阿里云
访问控制

角色管理

文档版本：20190920

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

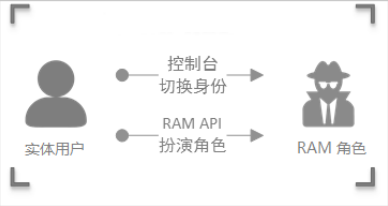
格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，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::1234567890 12****: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#unique_4。
   - 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#unique_5。

> 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

- #unique_6
- #unique_7
- #unique_8

2 创建RAM角色

2.1 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. 单击新建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. 选择云账号后，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，单击为角色授权可直接为该角色授权。详情请参见#unique_11。

相关文档
#unique_12

2.2 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。

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. 单击新建RAM角色。
4. 选择可信实体类型为阿里云服务，单击下一步。
5. 输入角色名称和备注。

6. 选择受信服务后，单击完成。

> 说明:
> 更多受信服务请以实际界面为准。

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#unique_5。

相关文档
#unique_12

2.3 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. 单击新建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#unique_5。

相关文档
#unique_12

3 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

#unique_16

4 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。

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。

相关文档

#unique_18

5 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。

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. 单击确认。

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. 单击确认。

相关文档

#unique_20

6 编辑RAM角色策略内容

本文为您介绍如何通过修改角色的策略内容来改变允许扮演该角色的可信实体。

背景信息

策略中的`Principal`部分决定了允许扮演该角色的可信实体，通过修改`Principal`的内容可以改变该可信实体。

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. 在信任策略管理页签下，单击修改信任策略。

   说明:

   可以参考#unique_22编辑策略内容。
5. 单击确认。

7 修改RAM角色的可信实体

通过修改RAM角色的策略内容，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。

说明:

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，您可以通过以下几种方式来进行修改。修改后请务必进行测试并确保功能可以正常使用。

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，即可以被受信云账号下授权的RAM用户扮演。

以下述策略为例：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:

创建此角色时，请确保已创建好RAM用户`testuser`（其UPN为：testuser@123456789012****.onaliyun.com）。

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。

以下述策略为例：该RAM角色可以被当前云账号下的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。

以下述策略为例：该RAM角色可以被当前云账号（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"
}
```

8 使用RAM角色

本文针对受信实体为阿里云账号的RAM角色为您介绍RAM用户如何扮演RAM角色登录控制台。

前提条件

> 说明:
> 为了安全起见，阿里云不允许受信云账号以自己的身份扮演角色，如果一个实体用户想扮演某个RAM角色，该实体用户必须先以自己身份登录，然后将自己从实体身份切换到RAM角色身份。

使用RAM角色前，请先完成以下操作：

1. #unique_25。
2. 为该RAM用户创建访问密钥或设置登录密码。
   - 关于如何创建访问密钥，请参见#unique_26。
   - 关于如何设置登录密码，请参见#unique_27。
3. #unique_28。
   - 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可以扮演哪个RAM角色。详情请参见#unique_29。

操作步骤

1. RAM用户登录RAM控制台。
2. 将鼠标悬停在右上角头像的位置，单击切换身份。
3. 在角色切换页面，输入相应账号别名或默认域名以及角色名，单击切换。

   > 说明:
   > 切换成功后，用户将以RAM角色身份登录控制台，控制台右上角头像位置将显示角色身份（即当前身份）和登录身份，此时用户只能执行该角色身份被授权的所有操作。

4. 在扮演角色身份时，将鼠标悬停在右上角头像的位置，单击返回登录身份可以切换回登录身份。

后续步骤

RAM用户也可以通过调用API扮演RAM角色。

当RAM用户被授予`AliyunSTSAssumeRoleAccess`权限策略之后，可以使用其访问密钥调用#unique_30接口，以获取某个角色的安全令牌，从而使用安全令牌访问阿里云。

相关文档

#unique_31

9 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

说明:

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. 单击确认。

相关文档

#unique_33

10 最佳实践

10.1 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

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。

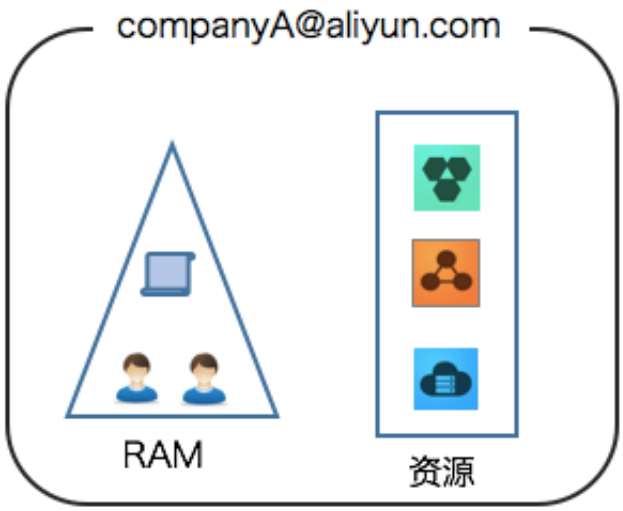
背景信息

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，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#unique_25。

- 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#unique_25。

- 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#unique_36。

- 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#unique_37。

- 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RAM用户更改登录密码，那么应该要求RAM用户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#unique_38。

- 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#unique_39。

- 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#unique_40。

- 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#unique_26。

- 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#unique_41。

- 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#unique_28。

- 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#unique_42。

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#unique_43。

11 常见问题

11.1 RAM角色和STS token常见问题

本文介绍了一些RAM角色和STS token的常见问题，为您提供说明和指导。

RAM角色有几种类型?

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
- 阿里云服务
- 身份提供商

三种类型的RAM角色分别可以被谁扮演?

- 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。特别的是，ECS实例RAM角色也属于这个类型，其可信实体为ECS服务，详情请参见#unique_46。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。

能否指定RAM用户具体可以扮演哪个RAM角色?

您也可以通过创建自定义策略指定RAM用户具体可以扮演的RAM角色。策略示例如下所示：

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Resource": "acs:ram:*:$accountId:role/$roleName"
        }
    ],
    "Version": "1"
}
```

说明:

- 上述自定义策略中的`Resource`为角色ARN，如何查看角色ARN请参见如何查看RAM角色的ARN?其中，`$accountId`为云账号ID，`$roleName`为RAM角色名称。

- 将上述自定义策略授权给RAM用户，便可以指定具体可以扮演的RAM角色。关于如何为RAM用户授权，请参见#unique_28。

如何查看RAM角色的ARN?

您可以登录RAM控制台，在RAM角色管理页签下，单击目标RAM角色名称，在基本信息区域下查看角色ARN。

为什么使用STS时会报错?

STS使用Java SDK生成临时账号密码报错的信息如下所示：

```
Error message: You are not authorized to do this action. You should be authorized by RAM.
```

出现上述现象是因为进行授权的RAM用户没有相应的权限，因此使用时系统会报错。

请为RAM用户添加系统策略（AliyunSTSAssumeRoleAccess）或自定义策略，详情请参见能否指定RAM用户具体可以扮演哪个RAM角色?

STS服务调用次数是否有上限?

STS服务有流控限制：100QPS。超过流控会被限制。

STS token的权限限制是什么?

STS token的权限：指定角色的权限与调用#unique_47接口时所设置的`Policy`的交集。

说明:

若在调用`AssumeRole`接口时不设置`Policy`参数，则返回的STS token将拥有指定角色的所有权限。

STS token的有效期是多久?

STS token的有效期为900秒~3600秒，默认值为3600秒。

说明:

您可以在调用#unique_47接口时设置`DurationSeconds`参数来限制STS token的有效时间。

STS获取的多个token是否同时有效?

STS token在过期之前都是有效的，无论是否创建了新的STS token。