

阿里云账号A可以撤销阿里云账号B对RAM角色 ecs-admin 的使用。

1. 阿里云账号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** 阿里云账号A也可以通过删除RAM角色ecs-admin来撤销阿里云账号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.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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

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，该阿里云账号下有超过100个ECS实例。

公司A有如下要求：

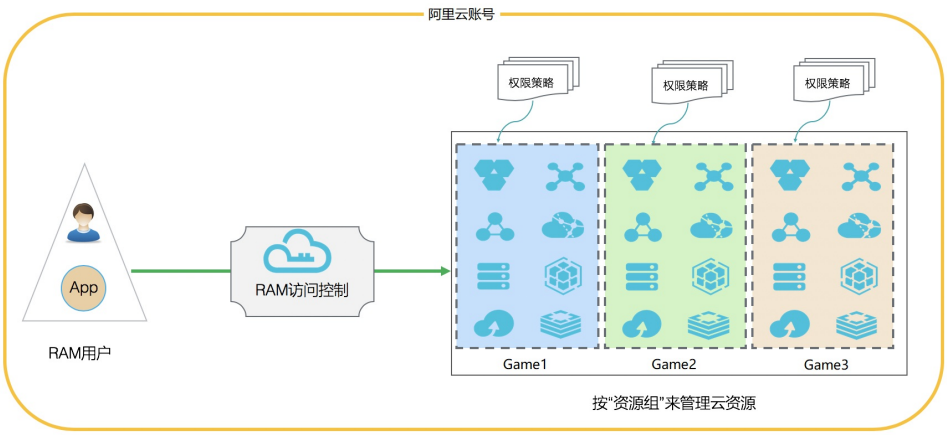
- 项目独立管理：每个管理员各自能够独立管理项目人员及其访问权限。
- 按项目分账：财务部门希望能够根据项目进行出账，以解决财务成本分摊的问题。
- 共享底层网络：客户希望云资源的底层网络默认共享。

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个阿里云账号（对应3个项目），每个阿里云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：每个阿里云账号有默认账单，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：阿里云账号之间是有安全边界的，不同阿里云账号之间的资源是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个阿里云账号，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，同一阿里云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个阿里云账号，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`。

   详情请参见创建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**，然后单击**创建资源组**。
4. 输入**资源组标识**和**资源组名称**后，单击**确定**。

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

5. 找到目标资源组，单击**权限管理**。
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**。
10. 单击**完成**。

    > 说明 如何将Bob或Charlie设置为资源组管理员，请参考上述步骤。

执行结果

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。

10.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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

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

规划2个RAM用户组，名称命名为：developer、operator。

规划2个RAM自定义策略，名称命名为：policyForDevTeam、policyForOpsTeam。

规划2个标签，如下：

- 其中5个实例绑定一对标签，标签键是team，标签值是dev。
- 另外5个实例绑定另一对标签，标签键是team，标签值是ops。

操作步骤

1. 使用阿里云账号登录ECS控制台，为ECS实例创建并绑定标签。
   i. 登录ECS控制台。
   ii. 在顶部菜单栏左上角处，选择地域。
   iii. 在左侧导航栏，选择**实例与镜像 > 实例**，找到目标ECS实例。
   iv. 将鼠标悬停在**标签**列下的 图标上，然后单击气泡框中的**编辑标签**。
   v. 单击**新建标签**。
   vi. 输入标签键和标签值，然后单击**确定**。

   按照上述步骤依次为5个ECS实例绑定标签 `team:dev` ，另外5个ECS实例绑定标签 `team:ops` 。
2. 使用阿里云账号登录RAM控制台，创建2个用户组：developer、operator。

   详情请参见创建用户组。
3. 使用阿里云账号登录RAM控制台，创建不同的RAM用户，分别添加到2个用户组下。

   详情请参见创建RAM用户、添加用户组成员。
4. 使用阿里云账号登录RAM控制台，创建2个自定义策略：policyForDevTeam和policyForOpsTeam，然后将自定义策略policyForDevTeam授权给用户组developer，将自定义策略policyForOpsTeam授权给用户组operator。

   详情请参见创建自定义策略、为用户组授权。

   > **说明** 授权后RAM用户将继承对应用户组的相关权限。

   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"
}
```

policyForOpsTeam策略内容如下：

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

权限策略说明：

- 带有 `Condition` 的 `"Action": "ecs:*"` 部分用于过滤标签为 `team:dev` 或 `team:ops` 的ECS实例。
- `"Action": "ecs:DescribeTag*"` 用于展示所有ECS标签。当RAM用户在操作ECS控制台时，系统显示所有标签供RAM用户选择，只有当RAM用户选择了对应标签后，系统才能根据选中的标签过滤相应资源。

结果验证

1. 使用RAM用户登录ECS控制台。
2. 在顶部菜单栏左上角处，选择地域。
3. 在左侧导航栏，选择**实例与镜像 > 实例**。
4. 在搜索栏旁边，单击**标签**。
5. 鼠标悬停在**标签键**上，选择对应的**标签值**，系统可以过滤出符合要求的ECS实例。 例如：在用户组developer中的RAM用户，可以通过标签 `team:dev` 过滤，查看有权限访问的ECS实例。

更多信息

利用标签对块存储、快照、镜像、安全组、弹性网卡、专有宿主机、SSH密钥对等ECS资源进行分组授权的方法与上述对实例分组授权的方法相同。

11.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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

假设您的账号购买了10个RDS实例，其中5个想要授权给developer团队，另外5个授权给operator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

利用标签对RDS分组授权的操作步骤与对ECS实例分组授权的操作步骤部分相同，详情请参见利用标签对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。

常见问题

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，请检查如下事项：

- 标签已被绑定到正确的实例上。
- 权限策略与实例上的标签键、标签值完全相同。

> 说明 RDS的标签键值不可以使用大写字母，若输入大写字母在保存时会被自动转换成小写字母。

- 登录到RDS控制台的RAM用户已被授予了期望的权限策略。
- 控制台展示的当前地域是期望地域。
- 已选中相应标签值，此时系统才可以过滤出相应资源。

> 说明 RAM用户登录RDS控制台后，控制台会提示“您没有指定资源的操作权限，请先对资源进行授权操作。”，请关掉该错误提示。出现该错误提示的原因是控制台默认展示所有资源，而当前RAM用户并没有查看所有资源的权限，所以会报错。

12.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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对ECS进行权限管理前，请先了解以下常用的权限策略：
  - 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。
- 使用RAM对ECS进行权限管理前，请先了解ECS的权限定义。详情请参见鉴权规则。

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。

   关于如何创建自定义策略，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. 在**引用记录**页签下，单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM用户名称后，单击需要授权的RAM用户。
5. 单击**确定**。

> **说明** 更多为RAM用户或用户组授权的方式，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，但使用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用户仅可以查看青岛的ECS实例，但不允许查看磁盘及快照信息。**

```
{
 "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Region+资源类型的级别。如果您想授权RAM用户查看其他地区的ECS实例，可以将 `Resource` 中的 `cn-qingdao` 替换为其他区域ID。关于区域ID，详情请参见。

- 示例3：授权RAM用户创建快照。

  如果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为 `inst-01` ，磁盘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"
}
```

13.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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对OSS进行权限管理前，请先了解几个常用的权限策略：
  - 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。
- 使用RAM对OSS进行权限管理前，请先了解OSS的权限定义。详情请参见访问控制概述。

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。

   关于如何创建自定义策略，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. 在**引用记录**页签下，单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM用户名称后，单击需要授权的RAM用户。
5. 单击**确定**。

> 说明 更多为RAM用户或用户组授权的方式，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用户完全管理一个名为 `myphotos` 的存储空间。

```
{
  "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存储空间中的资源。

- 授权RAM用户通过OSS SDK或OSS命令行工具列出并读取一个存储空间中的资源。存储空间名称为 `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 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/*"
    }
  ]
}
```

- 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: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"]
        }
      }
    }
  ]
}
```

- 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: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"]
          }
        }
      }
    ]
}
```

> **说明** 因为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。

- 示例4：OSS目录级别的授权。

  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: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": [
```

```
                "oss:Prefix":[
                  "",
                  "hangzhou/",
                  "hangzhou/2015/*"
                ]
              }
            }
          }
        ]
}
```

14.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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对RDS进行权限管理前，请先了解以下常用的权限策略：
  - 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。
- 使用RAM对RDS进行权限管理前，请先了解RDS的权限定义。详情请参见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。
2. 找到创建好的权限策略，单击其权限策略名称。
3. 在**引用记录**页签下，单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM用户名称后，单击需要授权的RAM用户。
5. 单击**确定**。

> **说明** 更多为RAM用户或用户组授权的方式，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"
}
```

15.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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

- 使用RAM对SLB进行权限管理前，请先了解几个常用的权限策略：
  - 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。
- 使用RAM对SLB进行权限管理前，请先了解SLB的权限定义。详情请参见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。

   关于如何创建自定义策略，请参见创建自定义策略。
2. 找到创建好的权限策略，单击权限策略名称。
3. 在**引用记录**页签下，单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM用户名称后，单击需要授权的RAM用户。
5. 单击**确定**。
6. 单击**完成**。

> 说明 更多为RAM用户或用户组授权的方式，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用户管理两台指定的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两个实例给某个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，但只能管理其中两个实例。
> - `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，但是使用API、CLI或SDK直接对两个实例进行管理是可以的。

- 示例2：将ECS实例加入负载均衡器 `slb-001` 。实例ID为 `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实例的权限，但该用户在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没有授予关于ECS服务器的两个权限：
>
> - 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": "ecs:DescribeInstances",
  "Resource": "*"
 },
 {
  "Effect": "Allow",
  "Action": "slb:*",
  "Resource": [
   "acs:ecs:*:*:instance/i-instance001",
   "acs:ecs:*:*:instance/i-instance002"
  ]
 }
 ],
 "Version": "1"
}
```

说明 上述权限策略表示：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：将ECS实例 i-instance001 和 i-instance002 添加为这两个负载均衡实例的后端服务器或设置ECS服务器的权重等。使用此权限的过程中，RAM用户在选择ECS实例时可以看到所有实例的列表。

16.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

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对CDN进行权限管理前，请先了解以下常用的权限策略：
  - 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。
- 使用RAM对CDN进行权限管理前，请先了解CDN的权限定义。详情请参见RAM鉴权。

操作步骤

1. 创建自定义策略。

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

> 说明 上述自定义策略表示授权RAM用户执行CDN只读、刷新缓存及预热的操作。您可以根据需要修改自定义策略内容，从而授权RAM用户不同的权限。关于 Action 或 Resource 的使用规则，请参见权限策略基本元素。

2. 找到创建好的权限策略，单击其权限策略名称。
3. 在**引用记录**页签下，单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM用户名称后，单击需要授权的RAM用户。
5. 单击**确定**。

> 说明 更多为RAM用户或用户组授权的方式，请参见为RAM用户授权和为用户组授权。

17.使用RAM对VPC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，从而对专有网络（VPC）进行权限管理，以满足RAM用户操作VPC的多种需求。

前提条件

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对VPC进行权限管理前，请先了解几个常用的权限策略：
  - AliyunVPCFullAccess：为RAM用户授予VPC的完全管理权限。
  - AliyunVPCReadOnlyAccess：为RAM用户授予VPC的只读访问权限。
- 使用RAM对VPC进行权限管理前，请先了解VPC的权限定义。详情请参见RAM鉴权。

将自定义权限策略授权给RAM用户

1. 使用阿里云账号登录RAM控制台。
2. 创建自定义权限策略。 详细信息，请参见创建自定义策略和VPC授权样例。
3. 在**权限策略管理**页面，找到目标权限策略，单击权限策略名称。
4. 单击**引用记录**页签，然后单击**新增授权**。
5. 在**被授权主体**区域，输入需要授权的RAM用户的名称或ID。
6. 单击**确定**。
7. 单击**完成**。

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

VPC授权样例

- 示例1：对VPC的管理授权

  假设您的主账号ID为1234567，授权子账号管理该账号下的所有VPC，使某个RAM用户具有操作所有VPC的权限。

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*"
      ],
      "Resource": [
        "acs:vpc:*:1234567:*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- 示例2：对VPC中VSwitch的管理授权

  假设您只想授权青岛地域下的VSwitch的管理权限，使某个RAM用户可以对青岛地域下的VSwitch进行创建、删除、绑定子网路由、解绑子网路由的操作，对于其它地域的VSwitch只有查看权限。

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

- 示例3：只允许操作特定地域下的路由表以及路由表中的路由条目

  假设您的主账号ID为11111111，在多个地域创建了VPC，该权限只授予某个RAM用户对杭州地域VPC的操作权限，且操作权限仅限于：允许新增、删除路由条目，允许创建子网路由并绑定VSwtich，对于其它地域的云产品只有查看权限。

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

```
        "Condition": {}
      },
      {
        "Effect": "Allow",
        "Action": [
          "slb:*Describe*"
        ],
        "Resource": [
          "*"
        ],
        "Condition": {}
      },
      {
        "Effect": "Allow",
        "Action": [
          "rds:*Describe*"
        ],
        "Resource": [
          "*"
        ],
        "Condition": {}
      },
      {
        "Effect": "Allow",
        "Action": [
          "vpc:*Describe*",
          "vpc:*RouteEntry*",
          "vpc:*RouteTable*"
        ],
        "Resource": [
"acs:vpc:cn-hangzhou:11111111:*/*"
        ],
        "Condition": {}
      }
    ]
}
```

- 示例4：只允许修改特定路由表中的路由条目

  假设您只希望RAM用户新增、删除特定路由表中的路由条目。

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*RouteEntry*"
      ],
      "Resource": [
        "acs:vpc:cn-qingdao:*:routetable/vtb-m5e64ujkb7xn5zlq0xxxx"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

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

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

通过ActionTrail控制台查看事件

1. 登录操作审计控制台。
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. 找到目标事件，单击+。
5. 单击**查看事件**。

ActionTrail记录的操作

ActionTrail可以记录RAM的以下操作信息，关于操作记录的详细信息，请参见操作事件结构定义。

- 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"
  }
}
```

19.使用RAM对操作审计进行权限管理

通过RAM的权限管理功能，您可以创建自定义策略并授予RAM用户，RAM用户便可以登录操作审计服务进行相应的操作。

前提条件

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对操作审计进行授权前，请先了解操作审计的权限定义。详情请参见RAM鉴权。

操作步骤

1. 创建RAM用户。
2. 创建自定义策略。

   您可以根据下述权限策略示例创建自定义策略。
3. 为RAM用户授权。

权限策略示例

- 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"
      }
    }
  }]
}
```