ALIBABA CLOUD

Alibaba Cloud

访问控制

产品简介

文档版本：20210120

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是访问控制

访问控制（RAM）是阿里云提供的管理用户身份与资源访问权限的服务。

功能特性

RAM允许在一个阿里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权限，从而实现不同用户拥有不同资源访问权限的目的。RAM的功能特性如下：

- 集中控制RAM用户及其密钥：管理每个RAM用户及其访问密钥，为用户绑定多因素认证（MFA）设备。
- 集中控制RAM用户的访问权限：控制每个RAM用户访问资源的权限。
- 集中控制RAM用户的资源访问方式：确保RAM用户在指定的时间和网络环境下，通过安全信道访问特定的阿里云资源。
- 集中控制云资源：对RAM用户创建的实例或数据进行集中控制。当用户离开组织时，实例或数据不会丢失。
- 单点登录管理（SSO）：支持与企业身份提供商（IdP）进行用户SSO或角色SSO。

应用场景

应用场景	描述
用户管理与分权	企业A的某个项目（Project-X）上云，购买了多种阿里云资源，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。项目里有多个员工需要操作这些资源，由于每个员工的工作职责不同，需要的权限也不同。
移动应用使用临时安全令牌访问阿里云	企业A开发了一款移动应用（App），并购买了对象存储（OSS）服务。App需要直连OSS上传或下载数据，但是App运行在用户自己的移动设备上，这些设备不受企业A的控制。
跨阿里云账号的资源授权	企业A购买了多种阿里云资源来开展业务，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。企业A希望将部分业务授权给企业B。
对云上应用进行动态身份管理与授权	企业A购买了ECS实例，并计划在ECS中部署企业的应用程序。这些应用程序需要使用访问密钥（AccessKey）访问其它云服务API。

产品优势

使用RAM，您可以创建、管理RAM用户（例如员工、系统或应用程序），并可以控制这些RAM用户对资源的操作权限。当您的企业存在多用户协同操作资源的场景时，RAM可以让您避免与其他用户共享阿里云账号密钥，按需为用户分配最小权限，从而降低企业的信息安全风险。

学习路径图

您可以通过RAM学习路径图快速了解RAM，学习基础操作，并利用丰富的API、SDK包和便捷工具进行二次开发。

2.基本概念

本文解释了RAM的基本概念，帮助您正确理解和使用RAM。

身份管理相关概念

概念	说明
阿里云账号（主账号，Alibaba Cloud account）	开始使用阿里云服务前，首先需要注册一个阿里云账号。阿里云账号是阿里云资源归属、资源使用计量计费的基本主体。阿里云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。 默认情况下，资源只能被阿里云账号所访问，任何其他用户访问都需要获得阿里云账号的显式授权。阿里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（RAM）中有三种身份：RAM用户、用户组和RAM角色。其中RAM用户和用户组是RAM的一种实体身份类型，RAM角色是一种虚拟用户身份。
默认域名（Default domain name）	阿里云为每个阿里云账号分配了一个**默认域名**，格式为：`<AccountAlias>.onaliyun.com`。默认域名可作为RAM用户登录或单点登录（SSO）等场景下该阿里云账号的唯一标识符。 关于如何设置默认域名，请参见管理默认域名。
账号别名（企业别名，Enterprise alias）	当RAM用户登录时，登录名称的后缀表示可以使用账号别名、默认域名或域别名中的任何一种。 每个阿里云账号可以在RAM中设置一个全局唯一的账号别名。账号别名主要用于RAM用户登录，登录成功后可作为显示名。 例如：企业可以为其阿里云账号设置账号别名为：company1，该阿里云账号下的RAM用户alice可以使用alice@company1进行登录，登录成功后，用户的显示名为：alice@company1。
域别名（Domain alias）	如果您持有公网上可以解析的域名，那么您可以使用该域名替代您的默认域名，该域名称为**域别名**。域别名就是指默认域名的别名。 **说明** 域别名必须经过域名归属验证后才能使用。验证通过后，您可以使用域别名替代默认域名，用于所有需要使用默认域名的场景。 关于如何设置域别名，请参见创建并验证域别名。

概念	说明
RAM用户（RAM user）	RAM用户是RAM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。 • 一个阿里云账号下可以创建多个RAM用户，对应企业内的员工、系统或应用程序。 • RAM用户不拥有资源，不能独立计量计费，由所属阿里云账号统一控制和付费。 • RAM用户归属于阿里云账号，只能在所属阿里云账号的空间下可见，而不是独立的阿里云账号。 • RAM用户必须在获得阿里云账号的授权后才能登录控制台或使用API操作阿里云账号下的资源。 关于如何创建RAM用户，请参见创建RAM用户。
登录密码（Password）	登录密码是登录阿里云的身份凭证，用于证明用户真实身份的凭证。 说明 请妥善保管您的登录密码并定期更换。 关于如何设置登录密码，请参见修改云账号登录密码和修改RAM用户登录密码。
访问密钥（AccessKey）	访问密钥指的是访问身份验证中用到的AccessKey ID和AccessKey Secret。您可以使用访问密钥（或阿里云服务SDK）创建一个API请求，RAM通过使用AccessKey ID和AccessKey Secret对称加密的方法来验证某个请求的发送者身份，身份验证成功后将可以操作相应资源。 AccessKey ID和AccessKey Secret一起使用，AccessKey ID用于标识用户，AccessKey Secret用于加密签名字符串和RAM用来验证签名字符串的密钥。 说明 AccessKey Secret只在创建时显示，不支持查询，请妥善保管。 关于如何创建访问密钥，请参见为RAM用户创建访问密钥。
多因素认证（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。这些多重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，再次登录阿里云时，系统将要求输入两层安全要素： 1. 第一安全要素：用户名和密码 2. 第二安全要素：多因素认证设备生成的验证码 关于如何设置多因素认证，请参见为云账号设置多因素认证和为RAM用户设置多因素认证。

概念	说明
用户组（RAM user group）	用户组是RAM的一种实体身份类型，用户组可以对职责相同的RAM用户进行分类并授权，从而更好的管理用户及其权限。 • 在RAM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RAM用户产生影响。 关于如何创建用户组，请参见创建用户组。 • 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RAM用户。 关于如何为用户组授权，请参见为用户组授权。
RAM角色（RAM role）	RAM角色是一种虚拟用户，与实体用户（阿里云账号、RAM用户和云服务）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。 • 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RAM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。 • RAM角色：RAM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。RAM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RAM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RAM可信实体的不同，RAM支持以下三种类型的角色： • **阿里云账号**：允许RAM用户所扮演的角色。扮演角色的RAM用户可以属于自己的阿里云账号，也可以属于其他阿里云账号。此类角色主要用来解决跨账号访问和临时授权问题。 • **阿里云服务**：允许云服务所扮演的角色。此类角色主要用于授权云服务代理您进行资源操作。 • **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阿里云的SSO。 关于如何创建RAM角色，请参见创建可信实体为阿里云账号的RAM角色、创建可信实体为阿里云服务的RAM角色和创建可信实体为身份提供商的RAM角色。
单点登录（SSO）	阿里云支持基于SAML 2.0的SSO（Single Sign On，单点登录），也称为身份联合登录。 企业根据自身需要，使用支持SAML 2.0的企业 IdP（例如：AD FS）与阿里云进行SSO。阿里云提供以下两种基于SAML 2.0协议的SSO方式： • 用户SSO：阿里云通过IdP颁发的SAML断言确定企业用户与阿里云RAM用户的对应关系 。企业用户登录后，使用该RAM用户访问阿里云。详情请参见进行用户SSO。 • 角色SSO：阿里云通过IdP颁发的SAML断言确定企业用户在阿里云上可以使用的RAM角色。企业用户登录后，使用SAML断言中指定的RAM角色访问阿里云。详情请参见进行角色SSO。
元数据文档（Metadata file）	元数据文档由企业IdP提供，一般为XML格式，包含IdP的登录服务地址、用于验证签名的公钥及断言格式等信息。

概念	说明
身份提供商（IdP）	一个包含有关外部身份提供商元数据的RAM实体，身份提供商可以提供身份管理服务。 • 企业本地IdP：Microsoft Active Directory Federation Service （AD FS）以及Shibboleth等。 • Cloud IdP：Azure AD、Google G Suite、Okta以及OneLogin等。
服务提供商（SP）	利用IdP的身份管理功能，为用户提供具体服务的应用，SP会使用IdP提供的用户信息。一些非SAML协议的身份系统（例如：OpenID Connect），也把服务提供商称作IdP的信赖方。
安全断言标记语言（SAML 2.0）	实现企业级用户身份认证的标准协议，它是SP和IdP之间实现沟通的技术实现方式之一。SAML 2.0已经是目前实现企业级SSO的一种事实标准。
SAML断言（SAML assertion）	SAML协议中用来描述认证请求和认证响应的核心元素。例如：用户的具体属性就包含在认证响应的断言里。
信赖（Trust）	建立在SP和IdP之间的互信机制，通常由公钥和私钥来实现。SP通过可信的方式获取IdP的SAML元数据，元数据中包含IdP签发SAML断言的签名验证公钥，SP则使用公钥来验证断言的完整性。

访问控制相关概念

概念	说明
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）。 操作分为两大类： • 资源管控操作：指云资源的生命周期管理及运维管理操作，所面向的用户一般是资源购买者或组织内的运维员工。例如：ECS的实例创建、停止或重启或OSS存储空间的创建、修改或删除等。 • 资源使用操作：指使用资源的核心功能，所面向的用户一般是组织内的研发员工或应用系统。例如：ECS实例操作系统中的用户操作或OSS存储空间的数据上传或下载。 说明 ◦ 对于弹性计算和数据库等产品，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。例如：ECS实例操作系统的权限控制或MySQL数据库提供的权限控制。 ◦ 对于存储类等产品，例如：OSS或Table Store等，资源管控操作和资源使用操作都可以通过RAM来实现。

概念	说明
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。权限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权限策略语法和结构。 在RAM中，权限策略是一种资源实体。RAM支持以下两种权限策略： • 阿里云管理的**系统策略**：统一由阿里云创建，用户只能使用不能修改，策略的版本更新由阿里云维护。 • 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。 通过为RAM用户、用户组或RAM角色绑定权限策略，可以获得权限策略中指定的访问权限。详情请参见为RAM用户授权、为用户组授权和为RAM角色授权。
被授权主体（Principal）	获得策略中定义的权限主体，被授权主体可以为RAM用户、用户组或RAM角色。
效力（Effect）	权限策略基本元素之一，表示授权效力。取值为：允许（Allow）或拒绝（Deny）。
操作（Action）	权限策略基本元素之一，表示对具体资源的操作。取值为：云服务所定义的API操作名称。
限制条件（Condition）	权限策略基本元素之一，表示授权生效的限制条件。
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，例如：OSS存储空间或ECS实例等。

3.使用限制

本文列举了RAM的使用限制。

限制分类	限制项	最大值
RAM用户	一个云账号中的RAM用户个数	1000
	RAM用户名称的字符数	64
	一个RAM用户可加入的用户组个数	5
	一个RAM用户可创建的访问密钥个数	2
	一个RAM用户可绑定的多因素认证设备个数	1
	一个RAM用户可以绑定的系统策略个数	20
	一个RAM用户可以绑定的自定义策略个数	10
用户组	一个云账号中的用户组个数	50
	用户组名称的字符数	64
	一个用户组可以绑定的系统策略个数	20
	一个用户组可以绑定的自定义策略个数	5
RAM角色	一个云账号中的RAM角色个数	1000
	RAM角色名称的字符数	64
	一个RAM角色可以绑定的系统策略个数	20
	一个RAM角色可以绑定的自定义策略个数	5
账号别名	账号别名的字符数	64 **说明** 账号别名支持3~64个字符。
权限策略	权限策略名称的字符数	128
多因素认证设备	一个云账号中可创建的多因素认证设备个数	1000

限制分类	限制项	最大值
自定义策略	一个云账号中可创建的自定义策略个数	1500
	自定义策略内容的字符数	2048
	自定义策略版本数	5
身份提供商	一个云账号中可创建的身份提供商个数	100
	一个身份提供商包含的IdP个数	1
	一个身份提供商中的IdP包含的证书个数	2

4.支持RAM的云服务

本文罗列了与访问控制（RAM）相集成的阿里云服务，并提供每个服务支持的授权粒度、系统策略以及相关文档，方便您查询和使用。

支持RAM的云服务列表

以下表格分别罗列了阿里云各个模块下支持RAM的云服务：弹性计算、数据库、存储与CDN、网络、分析、云通信、管理与监控、应用服务、物联网IOT、消息队列MQ、互联网中间件、视频服务、大数据（数加）、安全（云盾）、云市场、域名与网站、会员服务、费用中心、工单、消息。

关于阿里云各个模块下支持STS的云服务，请参见支持STS的云服务。

每个表格包含以下信息：

- 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，“○”表示该服务未接入控制台。
- 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，“○”表示该服务未提供API。
- 授权粒度：当前服务提供的最小授权粒度，“-”表示暂无。

  在与RAM集成时，各产品针对RAM用户定义了不同级别的授权粒度：

  - 服务级别：将云服务作为一个整体进行授权。一个RAM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：API级别的授权。一个RAM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。
  - 资源级别：对执行资源的指定操作进行授权（最细的授权粒度）。例如：授权一个RAM用户仅可对某一台云服务器进行重启操作。
- 系统策略：当前云服务支持的系统策略，“-”表示暂无。
- 相关文档：当前服务与RAM相关的文档链接，“-”表示暂无。

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 • AliyunECSNetworkInterfaceManagementAccess	鉴权规则
弹性伸缩Auto Scaling	√	√	服务级别	• AliyunESSFullAccess • AliyunESSReadOnlyAccess	API使用须知
容器服务Kubernetes版	√	√	资源级别	• AliyunCSFullAccess • AliyunCSReadOnlyAccess	使用子账号

服务名	控制台	API	授权粒度	系统策略	相关文档
容器镜像服务	√	√	资源级别	• AliyunContainerRegistryFullAccess • AliyunContainerRegistryReadOnlyAccess	仓库访问控制
资源编排ROS	√	√	服务级别	• AliyunROSFullAccess • AliyunROSReadOnlyAccess	使用RAM控制资源访问
批量计算	√	√	服务级别	-	-
函数计算	√	√	资源级别	• AliyunFCFullAccess • AliyunFCInvocationAccess • AliyunFCReadOnlyAccess	子账号控制台快速指导
弹性高性能计算E-HPC	√	√	服务级别	• AliyunEHPCFullAccess • AliyunEHPCReadOnlyAccess	-
轻量应用服务器	√	○	服务级别	AliyunSWASFullAccess	-
弹性容器实例ECI	√	√	资源级别	• AliyunECIFullAccess • AliyunECIReadOnlyAccess	如何为子账号授权
Web应用托管服务（Web+）	√	√	操作级别	• AliyunWebPlusFullAccess • AliyunWebPlusReadOnlyAccess	-
运维编排服务	√	√	资源级别	• AliyunOOSFullAccess • AliyunOOSReadOnlyAccess	鉴权规则

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PolarDB	√	√	操作级别	• AliyunPolardbReadOnlyAccess • AliyunPolardbFullAccess	创建和使用子账号
云数据库RDS版	√	√	资源级别	• AliyunRDSFullAccess • AliyunRDSReadOnlyAccess	RAM资源授权
云数据库MongoDB版	√	√	资源级别	• AliyunMongoDBFullAccess • AliyunMongoDBReadOnlyAccess	-

服务名	控制台	API	授权粒度	系统策略	相关文档
云数据库Redis版	√	√	资源级别	• AliyunKvstoreFullAccess • AliyunKvstoreReadOnlyAccess	RAM鉴权
云数据库Memcache版	√	√	服务级别	• AliyunOCSFullAccess • AliyunOCSReadOnlyAccess	-
云数据库HBase	√	√	资源级别	• AliyunHBaseFullAccess • AliyunHBaseReadOnlyAccess	
时序数据库TSDB	√	√	操作级别	-	-
云原生数据仓库ADB PostgreSQL版	√	√	资源级别	• AliyunGPDBFullAccess • AliyunGPDBReadOnlyAccess	API的鉴权规则
云原生数据仓库ADB MySQL版	√	√	资源级别	• AliyunADBFullAccess • AliyunADBReadOnlyAccess	RAM子账号和权限
数据传输服务DTS	√	√	操作级别	• AliyunDTSFullAccess • AliyunDTSReadOnlyAccess	
数据库备份DBS	√	√	服务级别	• AliyunDBSFullAccess • AliyunDBSReadOnlyAccess	-
数据库自治服务DAS	√	√	服务级别	• AliyunHDMReadOnlyAccess • AliyunHDMFullAccess	子账号如何使用DAS
云原生分布式数据库 PolarDB-X（原DRDS升级版）	√	√	资源级别	• AliyunDRDSReadOnlyAccess • AliyunDRDSFullAccess	DRDS支持的资源授权
数据库和应用迁移服务ADAM	√	○	服务级别	• AliyunADAMReadOnlyAccess • AliyunADAMFullAccess	RAM 子账号
数据库网关DG	√	√	资源级别	• AliyunDGFullAccess • AliyunDGReadOnlyAccess	-
可信账本数据库	√	√	资源级别	• AliyunLedgerDBFullAccess • AliyunLedgerDBReadOnlyAccess	子账号授权

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	RAM Policy概述
文件存储NAS	√	√	操作级别	• AliyunNASFullAccess • AliyunNASReadOnlyAccess	管理权限组
表格存储Tablestore	√	√	资源级别	• AliyunOTSFullAccess • AliyunOTSReadOnlyAccess • AliyunOTSWriteOnlyAccess	自定义权限
云存储网关	√	√	服务级别	AliyunHCSSGWFullAccess	-
混合云备份	√	○	资源级别	• AliyunHBRFullAccess • AliyunHBRReadOnlyAccess	-
闪电立方	√	○	服务级别	AliyunMGWFullAccess	-
全站加速	√	√	资源级别	• AliyunDCDNFullAccess • AliyunDCDNReadOnlyAccess	-
CDN	√	√	资源级别	• AliyunCDNFullAccess • AliyunCDNReadOnlyAccess	RAM鉴权

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	RAM鉴权
负载均衡	√	√	资源级别	• AliyunSLBReadOnlyAccess • AliyunSLBFullAccess	RAM鉴权
弹性公网IP	√	√	资源级别	• AliyunEIPFullAccess • AliyunEIPReadOnlyAccess	RAM鉴权
高速通道	√	√	资源级别	• AliyunExpressConnectFullAccess • AliyunExpressConnectReadOnlyAccess	RAM鉴权

服务名	控制台	API	授权粒度	系统策略	相关文档
NAT网关	√	√	资源级别	• AliyunNATGatewayReadOnlyAccess • AliyunNATGatewayFullAccess	RAM鉴权
VPN网关	√	√	资源级别	• AliyunVPNGatewayFullAccess • AliyunVPNGatewayReadOnlyAccess	RAM鉴权
共享带宽	√	√	资源级别	• AliyunCommonBandwidthPackageReadOnlyAccess • AliyunCommonBandwidthPackageFullAccess	-
全球加速	√	√	资源级别	• AliyunGlobalAccelerationReadOnlyAccess • AliyunGlobalAccelerationFullAccess	RAM鉴权
智能接入网关	√	√	资源级别	-	RAM鉴权
云企业网	√	√	资源级别	• AliyunCENReadOnlyAccess • AliyunCENFullAccess	RAM鉴权

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 • AliyunEMRDevelopAccess • AliyunEMRFlowAdmin	-
数据湖分析	√	√	操作级别	• AliyunDLAFullAccess • AliyunDLAReadOnlyAccess	-

云通信

服务名	控制台	API	授权粒度	系统策略	相关文档
短信服务	√	√	服务级别	-	-

管理与监控

服务名	控制台	API	授权粒度	系统策略	相关文档
云监控	√	√	操作级别	• AliyunCloudMonitorFullAccess • AliyunCloudMonitorReadOnlyAccess	访问控制
操作审计	√	√	资源级别	-	RAM鉴权
访问控制	√	√	资源级别	• AliyunRAMFullAccess • AliyunRAMReadOnlyAccess	RAM鉴权
密钥管理服务	√	√	资源级别	• AliyunKMSFullAccess • AliyunKMSReadOnlyAccess • AliyunKMSCryptoAccess	使用RAM实现对资源的访问控制
智能顾问	×	×	操作级别	-	-
资源管理	√	√	资源级别	• AliyunResourceDirectoryFullAccess • AliyunResourceDirectoryReadOnlyAccess	RAM鉴权
配置审计	√	√	服务级别	• AliyunConfigFullAccess • AliyunConfigReadOnlyAccess	RAM鉴权

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	鉴权规则
邮件推送	√	√	服务级别	• AliyunDirectMailFullAccess • AliyunDirectMailReadOnlyAccess	-
API网关	√	√	服务级别	• AliyunApiGatewayFullAccess • AliyunApiGatewayReadOnlyAccess	使用 RAM 管理 API
区块链服务 BaaS	√	√	资源级别	-	Hyperledger Fabric RAM鉴权
小程序云	√	√	操作级别	• AliyunMPCAFullAccess • AliyunMPCAReadOnlyAccess	-

服务名	控制台	API	授权粒度	系统策略	相关文档

物联网IOT

服务名	控制台	API	授权粒度	系统策略	相关文档
物联网平台	√	√	资源级别	• AliyunIOTFullAccess • AliyunIOTReadOnlyAccess	RAM用户访问
物联网边缘计算	√	√	资源级别	• AliyunIOTFullAccess • AliyunIOTReadOnlyAccess	云资源访问

消息队列MQ

服务名	控制台	API	授权粒度	系统策略	相关文档
消息队列for Apache Rocket MQ	√	√	资源级别	• AliyunMQFullAccess • AliyunMQPubOnlyAccess • AliyunMQSubOnlyAccess	RAM主子账号授权
消息服务MNS	√	√	资源级别	• AliyunMNSFullAccess • AliyunMNSReadOnlyAccess	-

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	子账号管理
应用实时监控服务ARMS	√	√	服务级别	AliyunARMSFullAccess	借助RAM用户实现分权
应用配置管理	√	√	资源级别	AliyunACMFullAccess	访问权限控制
全局事务服务	√	√	服务级别	• AliyunGTSFullAccess • AliyunGTSReadOnlyAccess	-

视频服务

服务名	控制台	API	授权粒度	系统策略	相关文档

服务名	控制台	API	授权粒度	系统策略	相关文档
媒体处理	√	√	服务级别	• AliyunMTSFullAccess • AliyunMTSPlayerAuth	子帐号使用控制台说明
视频点播	√	√	服务级别	• AliyunVODFullAccess • AliyunVODReadOnlyAccess • AliyunVODPlayAuth • AliyunVODUploadAuth	-
视频直播	√	√	资源级别	AliyunLiveFullAccess	API鉴权规则
音视频通信RTC	√	√	资源级别	-	-
云视频会议	√	○	资源级别	• AliyunCVCFullAccess • AliyunCVCReadOnlyAccess	-

大数据（数加）

服务名	控制台	API	授权粒度	系统策略	相关文档
DataWorks	√	√	服务级别	AliyunDataWorksFullAccess	用户使用子账号
Quick BI	√	√	服务级别	-	-
机器学习PAI	√	√	服务级别	-	-
公众趋势分析	√	√	服务级别	-	-
DataV数据可视化	√	√	服务级别	-	-
MaxCompute	√	√	服务级别	-	-
阿里云Elasticsearch	√	√	资源级别	• AliyunElasticsearchReadOnlyAccess • AliyunElasticsearchFullAccess	授权资源类型
机器翻译	×	×	服务级别	-	-
图像搜索	√	√	资源级别	• AliyunImagesearchReadOnlyAccess • AliyunImagesearchFullAccess	授权访问鉴权规则

安全（云盾）

服务名	控制台	API	授权粒度	系统策略	相关文档
云安全中心（态势感知）	√	√	服务级别	• AliyunYundunSASFullAccess • AliyunYundunSASReadOnlyAccess	-
云安全中心（安骑士）	√	√	服务级别	• AliyunYundunAegisFullAccess • AliyunYundunAegisReadOnlyAccess	-
DDoS基础防护	√	√	服务级别	• AliyunYundunDDosFullAccess • AliyunYundunDDosReadOnlyAccess	-
DDoS高防	√	√	服务级别	• AliyunYundunHighFullAccess • AliyunYundunHighReadOnlyAccess	-
DDoS高防（国际）	√	○	服务级别	• AliyunYundunAntiDDoSPremiumFullAccess • AliyunYundunAntiDDoSPremiumReadOnlyAccess	-
游戏盾	√	○	服务级别	AliyunYundunGameShieldReadOnlyAccess	-
Web应用防火墙（网络安全）	√	√	服务级别	• AliyunYundunWAFFullAccess • AliyunYundunWAFReadOnlyAccess	-
SSL证书（应用安全）	√	√	服务级别	• AliyunYundunCertFullAccess • AliyunYundunCertReadOnlyAccess	-
漏洞扫描（应用安全）	√	√	服务级别	AliyunYundunAvdsFullAccess	-
内容安全（业务安全）	√	√	服务级别	AliyunYundunGreenWebFullAccess	-
爬虫风险管理	√	○	服务级别	• AliyunYundunAntibotFullAccess • AliyunYundunAntibotReadOnlyAccess	-

服务名	控制台	API	授权粒度	系统策略	相关文档
金融级实人认证	√	√	服务级别	• AliyunAntCloudAuthFullAccess • AliyunAntCloudAuthReadOnlyAccess	-

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	√	√	资源级别	• AliyunDNSFullAccess • AliyunDNSReadOnlyAccess	-
域名	√	√	资源级别	AliyunDomainFullAccess	Domain API鉴权规则
云虚拟主机	×	×	-	-	-
企业邮箱	×	×	-	-	-

会员服务

服务名	控制台	API	授权粒度	系统策略	相关文档
备案	√	○	服务级别	AliyunBeianFullAccess	-

费用中心

服务名	控制台	API	授权粒度	系统策略	相关文档
费用中心	√	√	服务级别	• AliyunBSSFullAccess • AliyunBSSReadOnlyAccess • AliyunBSSOrderAccess • AliyunBSSRefundAccess	-

工单

服务名	控制台	API	授权粒度	系统策略	相关文档
工单	√	√	服务级别	AliyunSupportFullAccess	-

消息

服务名	控制台	API	授权粒度	系统策略	相关文档
消息中心	√	○	服务级别	AliyunNotificationsFullAccess	-

5.支持STS的云服务

本文按服务类别罗列了支持临时安全令牌（STS）访问和鉴权的阿里云服务，方便您查询和使用。

有关STS的介绍和应用场景，请参见什么是STS和RAM角色概览。

支持STS的云服务列表

以下表格分别罗列了阿里云各个模块下支持STS的云服务：弹性计算、数据库、存储与CDN、网络、分析、云通信、管理与监控、应用服务、物联网IOT、互联网中间件、消息队列MQ、视频服务、大数据（数加）、安全（云盾）、云市场、域名与网站、会员服务、费用中心、工单、消息。

每个表格包含以下信息：

- 服务名：支持STS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。
- 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，“○”表示该服务未提供API。

弹性计算

服务名	控制台	API
云服务器ECS	√	√
弹性伸缩Auto Scaling	√	√
容器服务Kubernetes版	√	√
容器镜像服务	√	√
资源编排ROS	√	√
批量计算BatchCompute	√	√
函数计算	√	√
弹性高性能计算	√	√
轻量应用服务器	×	○
弹性容器实例ECI	√	√
Web应用托管服务	√	√
运维编排服务	√	√

数据库

服务名	控制台	API
云数据库RDS版	√	√

服务名	控制台	API
云数据库MongoDB版	√	√
云数据库Redis版	√	√
云数据库Memcache版	√	√
时序数据库TSDB	√	√
云原生数据仓库ADB PostgreSQL版	√	√
数据传输服务DTS	√	√
数据库备份DBS	√	√
云原生分布式数据库PolarDB-X（原DRDS 升级版）	√	√
数据库网关	√	√
可信账本数据库	√	√

存储与CDN

服务名	控制台	API
对象存储OSS	√	√
文件存储NAS	√	○
表格存储	√	√
CDN	√	√
全站加速	√	√
云存储网关	√	○
混合云备份服务	√	○
闪电立方	×	○

网络

服务名	控制台	API
专有网络VPC	√	√
负载均衡	√	√
弹性公网IP	√	√

服务名	控制台	API
高速通道	√	√
NAT网关	√	√
VPN网关	√	√
全球加速	√	√
智能接入网关	√	√
云企业网	√	√

分析

服务名	控制台	API
E-MapReduce	√	√
数据湖分析	×	×

云通信

服务名	控制台	API
短信服务	√	√

管理与监控

服务名	控制台	API
云监控	√	√
操作审计	√	√
访问控制	√	√
密钥管理服务	√	√
智能顾问	×	×
配置审计	√	○
资源管理	√	√
Prometheus监控	√	√

应用服务

服务名	控制台	API
日志服务	√	√
邮件推送	√	√
API网关	√	√
区块链服务	√	√

物联网IOT

服务名	控制台	API
物联网平台	√	√
物联网边缘计算	×	×

互联网中间件

服务名	控制台	API
企业级分布式应用服务EDAS	×	√
应用实时监控服务ARMS	×	×
应用配置管理	√	√

消息队列MQ

服务名	控制台	API
消息队列RocketMQ	√	√
消息服务MNS	√	√
事件总线EventBridge	√	√

视频服务

服务名	控制台	API
媒体处理	√	√
视频点播	√	√
视频直播	√	√
音视频通信RTC	×	×

大数据（数加）

服务名	控制台	API
DataWorks	√	√
Quick BI	×	×
机器学习	×	×
公众趋势分析	×	×
DataV数据可视化	×	×
MaxCompute	√	√
阿里云Elasticsearch	√	√
机器翻译	×	×
图像搜索	√	√

安全（云盾）

服务名	控制台	API
云安全中心（态势感知）	√	○
安骑士（服务器安全）	√	○
DDoS基础防护	√	○
DDoS高防	√	○
DDoS高防（国际）	√	○
游戏盾	√	○
Web应用防火墙（网络安全）	√	○
SSL证书（应用安全）	√	○
漏洞扫描	√	○
内容安全（业务安全）	√	○
爬虫风险管理	√	○

云市场

服务名	控制台	API
云市场	√	×

域名与网站

服务名	控制台	API
云解析DNS	√	○
域名	√	√
云虚拟主机	×	×
企业邮箱	×	×

会员服务

服务名	控制台	API
备案	√	○

费用中心

服务名	控制台	API
费用中心	√	√

工单

服务名	控制台	API
工单	√	√

消息

服务名	控制台	API
消息中心	√	○