目录

概述

IAM角色是IAM身份类型的一种。IAM角色是一种虚拟用户身份，根据其身份可以确定具有确定其可执行和不可执行的操作的权限策略。

- 角色需要由具体的实体进行扮演代入，而不是唯一地与某个人员关联。
- 角色没有关联的标准长期凭证（如密码或访问密钥）。当具体实体扮演时，它会为您提供角色会话的临时安全凭证。

基本概念

术语	说明
IAM角色	IAM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。IAM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IAM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KRN	角色KRN是角色的全局资源描述符，用来指定具体角色。KRN遵循金山云KRN的命名规范。例如krn:ksc:iam::200**52:role/rolename。**创建角色后，单击角色名后，可在**基本信息**页查看其KRN。
授信实体	角色的可授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授信实体，角色只能被授信的实体扮演。授信实体可以是云账号、云服务或身份提供商。
权限策略	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	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	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	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金山云服务API。

角色类型

角色类型	说明	应用场景
金山云账号	允许金山云账号和IAM子用户扮演角色。可以是自己的金山云账号，也可以是其他金山云账号。	该类角色主要用于解决跨账号访问和临时授权问题。
金山云服务	允许云服务扮演的角色	该类角色主要用于解决跨云服务授权访问的问题。
身份提供商	允许身份提供商下的用户所扮演的角色。	该类角色主要用于实现与金山云的角色SSO

创建授信实体为金山云账号的角色

本文介绍如何创建授信实体为金山云账号的IAM角色。该IAM角色主要用于解决跨账号访问和临时授权问题。

操作步骤

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**界面，单击**新建角色**。
4. 在**新建角色**页面中，**设置授权实体类型**为**金山云账号**。
5. 输入角色名称和备注。
6. 设置载体信息。

   可以选择当前云账号或其他云账号，如果是其他云账，需要填写对应云账号账号ID。 可以在账号及安全查看账号ID
7. 单击**下一步**，完成角色创建。

   角色创建成功后，进入设置角色权限页面，您可以为该角色添加权限策略。

创建授信实体为金山云服务的角色

本文介绍如何创建授信实体为金山云服务的IAM角色。该IAM角色主要用于解决跨云服务授权访问的问题。

背景信息

授信实体为金山云服务的IAM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。

普通服务角色创建

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**界面，单击**新建角色**。
4. 在**新建角色**页面中，**设置授权实体类型**为**金山云服务**。
5. 选择**服务类型**为**普通服务角色**。
6. 输入角色名称和备注。
7. 选择授信云服务。

   可以选择的授信云服务以控制台显示为准

8. 单击**下一步**，完成角色创建。

   角色创建成功后，进入设置角色权限页面，您可以为该角色添加权限策略。

服务关联角色创建

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**界面，单击**新建角色**。
4. 在**新建角色**页面中，**设置授权实体类型**为**金山云服务**。
5. 选择**服务类型**为**普通服务角色**。
6. 选择授信云服务。

   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。

7. 单击**确定**，完成角色创建。

创建授信实体为身份提供商的角色

本文介绍如何创建授信实体为身份提供商的IAM角色。该IAM角色主要用于实现与金山云的角色SSO。

操作步骤

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**界面，单击**新建角色**。
4. 在**新建角色**页面中，**设置授权实体类型**为**身份提供商**。
5. 输入角色名称和备注。
6. 在设置载体信息， 选择身份提供商。
7. 单击**下一步**，完成角色创建。

   角色创建成功后，进入设置角色权限页面，您可以为该角色添加权限策略。

查看角色基本信息

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

操作步骤

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**页面，单击目标**角色名称**。
4. 在角色详情基本信息区域，可查看IAM角色名称、创建时间和KRN等信息。

修改IAM角色

角色一旦创建，角色名称不可修改，仅支持修改角色备注。

删除IAM角色

当不再需要某个IAM角色时，可以删除该IAM角色。删除后关联的策略会解除，授信的实体将无法使用策略权限。

操作步骤

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**页面，在目标**角色名称**操作列单击**删除**。
4. 在确认删除弹窗中，单击确定。

为IAM角色授权

本文介绍如何为IAM角色授权。

限制说明

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。

方式一：在角色管理列表为IAM角色授权

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**页面，在目标**角色名称**操作列单击**添加权限**。
4. 在添加权限面板，为用户组添加权限。
5. 单击**确定**，完成权限添加。

方式二：在授权页面IAM角色授权

1. 登录访问控制控制台。
2. 选择**权限管理** > **授权**。
3. 在**授权列表**页面， 单击**新建授权**按钮。
4. 在**新建授权**面板，选择要授权的IAM角色和授权的策略。
5. 单击**确定**，完成权限添加。

方式三：在策略页面为IAM角色授权

1. 登录访问控制控制台。
2. 选择**权限管理** > **授策略**。
3. 在**策略列表**页面，找到要授权的目标策略，单击**操作**列的**关联对象**按钮。
4. 在**关联对象**面板，选择要授权的IAM角色。
5. 单击**确定**，完成权限添加。

查看IAM角色权限

本文介绍如何查看IAM角色权限。

操作步骤

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**页面，单击目标**角色名称**。
4. 在**关联策略**页签中，查看IAM角色的权限。

为IAM角色移除授权

当IAM角色不再需要某些权限或离开组织时，可以将这些权限移除。

限制说明

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。

方式一：在角色列表为IAM角色移除权限

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**页面，单击目标**角色名称**。
4. 在**关联策略**页签中，单击目标权限策略操作列的**解除**操作按钮。
5. 在**确认弹窗**中，单击**确定解除**。

方式二：在授权页面为为IAM角色移除权限

1. 登录访问控制控制台。
2. 选择**权限管理** > **授权**。
3. 在**授权列表**页面， 单击目标授权操作列的**解除**操作按钮。
4. 在**确认弹窗**中，单击**确定解除**。

方式三：在策略页面为为IAM角色移除权限

1. 登录访问控制控制台。
2. 选择**权限管理** > **授策略**。
3. 在**策略列表**页面，找到要授权的目标策略，单击**策略名称**。
4. 在**策略**详情，单击**关联对象**页签。
5. 在**关联对象列**表中，单击目标对象操作列的**解除**操作按钮。
6. 在**确认弹窗**中，单击**确定解除**。

使用角色

本文为您介绍IAM子用户如何通过控制台和API扮演授信实体为仅云账号的IAM角色。

> 角色登录仅支持子IAM子用户身份登录，主账号暂不支持角色登录

前提条件

1. 创建IAM子用户。请参见文档创建IAM子用户。
2. 为IAM子用户创建访问密钥。请参见文档为IAM子用户创建访问密钥。
3. 为IAM子用户授权。
   - 您需要未IAM子用户添加系统策略：STSAssumeRoleAccess（提供STS服务AssumeRole接口的权限）。
     - 授权文档请参考为IAM子用户授权。

通过控制台扮演IAM角色

IAM子用户或角色SSO登录控制台后，可以通过切换身份的方式扮演IAM角色。

1. 使用IAM子用户登录控制台。
2. 将书本悬停在右上角用户名的位置，会出现悬浮弹层。
3. 在弹层中点**击切换身份**。
4. 在**角色切换**页面，选择要切换的角色。
5. 单击确定。

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

调用API扮演IAM角色

有权限的IAM子用户可以使用其访问密钥调用AssumeRole API，以获取某个IAM角色的安全令牌（STS Token）。