

目录

目录	1
权限系统概览	2
什么是子账号用户?	2
怎么对子账号用户授权?	2
CDN权限说明	2
CDN管理员权限	2
子账号权限	2
用户策略说明	2
CDN系统策略	2
CDN自定义策略	3
子账号权限生效资源说明	5
用户策略举例	5
子账号用户配置	5
创建子账号用户	5
新建子账号用户	6
授权策略	6
创建自定义策略	6
编辑子账号用户	7
基本信息	8
控制台登录	8
子账号安全	9
多因素设备验证	9
编辑群组	10
关联策略编辑	10
用户AK密钥	12
删除子账号	13
子账号用户登录	13
复制登录链接	13
控制台登录页面登录	14
策略配置示例	14
CDN功能全部管理权限配置示例	15
CDN功能查询管理权限配置示例	15
CDN自定义用户权限部分资源配置示例	16

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\(IAM\)](#)。

CDN权限说明

本章主要介绍金山云CDN权限说明。

- [CDN管理员权限](#)
- [子账号权限](#)

CDN目前已经接入新版的IAM（Identity and Access Management），根据功能属性的不同对CDN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。

CDN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CDN产品，将自动获得最高权限，即“CDNFullAccess”权限，拥有CDN功能全部管理权限。

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CDN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CDN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。

- [CDN系统策略](#)
- [CDN自定义策略](#)
- [子账号权限生效资源说明](#)
- [用户策略举例](#)

CDN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 CDN；
- 操作（Action）：选择允许的 CDN 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CDN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。

CDN系统策略

策略名称	策略KRN	策略描述	策略版本	默认策略
CDNFullAccess	krn:ksc:iam::ksc:policy\CDNFullAccess	提供CDN功能全部管理权限 v1		是
CDNReadOnlyAccess	krn:ksc:iam::ksc:policy\CDNReadOnlyAccess	提供CDN功能查询管理权限 v1		是

CDN 自定义策略

CDN创建自定义策略支持三种方式:

- 按业务权限创建 从服务/功能权限列表中选择并开启，形成策略，如下图:

按业务权限方式的功能权限和对应API说明，如下表:

API分类	API有哪些	API中文说明
	GetAreaData	用户区域统计
	GetBandwidthData	新版查询带宽信息
	GetBandwidthDataByDir	目录带宽接口
	GetDomainRankingListData	控制台域名排行
	GetFlowData	新版查询流量信息接口
	GetFlowDataByDir	目录流量接口
	GetHitRateData	新版查询命中率信息接口
	GetHitRateDetailedData	新版查询命中率详情接口
	GetHttpCodeData	状态码信息查询
	GetHttpCodeDetailedData	状态码详情
	GetIspData	运营商占比统计
	GetPeakBandwidthData	获取带宽峰值信息接口
	GetProvinceAndIspBandwidthData	省份+运营商带宽查询接口
	GetProvinceAndIspFlowData	省份+运营商流量查询接口
1	点播统计分析	GetProvinceAndIspHitRateDetailedData 省份+运营商命中率详情查询 GetProvinceAndIspHttpCodeData 省份+运营商状态码查询 GetProvinceAndIspHttpCodeDetailedData 省份+运营商状态码详情查询 GetProvinceAndIspPvData 省份+运营商请求数查询 GetPvData 新版查询请求数信息接口 GetSrcHttpCodeData 回源状态码统计(饼图) GetSrcHttpCodeDetailedData 回源状态码详情统计 GetSubDomainsBandwidthData 泛域名子域名带宽 GetSubDomainsFlowData 泛域名子域名流量 GetSubDomainsPvData 泛域名子域名请求数 GetTopIpData TOPIP统计 GetTopReferData TOPRefer查询 GetTopUrlData TOPURL查询 GetUvData 独立IP的请求个数 GetBandwidthPeriodRatioData 带宽环比查询
2	直播统计分析	GetLiveOnlineUserDataByDomain 直播按域名维度统计在线人数 GetLiveOnlineUserDataByStream 按流名维度的直播在线人数数据 GetLiveFlowDataByStream 直播按流维度查询流量 GetLiveBandwidthDataByStream 直播按流维度查询带宽 GetLiveTopOnlineUserData 直播TopN按流维度在线人数排名 GetLivePlayStatData 直播域名及流维度带宽、在线人数统计 GetPlayTimeDataByStream 按照流维度统计观看时长 GetPlayTimeDataByDomain 按照域名维度统计观看时长
3	日志管理	SetDomainLogService 设置用户日志 GetDomainLogServiceStatus 获取用户日志设置状态 GetDomainLogs 获取日志下载URL
4	内容管理	RefreshCaches 刷新接口 PreloadCaches 预热缓存 GetRefreshOrPreloadTask 刷新预热进度查询接口 GetRefreshOrPreloadQuota 查询操作剩余量
5	证书管理	SetCertificate 更新证书 RemoveCertificates 删除证书 GetCertificates 获取用户证书列表 ConfigCertificate 为域名配置证书
6	启动停用域名	StartStopCdnDomain 启用或停用域名根据域名id SetTestUrlConfig 设置加速域名的测试URL SetReferProtectionConfig 设置加速域名的Refer防盗链功能 SetIpProtectionConfig 设置IP防盗链 SetIgnoreQueryStringConfig 设置过滤参数功能 SetCacheRuleConfig 设置缓存策略 SetBackOriginHostConfig 设置回源host功能 ModifyCdnDomainBasicInfo 修改域名基本信息 SetVideoSeekConfig 设置视频拖拽
7	修改域名配置	SetHttpHeadersConfig 设置HTTP头 DeleteHttpHeadersConfig 删除HTTP头 GetHttpHeaderList 获取HTTP头列表 SetOriginAdvancedConfig 设置高级回源 SetRequestAuthConfig 设置时间戳+共享密钥防盗链 SetHttp2OptionConfig 设置HTTP/2接口 SetForceRedirectConfig 设置强制跳转接口 SetPageCompressConfig 设置智能压缩接口 SetErrorPageConfig 设置自定义错误页面接口 GetBandwidthPeriodRatioData 设置自定义错误页面接口
8	查询域名配置	GetValidDomainList 获取有效域名 GetDomainConfigs 设置备注信息 GetCdnDomains 根据用户查询域名信息列表 GetCdnDomainBasicInfo 获取指定加速域名配置的基本信息
9	添加域名	AddCdnDomain 添加域名
10	删除域名	DeleteCdnDomain 删除域名

11	计费管理	GetBillingMode GetBillingData	获取计费方式接口 获取计费数据
----	------	----------------------------------	--------------------

当前共包括 11个分类, 63个API。

按业务权限方式的资源说明, 如下图:

可操作的资源对象为“*”

- 按策略生成器创建 从列表中选择服务和操作, 生成策略语法, 如下图:

按策略生成器功能分类描述, 如下表:

	Action	描述	是否资源粒度
直播统计分析	GetLiveOnlineUserDataByDomain	直播按域名维度统计在线人数	否
	GetLiveOnlineUserDataByStream	按流名维度的直播在线人数数据	否
	GetLiveFlowDataByStream	直播按流维度查询流量	否
	GetLiveBandwidthDataByStream	直播按流维度查询带宽	否
	GetLiveTopOnlineUserData	直播TopN按流维度在线人数排名	否
	GetLivePlayStatData	直播域名及流维度带宽、在线人数统计	是
	GetPlayTimeDataByStream	按照流维度统计观看时长	否
	GetPlayTimeDataByDomain	按照域名维度统计观看时长	否
	SetTestUrlConfig	设置加速域名的测试URL	是
	SetReferProtectionConfig	设置加速域名的Refer防盗链功能	是
域名详细配置	SetIpProtectionConfig	设置IP防盗链	是
	SetIgnoreQueryStringConfig	设置过滤参数功能	是
	SetCacheRuleConfig	设置缓存策略	是
	SetBackOriginHostConfig	设置回源host功能	是
	GetDomainConfigs	查询域名详细配置信息	是
	ModifyCdnDomainBasicInfo	修改域名基本信息	是
	GetCdnDomainBasicInfo	获取指定加速域名配置的基本信息	是
域名基础配置	AddCdnDomain	添加域名	否
	GetAreaData	用户区域统计	否
	GetBandwidthData	新版查询带宽信息	否
	GetBandwidthDataByDir	目录带宽接口	是
	GetDomainRankingListData	控制台域名排行	否
	GetFlowData	新版查询流量信息接口	否
	GetFlowDataByDir	目录流量接口	是
	GetHitRateData	新版查询命中率信息接口	否
	GetHitRateDetailedData	新版查询命中率详情接口	否
	GetHttpCodeData	状态码信息查询	否
	GetHttpCodeDetailedData	状态码详情	否
	GetIspData	运营商占比统计	否
	GetPeakBandwidthData	获取带宽峰值信息接口	否
	GetProvinceAndIspBandwidthData	省份+运营商带宽查询接口	否
	GetProvinceAndIspFlowData	省份+运营商流量查询接口	否
	GetProvinceAndIspHitRateDetailedData	省份+运营商命中率详情查询	否
	GetProvinceAndIspHttpCodeData	省份+运营商状态码查询	否
	GetProvinceAndIspHttpCodeDetailedData	省份+运营商状态码详情查询	否
	GetProvinceAndIspPvData	省份+运营商请求数查询	否
	GetPvData	新版查询请求数信息接口	否
点播统计分析	GetSrcHttpCodeData	回源状态码统计(饼图)	否
	GetSrcHttpCodeDetailedData	回源状态码详情统计	否
	GetSubDomainsBandwidthData	泛域名子域名带宽	是
	GetSubDomainsFlowData	泛域名子域名流量	是
	GetSubDomainsPvData	泛域名子域名请求数	是
	GetTopIpData	TOPIP统计	否
	GetTopReferData	TOPRefer查询	否
	GetTopUrlData	TOPURL查询	否
	GetUvData	独立IP的请求个数	否
	SetDomainLogService	设置用户日志	是
日志管理	GetDomainLogServiceStatus	获取用户日志设置状态	是
	GetDomainLogs	获取日志下载URL	是
	RefreshCaches	刷新接口	否
内容管理	PreloadCaches	预热缓存	否
	GetRefreshOrPreloadTask	刷新预热进度查询接口	否
	GetRefreshOrPreloadQuota	查询操作剩余量	否
计费管理	GetBillingMode	获取计费方式接口	否
	GetBillingData	获取计费数据	否
	SetCertificate	更新证书	否
证书管理	RemoveCertificates	删除证书	否
	GetCertificates	获取用户证书列表	否
	ConfigCertificate	为域名配置证书	是

表中共 66个API。

按策略生成器的资源说明, 如下图:

完成“操作”的选择后，直接点击生成按钮，KRN处显示为“*”。

- 按策略语法创建 基于系统策略、空白模板编辑，来创建策略：

手动指定Action, Resource处为“*”。

子账号权限生效资源说明

如下图所示，用户有域名资源R1~R6，R1和R2在项目P1内，R3和R4在项目P2内，R5和R6在项目P3内；创建子账号U1和U2，希望U1对R1~R4有一定的管理权限，U2对R5~R6有一定的管理权限。



需要，编辑项目P1和P2，添加成员 U1，编辑项目P3，添加成员U2。

更多项目制说明可参考[项目管理](#)。

用户策略举例

```
{
  "Version": "2015-11-01",
  "Statement": [
    {
      "Sid": "Stmt14985654482691",
      "Effect": "Allow",
      "Action": [
        "cdn:GetBandwidthData",
        "cdn:GetFlowData",
        "cdn:GetPvData",
        "cdn:GetHitRateData",
        "cdn:SetReferProtectionConfig",
        "cdn:DeleteCdnDomain",
        "cdn:AddCdnDomain",
        "cdn:GetServiceIpData",
        "cdn:PreloadCaches"
      ],
      "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](#)
- [编辑子账号用户](#)
- [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CDN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【用户】，即进入【用户管理】页面。

概览

欢迎您使用访问控制 (IAM) 系统!

IAM用户登录链接: [设置快速登录方式](#)

项目 NEW 用户 NEW 群组 自定义策略 角色

常见答疑

[IAM的最佳实践，即如何使用好权限管理?](#) HOT

[新建用户等操作类行为，为什么会提示超出上限?](#)

[新版IAM子用户如何登录控制台?](#)

[Access KEY的正确使用方式是什么，SK密钥丢失了怎么办?](#)

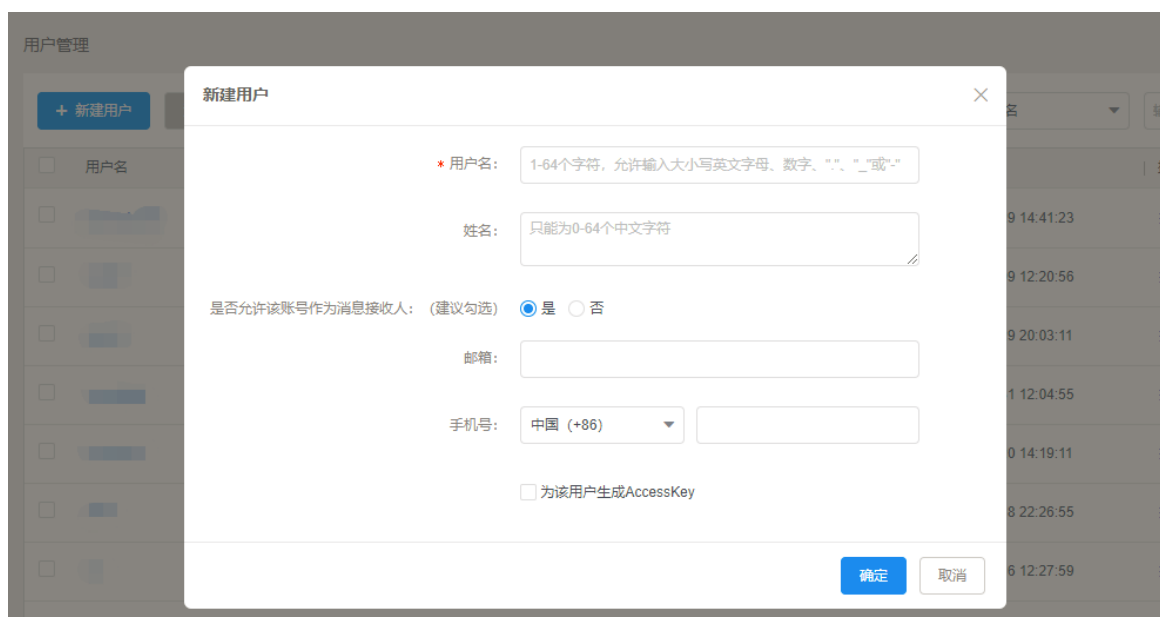
IAM使用答疑邮箱: iam@kingsoft.com

IAM问题反馈: [提交工单](#)



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，保存后即可创建一个子账号用户。其中用户名必填项，一旦创建不可修改，姓名、邮箱、手机非必填项，手机号码经过验证后可用于接收消息。



授权策略

【人员管理】页面点击【授权】，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。



创建自定义策略

点击【自定义策略】，进入策略管理页面，点击【新建策略】即进入【设置策略类型】页面，在三种创建方式中选择一种进行策略编辑，策略创建成功后即可对用户进行授权。

概览

欢迎您使用访问控制 (IAM) 系统!

IAM用户登录链接: [IAM用户登录链接](#) [设置快捷登录方式](#)

项目 [↑](#) [NEW](#) 用户 [↑](#) 群组 [↑](#) [NEW](#) **自定义策略** [↑](#) 角色 [↑](#)

常见答疑

[IAM的最佳实践, 即如何使用好权限管理?](#) [HOT](#)

[新建用户等操作类行为, 为什么会提示超出上限制?](#)

[新版IAM子用户如何登录控制台?](#)

[Access KEY的正确使用方式是什么, SK密钥丢失了怎么办?](#)

IAM使用答疑邮箱: iam@kingsoft.com

IAM问题反馈: [提交工单](#)

策略管理

系统策略 自定义策略

[+ 新建策略](#) [删除](#) 15/50, 最多可创建50个自定义策略

策略名称	备注	创建时间	操作
		2018-05-22 16:11:49	关联对象 删除
	提供系统管理员的管理权限 (最大权限)	2017-08-30 11:17:02	关联对象 删除
	提供系统管理员的管理权限 (最大权限)	2017-07-31 12:00:04	关联对象 删除

策略管理

系统策略 自定义策略

[+ 新建策略](#) [删除](#) 15/50, 最多可创建50个自定义策略

选择策略创建方式

- 按业务权限创建** [NEW](#)
从服务/功能权限列表中选择并开启, 形成策略
- 按策略生成器创建
从列表选择服务和操作, 快速生成策略语法
- 按策略语法创建
通过复制系统策略、自定义策略或创建空白文档, 编写策略

策略名称	备注	创建时间	操作
			关联对象 删除
			关联对象 删除
			关联对象 删除
			关联对象 删除

详细编

编辑策略方式请参考[策略配置示例](#)文档。

编辑子账号用户

在[用户管理](#)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, 该页面展示客户用户的详细信息, 可编辑用户基本信息, 设置控制台登录、子账号安全、多因素设备设置、加入群组、关联策略、AK密钥设置。

用户管理

[+ 新建用户](#) [添加到组](#) [删除](#) 19/100, 最多可创建100个用户

用户名	姓名	邮箱	手机号	创建时间	操作
				2018-08-01 16:25:21	授权 添加到组 删除
testbiubiubiu				2018-06-29 14:41:23	授权 添加到组 删除

The screenshot displays the 'User Management' interface for a user named '1'. It is divided into several sections: 'Basic Information' (with an 'Edit User Information' button), 'Console Login' (with an 'Enable Console Login' button), 'Sub-user Security' (with a toggle for 'Allow user self-management password' set to 'On'), and 'Multi-factor Authentication' (with an 'Enable Virtual MFA Device' button). The MFA section shows 'MFA Device: Virtual MFA Device' and 'Enabled Status: Not Enabled'. Below these are buttons for 'Add Group' and 'Remove Group', and a table with columns for 'Group Name', 'Creation Time', and 'Action', which is currently empty.

基本信息

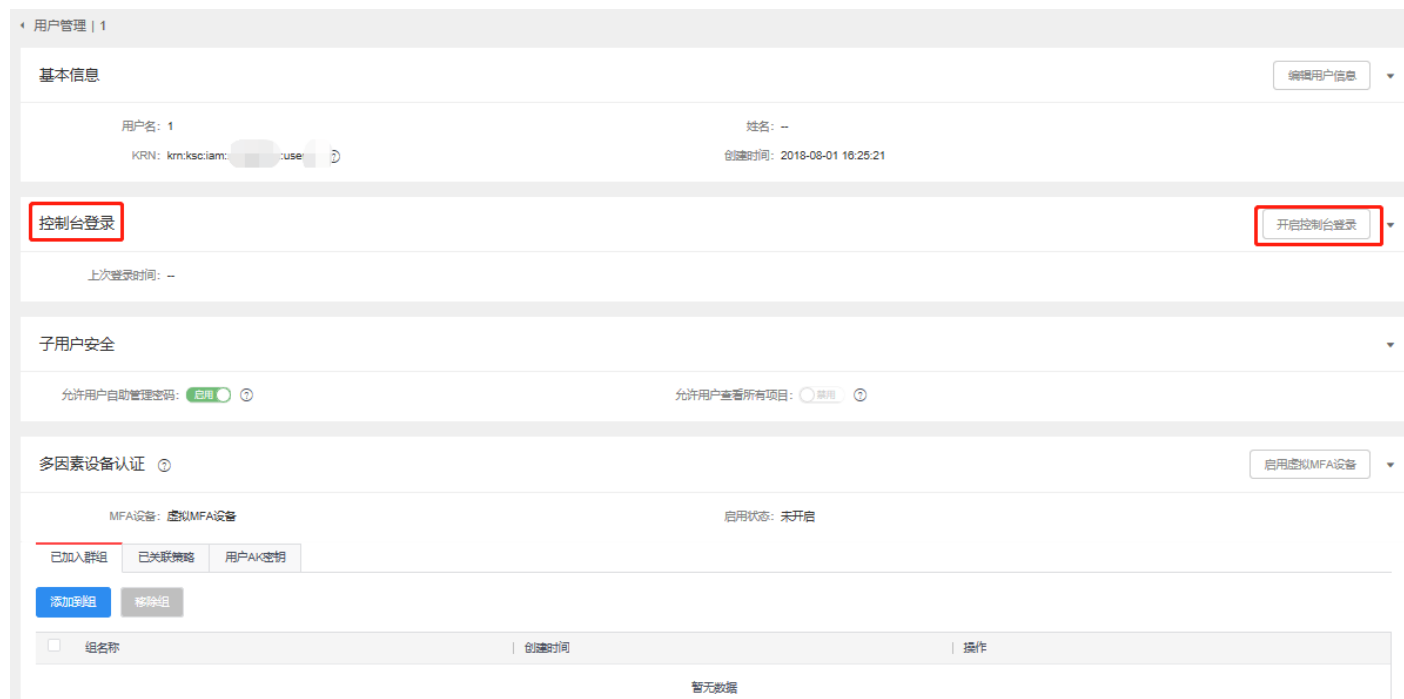
此处显示用户基本信息，亦可编辑用户信息，包括姓名，手机号、邮箱

This screenshot is identical to the previous one, but with the 'Basic Information' tab and the 'Edit User Information' button highlighted with red boxes to indicate the focus of the subsequent section.

The screenshot shows the 'Edit User Information' modal dialog box. It contains input fields for 'Name' (with a red asterisk and a tooltip '只能是0-04个中文字符'), 'Email', and 'Mobile'. The 'Name' field is currently empty. At the bottom of the dialog are 'Confirm' and 'Cancel' buttons. The background interface is dimmed, with the 'Edit User Information' button still highlighted in red.

控制台登录

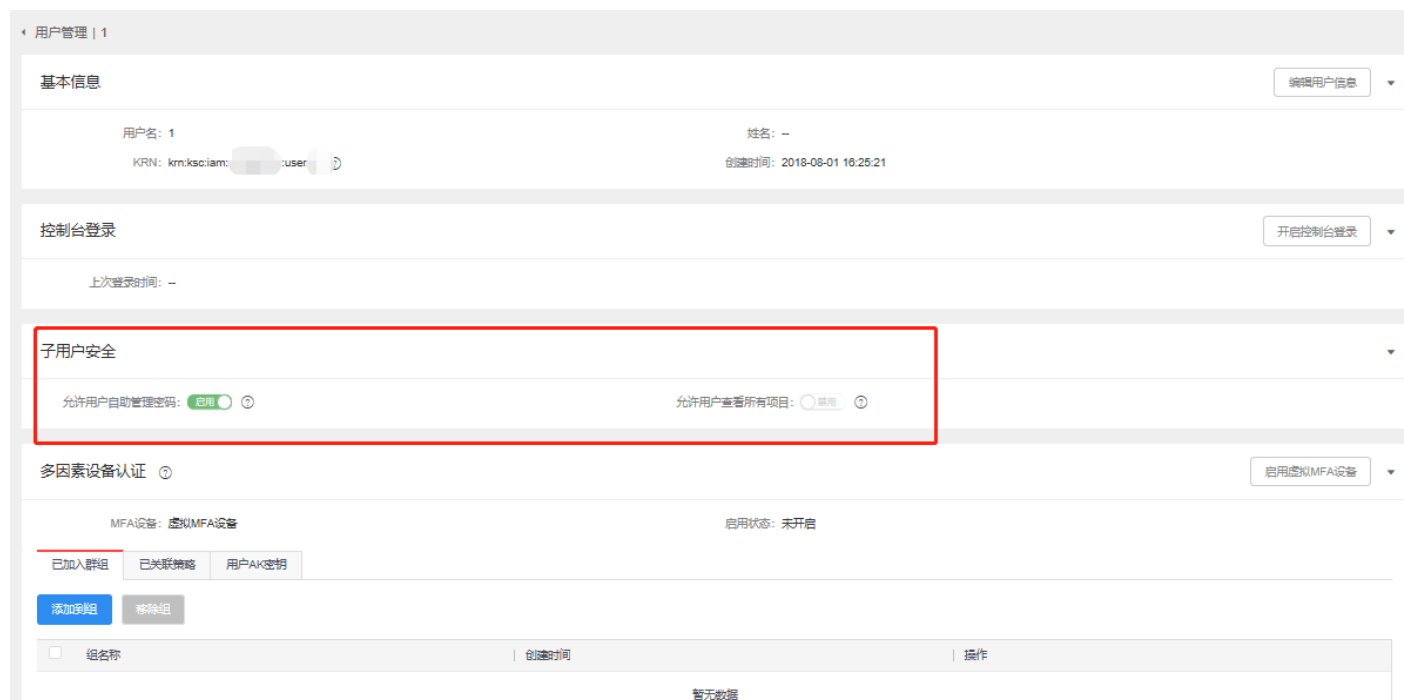
开启控制台登录即可设置子账号控制台登陆密码



子账号安全

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

用户管理 | 1

基本信息 编辑用户信息

用户名: 1 姓名: --
KRN: krm:ksclam::user 创建时间: 2018-08-01 16:25:21

控制台登录 开启控制台登录

上次登录时间: --

子用户安全

允许用户自助管理密码: 启用 ? 允许用户查看所有项目: 禁用 ?

多因素设备认证 ? 启用虚拟MFA设备

MFA设备: 虚拟MFA设备 启用状态: 未开启

已加入群组 已关联策略 用户AK密钥

添加群组 移除组

组名称	创建时间	操作

编辑群组

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, 点击移除组即可将用户从当前群组中移除。

用户管理 | 1

基本信息 编辑用户信息

用户名: 1 姓名: --
KRN: krm:ksclam::user 创建时间: 2018-08-01 16:25:21

控制台登录 开启控制台登录

上次登录时间: --

子用户安全

多因素设备认证 ? 启用虚拟MFA设备

MFA设备: 虚拟MFA设备 启用状态: 未开启

已加入群组 已关联策略 用户AK密钥

添加群组 移除组

添加到组

选择群组 (共1个)

群组
<input checked="" type="checkbox"/> testqunzu 1

已选择 (0个)

群组

关闭

已加入群组 已关联策略 用户AK密钥

添加群组 移除组

组名称	创建时间	操作
	2018-06-29 14:44:00	移除组

关联策略编辑

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【关联策略】即可选择策略将策略添加到当前用户;
- 解除策略: 点击【解除】, 确认接触后即可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。

用户管理 | 1

编辑用户信息

基本信息

用户名: 1 姓名: --
KRN: km:ksciam: .user 创建时间: 2018-08-01 16:25:21

控制台登录

上次登录时间: --

子用户安全

允许用户自助管理密码: 已启用 允许用户查看所有项目: 禁用

多因素设备认证

启用虚拟MFA设备 启用状态: 未开启

MFA设备: 虚拟MFA设备

已加入群组 已关联策略 用户AK密钥

关联策略

策略名称	关联时间	操作
IAMChangePasswd	2018-08-01 16:25:21	解除 显示

用户管理 | 1

编辑用户信息

基本信息

用户名: 1 姓名: --
KRN: km:ksciam: .user 创建时间: 2018-08-01 16:25:21

控制台登录

上次登录时间: --

子用户安全

允许用户自助管理密码: 已启用 允许用户查看所有项目: 禁用

多因素设备认证

启用虚拟MFA设备 启用状态: 未开启

MFA设备: 虚拟MFA设备

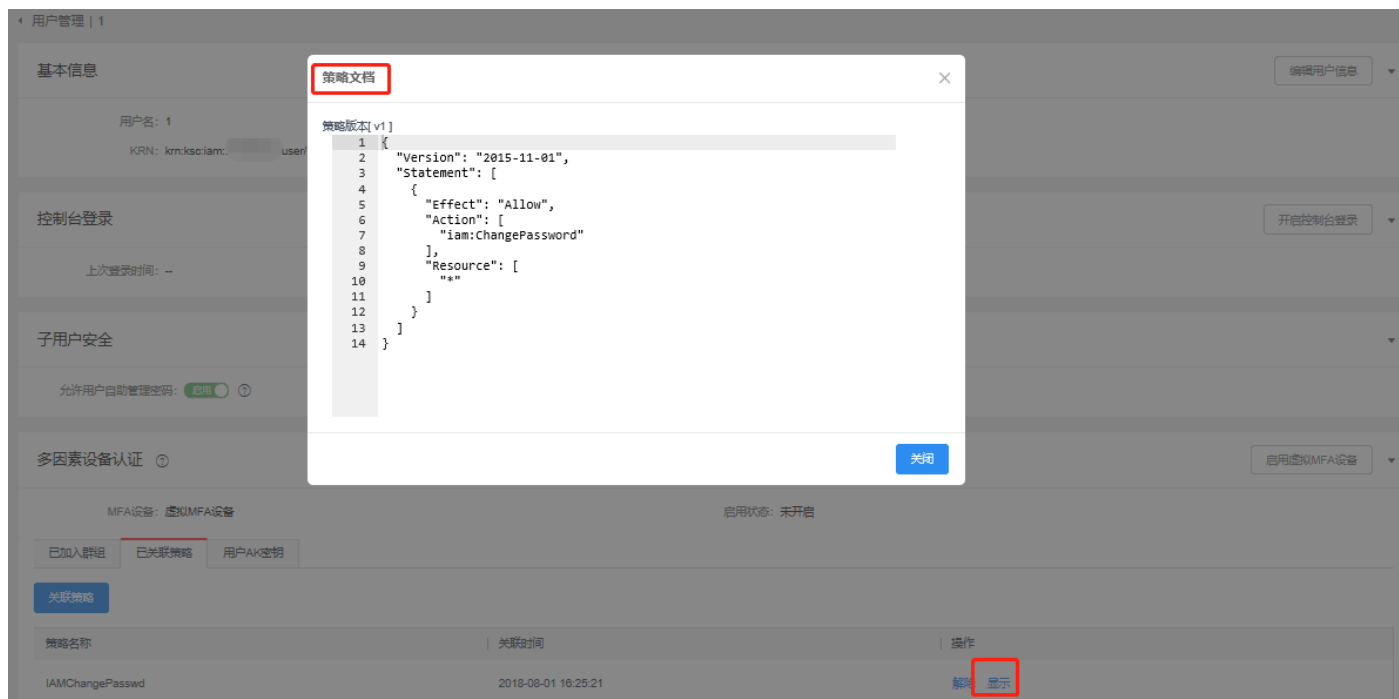
已加入群组 已关联策略 用户AK密钥

关联策略

策略名称	关联时间	操作
IAMChangePasswd	2018-08-01 16:25:21	解除 显示

解除后将无法获得该策略所描述的操作权限

确认解除 取消

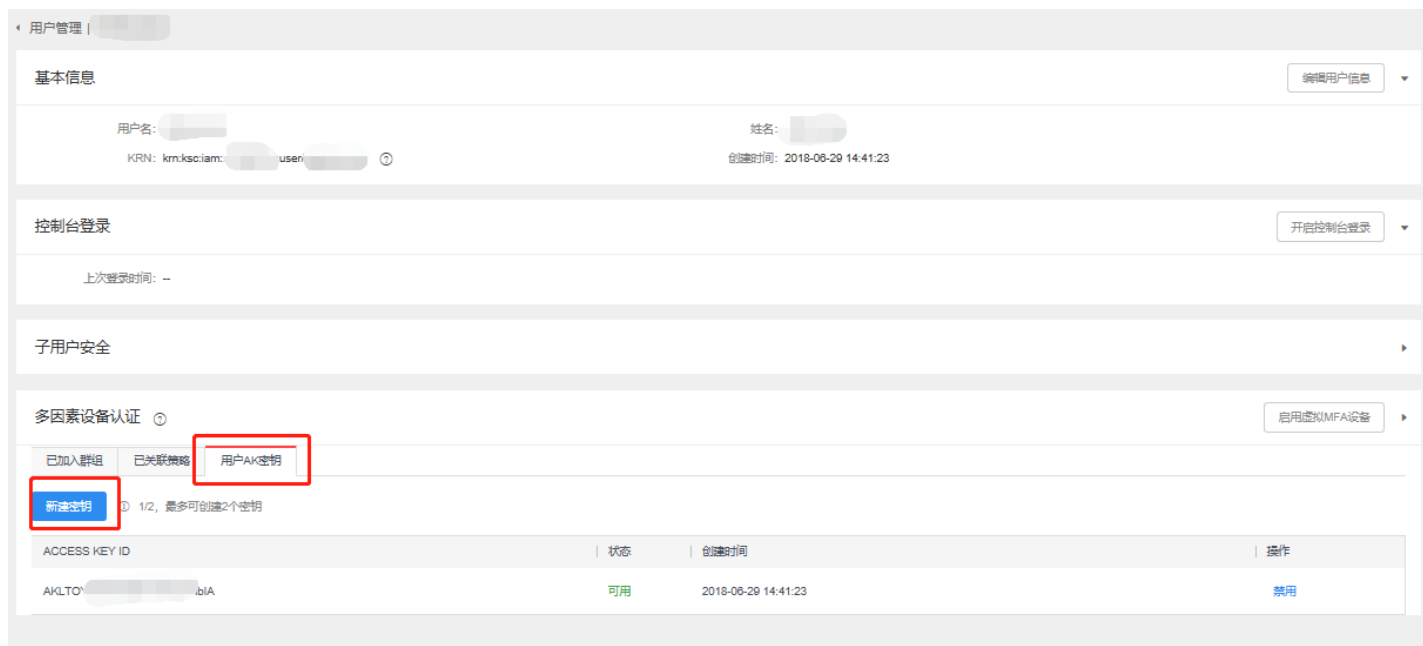


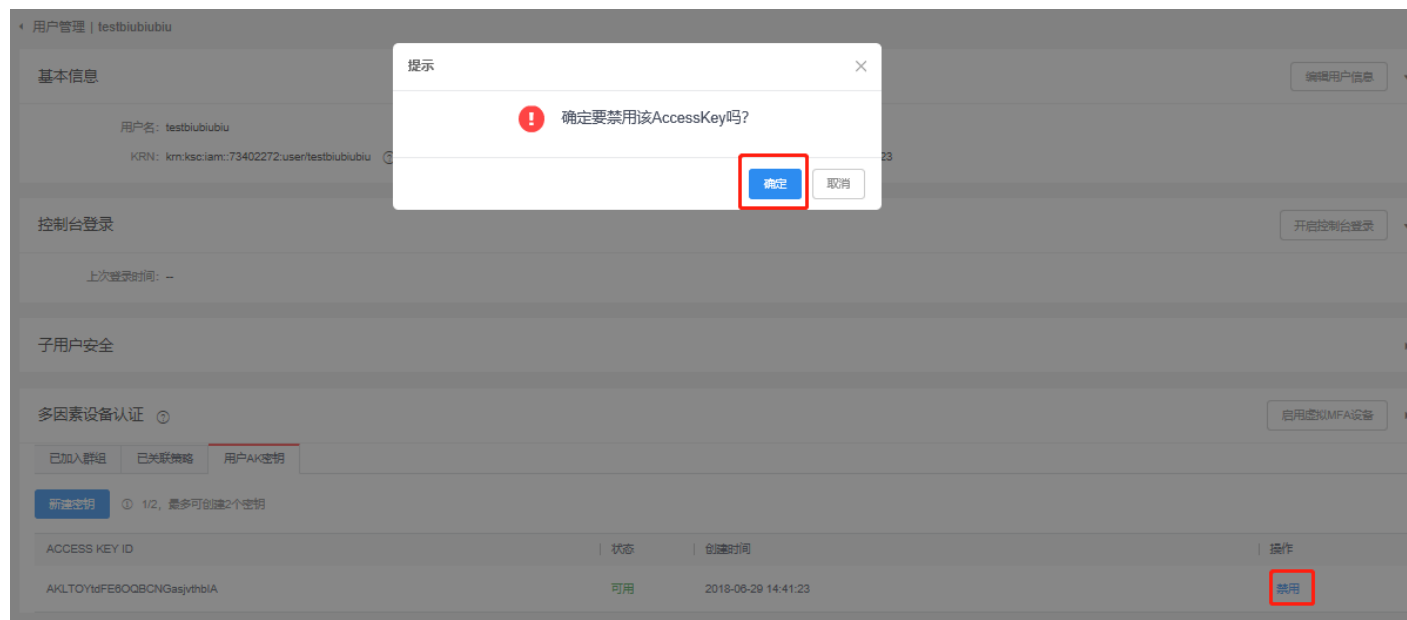
用户AK密钥

此处显示用户用户KA密钥信息，亦可编辑用户KA密钥信息

- 新建密钥：点击【新建密钥】即可为当前客户添加密钥，最多可创建2个密钥；
- 禁用密钥：点击【禁用】即可禁用该密钥。

注：此操作涉及敏感操作须进行验证，按提示操作即可





删除子账号

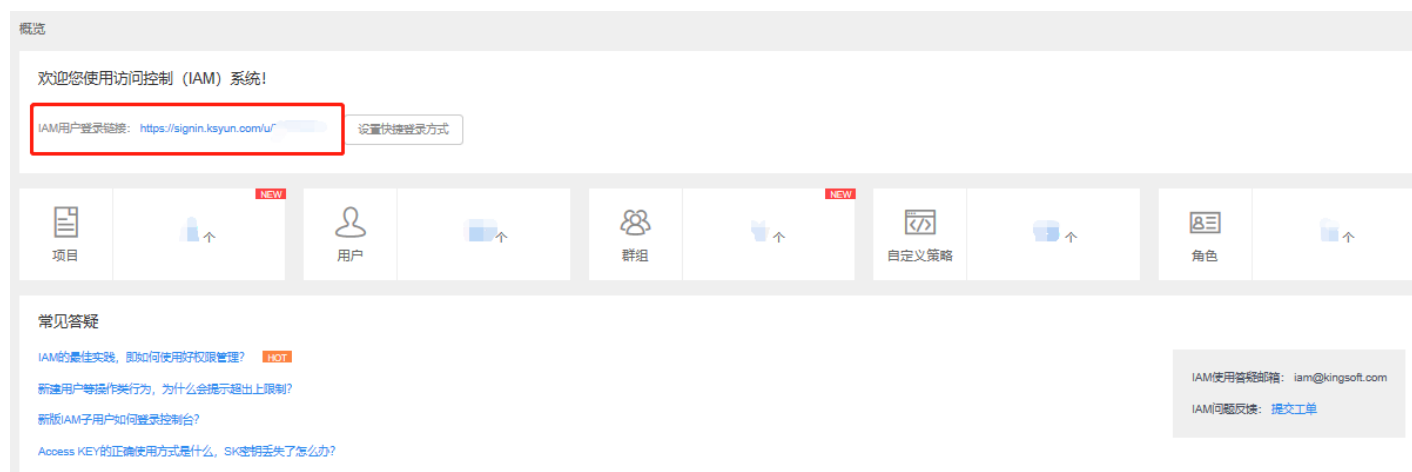
【用户管理】页面选中用户点击上方【删除】或直接点击用户操作中的【删除】即可将子账号删除 注：此操作涉及敏感操作须进行验证，按提示操作即可



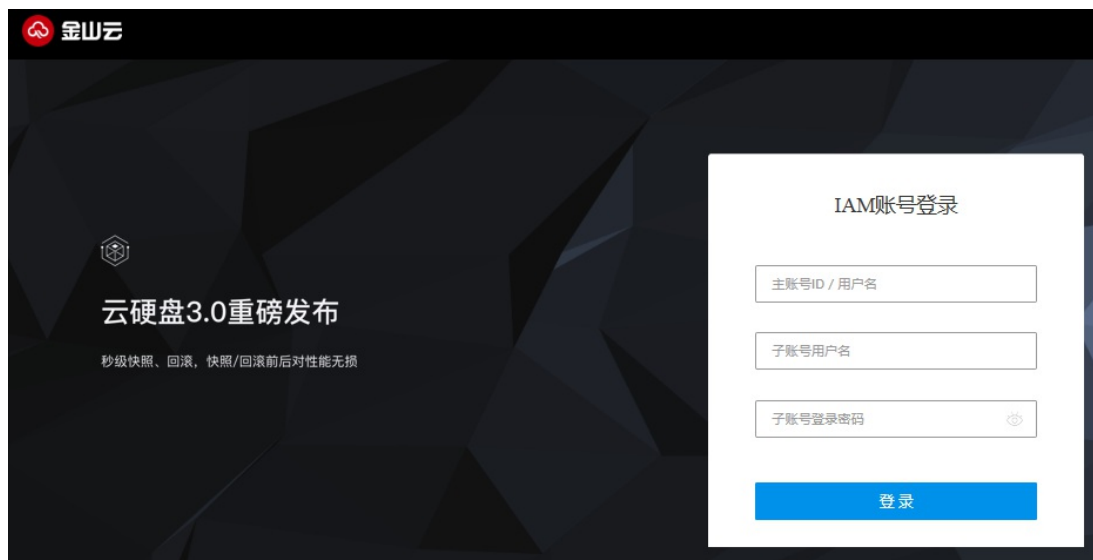
子账号用户登录

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，输入账号ID/用户名、子账号用户名和子账号密码即可登录

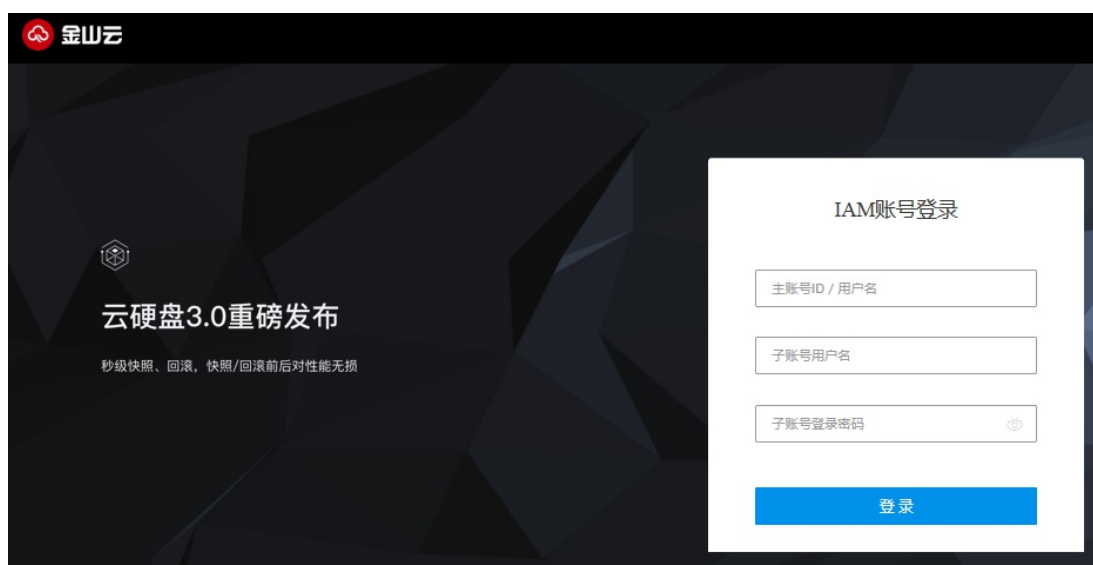


控制台登录页面登录

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

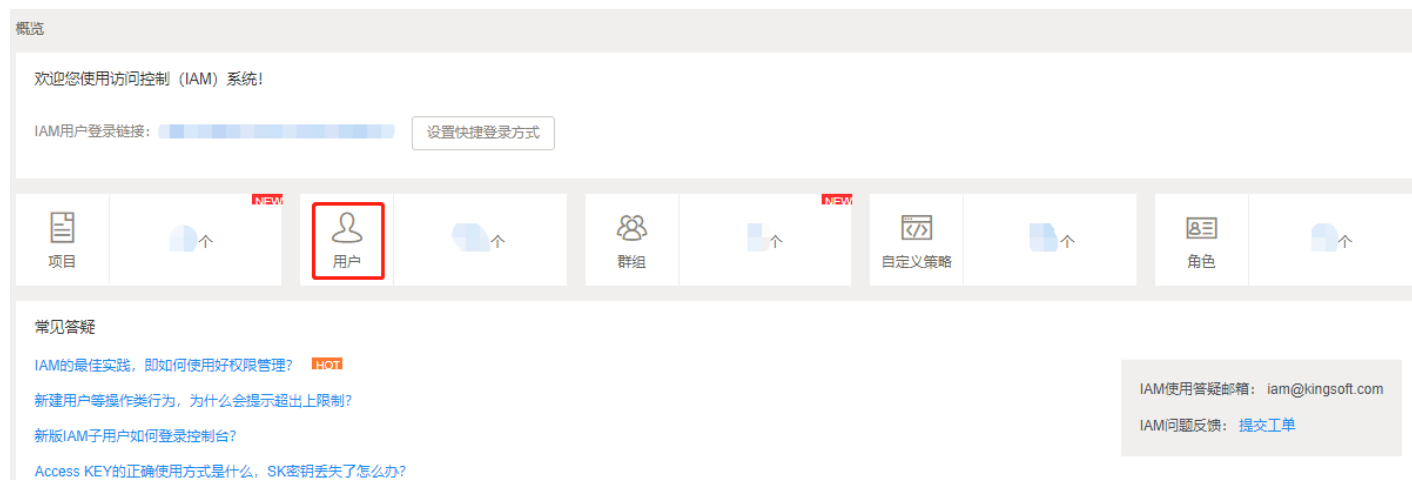
策略配置示例

本章主要介绍金山云权限配置示例。

- [CDN功能全部管理权限配置示例](#)
- [CDN功能查询管理权限配置示例](#)
- [CDN自定义用户权限部分资源配置示例](#)

CDN功能全部管理权限配置示例

第一步 登录[身份访问与控制](#)页面, 点击【人员管理】进入用户管理页面



第二步 进入用户管理页面, 点击【授权】



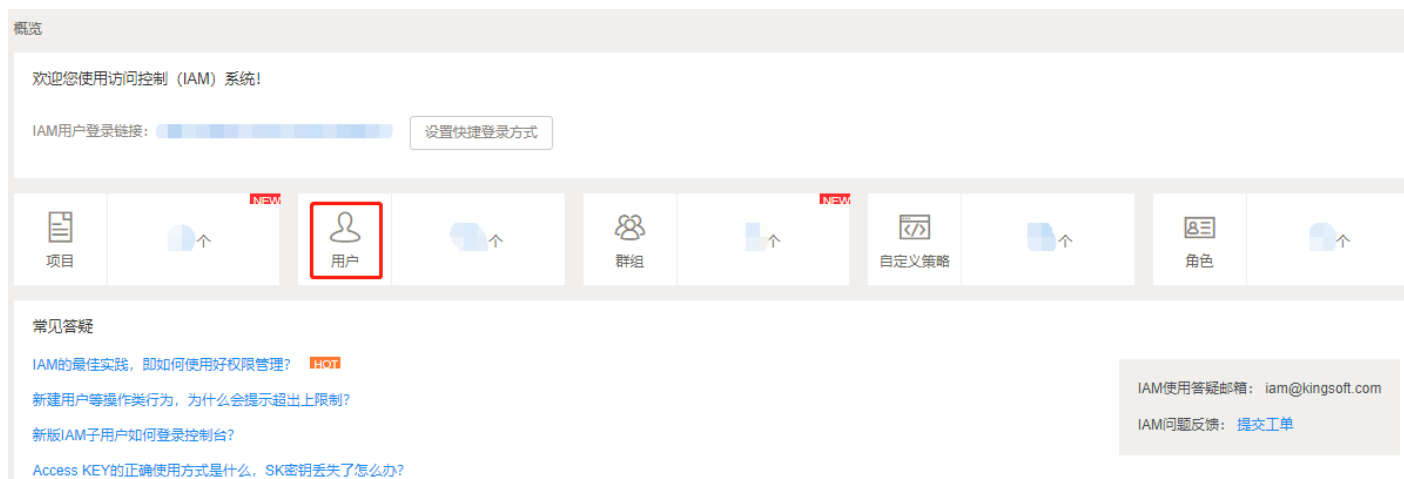
第三步 在授权策略列表中选择CDNFullAccess, 可通过上方搜索框进行搜索, 选择成功后点击【关闭】



此时便完成了子账号用户CDN功能全部管理权限的配置, 表明子账号具有主账号CDN的全部管理权限。

CDN功能查询管理权限配置示例

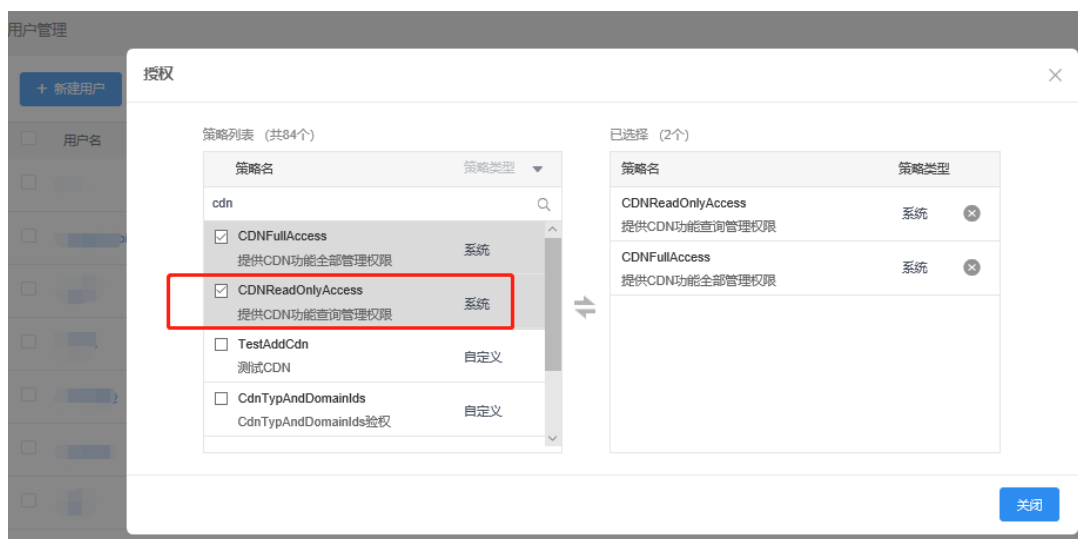
第一步 登录[身份访问与控制](#)页面, 点击【人员管理】进入用户管理页面



第二步 进入用户管理页面，点击【授权】



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



此时便完成了子账号用户CDN功能查询管理权限的配置，表明子账号具有主账号CDN的查询权限。

CDN自定义用户权限部分资源配置示例

背景：某客户在金山云服务的域名有20个，其中域名1-10是点播类业务，域名11-20是下载类业务，分属两个团队。现基于业务需要，需要创建两个子用户

资源	项目	子账号	权限
1	域名 1-10 VOD	son_1	FullAccess
2	域名 11-20 Download	son_2	内容管理

son_1 拥有点播类业务的全部权限，son_2拥有下载内容的刷新和预热权限

第一步 创建子账号 son_1 和son_2,

第二步 创建项目 VOD和Download,

起名VOD

添加成功

同理，创建Download；

第三步 修改项目信息。修改域名的项目归属，并将对应子账号添加到项目中。

勾选域名1-10，点击“更改项目组”为“VOD”

点击项目VOD，编辑成员，

添加son_1

同法，将son_2 添加到Download项目组，完成子用户和项目组的关联

第四步 创建并绑定策略。 son_1是FullAccess权限，所以使用系统权限模板即可，可以直接授权。

son_2是用户自定义权限，我们需要新建后，再绑定策略： 以“按业务权限创建”方式创建

启动“内容管理”

创建完成

点击“关联对象”

选择“son_2”

完成策略绑定

也可以通过“按策略生成器”、“按策略语法创建”完成创建，请参考[用户策略说明](#)