访问控制

产品简介

产品简介

产品概述

RAM (Resource Access Management) 是阿里云为客户提供的 **用户身份管理** 与 **资源访问控制** 服务。使用 RAM，您可以创建、管理用户账号（比如员工、系统或应用程序），并可以控制这些用户账号对您名下资源具有的操作权限。当您的企业存在多用户协同操作资源时，使用 RAM 可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，从而降低您的企业信息安全风险。

使用 RAM 进行身份管理和资源访问控制

RAM 允许在一个云账户下创建并管理多个用户身份，并允许给单个身份或一组身份（Identity）分配不同的授权策略（Policy），从而实现不同用户拥有不同的云资源访问权限。

用户身份

RAM 用户身份是指任意的通过控制台或 OpenAPI 操作阿里云资源的人、系统或应用程序。为了支持多种应用场景的身份管理，RAM 支持两种不同的用户身份类型：RAM-User 和 RAM-Role。

> RAM-User 是一种实体身份，有确定的身份 ID 和身份认证密钥，它通常与某个确定的人或应用程序一一对应。
>
> RAM-Role 是一种虚拟身份，有确定的身份 ID，但没有确定的身份认证密钥。

RAM-Role 需要与某个实体身份进行关联之后才能被使用。一个 RAM-Role 可以与多种实体身份关联，比如可以与当前云账号下的 RAM-User 关联，与其它云账号下的 RAM-User 关联，与阿里云服务（EMR/MTS/...）关联，与外部实体身份（如企业本地账号）关联。

授权策略

RAM 允许在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。管理员可以将一个或多个授权策略分配给 RAM 用户（包括 RAM-User 和 RAM-Role）。

RAM 授权策略语言可以表达精细的授权语义，可以指定对某个 API-Action 和 Resource-ID 授权，也可以支

持多种限制条件（源 IP、访问时间、多因素认证等）。

云账户 vs RAM 用户

从 **归属关系** 上看，云账户与 RAM 用户是一种主子关系。

云账户是阿里云资源归属、资源使用计量计费的基本主体。

RAM 用户只能存在于某个云账户下的 RAM 实例中。RAM 用户不拥有资源，在被授权操作时所创建的资源归属于主账户；RAM 用户不拥有账单，被授权操作时所发生的费用也计入主账户账单。

从 **权限角度** 看，云账户与 RAM 用户是一种 root 与 user 的关系（类比 Linux系统）。

Root 对资源拥有一切操作控制权限。

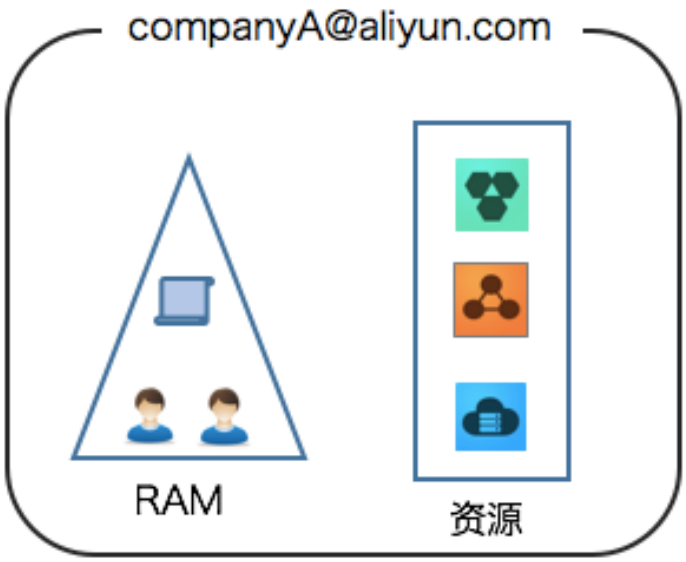
User 只能拥有被 root 所授予的某些权限，而且 root 在任何时刻都可以撤销 user 身上的权限。

使用 RAM 进行企业级云资源管理

RAM 适用具有如下特点的企业场景：

- 希望很简单就能管理每个操作人员（或应用）的账号及权限。
- 不需要分别核算每个操作人员（或应用）的成本和费用。

其具体需求如下图所示：



- 您的企业只需使用一个云账号(比如 companyA@aliyun.com)。
- 所有资源都归属于该云账号的名下，云账号是资源的 Owner（掌握完全控制权的人），也是账单的支付者。
- 通过 RAM 为您名下的操作员（对资源进行运维管控操作）创建独立的用户账号并进行授权管理。
- 用户账号不拥有资源（对其所创建的资源默认没有访问权限），只能操作被授权的资源。
- 用户账号操作所发生费用都计入主账号名下，不支持用户账号的独立计量计费。

功能特性

RAM 帮助您进行 **用户身份管理** 和 **资源访问控制** ，具体提供以下功能：

集中控制 RAM 用户及其密钥

在云账号下创建并管理用户及其访问密钥，并为用户绑定/解绑多因素认证设备。

集中控制 RAM 用户的访问权限

为每个用户或用户组绑定一个或多个授权策略，限制用户对指定资源的操作权限。

集中控制 RAM 用户的资源访问方式

要求用户必须使用安全信道（如SSL）、在指定时间范围、或在指定源 IP 条件下才能操作指定的云资源。

集中控制 RAM 角色与外部账号的身份联盟管理

使用 RAM 角色与外部身份系统（比如您的企业本地域账号、您的 App 用户账号）进行关联，实现直接使用外部身份登录到一个 RAM 角色身份访问阿里云控制台或 API。

集中控制云资源

对用户创建的实例或数据进行集中控制。当用户离开您的组织时，这些实例或数据仍然受您的完全控制。

统一账单

云账户接收包括所有 RAM 用户的资源操作所发生的费用的单一账单。

应用场景

RAM 的典型应用场景包括：企业子账号管理与分权、不同企业之间的资源操作与授权管理，和针对不可信客户端 app 的临时授权管理。

企业子账号管理与分权

企业 A 购买了多种云资源（如 ECS 实例/ RDS 实例/ SLB 实例/ OSS 存储桶/...），A 的员工需要操作这些云资源，比如有的负责购买，有的负责运维，还有的负责线上应用。由于每个员工的工作职责不一样，需要的权限也不一样。

需求说明：

> 出于安全或信任的考虑，A 不希望将云账号密钥直接透露给员工，而希望能给员工创建相应的用户账号。
>
> 用户账号只能在授权的前提下操作资源，不需要对用户账号进行独立的计量计费，所有开销都算在 A 的头上。
>
> A 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。

不同企业之间的资源操作与授权管理

A 和 B 代表不同的企业。A 购买了多种云资源（如 ECS 实例/ RDS 实例/ SLB 实例/ OSS 存储桶/...）来开展业务。

需求说明：

A 希望能专注于业务系统，而将云资源运维监控管理等任务委托或授权给企业 B。

企业 B 可以进一步将代运维任务分配给 B 的员工，B 可以精细控制其员工对 A 的云资源操作权限。

如果 A 和 B 的这种代运维合同终止，A 随时可以撤销对 B 的授权。

针对不可信客户端 app 的临时授权管理

企业 A 开发了一款移动 app，并购买了 OSS 服务。移动 app 需要上传数据到 OSS（或从 OSS 下载数据）。

需求说明：

A 不希望所有 app 都通过 appServer 来进行数据中转，而希望让 app 能直连 OSS 上传/下载数据。

由于移动 app 运行在用户自己的终端设备上，这些设备并不受 A 的控制。出于安全考虑，A 不能将访问密钥保存到移动 app 中。

A 希望将安全风险控制到最小，比如，每个移动 app 直连 OSS 时都必须使用最小权限的访问令牌，而且访问时效也要很短（比如 30 分钟）。

相关术语

本文罗列了 RAM 中用到的主要术语，帮助您正确理解和使用 RAM。

身份管理相关术语

云账户（主账户）

云账户是阿里云资源归属、资源使用计量计费的基本主体。当用户开始使用阿里云服务时，首先需要注册一个云账户。云账户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权限。

默认情况下，资源只能被属主（ResourceOwner）所访问，任何其他用户访问都需要获得属主的显式授权。所以从权限管理的角度来看，云账户就是操作系统的 root 或 Administrator，所以我们有时称它为 **根账户** 或 **主账户**。

云账户别名（Alias）

每个云账户可以在 RAM 中为自己设置一个全局唯一的别名。别名主要用于 RAM 用户登录以及成功登录后的显示名。

比如，云账号 admin@abc.com 为自己设置一个别名为 abc.com，那么其名下的 RAM 用户 alice 成功登录后，显示名就是 alice@abc.com。

身份凭证（Credential）

身份凭证是用于证明用户真实身份的凭据，它通常是指登录密码或访问密钥（Access Key）。身份凭证是秘密信息，用户必须保护好身份凭证的安全。

> **登录名/密码（Password）**。您可以使用登录名和密码登入阿里云控制台，查看订单、账单或购买资源，并通过控制台进行资源操作。
>
> **访问密钥（AccessKey）**。您可以使用访问密钥构造一个 API 请求（或者使用云服务 SDK）来操作资源。
>
> **多因素认证（MFA）**。Multi-Factor Authentication, 是一种简单有效的最佳安全实践方法，它能够在用户名和密码之外再额外增加一层安全保护。启用 MFA 后，用户登录阿里云网站时，系统将要求输入用户名和密码（第一安全要素），然后要求输入来自其MFA设备的可变验证码（第二安全要素）。这些多重要素结合起来将为您的账户提供更高的安全保护。

RAM 用户

RAM 允许在一个云账户下创建多个 RAM 用户（可以对应企业内的员工、系统或应用程序）。RAM 用户不拥有资源，没有独立的计量计费，这些用户由所属云账户统一控制和付费。RAM 用户是归属于云账户，只能在所属云账户的空间下可见，而不是独立的云账户。RAM 用户必须在获得云账户的授权后才能登录控制台或使用 API 操作云账户下的资源。

RAM 用户有两种身份类型：RAM-User 和 RAM-Role。

- RAM-User 是一种实体身份类型，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。
- RAM-Role 是一种虚拟身份类型，它没有确定的身份凭证，它必须关联到某个实体身份上才能使用。

RAM-Role

RAM 角色。传统意义上的角色（教科书式角色）是指一组权限集合，它类似于 RAM 里的 Policy。如果一个用户被赋予了某种角色，也就意味着该用户被赋予了一组权限，然后该用户就能访问被授权的资源。

RAM 角色不同于教科书式角色。RAM 角色是一种虚拟用户（或影子账号），它是 RAM 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 RAM 用户的差别主要在使用方法上，RAM 角色需要被一个授信的实体用户扮演，扮演成功后实体用户将获得 RAM 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。

RAM-Role 与 Textbook-Role（教科书式角色）的差异如下：

- （相同点）RAM-Role 和 Textbook-Role 都可以绑定一组权限集。

  （不同点）RAM-Role 是一种虚拟身份或影子账号，它有独立的身份 ID，除了绑定权限之外，还需要指定演员列表（Roleplayers），它主要用于解决与身份联盟（Identity Federation）相关的问题。Textbook-Role 通常只表示一组权限的集合，它不是身份，主要用于简化授权管理。

  RAM-Role 的扮演与切换：

  从登录身份切换到角色身份（SwitchRole）：一个实体用户（比如 RAM-User）登录到控制台后，可以选择 **切换到某个角色**，前提是这个实体用户已经被关联了角色。每次只能切换进入某一种角色。当用户从 **登录身份** 进入 **角色身份** 时，用户只能使用角色身份上所绑定的权限，而登录身份上绑定的权限会被屏蔽。如果需要使用登录身份的权限，那么需要从角色身份切换回到登录身份。

  从实体身份通过程序调用方式扮演角色（AssumeRole）：如果一个实体用户（比如 RAM-User）关联了某个 RAM-Role，那么该用户可以使用访问密钥（AccessKey）来调用 STS 服务的 AssumeRole 接口来获得这个 RAM-Role 的一个临时访问密钥。临时访问密钥有过期时间和受限制的访问权限（不会超过该角色所绑定的权限集），通常用于解决临时授权问题。

访问控制相关术语

资源（Resource）

资源是云服务呈现给用户与之交互的对象实体的一种抽象，如 OSS 存储桶或对象，ECS 实例等。

我们为每个资源定义了一个全局的阿里云资源名称（Aliyun Resource Name, ARN）。格式如下：

```
acs:<service-name>:<region>:<account-id>:<resource-relative-id>
```

格式说明：

- acs: Alibaba Cloud Service 的首字母缩写，表示阿里云的公有云平台。
- service-name: 阿里云提供的 Open Service 的名字，如 ecs, oss, odps 等。
- region: 地区信息。如果不支持该项，可以使用通配符“*”号来代替。
- account-id: 账号 ID，比如 1234567890123456。
- resource-relative-id: 与 service 相关的资源描述部分，其语义由具体 service 指定。以 OSS 为例，acs:oss::1234567890123456:sample_bucket/file1.txt 表示公有云平台 OSS 资源，OSS 对象名称是 sample_bucket/file1.txt，对象的 Owner 是 1234567890123456。

权限（Permission）

权限分为：允许（Allow）或拒绝（Deny）一个用户对某种资源执行某种操作。

操作可以分为两大类：**资源管控操作** 和 **资源使用操作**。

> 资源管控操作是指云资源的生命周期管理及运维管理操作，比如 ECS 的实例创建、停止、重启等，OSS 的 Bucket 创建、修改、删除等；所面向的用户一般是资源购买者或您组织内的运维员工。
>
> 资源使用操作是指使用资源的核心功能，比如 ECS 实例操作系统中的用户操作，OSS Bucket 的数据上传/下载；所面向的用户一般是您组织内的研发员工或应用系统。
>
> **注意**：对于弹性计算和数据库产品，资源管控操作可以通过 RAM 来管理，而资源使用操作是在每个产品的实例内进行管理，比如 ECS 实例操作系统的权限控制，MySQL 数据库提供的权限控制。单对于存储类产品，如 OSS, Table Store 等，资源管控操作和资源使用操作都可以通过 RAM 来管理。

授权策略（Policy）

授权策略是描述权限集的一种简单语言规范。RAM 支持的语言规范请参见 **授权策略语言**。 RAM 支持两种类型的授权策略：云平台管理的 **系统访问策略** 和客户管理的 **自定义访问策略**。

> 对于阿里云管理的系统访问策略，用户只能使用，不能修改，阿里云会自动完成系统访问策略的版本更新。
>
> 对于客户管理的自定义访问策略，用户可以自主创建和删除，策略版本由客户自己维护。

支持 RAM 的云服务

许多阿里云服务都与 RAM 相集成，本文按服务类别罗列了这些服务，并提供每个服务支持的 RAM 授权粒度、系统策略，以及相关 RAM 文档的链接，方便您使用及查询。

在集成 RAM 功能时，各产品针对子用户定义了不同级别的授权粒度，具体有：

- 服务级别：将云产品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。
- 操作级别：在 API 级别进行授权；一个子用户可以对指定云产品的某类资源执行某几个指定的操作。
- 资源级别：对执行资源的指定操作进行授权，这是最细的授权粒度；例如：授权一个子用户仅可对某

一台云服务器进行重启操作。

支持 RAM 的云服务列表

以下表格分别罗列了 弹性计算、云数据库、存储与 CDN、网络、分析、云通信、监控与管理、应用服务、互联网中间件、移动服务、视频服务、大数据（数加）、安全（云盾）、云市场、域名与网站下，已支持 RAM 的云服务。每个表格具体包含如下信息：

- 服务名：支持 RAM 的云服务的名称。
- 控制台：当前服务是否支持在控制台进行访问控制，“√”表示支持，“×”表示不支持，“○”表示不提供。
- API：当前服务是否支持通过 API 进行访问控制，“√”表示支持，“×”表示不支持，“○”表示不提供。
- 授权粒度：当前服务提供的最小授权粒度。
- 系统策略：当前服务支持的系统策略。
- 相关文档：当前服务应用 RAM 相关的文档链接。

弹性计算

服务名	控制台	API	授权粒度	系统策略	相关文档
云服务器 ECS	√	√	资源级别	AliyunECSFullAccess AliyunECSReadOnlyAccess	ECS 鉴权规则
负载均衡 SLB	√	√	资源级别	AliyunSLBFullAccess AliyunSLBReadOnlyAccess	SLB 鉴权规则
弹性伸缩 AutoScaling	√	√	服务级别	AliyunESSFullAccess AliyunESSReadOnlyAccess	弹性伸缩 API 使用须知
容器服务	√	√	服务级别	-	容器服务 访问控制
资源编排 ROS	√	√	服务级别	-	资源编排 使用 RAM
批量计算 BatchCompute	√	√	服务级别	AliyunBatchComputeFullAccess	-

云数据库

服务名	控制台	API	授权粒度	系统策略	相关文档
云数据库	√	√	资源级别	AliyunRDSF	RDS 鉴权规

RDS 版				ullAccess AliyunRDSReadOnlyAccess	则
云数据库 MongoDB 版	√	√	资源级别	AliyunMongoDBFullAccess AliyunMongoDBReadOnlyAccess	MongoDB 鉴权规则
云数据库 Redis 版	√	√	资源级别	AliyunKvstoreFullAccess AliyunKvstoreReadOnlyAccess	Redis 鉴权规则
云数据库 Memcache 版	√	√	服务级别	AliyunOCSFullAccess AliyunOCSReadOnlyAccess	-
云数据库 HybirdDB for MySQL	√	√	资源级别	AliyunPetaDataFullAccess AliyunPetaDataReadOnlyAccess	-
云数据库 Hbase 版	√	√	资源级别	-	-
数据传输服务 DTS	√	√	服务级别	AliyunDTSFullAccess AliyunDTSReadOnlyAccess	DTS 授权及使用子账号

存储与 CDN

服务名	控制台	API	授权粒度	系统策略	相关文档
对象存储 OSS	√	√	资源级别	AliyunOSSFullAccess AliyunOSSReadOnlyAccess	OSS 权限控制 OSS 授权策略配置 OSS 权限管理最佳实践 授权策略在线配置工具
文件存储 NAS	√	○	服务级别	AliyunNASFullAccess AliyunNASReadOnlyAccess	文件存储 使用 RAM 授权

表格存储	√	√	资源级别	AliyunOTSFullAccess AliyunOTSReadOnlyAccess AliyunOTSWriteOnlyAccess	表格存储 自定义权限
CDN	√	√	资源级别	AliyunCDNFullAccess AliyunCDNReadOnlyAccess	CDN 鉴权规则

网络

服务名	控制台	API	授权粒度	系统策略	相关文档
专有网络 VPC	√	√	资源级别	AliyunVPCFullAccess AliyunVPCReadOnlyAccess	VPC 鉴权规则
弹性公网 IP	√	√	资源级别	AliyunEIPFullAccess AliyunEIPReadOnlyAccess	弹性公网 IP 鉴权规则
高速通道 ExpressConnect	√	√	资源级别	AliyunExpressConnectFullAccess AliyunExpressConnectReadOnlyAccess	高速通道 鉴权规则

分析

服务名	控制台	API	授权粒度	系统策略	相关文档
E-MapReduce	√	√	服务级别	AliyunEMRFullAccess	E-MapReduce 角色授权
开放搜索	√	√	服务级别	AliyunOpenSearchFullAccess AliyunOpenSearchReadOnlyAccess	开放搜索 鉴权规则

云通信

服务名	控制台	API	授权粒度	系统策略	相关文档
消息服务	√	√	资源级别	AliyunMNSFullAccess AliyunMNSReadOnlyAccess	消息服务 鉴权规则
移动推送	√	√	服务级别	AliyunMPushFullAccess AliyunMPushReadOnlyAccess	-
邮件推送	√	√	服务级别	AliyunDirectMailFullAccess AliyunDirectMailReadOnlyAccess	-
语言服务	√	√	服务级别	AliyunDyvmsFullAccess AliyunDyvmsReadOnlyAccess	语音服务 权限访问控制
流量服务	√	√	服务级别	AliyunDycdpFullAccess AliyunDycdpReadOnlyAccess	流量服务 权限访问控制
短信服务	√	√	服务级别	AliyunSMSFullAccess AliyunSMSReadOnlyAccess	短信服务 权限访问控制

监控与管理

服务名	控制台	API	授权粒度	系统策略	相关文档
云监控	√	√	服务级别	AliyunCloudMonitorFullAccess AliyunCloudMonitorReadOnlyAccess	云监控 访问控制
访问控制	√	√	资源级别	AliyunRAMFullAccess AliyunRAMReadOnlyAc	RAM API 参考

				cess AliyunSTSAssumeRoleAccess	
操作审计	√	√	资源级别	AliyunActionTrailFullAccess AliyunActionTrailReadOnlyAccess	操作审计 RAM 支持的操作和资源
密钥管理	√	√	资源级别	-	KMS 鉴权规则

应用服务

服务名	控制台	API	授权粒度	系统策略	相关文档
日志服务	√	√	资源级别	AliyunLogFullAccess AliyunLogReadOnlyAccess	日志服务 RAM 子用户使用 日志服务 鉴权规则
性能测试服务	√	√	服务级别	AliyunPTSFullAccess	性能测试 RAM
API 网关	√	√	服务级别	AliyunApiGatewayFullAccess AliyunApiGatewayReadOnlyAccess	-
物联网套件	√	√	资源级别	AliyunIOTFullAccess AliyunIOTReadOnlyAccess	物联网套件 鉴权规则
智能对话分析服务	√	√	资源级别	-	-

互联网中间件

服务名	控制台	API	授权粒度	系统策略	相关文档
企业级分布式应用服务 EDAS	√	×	服务级别	AliyunEDASFullAccess	EDAS 子账号管理
分布式关系型数据库服务 DRDS	√	×	资源级别	AliyunDRDSFullAccess AliyunDRDSReadOnlyAc	DRDS 支持的资源授权

				cess	
业务实时监控服务 ARMS	√	×	服务级别	AliyunARMSFullAccess	-

移动服务

服务名	控制台	API	授权粒度	系统策略	相关文档
移动用户反馈	√	√	服务级别	AliyunFeedbackFullAccess AliyunFeedbackReadOnlyAccess	移动用户反馈 鉴权规则
移动热修复	√	√	服务级别	AliyunHotfixFullAccess AliyunHotfixReadOnlyAccess	移动热修复 鉴权规则

视频服务

服务名	控制台	API	授权粒度	系统策略	相关文档
媒体转码	√	√	服务级别	AliyunMTSFullAccess AliyunMTSPlayerAuth	媒体转码 子账号使用控制台说明
视频点播	√	√	服务级别	AliyunMTSFullAccess	-
视频直播	√	√	服务级别	AliyunMTSFullAccess	-

大数据（数加）

服务名	控制台	API	授权粒度	系统策略	相关文档
大数据开发套件	√	√	服务级别	-	大数据开发套件 子账号登录
Quick BI	√	√	服务级别	-	-
机器学习	√	√	服务级别	-	-
推荐引擎	√	√	服务级别	-	-
公众趋势分析	√	√	服务级别	-	-

DataV 数据可视化	√	√	服务级别	-	-
智能语音交互	√	√	服务级别	AliyunSCAFullAccess AliyunSCAReadOnlyAccess	-
流计算	√	√	服务级别	-	流计算 角色授权
画像分析	√	√	服务级别	-	-
企业图谱	√	√	服务级别	-	-

安全（云盾）

服务名	控制台	API	授权粒度	系统策略	相关文档
态势感知	√	○	服务级别	AliyunYundunSASFullAccess AliyunYundunSASReadOnlyAccess	-
服务器安全(安骑士)	√	○	服务级别	AliyunYundunAegisFullAccess AliyunYundunAegisReadOnlyAccess	-
DDoS 基础防护	√	○	服务级别	AliyunYundunDDosFullAccess	-
DDoS 高防IP	√	○	服务级别	AliyunYundunHighFullAccess AliyunYundunHighReadOnlyAccess	-
Web 应用防火墙	√	○	服务级别	AliyunYundunWAFFullAccess AliyunYundunWAFReadOnlyAccess	-
先知(安全情报)	√	○	服务级别	AliyunYundunXianzhiFullAccess	-
安全管家	√	○	服务级别		-

加密服务	√	○	服务级别	AliyunYundunHSMFullAccess	-
内容安全	√	○	服务级别	AliyunYundunGreenWebFullAccess	-
数据风控	√	○	服务级别	AliyunYundunAFSFullAccess	-
证书服务	√	○	服务级别	AliyunYundunCertFullAccess	-
移动安全	√	○	服务级别	AliyunYundunJaqFullAccess	-
合作伙伴中心	√	○	服务级别	AliyunYundunPartnerFullAccess	-
数据库审计	√	○	服务级别	AliyunYundunDbAuditFullAccess	-
堡垒机	√	○	服务级别	AliyunYundunBastionHostFullAccess	-

云市场

服务名	控制台	API	授权粒度	系统策略	相关文档
云市场	√	○	服务级别	AliyunMarketplaceFullAccess	-

域名与网站

服务名	控制台	API	授权粒度	系统策略	相关文档
云解析DNS	√	○	服务级别	AliyunDNSFullAccess AliyunDNSReadOnlyAccess	-
HTTPDNS	√	○	服务级别	AliyunHTTPDNSFullAccess AliyunHTTPDNSReadOnlyAccess	-

支持 STS 的云服务列表

下表列出目前已支持 STS 的云服务产品。表格定义同 支持 RAM 的云服务列表。

服务	控制台	API
云服务器 ECS	√	√
云数据库 RDS	√	√
负载均衡 SLB	√	√
对象存储 OSS	√	√
专有网络 VPC	√	√
物联网套件 IoT	×	√
函数计算 FC	×	√