目录

产品概述

基本概念

- 账号（主账号、成员账号）

账号或称主账号是客户在金山云资源归属、资源计量、资源计费的主体。任何客户在使用金山云的服务前，都需要首先注册生成一个金山云账号，一般使用用户名作为账号的登录标识。

账号是其名下所有云计算资源的所有者，拥有名下全部资源的完全控制权限，能够对资源进行购买、续费、退订、升级等操作，拥有资源的订单、账单；云计算资源可被所属账号随意操作访问。

- 子用户

子用户是账号下的授权实体，也是归属于账号的一种资源。子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。

- 角色（role）

角色是一种虚拟用户（或影子用户），它是子用户类型的一种。这种虚拟用户有确定的身份，也可以被赋予一组权限(Policy)，但它没有确定的身份认证密钥（登录密码或AccessKey）。与普通子用户的差别主要在使用方法上，角色需要被授信给云账号（自己或其他云账号）使用，授信成功后云账号可依据实际情况赋予其下实体（子用户）扮演该角色，由此实体可获得该角色的临时安全令牌，使用这个临时安全令牌就能以角色身份访问被授权的资源，此时实体身份所对应的访问权限将被隐藏。

角色主要用于解决身份联盟(Identity Federation)相关需求，比如联合您的企业本地账号实现SSO（Single-Sign-On）、委托其他云账号及其下子用户操作您所控制的资源、委托云服务操作您所控制的资源。

- 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、EIP实例等；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，比如云服务器的创建、重启，KS3的bucket的创建等。数据操作是使用资源的动作，比如在云服务器中安装部署软件，在KS3的bucket上上传/下载对象。

管理操作都可以通过IAM进行授权控制，数据操作只有存储类产品如KS3才基于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。

产品设计思路

IAM服务允许在一个金山云账号下创建并管理多个子用户身份，并允许给每个子用户分配不同的授权策略(Policy)，从而实现不同子用户管理一个账号下不同的云计算资源的功能。

子用户身份是指通过控制台或openAPI操作金山云资源的人、系统或应用程序。IAM目前只支持一种身份标识，即子用户（IAM User），其有确定的身份和访问密钥，通常与某个人或者应用程序对应。

IAM允许在金山云账号下创建并管理多个授权策略，每个授权策略本质上是一组权限的集合。金山云账号可以将一个或多个授权策略分配给子用户。IAM授权策略语言可以表达精细的授权语义，可以指定对某个openAPI操作（Action）和资源（Resource）授权。

支持IAM功能的金山云产品/服务

产品/服务名称	英文缩写	控制台	openAPI
内容分发网络	CDN	暂不支持	支持
云主机	KEC	支持（新版）	支持
虚拟专有网路	VPC	支持（新版）	支持
弹性IP	EIP	支持（新版）	支持
负载均衡	SLB	支持（新版）	支持
访问控制	IAM	支持	支持
云物理主机	EPC	支持	支持
托管Hadoop	KMR	支持（服务粒度）	支持（服务粒度）
域名服务	DNS	支持	支持
安全服务	KAS	支持（服务粒度）	支持（服务粒度）
共享带宽	BWS	支持	支持

使用场景

集团公司集中管理子公司资源 （账号组——账号）

集团公司有多个子公司在金山云购买了云计算资源，每个子公司的云资源互相隔离，且财务独立核算，集团公司希望能够具备统一管理并查看这些公司云计算资源、订单和账单的权限。 账号组-账号适用于这种场景，既满足了资源隔离和财务独立核算的需求，也能够让集团公司集中管理、查询全部子公司的资源和财务情况。

企业内部云计算资源的分权管理和使用 （账号——子用户）

企业Alice在金山云购买多种云计算资源（如KEC实例/RDS实例/SLB实例/KS3存储等），其不同部门的员工需要操作这些资源，由于员工的职责不一样，所需要的权限也不一样。 为了降低企业信息安全风险，企业Alice不希望共享其云账号的密码/访问密钥给所有需要的员工（等于授权所有操作权限），而是希望给每个员工能够完成其工作的最小管理权限的用户账号（或称子用户），且这些用户账号的权限可以灵活赋予和收回，用户账号也可以被云账号随时禁用或删除。 用户账号只有在授权后能够操作相应资源，不需要独立的计量计费，成本开销都归属于企业Alice。 账号-子用户适用于这种场景，既满足了授权管理的需求，也降低了共享账号的风险。

不同企业之间的资源操作与授权管理 （跨账号——角色）

不同企业间需要进行云资源的共享。blue公司购买了金山的多种云资源后，将产品的运维工作转授给carry公司运营，carry公司希望可以进一步将blue的资源访问权限分配给员工qian或多个员工，并能够精细化随时控制员工对blue赋予资源的操作权限。如果双方合同到期， Blue公司可以撤销对 carry公司的授权。

操作过程如下：

一、blue创建角色D，添加carry为授信云账号，并附加角色D相应的策略。

二、carry创建子用户qian，并附加qian去扮演/切换角色的权限。

三、qian拥有了操作云账号blue下角色D关联策略的权限。

快速入门

为员工创建“子用户”账号并授权

当需要给员工授权访问某金山云账户下的云计算资源时，整体操作步骤如下：

1. 使用金山云主账户/密码登录控制台；
2. 创建子用户；
3. 为子用户设置登录密码或者创建访问密钥；
4. 为子用户添加授权策略；
5. 向员工提供子用户登录链接URL、用户名和登录密码或者访问密钥；
6. 员工使用子用户身份登录并使用控制台或者使用访问密钥调用openAPI；

创建子用户

1. 使用金山云账户/密码登录控制台（新版）；
2. 选择“访问控制”一级菜单->选择“人员管理”二级菜单；
3. 在“子用户”列表页面，点击“新建用户”按钮，进入“新建用户”对话框，如下图：

4. 子用户创建支持批量，可同时创建10个用户；在创建子用户的同时可以选择子用户访问方式；填写用户登录信息后，点击“确定”按钮，完成子用户的创建。

为子用户设置登录密码

1. 使用金山云账户/密码登录控制台（新版）；
2. 选择“访问控制”一级菜单->选择“人员管理”二级菜单；
3. 在“子用户”列表页面，点击某子用户名，进入“用户详情”页面，在“安全管理”栏，点击“控制台登录管理”旁边的“修改设置”按钮， 进入“修改设置”对话框，如下图：

4. 可以选择系统自动生成或者自定义用户密码，并可以指定要求用户在下次登录时创建新密码。

为IAM用户创建访问密钥

1. 使用金山云账户/密码登录控制台（新版）；
2. 选择“访问控制”一级菜单->选择“人员管理”二级菜单；
3. 在“子用户”列表页面，点击某子用户名，进入“用户详情”页面，在“安全管理”栏，点击“创建密钥”，最多可创建2个秘钥，如下图：

4. 可以选择直接显示安全凭证或者下载安全凭证，即访问密钥的详细信息。

为子用户添加授权策略

1. 使用金山云账户/密码登录控制台（新版）；
2. 选择“访问控制”一级菜单->选择“人员管理”二级菜单；
3. 在“子用户”列表页面，点击某子用户名，进入“用户详情”页面，在“”关联策略”栏，可以查看当前子用户已关联策略列表tab页，点击“添加权限”按钮新增关联策略，如下图：

查看子用户登录链接

1. 使用金山云账户/密码登录控制台（新版）；
2. 选择“访问控制”一级菜单->选择“概览”二级菜单；
3. 在“账户信息”页面，能够看到当前账户的子用户登录链接

4. 将登录链接发给子用户所属者，其可以使用子用户的登录入口来登录控制台并进行相应操作。

计费模式和开通说明

IAM服务是否收费？

IAM服务目前不收费。

如何申请开通使用账号组和IAM服务？

IAM服务针对所有金山云客户开放，只要拥有金山云账号，就可以登录控制台使用IAM的功能，不需要额外的申请开通。创建子用户成功后，子用户可以通过子用户专用登录入口：
https://passport.ksyun.com/iam-login.html 登录使用。

术语说明

术语	全称	中文	说明
Account	Member Account	账号（账户）	指一个金山云账号，账号是资源的拥有者，任何资源均隶属于某个账号
User	IAM User	子用户	指一个金山云账号下的IAM子用户(又称子用户)，子用户不拥有资源，能够操作主账号授予权限的资源
Role	IAM Role	角色	指一个金山云账号下创建的角色
KsyunId	Ksyun LoginId	金山云登录标识	指一个金山云账号的登录标识
AccountId	Ksyun AccountId	金山云账户ID	指一个金山云账户的ID（又称内标），为最长20位的数字标识
Policy	Authorization Policy	策略	指一个金山云账号下的授权策略，代表了一组权限（目标操作&目标资源）；金山云支持全局系统策略和自定义策略
Policy Document	Authorization Policy Document	策略文档	是授权策略的具体表现形式，目前为json格式的权限控制描述文档
IAM	Identity and Access Management	访问控制	金山云的身份管理、认证、授权和访问控制服务
AK	AccessKey	访问密钥	由AccessKeyId和SecretAccessKey组成，用于API请求的身份认证
AKId	AccessKeyId	访问密钥ID	指一个访问密钥的唯一标识
SK	SecretKey	私有访问密钥	指一个访问密钥的共享密钥，用于API签名
Entity		实体	指一种操作的发出者，金山云目前支持两种实体：账号和IAM用户
KRN	Kingsoft Resource Name	金山云资源名称	指金山云全局唯一的资源标识名称，用于在策略文档中标识资源，形如krn:ksc:<service-name>:<region-name>:<account-id>:<resourcetype>/<resource-id>
MFA	Multi-Factor Authentication	多因素身份验证	MFA是在用户名/口令之外额外增加的一种认证措施，因此能够提升用户账户的安全性。金山云目前提供虚拟MFA校验功能。
Group(Iam)	IAM Group	用户组	金山云多个相同职能的用户（IAM用户的集合）
Project		项目	项目是零到多个确定资源（KRN）的集合，等价于多个资源的KRN，IAM将账户下的资源进行逻辑划分