目录

权限系统概览

本章主要介绍金山云权限系统概览。

- 什么是子账号用户
- 怎么对子账号用户授权

对于金山云的大型企业客户，一般都会使用多种云服务并购买大量云计算资源。对于这些客户而言，其可能拥有多家子公司/部门，且每个公司/部门独立财务核算，因此需要云计算资源在子公司/部门之间隔离互不干扰。

权限系统是为了便于企业客户，对其账号内使用的云产品、云资源，包括其他各类数据信息进行管理、查询权限的划分，以达到对操作的控制及敏感信息的保护等目的。

为了满足用户各项灵活功能权限划分的需求，金山云推出了身份与访问控制服务，即IAM （Identity and Access Management）。创建者可灵活配置子用户允许查看的云产品、操作对象和资源对象，更加细粒度的进行权限指派。

什么是子账号用户？

子账号用户即IAM用户,是账号下的授权实体，也是归属于账号的一种资源。IAM用户不拥有任何云计算资源、不能独立计量和计费，只能被主账号授权管理其名下的各种资源，其所管理的资源归属于主账号（由主账号付费），且没有独立的账单。

子账号用户在获得主账号的授权后，能够被设置密码和访问密钥，从而登录控制台和使用openAPI管理主账号的资源。

怎么对子账号用户授权？

对子账号用户授权等管理操作都可以通过IAM进行授权控制，每种产品基于IAM所能够进行控制的操作参考该产品的openAPI文档。

IAM系统通过操作（Action）和资源（Resource）授权。

- 资源（Resource） 资源是金山云的客户操作或者使用云服务的对象实体，比如云服务器实例、CDN域名资源；为方便在IAM的策略文档中描述一个资源，我们使用KRN（Kingsoft Resource Name）唯一标识一个金山云资源。
- 操作（Action） 操作是金山云客户管理或者使用云计算资源动作，可以分为管理操作和数据操作两大类。管理操作是对资源生命周期和运维的管理动作。数据操作是使用资源的动作。

更多IAM介绍相关操作请参考身份与访问控制。

云直播权限说明

本章主要介绍金山云云直播权限。

- 云直播管理员权限
- 子账号权限

云直播IAM（Identity and Access Management），根据功能属性的不同对云直播的所有操作进行了划分，每一项功能的权限包含了对应的控制台操作及对应的API操作。

云直播管理员权限

创建者（主账号用户）是金山云账号的拥有者，默认拥有最高权限。默认具有管理员功能。

创建者如果购买云直播产品，将自动获得最高权限，即"KLSFullAccess"+"KLSConsoleFullAccess"权限，拥有云直播全部OpenAPI接口管理和云直播控制台的全部权限。

子账号权限

- 子账号一定是由创建者创建生成的，不能自己生成。
- 子账号的权限不得高于云直播管理员权限。
- 创建者创建子账号时，需要关联权限策略，否则子账号用户无法正常使用云直播产品和服务。
- 创建者创建子账号后，需要在项目管理中，添加子账号。 注意：子账号的权限仅对所在的项目组内的资源生效。

更多子账号功能，需要按照权限策略进行配置，请参考用户策略说明和子账号用户配置。

用户策略说明

本章主要对用户策略做简要说明。

- 云直播系统策略
- 云直播自定义策略
- 子账号权限生效资源说明
- 用户策略举例

云直播权限通过将用户关联用户策略实现。

一条策略由服务类型、操作（Action）、资源（Resource)三个因素组成：

- 服务类型：选择要设置的权限类型，如云直播；
- 操作（Action）：选择允许的云直播操作，如统计分析查询、自助管理等，详情参考子账号用户配置和策略配置示例；
- 资源（Resource）：逐一为各个功能指定其允许操作的资源对象，在云直播中，资源就是子账号所在项目中的域名，在策略语法中表现为"*"。

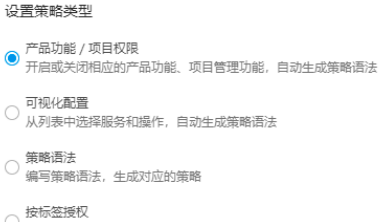
策略分为两种类型： 系统策略：即预先注册进KOP的系统策略，系统策略不能被更改。 自定义策略：由主账号用户按照策略规则进行策略自定义。

云直播系统策略

策略名称	策略描述	服务类型
KLSConsoleFullAccess	提供视频云直播控制台的全部权限	-
KLSFullAccess	提供云直播全部OpenAPI接口管理权限	-

云直播自定义策略

云直播创建自定义策略支持四种类型：

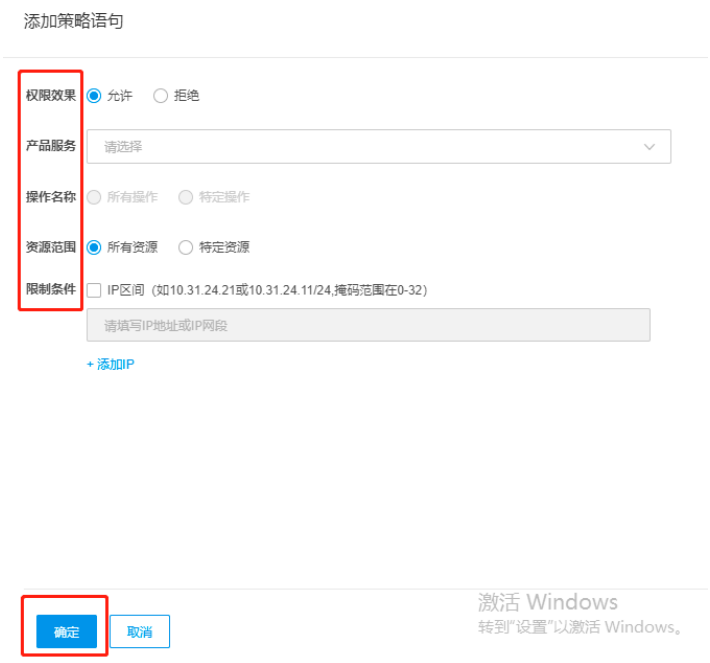


- 按产品功能 / 项目创建权限 选择产品功能 / 项目权限，选择服务类型并点击下一步，如下图： 在操作列选择需要开启的功能权

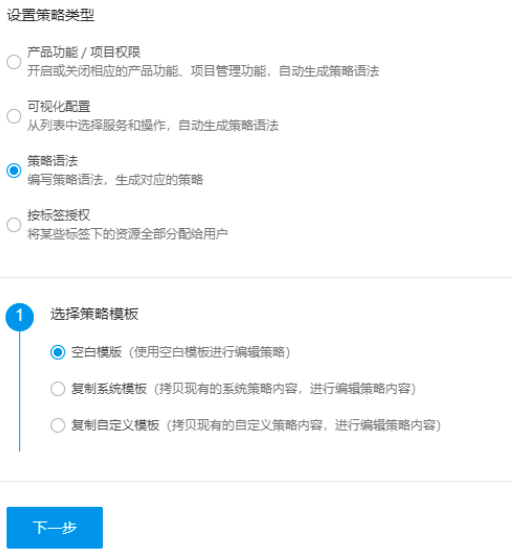
限进行开启，如下图 点击创建策略，即创建完成

- 按可视化配置创建权限 选择可视化配置权限，点击添加策略语句，如下图

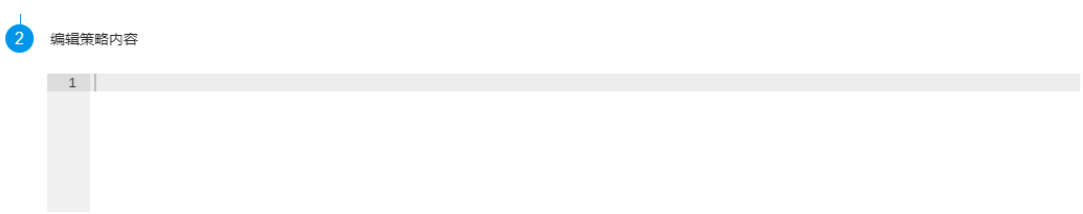
设置权限效果-产品服务-资源范围-限制条件，点击确定即可生成策略内容



点击创建策略，即创建完成



- 按策略语法创建权限 基于系统策略、空白模板、自定义策略编辑，来创建策略；点击下一步，手动编辑语法；



点击创建策略，即创建完成

- 按标签授权创建权限： 选择标签授权权限，基于标签策略，来创建策略，如下图

用户策略举例

```
{
    "Version": "2015-11-01",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kls:ListRealtimePubStreamsInfo",
                "kls:ListHistoryPubStreamsInfo",
                "kls:ListHistoryPubStreamsErrInfo",
                "kls:listRelayStreamsInfo",
                "kls:listRelayErrInfo",
                "kls:ListStreamDurations",
                "kls:GetBlacklist",
                "kls:CheckBlacklist",
                "kls:ListRecordingTasks",
                "kls:ListHistoryRecord",
                "kls:GetRecordTask",
                "kls:ListStreamRecordContent"
            ],
            "Resource": "*"
        }
    ]
}
```

- Effect：定义时取值"allow"或“deny”。
- Action：通过选择开放的接口的名称，最大范围可以选择“*”。
- Resource：要求选择“*”。

更多策略配置示例可参考策略配置示例。

子账号用户配置

本章主要介绍金山云子账号用户配置方法。

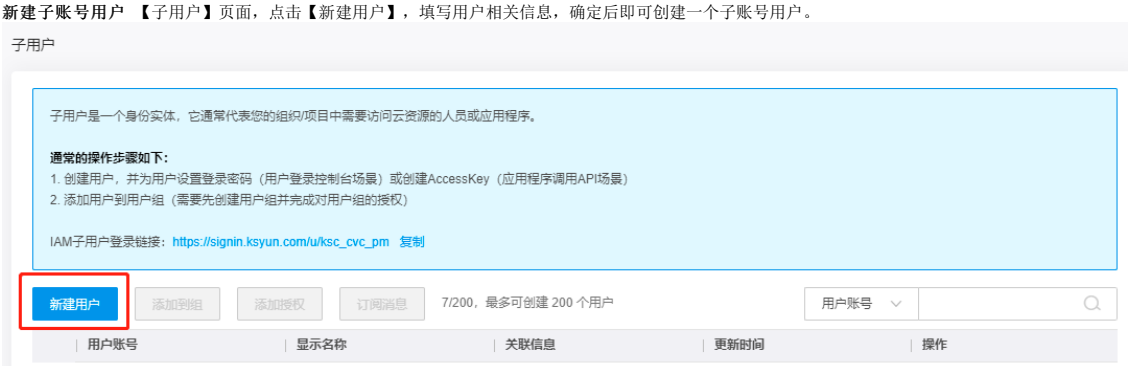
- 创建子账号用户
- 编辑子帐号用户
- 子账号用户登录

子账号用户即“IAM用户”。子账号用户本身无需注册金山云，开通云直播服务，子账号由创建者将其添加至用户管理列表中。

创建子账号用户

登录身份与访问控制页面，点击【子用户】，即进入【子用户】页面。

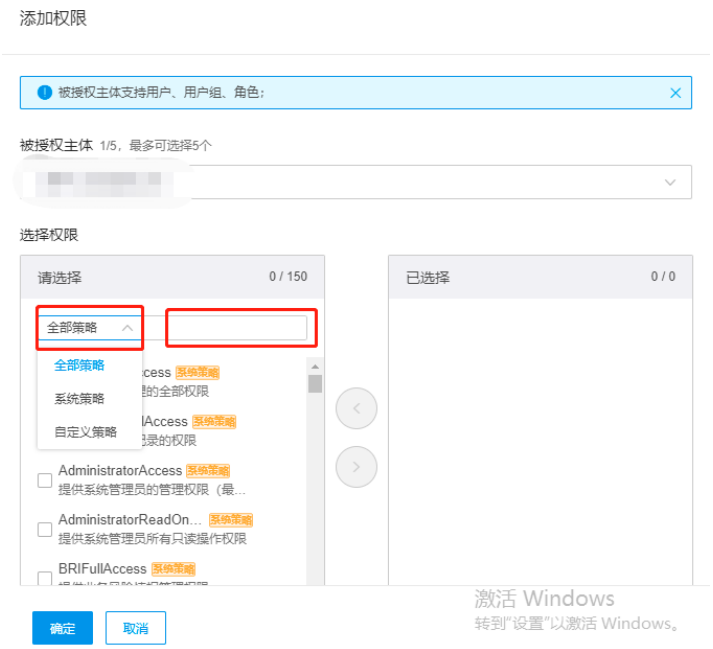
新建子账号用户 【子用户】页面，点击【新建用户】，填写用户相关信息，确定后即可创建一个子账号用户。



其中登录账号、显示名称必填项，一旦创建不可修改，邮箱、手机非必填项，手机邮箱经过验证后可用于接收消息。

授权策略 【子用户】页面点击【添加权限】，在策略列表中可选择一条或多条策略授权给子账号用户。

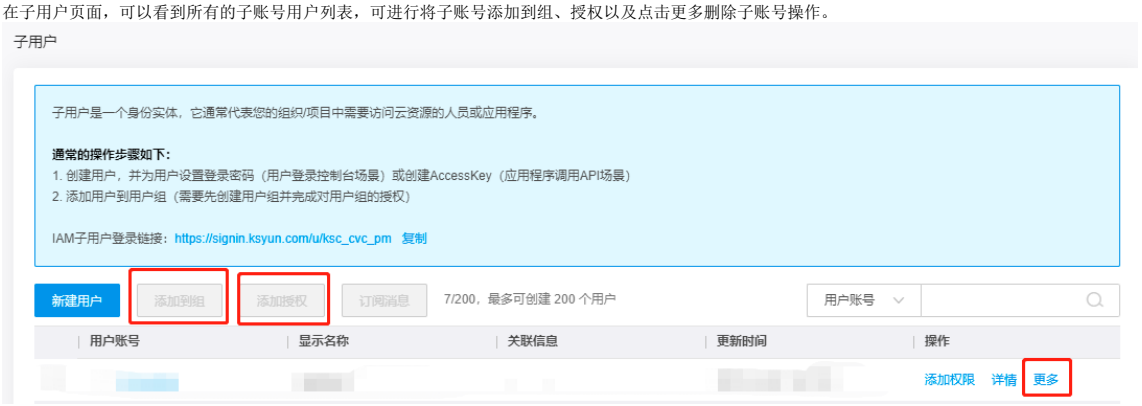
支持策略搜索及类型过滤，支持模糊搜



索，策略类型包括系统及自定义策略。

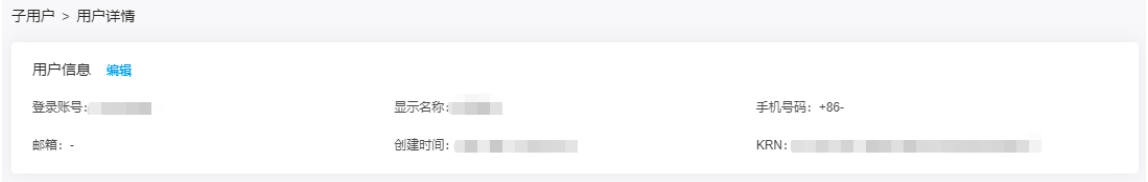
编辑子账号用户

在子用户页面，可以看到所有的子账号用户列表，可进行将子账号添加到组、授权以及点击更多删除子账号操作。

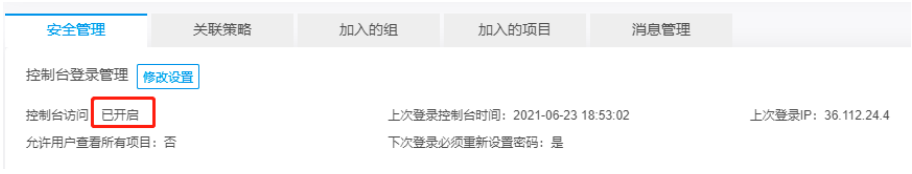


点击用户名称即可进入用户详情页面，该页面展示用户的详细信息，可编辑用户基本信息，设置控制台登录、多因素设备认证、AK密匙设置、关联策略、加入的组。

基本信息 此处显示用户基本信息，亦可编辑用户信息，包括显示名称、手机号、邮箱



安全管理 安全管理包含控制台登录、创建秘钥



控制台登录 开启控制台登录即可设置子账号控制台登陆密码

创建秘钥 此处可对子账号用户安全进行相关设置

- 启用/禁用用户自助管理密码（拥有AdministratorAccess权限的子用户不受此功能开关限制）；
- 启用/禁用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 ）。

多因素设备验证 启用虚拟MFA设备，绑定设备后，可在登录时通过一组6位动态码来进行二次校验。

加入的组 此处可对用户所属群组信息进行编辑

- 添加：点击添加【添加到组】即可将当前用户添加到相应群组中；
- 解除：对已经加入群组的用户，点击解除即可将用户从当前群组中移除。

关联策略 此处显示用户用户关联策略信息，亦可编辑用户关联策略信息

- 关联策略：点击【添加权限】即可选择策略将策略添加到当前用户；
- 解除策略：点击【解除】，确认解除后即可将解除用户与当前策略的关联，解除策略后将无法获得该策略所描述的操作权限；
- 显示策略：点击【显示】策略，即弹窗显示当前策略信息。

删除子账号 【子用户】页面选择用户点击更多【删除】

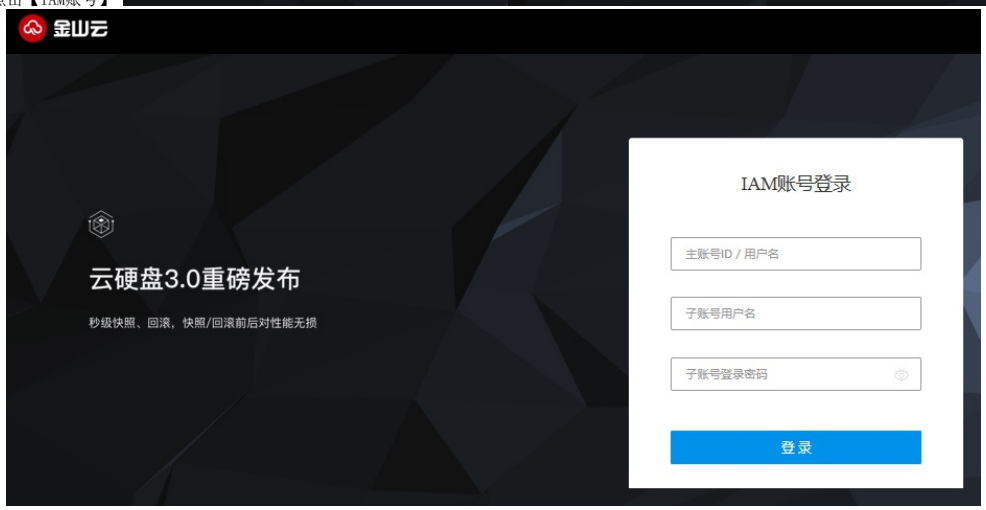
子账号用户登录

复制登录链接 进入身份与访问控制页面，复制IAM用户登录链接

在新页面打开链接，输入主账号ID/用户名、子用户名和子账号密码即可登录

控制台登录页面登录 进入控制台登录页面，点击【IAM账号】

输入主账号ID、子账号用户名和密码即可登录



登录后，控制台仅显示子账号所在项目组内的域名资源

策略配置示例

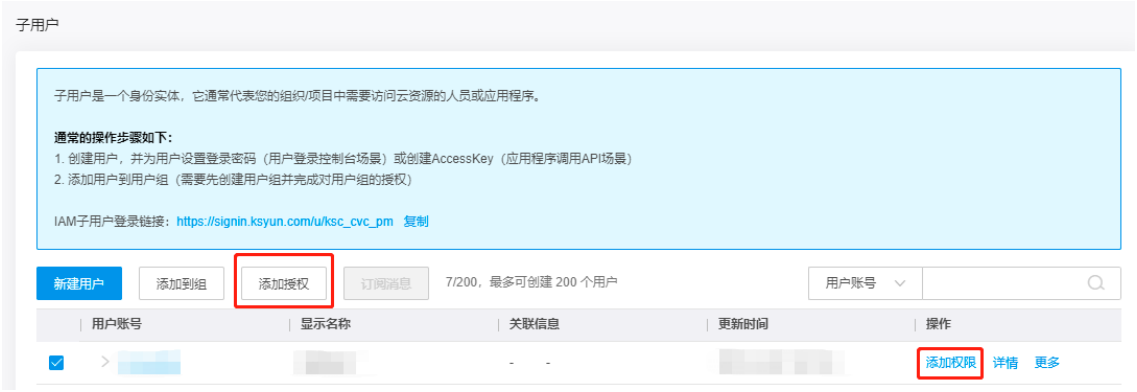
本章主要介绍金山云权限配置示例。

- 云直播全部OpenAPI接口管理权限配置示例

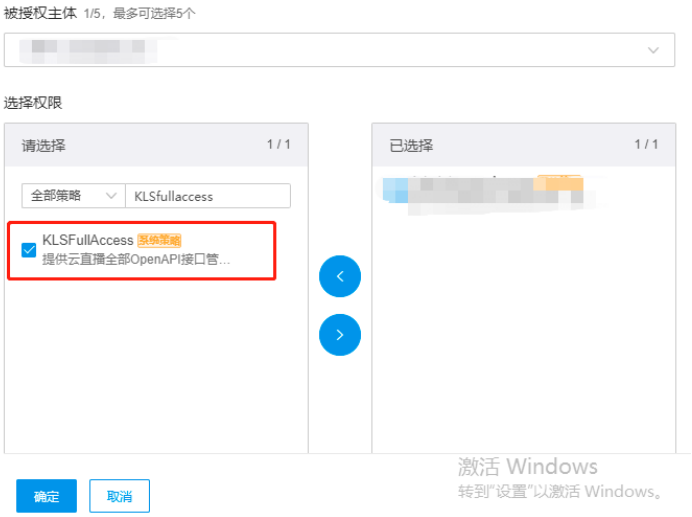
云直播全部OpenAPI接口管理权限配置示例

第一步 登录身份访问与控制页面,点击【子用户】进入子用户页面

第二步 进入用户管理页面，选择用户，点击【授权】或【添加权限】



第三步 在授权策略列表中选择KLSFullAccess，可通过上方搜索框进行搜索，选择成功后点击【确定】



此时便完成了云直播全部OpenAPI接口管理权限的配置，表明子账号具有全部OpenAPI接口的管理权限。