目录

产品简介

什么是访问控制

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。访问控制为免费产品，只要经过实名认证的金山云主账号就可以直接使用。

> 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主账号密钥，您可以创建子用户并按需为子用户分配最小权限，从而降低企业的安全风险。 使用访问控制前，您先需要拥有一个金山云主账号，然后您可以在主账号名下创建、管理子用户（例如员工、系统或应用程序），并可以控制这些子用户对资源的访问操作权限，对系统服务的访问操作权限（如账单查询、下载等）。

功能特性

1. 管理访问权限

在主账号名下创建子用户，管理每个子用户的账号信息、登录密码、访问密钥、多因素认证等。

2. 精细化的权限管理

控制子用户的访问权限，给子用户分配主账号下资源的访问和管理权限。

（1）丰富的权限策略：针对不同的资源，授权给不同的人员不同的访问权限。当前系统支持两种权限策略：

- 系统策略：IAM提供了多种满足日常运维人员职责所需要的系统权限策略。
- 自定义策略：如果系统权限策略不能满足您的需求，您还可以创建自定义权限策略。

（2）精细的控制粒度

- 支持在资源级和操作级给子用户、用户组和角色授予访问权限。
- 支持根据请求源IP区间、资源范围等条件属性创建更精细的资源访问控制策略。

3. 身份联合登录（单点登录SSO）

金山云提供SSO功能，支持用户使用企业身份提供商IdP账号单点登录金山云，无需再创建金山云账号。目前金山云支持两种SSO登录方式：

- 通过角色SSO：企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色来登录金山云。
- 通过用户SSO：企业员工在登录后，将以子用户身份访问金山云。

使用场景

场景	场景描述	企业要求	解决方案
子用户管理与授权	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： 1. 不希望多员工共享同一个主账号，共享主账号可能导致密码或访问密钥泄露。 2. 希望能给员工创建独立账号（操作员账号）并独立分配权限。 3. 希望员工的账号只能在授权的前提下操作资源，所有员工的账号的所有操作行为都有记录。 4. 希望随时可以撤销用户账号身上的权限，也可以随时删除其创建的用户账号。	1. 创建子用户：使用访问控制的子用户管理功能，给员工或应用程序创建子用户。 2. 为子用户授权：根据员工对资源所需的访问操作权限，授予子用户刚好完成工作所需的权限策略。

用户组管理与授权	企业A的某个项目上云，购买了多种金山云资源现在由企业A内部某个团队的多个员工一同管理云上资源，企业A需为该团队内的成员分配相同的访问管理权限。	企业A有如下要求： 1. 希望可以统一给所有团队成员授权，无需对每个用户单独操作授权。 2. 当该团队新加入某个成员时，只需将其移动到相应职责的组下，即可获得相同的权限 3. 当团队的权限发生变化时，只需修改组的权限策略，即可应用到所有团队成员里。	1. 创建用户组：使用访问控制的用户组管理功能，创建用户组。 2.为用户组添加子用户：将拥有相同权限策略的子用户添加到用户组里。 3. 为用户组授权：根据该用户组对资源拥有的权限，为用户组添加权限策略，对应到用户组内的每一个用户。
角色管理与授权	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： 1. 企业A希望能专注于业务系统，仅作为资源owner。 2. 企业A希望当企业B的员工加入或离职时，可以将企业A的资源访问权限分配给企业B的子用户（员工或应用）。 3. 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。	访问控制的角色管理支持授权其他金山云主账号通过角色扮演方式访问控制台。 1. 企业A在其主账号下创建一个角色，并为角色授予合适的权限，允许金山云主账号B使用该角色。 2. 企业B在其主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的主账号对角色使用权限。撤销后，企业B的下的所有子用户对角色使用的权限将自动撤销。
权限策略	企业A内部有多个团队，团队内有多个成员，每个成员所管理的资源以及对资源的操作权限不同。	企业A有如下要求： 1. 对不同的团队成员授予不同的管理权限 2. 对于常见的权限策略，金山云可以提供，企业直接使用。 3. 支持企业内部特殊的权限策略自定义。	访问控制支持以下两种权限策略： 1. 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。 2. 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
单点登录SSO	企业A已有自己内部的账号体系，希望企业内成员以这套账号体系管理使用金山云资源，不必在金山云主账号下为每一位组织成员创建子用户身份。	企业A有如下要求： 1. 无需为企业内每个成员创建金山云账号 2. 您希望根据用户在本地IdP中加入的组或者用户的某个特殊属性，来区分云上拥有的权限。当进行权限调整时，只需要在本地进行分组或属性的更改。 3. 您希望从金山云的登录页面开始发起登录，而非直接访问您IdP的登录页面。	使用金山云的SSO服务管理企业账号登录。目前金山云提供以下两种 SSO 方式： 1. 角色SSO：通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色来登录金山云。 2. 用户SSO：通过用户SSO，企业员工登录后将以子用户访问金山云
子用户安全设置	企业内部多个用户同时管理云上资源时，企业希望通过一些操作或验证来加强用户的账号安全，避免由于盗号带来的企业损失。	企业A有如下要求： 1. 对用户的登录密码强度要求可做限制要求。 2. 增加对用户的登录二次验证操作，提高其安全性。	访问管理提供安全设置与多因素认证功能。 1.安全设置：企业可对用户的密码强度进行设置，包含密码长度、密码有效期、密码必须包含策略、可尝试的错误密码次数等设置。 2. 多因素认证：在用户名和登录密码之外再增加一层安全保护。目前访问控制提供三种验证方式：虚拟MFA设备（金山云小程序）、手机号验证、邮箱验证，当用户登录控制台或进行敏感操作时的二次身份验证，以此保护您的账号更安全。
项目管理与授权	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个金山云主账号，主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。	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. 创建子用户，并将子用户加入到对应的项目成员中。 3. 为子用户授予工作所需的权限策略，授权后对应子用户只能管理已加入的项目的资源。

访问方式

完成主账号的注册登录后，您可以通过以下方式使用IAM管理子用户身份与资源访问权限：

1. 访问控制控制台：您可直接登录访问控制控制台完成相关操作。
2. OpenAPI：您可以使用访问控制提供的OpenAPI接口以编程方式访问。

基本概念

本文解释了IAM的基本概念，帮助您正确理解和使用IAM。

身份管理相关概念

概念	说明
主账号	开始使用金山云服务前，首先需要注册一个主账号，该帐号是您的金山云资源归属、资源使用计费计量的基本主体。主账号为其名下所拥有的资源付费，并对其名下所有资源拥有完全控制权限。 1. 个人认证：同一个证件信息默认仅支持一个金山云主账号认证。 2.企业认证：同一个企业主体，支持多个主账号同时认证。也就是说同一个企业主体下可以拥有多个UID不同的主账号。 3. 默认情况下，资源只能被主账号所访问，任何其他用户访问都需要获得主账号的授权。可以创建子用户并为子用户设置权限。
子用户	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。 1. 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。 2. 子用户不拥有资源，不能独立计量计费，由所属主账号统一控制和付费。 3. 子用户归属于主账号，只能在所属主账号的空间下可见，而不是独立的主账号。 4. 子用户必须在获得主账号的授权后才能登录控制台或使用API访问操作主账号下的资源。
用户组	用户组是多个相同职能的子用户的集合，客户可以根据业务需求创建不同的用户组。 1.创建用户组，为用户组关联权限策略，把子用户加入到用户组，实现为多个不同的子用户分配相同的权限。 2. 在子用户权限发生变化时，只需将其移动到相应权限的用户组下，不会对其他子用户产生影响。 2. 当用户组的权限发生变化时，只需修改用户组的权限策略，即可应用到所有子用户。
角色	角色：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。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3种类型的角色： 1. 金山云账号：允许金山云账号和其子用户所扮演的角色。扮演角色的子用户可以属于自己的金山云主账号，也可以属于其他金山云主账号。此类角色主要用来解决跨账号访问和临时授权问题。 2. 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。 3. 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）。
访问密钥	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。
SSO	金山云支持基于SAML 2.0的SSO（Single Sign On，单点登录），也称为身份联合登录。 金山云支持两种 SSO 登录方式： 1. 通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色来登录金山云。 2. 通过用户SSO，企业员工在登录后，将以子用户身份访问金山云。
多因素身份验证	多因素认证是一种简单有效的安全实践，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，再次登录金山云时，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 （1）MFA：金山云小助手小程序验证码验证 （2）邮箱：绑定邮箱验证 （3）手机号：绑定手机号验证

访问控制相关概念

概念	说明
权限	权限对应的范围包含两个方面：（1）是否允许用户对资源的访问操作管理权限（2）是否允许用户对控制台功能的操作管理权限。权限分为：允许（Allow）或拒绝（Deny）。
权限策略	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： 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。 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。
授权主体	获得策略中定义的权限主体，授权主体可以为子用户、用户组或角色。

效果	权限策略基本元素之一，表示授权效果。取值为：允许（Allow）或拒绝（Deny）。
操作	权限策略基本元素之一，表示对具体资源的操作。
条件	权限策略基本元素之一，表示授权生效的条件。
资源	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 。

使用限制

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

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级别、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：

- 云服务：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。
- 授权级别： 当前服务提供的最小授权级别。

  说明：其中授权级别分为服务级、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。一个子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。一个子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，这是最小的授权级别。例如：一个子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
裸金属服务器	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

网络

云服务	授权级别	根据标签进行授权	系统策略
经典型负载均衡	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
关系型数据库(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
DDoS原生高防	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	-	-

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

密码管理

提高密码复杂度：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。 避免密码共享：为每个

人创建专属账号，并分配相应权限，坚决避免密码共享，多人共用账号。

密钥管理

不使用主账号密钥：主账号对名下资源拥有完全控制权限，为避免主账户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。 规范使用子用户密钥：合理限制子用户权限，子用户密钥闲置需及时处理，避免长期限制。

多因素认证管理

建议您为所有用户都启用多因素认证，在用户名和登录密码之外再增加一层安全保护。目前访问控制提供三种验证方式：虚拟MFA设备（金山云小程序）、手机短信验证、邮箱验证，当用户登录控制台或进行敏感操作时的二次身份验证，以此保护您的账号更安全。

权限管理

建议	方案详情
使用子用户访问金山云资源	在日常进行云资源操作管理时，最大程度上减少使用主账号的身份凭证访问金山云资源，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。
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。
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，您可以通过新建用户组的功能，来对差异化的职能用户进行赋权操作，并实现集中管理。可以通过为每个用户组赋予合适的授权策略，依据组织变动调整或移除用户，即能实现用户组内的所有用户共享相同的权限时生效。
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。
将身份管理、策略及授权管理、操作与资源管理分离	当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子用户并赋予不同的策略。