目录

角色概览

角色机制是向您信任的实体进行授权的一种安全方法。根据不同应用场景，受信任的实体可能有：

- 您云账户下的一个子用户（可能是代表一个移动App的后端服务）
- 其他云账户中的子用户（需要进行跨账户的资源访问）
- 实例上运行的应用程序代码（需要对云资源执行操作）
- 某些金山云服务（需要对您账户中的资源进行操作才能提供服务）

> 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
角色	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。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

应用场景

临时授权访问

通常情况下，建议您通过服务端调用API，尽可能保证访问密钥不被泄露。但是有些上传文件的场景可以采用客户端直传的形式，避免服务端中转带来的多余开销。此时，可以由服务端下发临时安全令牌，客户端通过临时安全令牌进行资源直传。

跨账号访问

当您拥有多个金山云账号，例如：账号A和账号B，希望实现账号A访问账号B的指定资源。此时，您可以在账号B下创建可信实体为账号A的角色，并授权允许账号A下的某个子用户或角色可以扮演该角色，然后通过该角色访问账号B的指定资源。

跨服务访问

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：配置审计服务要读取您的云资源信息，以获取资源列表和资源配置变更历史，就需要获取ECS、RDS等产品的访问权限。此时，您可以创建可信实体为金山云服务的角色解决该问题。推荐您优先使用服务关联角色，对于不支持服务关联角色的云服务，请使用普通服务角色。

单点登录（角色SSO）

金山云与企业进行角色SSO时，金山云是服务提供商，而企业自有的身份管理系统则是身份提供商。通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色登录金山云。此时，您可以创建可信实体为身份提供商的角色解决该问题。

使用流程

1. 使用金山云账号（主账号）或具有管理员权限的子用户登录IAM控制台。
2. 创建角色。
   - 创建授信实体为金山云账号的角色
   - 创建授信实体为金山云服务的角色
   - 创建授信实体为身份提供商的角色
3. 为角色授权。
   - 具体操作，请参见为角色授权。
4. 可信实体通过控制台或调用API扮演角色并获取角色的安全令牌。
   - 具体操作，请参见使用角色
5. 可信实体通过角色身份访问被授权的云资源。

使用限制

关于角色的使用限制，请参见使用限制

服务关联角色

可信云服务可以通过角色扮演的方式访问其他云服务的资源。可信实体为金山云服务的角色分为两种：普通服务角色和服务关联角色。本文主要介绍服务关联角色。

什么是服务关联角色

- 服务关联角色是一种可信实体为金山云服务的角色，旨在解决跨云服务的授权访问问题。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地配置云服务正常操作所必需的权限，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。

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IAM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。具体操作，请参见 创建服务关联角色。

说明：服务关联角色会占用您的角色配额。当角色数量超限时，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。

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。 删除角色。
- 当您尝试删除一个服务关联角色时，IAM会先检查这个角色是否仍被云资源使用：

如果为否，您可以成功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，但可以根据删除失败的提示信息，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。

创建和删除服务关联角色所需的权限

- 通过子用户创建或删除服务关联角色时，子用户必须具备对应权限。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，因此子用户如果具有该云服务的管理员权限，也可以为该云服务创建服务关联角色。

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：子用户、其他角色）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

- 支持服务关联角色的云服务，请参见支持服务关联角色的云服务。
- 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角色。该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，如果是其他云账号，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角色。该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**服务关联角色**。
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角色。该角色主要用于实现与金山云的角色SSO。

前提条件

请确保您已创建了身份提供商

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. 在设置载体信息， 选择身份提供商。
6. 输入角色名称和备注。
7. 单击**下一步**，完成角色创建。

后续步骤

8. 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，详见，为角色授权。

查看角色信息

本文为您介绍如何查看角色基本信息，角色载体、关联策略、加入的项目等信息。

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**或**操作列下的详情**。
4. 在角色详情可查看基本信息、角色载体、关联策略、加入的项目等信息。

注意：角色一旦创建，角色名称不可修改，仅支持修改角色备注。

删除角色

当不再需要某个角色时，可以删除该角色。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。

删除后：关联的策略会解除，授信的账号将无法使用策略权限。

为角色授权

本文介绍如何为角色授权。

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：在策略页面为角色授权

1. 登录访问控制控制台。
2. 选择**权限管理** > **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，选择要授权的角色。
5. 单击**确定**，完成权限添加。

查看角色权限

本文介绍如何查看角色权限。

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**或**操作列的详情**。
4. 在**关联策略**页签中，查看角色的权限。
5. 在详情页点击关联策略，查看角色的权限策略。

为角色移除授权

当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**或**操作列的详情**。
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：在策略页面为为角色移除权限

1. 登录访问控制控制台。
2. 选择**权限管理** > **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

本文为您介绍子用户如何通过控制台和API扮演授信实体为仅云账号的角色。

> 角色登录仅支持子子用户身份登录，主账号暂不支持角色登录

前提条件

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

通过控制台扮演角色

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角色。

1. 使用子用户登录控制台。
2. 将鼠标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，子用户将以角色身份登录控制台，此时子用户只能执行该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扮演角色

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