目录

产品简介

访问控制（ Identity and Access Management ，IAM）是金山云提供的管理用户身份与资源访问权限的基础服务。 可以实现安全且精细化管理金山云云服务和资源的访问。

产品功能

管理访问权限

访问控制允许在一个金山云账号下创建并管理多个身份，并允许给单个身份或一组身份分配不同的资源及操作权限。

当您的企业存在多用户协同操作资源的场景时，访问控制可以让您避免与其他用户共享金山云云账号密钥，按需为用户分配最小权限，从而降低企业的信息安全风险。

精细化的权限管理

可以针对不同的资源，授权给不同的人员不同的访问权限。 例如可以运行某些子用户拥有某个KEC实例的重启权限，而另外一些子用户没有某个KEC实例的重启权限。

通过用户组批量管理权限

您不需要为每个用户进行单独的授权，只需规划用户组，并将对应权限授予用户组，然后将用户添加至用户组中，用户就继承了用户组的权限。如果用户权限变更，只需在用户组中删除用户或将用户添加进其他用户组，实现快捷的用户授权。

跨金山云账号的资源授权

当一个企业希望将部分业务授权给另一个企业时，可以使用IAM角色进行跨云账号授权来管理资源的授权及访问。

设置账号安全策略

通过设置IAM子用户的登录验证策略、密码策略、敏感操作验证策略等来提高用户信息和系统数据的安全性。

联合身份认证

如果您已经有自己的身份认证系统，您不需要在金山云中重新创建用户，可以通过身份提供商功能直接访问金山云，实现单点登录。

访问方式

您可以通过以下任何一种方式使用访问控制相关功能。

- 管理控制台

  您可以通过基于浏览器的可视化界面，即控制台访问。

- OpenAPI

  您可以使用访问控制提供的OpenAPI接口以编程方式访问I。

使用场景

用户管理与分权

场景描述

企业A的某个项目上云，购买了多种金山云资源。其团队成员或应用程序需要使用资源 ，每个团队成员的职责不同，需要的权限也不同。为了降低企业信息安全风险，企业管理员 A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）。 企业A有如下要求：

- 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。
- 这些用户账号的权限可以灵活赋予和收回。
- 用户账号也可以被随时禁用或删除。

解决方案

您可以使用访问控制的用户管理功能，给员工或应用程序创建IAM子用户，并授予IAM子用户刚好完成工作所需的系统策略。

IAM子用户支持以下2种方式访问金山云资源：

- 通过IAM子用户的用户名或密码登录金山云控制台。
- 为IAM子用户分配AK密钥，应用程序可以使用分配额AK密钥调用相关OPENAPI接口。

资源分组与授权

场景描述

企业A有多个项目同时上云，每个项目都会用到多种云资源。企业只有1个云账号，云账号下有上百个实例。企业A希望项目独立管理，每个管理员各自能够独立管理项目人员及其访问权限。

解决方案

您可以使用访问控制和项目管理的功能实现以上诉求：

1. 按照应用创建多个项目，将资源加入到对应项目中。
2. 创建IAM子用户，并将IAM子用户加入到对应的项目成员中。
3. 为IAM子用户授予工作所需的系统策略。授权后对应IAM子用户只能管理已加入的项目的资源。

跨帐号的资源操作与授权

场景描述

企业A购买了多种金山云资源来开展业务，例如：KEC实例、RDS实例、SLB实例和KS3存储空间等。企业A希望将部分业务授权给企业B。 企业A有如下要求：

- 企业A希望能专注于业务系统，仅作为资源Owner。企业A希望可以授权账号B来操作部分业务，例如：云资源运维、监控以及管理等。
- 企业A希望当企业B的员工加入或离职时，无需做任何权限变更。企业B可以进一步将企业A的资源访问权限分配给企业B的IAM用户（员工或应用），并可以精细控制其员工或应用对资源的访问和操作权限。
- 企业A希望如果双方合同终止，企业A随时可以撤销企业B的授权。

解决方案

访问控制的角色管理支持授权其他云账号通过角色扮演方式访问控制台:

1. 企业A在其云账号下创建一个IAM角色，并为IAM角色授予合适的权限，允许金山云账号B使用该角色。
2. 企业B在其云账号下创建一个子用户。并且给子用户添加扮演/切换角色的权限 。
3. 企业B的员工可以使用子用户登录控制台，切换角色操作企业A授权的资源。
4. 如果双方合同终止，企业A只需要撤销企业B的云账号对IAM的角色使用权限。撤销后，企业B的下的所有子用户对IAM角色使用的权限将自动撤销

产品定价

访问控制（IAM）为免费产品，只要经过实名认证的金山云账号就可以直接使用，该产品暂不支持关闭。

实名认证流程请详见：

- 个人实名认证流程。
- 企业实名认证流程。

术语说明

金山云账号(Account)

当您首使用金山云时，需要注册一个账号， 该帐号是您的金山云资源归属、资源使用计费计量的主体，对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。

默认情况下， 资源只能被金山云账号所访问，任何其他用户访问都需要获得金山云账号的显式授权。金山云云账号就是操作系统的root或Administrator，所以我们有时称它为根账号或主账号。

身份(Identity)

访问控制中有三种身份：IAM子用户、用户组、IAM角色。 其中IAM子用户和用户组是IAM的一种实体身份类型，IAM角色是一种虚拟用户身份。 身份可以被被赋予一组权限策略 。

IAM用户(IAM User)

IAM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。

- 一个金山云账号下可以创建多个IAM用户，对应企业内的员工、系统或应用程序。
- IAM用户不拥有资源，不能独立计量计费，由所属金山云账号统一控制和付费。
- IAM用户归属于金山云账号，只能在所属金山云账号的空间下可见，而不是独立的金山云账号。
- IAM用户必须在获得金山云账号的授权后才能登录控制台或使用API操作金山云账号下的资源。

用户组(IAM Group)

用户组是IAM的一种实体身份类型，用户组可以对职责相同的IAM用户进行分类并授权，从而更好的管理用户及其权限。

- 在IAM用户职责发生变化时，只需将其移动到相应职责的用户组下，不会对其他IAM用户产生影响。
- 当用户组的权限发生变化时，只需修改用户组的权限策略，即可应用到所有IAM用户。

IAM角色(IAM Role)

IAM角色是一种虚拟用户，与实体用户（IAM子用户、用户组、IAM角色）和教科书式角色（Textbook role）不同。

- 实体用户：拥有确定的登录密码或访问密钥。如IAM子用户。
- 教科书式角色：教科书式角色或传统意义上的角色是指一组权限集合，类似于IAM里的权限策略。如果一个用户被赋予了这种角色，也就意味着该用户被赋予了一组权限，可以访问被授权的资源。
- IAM角色：IAM角色有确定的身份，可以被赋予一组权限策略，但没有确定的登录密码或访问密钥。IAM角色需要被一个受信的实体用户扮演，扮演成功后实体用户将获得IAM角色的安全令牌，使用这个安全令牌就能以角色身份访问被授权的资源。

根据IAM的可信实体不同，IAM支持以下2中类型的角色：

- **金山云账号**：允许金山云账号和其IAM用户所扮演的角色。扮演角色的IAM用户可以属于自己的金山云账号，也可以属于其他金山云账号。此类角色主要用来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**：允许受信身份提供商下的用户所扮演的角色。此类角色主要用于实现与金山云的单点登录（SSO）。

实体(Entity)

指一种操作的发出者，金山云目前支持两种实体：金山云账号和IAM子用户。

访问密钥(AccessKey)

由AccessKeyID和SecretAccessKey组成， 是调用金山云API接口的身份凭证，不能登录控制台。 AccessKeyID用于标识用户，SecretAccessKey用于验证用户的密钥。

权限(Permission)

权限是指是否允许用户对某种资源执行某种操作，权限分为：允许（Allow）或拒绝（Deny）。

权限策略(Policy)

权限策略是用语法结构描述的一组权限的集合，可以精确地描述被授权的资源集、操作集以及授权条件。

访问控制支持以下两种权限策略：

- 金山云管理的**系统策略**：统一由金山云创建，用户只能使用不能修改，策略的版本更新由金山云维护。
- 客户管理的**自定义策略**：用户可以自主创建、更新和删除，策略的版本更新由客户自己维护。

授权

授权是您将用户完成具体工作需要的权限策略授予给对应用户身份（IAM子用户、用户组、IAM角色）。对应用户身份获取到云服务权限后，可以对云服务进行操作。

多因素身份验证(MFA)

多因素认证是一种简单有效的最佳安全实践，在用户名和密码之外再增加一层安全保护。这些要素结合起来将为您的账号提供更高的安全保护。启用多因素认证后，再次登金山云时，系统将要求输入两层安全要素：

1. 第一层安全要素：用户名和密码
2. 第二层安全要素：多因素认证设备生成的验证码

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 。

金山云资源名称 （KRN）

为方便在策略文档中描述一个资源，我们使用KRN唯一标识一个金山云资源 。格式 形如krn:ksc:::/

使用限制

名称	配额
创建的子用户数量上限	1000
每个子用户同时拥有的访问密钥数量上限	2
每个主账户同时拥有的访问密钥数量上限	2
创建的自定义策略数量上限	200
每个自定义策略同时拥有的策略版本数量上限	5
每个子用户、角色同时可以附加的策略数量上限	60
每个自定义策略的策略文档字符数上限	2048
每个主账户下使用中的策略数量上限	500
每个主账户可以创建的角色数量上限	100
每个角色可配置的受信账号数量上限	20
每个主账户可以创建用户组数量上限	50
每个用戶組可以被附加的策略上限	10
每个用户可加入用户组上限	20
每个用户组可添加用户数量的上限	100

支持IAM的云服务

简介

访问控制（IAM）已支持对多数金山云产品服务进行权限管理，本文罗列了目前已与访问控制集成的服务，并提供每个服务支持的授权粒度、是否支持根据标签进行授权、系统策略等。

每个表格包含以下信息：

- 服务：支持访问控制的云服务名称，单击链接至对应的产品服务文档。
- 授权粒度： 当前服务提供的最小授权粒度。

  说明：其中授权粒度按照粒度粗细分为服务级、操作级和资源级三个级别。

  - 服务级： 将云服务作为一个整体进行授权。一个IAM用户只能处于对这个产品拥有所有权限和没有任何权限两种状态。
  - 操作级： API级别的授权。一个IAM用户可以对指定云服务的某类资源执行某几个指定的操作。 例如：授权某账号对云服务器服务进行只读操作。
  - 资源级：定义对特定资源是否有访问权限，这是最细的授权粒度.例如： 权一个IAM用户仅可对某一台云服务器进行重启操作。
- 根据标签进行授权：当前服务是否支持通过标签进行权限管理，“ ”表示支持，“-”表示暂不支持。
- 系统策略：当前云服务支持的系统策略，“-”表示暂无。

计算

云服务	授权级别	根据标签进行授权	系统策略

云服务器	资源级	√	KECAdminFullAccess：提供云主机全部操作管理的权限 KECFullAccess：提供云主机生命周期管理及映像管理的全部管理权限 KECReadOnlyAccess：提供云主机查询管理权限 KFSFullAccess：提供文件存储生命周期管理及映像管理的全部管理权限 KFSReadOnlyAccess：提供文件存储查询管理权限
云物理主机	操作级	√	EPCFullAccess：提供云物理主机功能全部管理权限 EPCReadOnlyAccess：提供云物理主机查询管理权限
容器实例	操作级	-	KCIFullAccess：容器实例完整操作权限 KCIReadOnlyAccess：容器实例只读权限
金山云容器引擎	操作级	-	KCEFullAccess：容器完整操作权限（含主机，网络，负载均衡，裸金属服务器，云盘） KCEReadOnlyAccess：容器只读权限
大米云主机	操作级	-	-

网络

云服务	授权级别	根据标签进行授权	系统策略
负载均衡	资源级	√	SLBConsoleFullAccess：提供负载均衡和EIP控制台全部管理权限 SLBConsoleReadOnlyAccess：提供负载均衡控制台查询功能全部管理权限 SLBFullAccess：提供负载均衡全部openAPI功能管理权限 SLBReadOnlyAccess：提供负载均衡查询openAPI的管理权限
虚拟私有网络	资源级	-	VPCConsoleFullAccess：提供虚拟专有网络和EIP控制台功能全部管理权限 VPCConsoleReadOnlyAccess：提供虚拟专有网络控制台查询功能全部管理权限 VPCFullAccess：提供虚拟专有网络全部openAPI接口管理权限 VPCReadOnlyAccess：提供虚拟专有网络查询openAPI接口管理权限
弹性ip	资源级	√	EIPConsoleFullAccess：提供弹性IP控制台功能全部管理权限 EIPConsoleReadOnlyAccess：提供弹性IP控制台查询功能全部管理权限 EIPFullAccess：提供弹性IP全部openAPI接口管理权限 EIPReadOnlyAccess：提供弹性IP查询openAPI接口管理权限
共享带宽	资源级	-	BWSConsoleFullAccess：提供共享带宽控制台功能全部管理权限 BWSConsoleReadOnlyAccess：提供共享带宽控制台查询功能全部管理权限 BWSFullAccess：提供共享带宽全部openAPI接口管理权限 BWSReadOnlyAccess：提供共享带宽查询openAPI接口管理权限

数据库

云服务	授权级别	根据标签进行授权	系统策略
云数据库KRDS	资源级	√	KRDSConsoleFullAccess：控制台完整权限。包括关系型数据库产品全部权限、以及查询主机列表、VPC列表和子网列表的权限，tag服务的操作权限，支付权限。 KRDSFullAccess：包括关系型数据库全部openAPI功能的权限 KRDSReadAccess：提供KRDS实例的只读权限 KRDSReadAccess-NoneData：控制台部分只读权限。包括关系型数据库产品的实例、参数组、安全组、日志权限。不包括备份页面的读取权限。
云数据库redis	资源级	√	KCSConsoleFullAccess：包括云数据库Redis产品全部权限、以及查询主机列表、VPC列表和子网列表的权限 KCSFullAccess：包括云数据库Redis产品全部openAPI功能的权限 KCSReadAccess：提供只读权限
云数据库MongoDB	操作级	-	MongoDBConsoleFullAccess：包括MongoDB型数据库产品全部权限、以及查询主机列表、VPC列表和子网列表的权限 MongoDBReadAccess：只读权限
分布式数据库	操作级	-	-
云数据库Memcached	操作级	√	MemcachedConsoleFullAccess：包括云数据库Memcached产品全部权限、以及查询主机列表、VPC列表和子网列表的权限 MemcachedFullAccess：包括云数据库Memcached全部openAPI功能的权限 MemcachedReadAccess：只读权限
分布式事务服务	操作级	-	-
云原生数据库KingDB	操作级	-	-

时序数据库InfluxDB	操作级	-	InfluxDBFullAccess：包括时序数据库InfluxDB产品全部权限、以及查询主机/云物理主机列表、VPC列表和子网列表的权限 InfluxDBReadAccess：包括时序数据库InfluxDB产品只读权限、以及查询主机/云物理主机列表、VPC列表和子网列表的权限
数据传输服务	操作级	-	DTSFullAccess：提供RDS控制台数据迁移服务全部管理权限
云数据库PostgreSQL	操作级	-	PostgreSQLFullAccess：PostgreSQL产品线全部策略，包括PostgreSQL产品线的只读权限，云主机产品线的列表权限，虚拟私有网络的Vpc和子网列表权限，tag全部权限 PostgreSQLReadOnlyAccess：PostgreSQL产品线只读策略，包括PostgreSQL产品线的只读权限，云主机产品线的列表权限，虚拟私有网络的Vpc和子网列表权限，tag查询权限
云数据库SQLServer	操作级	-	SQLServerFullAccess：SQLServer产品线全部策略，包括SQLServer产品线全部权限，云主机产品线的列表权限，虚拟私有网络的Vpc和子网列表权限，tag全部权限 SQLServerReadOnlyAccess：SQLServer产品线只读策略，包括SQLServer产品线的只读权限，云主机产品线的列表权限，虚拟私有网络的Vpc和子网列表权限，tag查询权限

存储与CDN

云服务	授权级别	根据标签进行授权	系统策略
内容分发网络	资源级	-	CDNFullAccess：提供CDN功能全部管理权限 CDNReadOnlyAccess：提供CDN功能查询管理权限
对象存储	资源级	-	KS3FullAccess：提供金山云对象存储的全部管理权限 KS3ReadOnlyAccess：提供金山云对象存储的只读权限
云硬盘	操作级	√	EBSFullAccess：提供EBS硬盘功能全部管理权限 EBSReadOnlyAccess：提供EBS硬盘信息查询管理权限
金山云边缘计算	操作级	-	-
高性能文件存储	资源级	-	KPFSFullAccess：提供金山云文件存储KPFS的全部管理权限 KPFSReadOnlyAccess：提供金山云文件存储KPFS的查询管理权限

视频服务

云服务	授权级别	根据标签进行授权	系统策略
云转码	操作级	-	KETFullAccess：提供云直播转码全部OpenAPI接口管理权限 KETReadOnlyAccess：提供云直播转码查询OpenAPI接口管理权限
云直播	操作级	-	KLSConsoleFullAccess：提供视频云直播控制台的全部权限 KLSConsoleReadOnlyAccess：提供视频云直播控制台的查询权限 KLSFullAccess：提供云直播全部OpenAPI接口管理权限 KLSReadOnlyAccess：提供云直播查询OpenAPI接口管理权限
金山云魔镜	操作级	-	-

大数据

云服务	授权级别	根据标签进行授权	系统策略
托管Hadoop集群	操作级	-	KMRFullAccess：提供KMR所有操作的权限
大数据云平台	操作级	-	-
查询引擎服务	操作级	-	KQESFullAccess：提供查询引擎服务权限
Elasticsearch服务	操作级	-	KESFULLAcess：提供KES操作全部权限
HBase服务	操作级	-	KHBaseFULLAcess：提供KHBase操作全部权限
日志服务	操作级	-	KlogReadOnlyAccess：- KsyunKLogDefaultPolicy：-

云安全

云服务	授权级别	根据标签进行授权	系统策略
高防IP	操作级	-	KADFullAccess：提供高防IP产品全部管理权限
高防防护包	操作级	-	KEADFullAccess：提供高防弹性IP产品全部管理权限 KEADReadOnlyAccess：提供高防弹性IP产品只读权限
服务器安全	服务级	-	KHSFullAccess：提供服务器安全产品全部管理权限
服务器安全-内部新版	操作级	-	KhsNewFullAccess：主机安全新版全部权限 KhsNewReadOnly：主机安全新版只读权限

Web应用防火墙	操作级	-	WAFFullAccess：提供web防火墙产品全部管理权限
密钥管理服务	操作级	-	KKMSConsoleFullAccess：提供密钥管理服务控制台功能全部管理权限 KKMSConsoleReadOnlyAccess：提供密钥管理服务控制台查询功能全部管理权限
证书管理	操作级	-	KCMFullAccess：提供证书管理产品全部管理权限 KCMReadOnlyAccess：提供证书管理产品查询权限
云安全管理中心	操作级	-	KSMFullAccess：提供云安全管理中心产品全部管理权限 KSMReadOnlyAccess：提供云安全管理中心产品只读权限
业务风险情报	操作级	-	BRIFullAccess：提供业务风险情报管理权限

开发与运维

云服务	授权级别	根据标签进行授权	系统策略
云监控	操作级	-	MonitorFullAccess：提供云监控openAPI全部管理权限 MonitorReadOnlyAccess：提供云监控openAPI只读管理权限
消息队列RabbitMQ	操作级	-	RabbitMQFullAccess：包括消息队列RabbitMQ产品全部权限、以及查询主机/物理主机列表、VPC列表和子网列表的权限 RabbitMQReadAccess：消息队列RabbitMQ产品线只读策略，包括RabbitMQ产品线的只读权限，云主机/云物理主机产品线的列表权限，虚拟私有网络的Vpc和子网列表权限
企业效能平台	操作级	-	KDFFullAccess：提供企业效能平台KDF的所有管理功能
api网关	操作级	-	-
微服务引擎	操作级	-	-

人工智能

云服务	授权级别	根据标签进行授权	系统策略
人工智能开发平台	操作级	-	-

企业应用

云服务	授权级别	根据标签进行授权	系统策略
云游戏	操作级	-	KCGFullAccess：提供云游戏全部openAPI接口管理权限

管理与审计

云服务	授权级别	根据标签进行授权	系统策略
操作审计	操作级	-	ActionTrailFullAccess：提供查询审计记录的权限
访问控制	资源级	-	BindVirtualMFADevice：子用户绑定虚拟MFA设备具有的权限 IAMChangePasswd：允许子用户修改自己的密码 IAMFullAccess：提供IAM功能的全部管理权限 IAMReadOnlyAccess：提供IAM查询管理权限 MFAmodifyAccess：允许用户管理MFA STSAssumeRoleAccess：提供STS服务AssumeRole接口的权限
标签v2	操作级	-	TAGFullAccess：标签（TAG）全读写访问 TAGReadOnlyAccess：标签（TAG）只读访问权限

用户中心

云服务	授权级别	根据标签进行授权	系统策略
财务	操作级	-	OrderReadOnlyAccess：财务只读权限 PayOrderAccess：订单支付权限 TradeAccountAccess：提供“费用中心-账户总览”页面的全部权限 TradeAccountAccess&CloudTicket：具备账户总览和云票模块的所有权限 TradeCouponsAccess：提供 “费用中心-现金券”页面的全部权限 TradeFullAccess：具有财务全部管理权限 TradeInvoiceManagementAccess：提供“费用中心-发票管理”页面的全部权限 TradeSettlementConfirmAccess：提供确认月结算单的权限 TradeSettlementFeedbackAccess：提供对月结算单进行问题反馈的权限 TradeSettlementReadOnlyAccess：提供查看月结算单的权限

联系人管理	操作级	-	ContactFullAccess：提供消息接收人管理和站内信管理的全部功能 SMSInMailReadOnlyAccess：提供站内信的只读权限 SMSReceiveReadOnlyAccess：提供消息接收人管理的只读权限
实时付费	操作级	-	-
统一账单	操作级	-	-
账单	操作级	-	BillFullAccess：通过OpenAPI获取账单数据权限

账号安全建议方案

安全保护

主账户和用户均启用 MFA

建议您为所有用户都绑定MFA（Multi-factor authentication，多因素认证），子用户的MFA设置在访问控制-人员管理-子用户的详情页面。

定期强制修改登录密码和轮转访问密钥

对主账户和子用户，建议定期强制修改登录密码并轮转访问密钥，这样即使安全凭证在不知情下泄露，由于定期轮转，其使用期限也受限，能够保障账户下云计算资源的安全。

提高密码的复杂度，降低弱口令破解、撞库风险

登录配置强密码策略，如混合使用中英文、符号、大小写，提高密码位数等措施。

使用子用户访问金山云

在日常进行云资源操作管理时，最大程度上减少主账号的身份凭证访问金山云的使用，更不要将身份凭证共享给他人，养成赋权子用户管理的习惯。

授权制约

遵循最小授权原则

最小授权原则是安全设计的基本原则，其要求给用户授权时，只授予满足工作所需要的权限的最小集合，从而防止过度授权而引起的权限滥用并降低账号泄露后的安全风险。

使用策略限制条件来增强安全性

建议您给用户授权时设置策略限制条件，约束生效场景，以增强安全等级。比如撰写策略时，condition配置（限制IP访问，地域，时间）等。

及时撤销无用权限

当一个子用户的身份由于工作职责变更而不再使用某些操作权限时，应当即使撤销该用户的权限。

权限配置

分离控制台与openAPI权限

不建议给一个子用户同时使用控制台和操作openAPI的权限。通常，对于员工，给予其子用户身份的登录密码并赋予相应操作权限，而对于系统或者应用程序，则给予其子用户身份的访问密钥。

不要为主账户创建访问密钥

由于主账户对名下资源拥有完全控制权限，包括所有控制台操作和openAPI访问，为避免主账户访问密钥泄露带来的灾难性损失，不建议为主账户创建访问密钥；建议通过创建子用户及其访问密钥，通过适当授权来执行必要操作控制。

将身份管理、策略及授权管理、操作与资源管理分离

为最大限度降低安全风险，需要将系统的权限进行较好的划分。在使用访问控制时，首先应该考虑将子用户的身份管理、策略及授权管理以及各产品的操作和资源管理权限进行分权，为每种权限建立不同的IAM用户并赋予不同的策略。

使用用户组功能给子用户分配权限

除了对子用户直接绑定授权策略，您可以通过新建群组的功能，来对差异化的职能用户进行赋权操作，并实现集中管理。可以通过为每个群组绑定合适的授权策略，依据组织变动调整或移除用户，即能实现群组内的所有用户共享相同的权限时时生效。