目录

主账号管理

正式开始使用访问控制服务之前，您需要先注册一个金山云账号。注册账号后，您可以在金山云官网登录，从而使用您需要的云服务。

- 注册金山云账号，详见：注册金山云
- 登录金山云账号，详见：登录金山云
- 关于账号管理的其他详情，可直接前往账号管理中心查看。

创建子用户并授权

本文介绍如何快速创建子用户并授予相关权限。子用户是一种身份，对应操作实体可以是具体的运维人员，也可以是某个应用程序。新建的子用户默认无任何权限，需要为其授权后才可以访问相应资源。

前提条件

已登录主账号或拥有管理员权限的的子用户，才可以进行子用户添加操作。

操作步骤

步骤一：创建子用户

1. 使用主账号或具有管理权限的子用户登录访问控制控制台。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 单击**新建用户**按钮，进入新建用户页面。
4. 在新建用户页面用户登录信息区域按提示填写信息。

   登录账号：必填，为子用户的用户名，一旦创建无法修改。 **显示名称**：必填，方便按照自身业务定义使用者对应名称。 **邮箱**：选填，用于接收消息。 **手机号**：选填，用于接收消息。
5. 在**访问方式**区域，选择访问方式。为了保障账号安全，建议只选择一种登录方式。
   - **控制台密码登录**：子用户使用账号密码访问金山云控制台

     设置控制台登录密码、下次登录是否要求重置密码、是否允许查看所有项目。
   - **编程访问**：自动为子用户用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问金山云。

     是否允许查看所有项目。
6. 在**选择策略**区域，选择为用户授予的策略。
7. 单击**确定**，完成子用户创建及授权。

步骤二：子用户登录金山云控制台

1. 使用新建的子用户登录金山云控制台。
2. 填入主账号ID/用户名、子用户名、子用户登录密码，单击确定，完成子用户登录。
3. （可选）如果您开启了多因素认证（MFA），则需要输入虚拟MFA设备生成的验证码。

创建用户组并授权

用户组是IAM中的一种实体身份类型，用户组可以对职责相同的子用户进行分类并授权，从而更高效地管理子用户及其权限。

操作步骤

步骤一：创建用户组

1. 使用主账号或具有管理权限的子用户登录访问控制控制台。
2. 选择**人员管理** > **用户组**，进入到用户组管理页面。
3. 单击**新建用户组**按钮，进入新建用户组页面。

4. 在新建用户组页面，按提示填写信息。填入用户组名、备注（可选）。
5. 点击下一步，选择用户组成员身份，为用户组添加关联策略。
6. 点击确定，完成用户组的创建及授权。也可点击上一步进行信息修改。

步骤二：为用户组添加子用户

1. 使用金山云账号（主账号）或具有管理权限的子用户登录访问控制控制台。
2. 选择**人员管理** > **用户组**，进入到用户组管理页面。
3. 在用户组列表页，点击操作列的**添加用户**。
4. 在添加用户页进行子用户添加操作，最多可选择10个。

用户进入用户组后将拥有该用户组的所有权限；若用户策略与组策略冲突时，默认 会以“Deny”处理。

5. 点击确定，完成在用户组里添加子用户。

步骤三：为用户组授权

1. 使用金山云账号（主账号）或具有管理权限的子用户登录访问控制控制台。
2. 选择**人员管理** > **用户组**，进入到用户组管理页面。
3. 在用户组列表页，点击操作列的**添加权限**。
4. 在添加权限页进行策略添加操作。
5. 点击确定，完成为用户组授权。

创建角色并授权

角色是一种虚拟用户，可以被授予一组权限策略。与子用户不同，角色没有恒定不变的身份凭证（登录密码或访问密钥），需要被一个可信实体扮演。扮演成功后，可信实体将获得角色的临时身份凭证，即安全令牌，使用该安全令牌就能以角色身份访问被授权的资源。

角色类型

根据不同的可信实体，角色分为以下三类：	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	

操作步骤

步骤一：创建角色

不同类型的角色创建方法略有差异，如下将以创建可信实体为金山云账号的角色为例为您介绍。更多信息，请参见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。

1. 使用主账号或具有管理权限的子用户登录访问控制控制台。
2. 选择**角色管理** ，进入到角色管理页面。
3. 单击**新建角色**按钮，进入新建角色页面。
4. 在新建角色面板，选择可信实体类型为金山云账号，按提示填写信息。
   - 设置角色信息

     a. 输入角色名称、b. 输入备注

   - 设置载体信息

     选择当前账号或其他云账号，并输入账号UID

5. 完成以上信息填写，点击下一步，选择策略，完成角色授权。也可点击取消，后续再该角色添加权限策略。