ALIBABA CLOUD

# 阿里云

## 访问控制

## 角色管理

文档版本：20201015

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<br>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<br>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<br>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<br>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`<br>*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角色概览

RAM角色（RAM role）与RAM用户一样，都是RAM身份类型的一种。RAM角色是一种虚拟用户，没有确定的身份认证密钥，需要被一个受信的实体用户扮演才能正常使用。

## RAM角色基本概念

***RAM角色（RAM role）***

RAM角色是一种虚拟用户，与实体用户（云账号、RAM用户和云服务）和教科书式角色（Textbook role）不同。

- 实体用户：拥有确定的登录密码或访问密钥。
- 教科书式角色：教科书式角色或传统意义上的角色是指一组权限集合，类似于RAM里的权限策略。如果一个用户被赋予了这种角色，也就意味着该用户被赋予了一组权限，可以访问被授权的资源。
- RAM角色：RAM角色有确定的身份，可以被赋予一组权限策略，但没有确定的登录密码或访问密钥。RAM角色需要被一个受信的实体用户扮演，扮演成功后实体用户将获得RAM角色的安全令牌，使用这个安全令牌就能以角色身份访问被授权的资源。

***角色ARN（Role ARN）***

ARN是角色的全局资源描述符，用来指定具体角色。ARN遵循阿里云ARN的命名规范。例如，某个云账号下的devops角色的ARN为：`acs:ram::123456789012****:role/samplerole`。创建角色后，单击角色名后，可在**基本信息**页查看其ARN。

***可信实体（Trusted entity）***

角色的可信实体是指可以扮演角色的实体用户身份。创建角色时必须指定可信实体，角色只能被受信的实体扮演。可信实体可以是受信的阿里云账号、受信的阿里云服务或身份提供商。

***权限策略（Policy）***

一个角色可以绑定一组权限策略。没有绑定权限策略的角色也可以存在，但不能访问资源。

***扮演角色（Assume role）***

扮演角色是实体用户获取角色身份的安全令牌的方法。一个实体用户调用STS API AssumeRole可以获得角色的安全令牌，使用安全令牌可以访问云服务API。

***切换身份（Switch role）***

切换身份是在控制台中实体用户从当前登录身份切换到角色身份的方法。一个实体用户登录到控制台之后，可以切换到被许可扮演的某一种角色身份，然后以角色身份操作云资源。当用户不需要使用角色身份时，可以从角色身份切换回原来的登录身份。

***角色令牌（Role token）***

角色令牌是角色身份的一种临时访问密钥。角色身份没有确定的访问密钥，当一个实体用户要使用角色时，必须通过扮演角色来获取对应的角色令牌，然后使用角色令牌来调用阿里云服务API。

## RAM角色的使用方法

1. RAM角色指定可信实体，即指定可以扮演角色的实体用户身份。
2. 可信实体通过控制台或调用API扮演角色并获取角色令牌。
   - 通过控制台扮演角色：切换身份是在控制台中实体用户从当前登录身份切换到RAM角色身份的方法，详情请参见使用RAM角色。
   - 通过调用API扮演角色：一个实体用户通过调用AssumeRole可以获得角色令牌，使用角色令牌可以

访问云服务API。

> 说明 扮演角色是实体用户获取RAM角色令牌的方法，角色令牌是角色身份的一种临时访问凭证，使用角色令牌可以访问阿里云资源。

3. 为RAM角色绑定权限策略，详情请参见为RAM角色授权。

> 说明 一个RAM角色可以绑定一组权限策略，没有绑定权限策略的角色也可以存在，但不能访问资源。

4. 受信实体通过扮演角色，使用角色令牌访问阿里云资源。

## RAM角色类型

根据RAM可信实体的不同，RAM支持以下三种类型的角色：

- **阿里云账号**：允许RAM用户所扮演的角色。扮演角色的RAM用户可以属于自己的云账号，也可以属于其他云账号。此类角色主要用来解决跨账号访问和临时授权问题。
- **阿里云服务**：允许云服务所扮演的角色。此类角色主要用于授权云服务代理您进行资源操作。
- **身份提供商**：允许受信身份提供商下的用户所扮演的角色。此类角色主要用于实现与阿里云的SSO。

## RAM角色的应用场景

- 移动应用使用临时安全令牌访问阿里云
- 跨阿里云账号的资源授权
- 对云上应用进行动态身份管理与授权

# 2.服务关联角色

受信云服务可以通过扮演RAM角色来访问其他的云资源。可信实体为阿里云服务的RAM角色分为普通服务角色和服务关联角色两种。本文主要介绍服务关联角色。

## 什么是服务关联角色

在某些场景下，一个云服务为了完成自身的某个功能，需要获取其他云服务的访问权限。例如：配置审计（Config）服务要读取您的云资源信息，以获取资源列表和变更历史，就需要获取ECS、RDS等产品的访问权限。阿里云提供了服务关联角色 SLR（Service Linked Role）来满足此类场景的需求。

服务关联角色是与某个云服务关联的角色。多数情况下，在您使用特定功能时，关联的云服务会自动创建或删除服务关联角色，不需要您主动创建或删除。通过服务关联角色可以更好的配置云服务正常操作所必须的权限，避免误操作带来的风险。

服务关联角色的权限策略由关联的云服务定义和使用，您不能修改或删除权限策略，也不能为服务关联角色添加或移除权限。

不支持服务关联角色的云服务，请使用普通服务角色获取其他云服务的访问权限。

## 创建服务关联角色

某些云服务将在您执行某些特定操作（例如：创建一个云资源或开启一个功能）时自动创建服务关联角色，您可以在RAM控制台的角色管理页面、API或CLI调用ListRoles的返回结果中查看自动创建的服务关联角色。

此外，您也可以主动创建服务关联角色，详情请参见创建服务关联角色。

> 说明
>
> - 服务关联角色会占用您的RAM角色配额。当RAM角色数量超限时，您仍然可以成功创建服务关联角色，但无法创建其他类型的角色。
> - 关于云服务自动创建服务关联角色的详情，请参见对应云服务的文档说明。

## 删除服务关联角色

某些云服务将在您执行某些特定操作（例如：删除所有资源或关闭一个功能）时自动删除已创建的服务关联角色，但您也可以从控制台主动删除。关于主动删除服务关联角色，详情请参见删除RAM角色。

当您尝试删除一个服务关联角色时，RAM会先检查这个角色是否仍被云资源使用：

- 如果为否，您可以直接删除该服务关联角色。
- 如果为是，您暂不能删除该服务关联角色，但可以查看哪些云资源在使用该角色。您需要找到对应的云资源并手动清理这些云资源，然后再删除该服务关联角色。

> 说明 关于删除服务关联角色的条件，请参见对应云服务的文档说明。

## 创建和删除服务关联角色所需的权限

您需要拥有指定的权限，才能创建或删除服务关联角色。自动创建服务关联角色的场景也需要具备对应权限。

> **说明** 创建服务关联角色的权限通常包含在其对应云服务的管理员权限策略（例如：AliyunESSFullAccess）中，因此只要具有该云服务的管理员权限，就可以为该云服务创建服务关联角色。

**权限策略示例：允许为资源管理（Resource Management）创建和删除服务关联角色。**

```
{
  "Action": [
    "ram:CreateServiceLinkedRole",
    "ram:DeleteServiceLinkedRole"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "resourcemanager.aliyuncs.com"
    }
  }
}
```

## 使用服务关联角色

服务关联角色仅限关联的对应云服务使用，其他身份（例如：普通RAM用户、其他RAM角色）都无法扮演该角色。

您可以在已创建的服务关联角色的**信任策略管理**页签中，通过 `Service` 字段查看可以使用该角色的云服务。

## 支持服务关联角色的云服务

| 云服务 | 服务名称 | 服务关联角色 | 相关文档 |
| --- | --- | --- | --- |
| 资源管理 | resourcemanager.aliyuncs.com | AliyunServiceRoleForResourceDirectory | 资源目录服务关联角色 |
| 配置审计 | config.aliyuncs.com | AliyunServiceRoleForConfig | 配置审计服务关联角色 |
| 云数据库 PolarDB | polardb.aliyuncs.com | AliyunServiceRoleForPolarDB | PolarDB服务关联角色 |
| 混合云备份服务 | dr.hbr.aliyuncs.com | AliyunServiceRoleForHbrDr | HBR ECS容灾的服务关联角色 |
| 运维编排 | bandwidthscheduler.oos.aliyuncs.com | AliyunServiceRoleForOOSBandwidthScheduler | OOS服务关联角色 |

| 云服务 | 服务名称 | 服务关联角色 | 相关文档 |
| --- | --- | --- | --- |
| | instancescheduler.oos.aliyuncs.com | AliyunServiceRoleForOOSInstanceScheduler | |
| 性能测试 | pts.aliyuncs.com | AliyunServiceRoleForPts | 借助RAM用户实现分权 |
| 混合云容灾服务 | hdr.aliyuncs.com | AliyunServiceRoleForHdr | HDR服务关联角色 |
| 弹性伸缩 | ess.aliyuncs.com | AliyunServiceRoleForAutoScaling | 授予弹性伸缩服务权限 |
| 时序数据库TSDB | hitsdb.aliyuncs.com | AliyunServiceRoleForTSDB | 时序数据库服务关联角色 |
| 云监控 | cloudmonitor.aliyuncs.com | AliyunServiceRolePolicyForCloudMonitor | 云监控服务关联角色 |
| 区块链服务BaaS | baas.aliyuncs.com | AliyunServiceRoleForBaaS | BaaS服务关联角色 |
| HTTPDNS | httpdns.aliyuncs.com | AliyunServiceRoleForHttpdns | HTTPDNS服务关联角色 |
| 移动推送 | cloudpush.aliyuncs.com | AliyunServiceRoleForCloudPush | 移动推送服务关联角色介绍 |
| 全局流量管理 | gtm.aliyuncs.com | AliyunServiceRoleForGTM | 全局流量管理服务关联角色 |
| 云解析DNS | alidns.aliyuncs.com | AliyunServiceRoleForDNS | 云解析DNS服务关联角色 |
| 敏感数据保护 | sddp.aliyuncs.com | AliyunServiceRoleForSDDP | 授权SDDP访问云资源 |
| CDN | cdn-ddos.cdn.aliyuncs.com | AliyunServiceRoleForCDNAccessingDDoS | 配置CDN联动DDoS高防 |

# 3.创建RAM角色

## 3.1. 创建可信实体为阿里云账号的RAM角色

阿里云支持三种类型的RAM角色。本文介绍如何创建可信实体为阿里云账号的RAM角色。

### 操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 单击**创建RAM角色**。
4. 选择可信实体类型为**阿里云账号**，单击**下一步**。
5. 输入**角色名称**和**备注**。
6. 选择云账号为当前云账号，单击**完成**。

> **说明** 若选择**其他云账号**，需要填写其他云账号的ID。

### 后续步骤

成功创建角色后，角色没有任何权限，单击**添加权限**可直接为该角色授权。详情请参见为RAM角色授权。

### 相关文档

- CreateRole

## 3.2. 创建可信实体为阿里云服务的RAM角色

阿里云支持三种类型的RAM角色。本文介绍如何创建可信实体为阿里云服务的RAM角色。

### 背景信息

可信实体为阿里云服务的RAM角色有两类：

- 普通服务角色：您需要自定义角色名称，选择受信服务，并自定义权限策略。
- 服务关联角色：您只需选择受信的云服务，云服务会自带预设的角色名称和权限策略。详情请参见服务关联角色。

### 创建普通服务角色

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 单击**创建RAM角色**。
4. 选择可信实体类型为**阿里云服务**，单击**下一步**。
5. 选择角色类型为**普通服务角色**。
6. 输入**角色名称**和**备注**。
7. 选择受信服务。

> **说明** 可以选择的受信服务请以控制台界面为准。

8. 单击**完成**。

成功创建角色后，角色没有任何权限，单击**为角色授权**可直接为该角色授权。详情请参见为RAM角色授权。

### 创建服务关联角色

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 单击**创建RAM角色**。
4. 选择可信实体类型为**阿里云服务**，单击**下一步**。
5. 选择角色类型为**服务关联角色**。
6. 选择云服务。 选择云服务后，可以查看云服务预定义的角色名称、备注和权限策略。单击**查看策略详情**查看权限策略的详情。

   > **说明** 可以选择的云服务请以控制台界面为准。

7. 单击**完成**。

### 相关文档

- CreateRole

## 3.3. 创建可信实体为身份提供商的RAM角色

阿里云支持三种类型的RAM角色。本文介绍如何创建可信实体为身份提供商的RAM角色。

### 操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 单击**创建RAM角色**。
4. 选择可信实体类型为**身份提供商**，单击**下一步**。
5. 输入**角色名称**和**备注**。
6. 选择身份提供商并查看限制条件后，单击**完成**。

   > **说明** 目前只支持一个条件关键字 `saml:recipient` ，必选且不能修改。

### 后续步骤

成功创建角色后，角色没有任何权限，单击**为角色授权**可直接为该角色授权。详情请参见为RAM角色授权。

### 相关文档

- CreateRole

# 4.查看RAM角色基本信息

本文为您介绍如何查看RAM角色基本信息，包括RAM角色名称、创建时间和ARN等信息。

## 操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，单击目标RAM角色名称。
4. 在**基本信息**区域，可以查看RAM角色基本信息。

> **说明** RAM角色信息只能查看，不能修改。

## 相关文档

- GetRole

# 5.为RAM角色授权

您可以为可信实体为阿里云账号、阿里云服务或身份提供商的RAM角色进行授权。本文为您介绍为RAM角色授权的几种方式。

> 说明 服务关联角色的权限策略由关联的云服务定义，您不能为服务关联角色授权。服务关联角色的详情，请参见服务关联角色。

## 方式一

您可以在RAM角色管理页面下为RAM角色授权。

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，找到目标RAM角色。
4. 单击**添加权限**，被授权主体会自动填入。
5. 在左侧**权限策略名称**列表下，单击需要授予RAM角色的权限策略。

   > 说明 在右侧区域框，选择某条策略并单击×，可撤销该策略。

6. 单击**确定**。
7. 单击**完成**。

## 方式二

您可以在RAM角色管理页面下为RAM角色进行精确授权。

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，找到目标RAM角色。
4. 单击**精确授权**。
5. 选择权限类型为**系统策略**或**自定义策略**。
6. 输入策略名称。
7. 单击**确定**。
8. 单击**关闭**。

## 方式三

您可以在授权页面下为RAM角色授权。

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**权限管理**菜单下，单击**授权**。
3. 单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM角色名称后，单击需要授权的RAM角色。
5. 在左侧**权限策略名称**列表下，单击需要授予RAM角色的权限策略。

> 说明 在右侧区域框，选择某条策略并单击×，可撤销该策略。

6. 单击确定。
7. 单击完成。

## 相关文档

- AttachPolicyToRole

# 6.为RAM角色移除权限

当RAM角色不再需要某些权限时，可以将这些权限移除。本文为您介绍移除RAM角色权限的几种方式。

> **说明** 服务关联角色的权限策略由关联的云服务定义，您不能移除服务关联角色的权限。服务关联角色的详情，请参见服务关联角色。

## 方式一

您可以在授权页面下为RAM角色移除权限。

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**权限管理**菜单下，单击**授权**。
3. 找到目标RAM角色，单击**移除授权**。
4. 单击**确定**。

## 方式二

您可以在RAM角色管理页面下的权限策略页签为RAM角色移除权限。

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，单击目标RAM角色名称。
4. 在**权限管理**页签下，找到目标权限策略，单击**移除权限**。
5. 单击**确定**。

## 相关文档

- DetachPolicyFromRole

# 7.修改RAM角色的信任策略

通过修改RAM角色的信任策略内容，可以修改RAM角色的可信实体。本文通过示例为您介绍如何修改RAM角色的可信实体为阿里云账号、阿里云服务或身份提供商。

## 背景信息

创建RAM角色时，您可以直接选择RAM角色的可信实体为阿里云账号、阿里云服务或身份提供商。一般情况下，创建RAM角色后，您不需要主动修改RAM角色的可信实体。如果某些特殊场景下确有需要，您可以通过本文所述的几种方式修改。修改后请务必进行测试并确保功能可以正常使用。

## 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，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，单击目标RAM角色名称。
4. 在**信任策略管理**页签下，单击**修改信任策略**。
5. 修改信任策略内容，然后单击**确定**。

## 修改RAM角色的可信实体为阿里云账号

若 `Principal` 中有 `RAM` 字段，表示该RAM角色的可信实体为**阿里云账号**，即可以被受信阿里云账号下授权的RAM用户、RAM角色扮演。

以下述信任策略为例：该RAM角色可以被阿里云账号（AccountID=123456789012****）下授权的任何RAM用户、RAM角色扮演。

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

若您将 `Principal` 中的内容更改如下，则表示该RAM角色可以被阿里云账号（AccountID=123456789012****）下的RAM用户 `testuser` 扮演。

```
      "Principal": {
        "RAM": [
          "acs:ram::123456789012****:user/testuser"
        ]
      }
```

> 说明 修改此策略时，请确保已创建好RAM用户 `testuser` 。

若您将 `Principal` 中的内容更改如下，则表示该RAM角色可以被阿里云账号（AccountID=123456789012****）下的RAM角色 `testrole` 扮演。

```
      "Principal": {
        "RAM": [
          "acs:ram::123456789012****:role/testrole"
        ]
      }
```

> 说明 修改此策略时，请确保已创建好RAM角色 `testrole` 。

## 修改RAM角色的可信实体为阿里云服务

若 `Principal` 中有 `Service` 字段，表示该RAM角色的可信实体为**阿里云服务**，即可以被受信云服务扮演。

以下述信任策略为例：该RAM角色可以被当前阿里云账号下的ECS服务扮演。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

## 修改RAM角色的可信实体为身份提供商

若 `Principal` 中有 `Federated` 字段，表示该RAM角色的可信实体为**身份提供商**，即可以被受信身份提供商下的用户扮演。

以下述信任策略为例：该RAM角色可以被当前阿里云账号（AccountID=123456789012****）中的身份提供商 `testprovider` 下的用户扮演。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Federated": [
          "acs:ram::123456789012****:saml-provider/testprovider"
        ]
      },
      "Condition":{
        "StringEquals":{
          "saml:recipient":"https://signin.aliyun.com/saml-role/sso"
        }
      }
    }
  ],
  "Version": "1"
}
```

## 说明

服务关联角色的信任策略由关联的云服务定义，您不能修改服务关联角色的信任策略。服务关联角色的详情，请参见服务关联角色。

# 8.设置角色最大会话时间

您可以通过控制台或API设置角色的最大会话时间。角色最大会话时间设置成功后，当您使用角色完成一些耗时较长的任务时，可以获得较长的登录会话时间；当您使用STS API扮演角色时，可以获取较长的STS Token有效期。

## 背景信息

- 角色最大会话时间的取值范围：3600秒~43200秒。默认值：3600秒。
- 服务关联角色不能设置角色最大会话时间。

## 通过控制台设置角色最大会话时间

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，单击目标RAM角色名称。
4. 在**基本信息**区域，单击**最大会话时间**右侧的**编辑**。
5. 输入最大会话时间，单击**确定**。

## 通过API设置角色最大会话时间

您可以调用CreateRole或UpdateRole，通过MaxSessionDuration或NewMaxSessionDuration参数设置角色最大会话时间。详情请参见CreateRole、UpdateRole。

## 后续步骤

设置完成后，您可以通过切换身份、角色SSO登录、STS API的方式扮演角色。详情请参见：

- 使用RAM角色
- 进行角色SSO
- AssumeRole
- AssumeRoleWithSAML

# 9.使用RAM角色

本文为您介绍RAM用户如何通过控制台和API扮演受信实体为阿里云账号的RAM角色。

## 前提条件

使用RAM角色前，请先完成以下操作：

1. 创建RAM用户。
2. 为该RAM用户设置登录密码或创建访问密钥。
   - 关于如何设置登录密码，请参见修改RAM用户登录密码。
   - 关于如何创建访问密钥，请参见为RAM用户创建访问密钥。
3. 为RAM用户授权。
   - 您可以为RAM用户添加系统策略 `AliyunSTSAssumeRoleAccess` 。
   - 您也可以为RAM用户添加自定义策略，指定该RAM用户可以扮演哪个RAM角色。详情请参见RAM角色和STS Token常见问题。

## 通过控制台扮演RAM角色

RAM用户或角色SSO登录后，可以通过切换身份的方式扮演RAM角色。

1. 使用RAM用户登录RAM控制台。
2. 将鼠标悬停在右上角头像的位置，查看**企业别名**并保存。
3. 单击**切换身份**。
4. 在**角色切换**页面，输入已保存的企业别名。

   > **说明** 企业别名也称为账号别名，**角色切换**页面除了填写企业别名，您也可以填写默认域名进行角色切换。关于默认域名，详情请参见管理默认域名。

5. 输入**角色名**。
6. 单击**切换**。

   切换成功后，RAM用户将以RAM角色身份登录控制台，此时RAM用户只能执行该RAM角色身份被授权的所有操作。

   在控制台右上角头像位置将会显示用户的登录身份（即登录时使用的身份，可能是RAM用户，也可能是RAM角色）和当前身份（即切换角色后的身份）。在不同情况下，用户登录身份和当前身份的取值如下表所示：

| 登录方式 | 登录身份 | 当前身份 |
| --- | --- | --- |
| RAM用户 | 显示格式为<当前登录的RAM用户名称>。 | 显示格式为<RoleName>/<RoleSessionName>。<br>○ RoleName：当前切换的角色名称。<br>○ RoleSessionName：当前登录的RAM用户名称，同登录身份。 |

| 登录方式 | 登录身份 | 当前身份 |
| --- | --- | --- |
| 角色SSO | RAM角色第一次登录（指通过角色SSO直接登录）后，只显示当前身份，不显示登录身份。<br>RAM角色登录（指通过角色SSO直接登录）后再次切换身份后，登录身份显示角色SSO的身份信息，显示格式为<RoleName>/<RoleSessionName>。<br>○ RoleName：角色SSO登录时的角色名称。<br>○ RoleSessionName：角色SSO登录时的RoleSessionName。<br>例如：外部IdP中的用户tom@example.local通过RAM角色test-saml-role1登录到控制台，然后再次使用角色alice-testrole切换身份，切换后显示登录身份为test-saml-role1/tom@example.local。 | 显示格式为<RoleName>/<RoleSessionName>。<br>○ RoleName：当前切换的角色名称。<br>○ RoleSessionName：角色SSO登录时的RoleSessionName。<br>例如：外部IdP中的用户tom@example.local通过RAM角色test-saml-role1登录到控制台，这时当前身份为test-saml-role1/tom@example.local，然后再次使用角色alice-testrole切换身份，此次当前身份为alice-testrole/tom@example.local，其中RoleSessionName保持不变。 |

角色登录会话有效期将以角色最大会话时间与登录Session过期时间中设置的较小值为准。详情请参见设置角色最大会话时间、设置RAM用户安全策略。

## 通过调用API扮演RAM角色

有权限的RAM用户可以使用其访问密钥调用AssumeRole接口，以获取某个RAM角色的安全令牌（STS Token），从而使用安全令牌访问阿里云。

> 说明 如果您通过扮演角色获取的STS Token发生泄漏，您可以回收所有已经颁发的STS Token。详情请参见RAM角色和STS Token常见问题。

## 相关链接

您也可以通过角色SSO登录控制台，详情请参见进行角色SSO。

# 10.删除RAM角色

当不再需要某个RAM角色时，可以删除该RAM角色。

## 前提条件

删除角色前，角色不能有任何权限策略。

## 操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色名称**列表下，找到目标RAM角色，单击**删除**。
4. 单击**确定**。

> **说明** 删除服务关联角色时，**操作**列会先显示**角色删除中...**，您需要等待几秒钟，直至提示删除成功。对于删除失败的情形，请在报错提示信息中单击**查看详情**，根据错误详情进行相应处理。

## 相关文档

- DeleteRole