目录

子用户概览

子用户简介

子用户是IAM的一种实体身份类型，有确定的身份ID和身份凭证，它通常与某个确定的人或应用程序一一对应。

子用户具备以下特点：

- 子用户创建成功后，归属于主账号，它不是独立的金山云主账号。
- 子用户不拥有资源，不能独立计量计费，由所属的主账号统一付费。
- 子用户必须在获得授权后，才能登录控制台或使用API访问主账号下的资源。
- 子用户拥有独立的登录账号密码和访问密钥。
- 一个主账号下可以创建多个子用户，对应企业内的员工、系统或应用程序。

您可以创建子用户并为其授权，实现不同子用户拥有不同资源访问权限的目的。当您的企业存在多用户协同访问资源的场景时，使用IAM可以按需为子用户分配最小权限，避免多用户共享主账号的登录账号密码或访问密钥，从而降低企业的安全风险。

使用流程

1. 使用主账号或具有管理员权限的子用户、角色登录访问控制控制台。
2. 创建子用户：具体操作，请参见创建子用户。
3. 设置登录参数。
    - 虽然您可以为子用户同时设置控制台登录密码和API调用的访问密钥AK（AccessKey），但出于安全的考虑，建议您针对不同用途的子用户仅设置一种登录方式。
    - 如果子用户代表的是应用程序，则需要通过API访问资源，您只需给它创建访问密钥。
    - 如果子用户代表的是员工，则需要通过控制台访问资源，您只需给它设置登录密码。具体设置方法如下：

（1）控制台登录

- 您需要启用子用户控制台登录、设置子用户密码强度、设置或修改登录密码、按需启用多因素认证（MFA）。具体操作，请参见修改控制台登录设置、设置子用户密码强度、修改子用户登录密码和为子用户开启MFA认证等。

    说明：如果您启用了用户SSO，则可以不开启控制台登录，用户也能通过SSO方式登录到金山云控制台。更多信息，请参见用户SSO概览。

（2）API调用

- 您需要为子用户创建访问密钥。具体操作，请参见为子用户创建访问密钥。

4. 为不同的子用户授予不同的资源访问权限。具体操作，请参见为子用户授权。
5. 使用子用户登录控制台或使用访问密钥调用API，请参见子用户登录金山云控制台和API概览。

使用限制

- 关于子用户的使用限制，请参见使用限制。

创建子用户

本文介绍如何快速创建子用户，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

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。 
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。

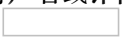
后续步骤

- 可以为用户添加权限策略，使子用户具有资源的访问能力。
- 可以将子用户添加到用户组，对子用户进行分类并授权。
- 子用户创建成功并授权策略后，可以使用子用户登录控制台。

修改子用户信息

本文为您介绍如何修改子用户的基本信息。子用户的登录账号不可修改，仅支持修改显示名称、邮箱、手机号码。

操作步骤

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。 
4. 在用户详情的**用户信息**区域，单击**编辑**。 
5. 在**编辑用户信息**的弹窗里，编辑要修改的信息。 
6. 单击**确定**，完成编辑。

查看子用户信息

本文为您介绍如何查看子用户信息，包括子用户基本信息、安全信息、已加入的用户组、被授予的权限策略等相关事件。

操作步骤

1. 使用金山云账号登录访问控制控制台。
2. 在左侧导航栏，**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户管理页面，查看全部子用户列表。
4. 您可以单击列表右上角的设置，自定义列表展示字段。  
5. 单击目标子用户名称或者单击详情，查看子用户详情信息。 
   - 在用户基本信息区域，查看子用户登录账号、显示名称、创建时间等信息。
   - 在安全管理页签，查看控制台登录管理设置、安全信息设置等。
   - 在关联策略页签，查看子用户被授予的权限策略。
   - 在加入的组页签，查看子用户已加入的用户组。
   - 在加入的项目页签，查看子用户已加入的项目。
   - 在消息管理页签，查看子用户接收的消息。 

删除子用户

操作需知

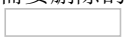
当不再需要某个子用户时，可以删除该子用户。

> 提示：删除的用户数据将无法恢复。如果用户存在最近登录记录或使用 AccessKey 的情况，建议您先禁用该用户控制台登陆或将AccessKey禁用，进行排查确认，然后再删除该用户。

删除用户会带来以下影响：

- 移除关联的权限策略
- 退出所有加入的用户组
- 解绑MFA绑定
- 删除用户 AccessKey
- 用户无法登录金山云

操作步骤

1. 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. 在子用户列表管理页面，找到需要删除的子用户。
4. 单击操作列的**更多** > **删除**。 
5. 在弹出的确认是否删除用户窗口，勾选知晓上述风险，单击确定删除，完成删除子用户操作。 

修改控制台登录设置

本文为您介绍如何修改子用户登录设置信息。

前提条件

已登录主账号或拥有管理员权限的子用户，才可以操作子用户修改控制台登录。

操作步骤

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。 
4. 在用户详情的**安全管理**页签区域，单击**修改设置**。 
5. 在**修改设置**的面板里，设置控制台登录参数。 
    - 控制台密码登录：关闭后，则不允许子用户登录控制台，仅可通过AccessKey以API或其他开发工具访问。
    - 子用户登录密码：支持生产默认密码或者自定义登录密码。请按需设置。
    - 要求重置密码：勾选后，下次子用户登录时需重置密码。
    - 登录保护：如果要求开启MFA认证，用户登录时需要通过二次身份校验。
    - 操作保护：如果要求开启MFA认证，用户进行敏感操作时需要通过二次身份校验。
    - 子用户查看所有项目：开启后，子用户登录控制台可以查看所有项目组，包括未来新建的项目组。
    - 登陆或操作保护任一项要求MFA认证，子用户在下次登录时需绑定MFA设备。
6. 单击**确定**，完成控制台登陆设置。

为子用户开启多因素认证

通过为子用户进行登录保护和操作保护设置，可以为其启用多因素认证。启用后可以为您的子账号提供更高的安全保护。

操作步骤

1. 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. 在子用户列表管理页面，单击目标用户的用户名或**操作**列**详情**，进入到用户详情页。
4. 在用户详情的**安全管理**页签区域，单击**修改设置**。
5. 在**修改设置**的面板里，设置登录保护和操作保护参数。 
    - 登录保护：如果要求开启MFA认证，用户登录时需要通过二次身份校验。
    - 操作保护：如果要求开启MFA认证，用户进行敏感操作时需要通过二次身份校验。

6. 单击**确定**，完成设置。

后续步骤

登录或操作保护任一项要求MFA认证，子用户在下次登录时需绑定MFA设备。

为子用户创建访问密钥

背景说明

为保证账号安全，强烈建议您给子用户创建访问密钥，不要给金山云账号（主账号）创建访问密钥。

什么是访问密钥（AccessKey）

如果为子用户创建了访问密钥（AccessKey），子用户可以通过API或其他开发工具访问金山云资源。 在调用金山云API时您需要使用AccessKey完成身份验证。AccessKey包括AccessKey ID和AccessKey Secret，需要一起使用。具体如下：

- AccessKey ID：用于标识用户。
- AccessKey Secret：用于验证用户的密钥。AccessKey Secret必须保密。

操作步骤

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**，进入到用户详情页。
4. 在用户详情的**安全管理**页签，单击**创建秘钥**。
5. 完成敏感操作验证。
6. 在**创建AccessKey**弹窗中，查看AccessKeyID和SecretAccessKey。
7. 您可以点击下载凭证或复制AccessKey信息保存子用户的密钥。

> SecretAccessKey只在创建时显示，不支持查询，请妥善保管。 若AccessKey泄露或丢失，则需要创建新的AccessKey，最多可以创建2个AccessKey。

为子用户禁用访问密钥

如果子用户不需要访问密钥（AccessKey），支持禁用其访问密钥。

操作步骤

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**，进入到用户详情页。
4. 在用户详情的**安全管理**页签，在目标密钥**操作**列单击**禁用**按钮。
5. 在确认弹窗中单击**确定**按钮，完成禁用。
6. 对于已禁用的访问密钥，可以单击操作列的启用，重新启用该访问密钥。也可点击删除，删除该密钥。

设置子用户密码强度与安全

为了保护账号安全，您可以编辑密码规则，包括密码长度、密码有效期和历史密码检查策略、密码元素等。下面的【密码强度设置】和【密码安全设置】仅对子用户生效。

> 主账号安全策略说明： 1、主账号登录session过期时间为12小时； 2、主账号密码连续输入错误3次，则会锁定账号30分钟，可通过修改密码或等待30分解除。 3、主账号密码连续输入错误超过5次，则会冻结，可通过修改密码解除。

操作步骤

密码强度设置

1. 登录访问控制控制台。
2. 选择**设置** > **安全设置**。
3. 在**安全设置**页面的密码强度设置区域， 单击**修改**按钮。
4. 在**密码强度设置**弹层中配置相关参数。

- **密码长度**：密码长度范围为8~32位，建议设置至少8位以上密码长度。
- **密码有效期**：建议设置有效期。可填写90-365天，超过密码有效期，登录后需修改密码。
- **历史密码检查策略**：建议设置。表示禁止使用前N次密码，取值范围为1~12。
- **密码中必须包含元素**：请根据需要勾选大写字母、小写字母、数字和符号。建议至少勾选2项。
- **密码过期后是否可登录**：不可登录表示密码过期后，不能登录控制台。需要通过金山云账号或具有管理员权限的子用户重置该子用户的密码后，才能正常登录。
- **1小时内密码错误尝试次数**：设置密码重试的次数（取值1-32），连续输入错误密码达到设定次数后，账号将被锁定一小时。 5. 单击**确定**完成设置。

密码安全设置

1. 登录访问控制控制台。
2. 选择**设置** > **安全设置**。
3. 在**安全设置**页面的密码安全设置区域， 单击**修改**按钮。
4. 在**密码安全设置**弹层中配置相关参数。
   - **保存MFA登录状态7天**：是否启用
     - **登录session过期时间**：可填写15-1440分钟。
     - **登录掩码设置**：最多设置100个地址。

5. 单击**确定**完成设置。

执行结果

设置成功后，此密码规则适用于所有子用户。

修改子用户登录密码

本文为您介绍如何为子用户修改账号密码。

操作步骤

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。
4. 在用户详情的**安全管理**页签区域，单击**修改设置**。
5. 在**修改设置**的面板里，找到子用户登录密码区域。
   - 选择自动生成默认密码，然后单击确定，会自动生成登录密码，请记录并妥善保管新密码。
   - 选择自定义登录密码，然后输入新的密码。输入的新密码必须符合密码强度要求。
6. 单击**确定**，完成密码修改。

子用户登录控制台

本文为您介绍子用户如何登录金山云控制台。

登录地址

子用户可以通过如下三个地址登录：

子用户概览页

1. 使用主账户或者已授权的子用户身份访问控制控制台。
2. 点击概览，链接地址即为子用户登录地址：

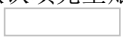
快捷登录设置页

1. 使用主账户或者已授权的子用户身份访问控制控制台。
2. 点击快捷登录设置，链接地址即为子用户登录地址：

官网登录页

1. 在官网登录页，点击右下角子用户登录。  

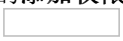
操作步骤

1. 通过子用户概览页以及快捷登录设置页进行子用户登录操作时，默认填充主账号用户名。
   - 用户输入子用户名、子用户登录密码，点击登录完成操作。 
2. 通过子官网登录页进行子用户登录操作。
   - 用户输入主账号ID/用户名、子用户名、子用户登录密码，点击登录完成操作。 

为子用户授权

为子用户授权后，子用户将可以访问相应的金山云资源。

方式一：在用户页面为子用户授权

1. 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. 在子用户列表，找到目标子用户，单击**操作**列的**添加权限**按钮。 
4. 在添加权限页面，为子用户选择要添加权限。 
5. 单击**确定**，完成权限添加。

方式二：在授权页面为子用户授权

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，选择要授权的子用户和授权的策略。 
5. 单击**确定**，完成权限添加。

方式三：在策略页面为子用户授权

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

查看子用户权限

本文为您介绍如何查看子用户的权限，包括查看子用户的个人权限和查看子用户继承用户组的权限。

查看子用户的个人权限

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。
4. 单击用户详情的**关联策略**页签。
5. 在**个人权限**页签，查看子用户的个人权限。 

查看子用户继承用户组的权限

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**，进入到用户详情页。
4. 单击用户详情的**关联策略**页签。
5. 在**继承用户组的权限**页签，查看子用户的继承用户组的权限。 

为子用户移除权限

当子用户不再需要某些权限时，可以移除相应权限。

方式一：在用户页面为子用户移除权限

1. 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. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。
4. 单击用户详情的**关联策略**页签。
5. 在**个人权限**页签，单击目标权限策略操作列的**解除**操作按钮。
6. 在确认弹窗中，单击**确定解除**。

方式二：在授权页面为子用户移除权限

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：在策略页面为子用户移除权限

1. 登录访问控制控制台。
2. 选择**权限管理** > **授策**。
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**移出**操作按钮。
6. 在确认弹窗中，单击**确定移出**。