阿里云
通用内容

通用参考

文档版本：20190423

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 文档使用指引

您可以从本文档获取阿里云帮助文档频道相关信息，包括但不限于文档使用对象、通用约定、法律声明、开源文档操作指南等信息。

1.1 文档及使用对象

阿里云产品主要的配套文档包括：

文档名称	介绍	读者对象
产品简介	提供本产品的简单介绍，包括产品架构（模块及功能）、功能特性、产品优势、应用场景。	初学者
产品定价	提供本产品的价格信息、计费策略和计算方式、欠费说明、实例及数据的保留策略说明。	财务人员
快速入门	介绍实例的创建（包括购买、续费、变配、释放等相关生命周期的详细说明），初始化配置的流程和步骤，以及相关的限制说明。	初学者
用户指南	提供完整的产品功能及操作指导，以及典型应用案例。	开发人员
最佳实践	提供本产品在典型场景下的应用，包括场景介绍、系统架构及本产品位置、实践方案。	高级开发人员
开发指南	详细介绍本产品支持的二次开发方式，包括API、SDK等，以及各个方式的调用方法和DEMO。	开发人员
常见问题	包括典型问题及处理方法、常见FAQ等。	所有人员

1.2 开源文档说明

如果您要对希望成为阿里云文档内容贡献者，请参考本文档指引操作并遵守内容开源规定。

1.2.1 内容开源规定

本文档为阿里云产品文档开源行为规定。如果用户参与阿里云内容开源社区的内容编辑修改，需遵循以下行为规定。

1. 用户权利和义务。
   a. 用户可以通过本开源社区获得阿里云对外发布文档的文件副本，包括但不限于使用、复制、修改文件副本，并提交修改至本社区。
   b. 用户对自己在阿里云开源社区上发布、上传的内容负责。
   c. 不得修改开源的目录结构、文件名称，不支持新增文件夹或文件。
2. 关于内容版权问题。
   a. 用户提交的内容必须是原创内容。
   b. 对于采纳的内容，阿里云有权根据相关规范修改用户提交的内容。
3. 内容要求。

   用户不得向阿里云上传、发布或提交：

   a. 违反任何法律法规或者道德道义的语言。
   b. 淫秽或包含或推断任何色情或性相关商品或任何其他内容，促进性的材料，或其他有害于未成年人的内容。
   c. 促进基于种族、性别、宗教、国籍、残疾、性取向或年龄的歧视的内容。
   d. 涉及任何计算机病毒或其他破坏性设备和代码，具有破坏、干扰、拦截或没收任何软件或硬件系统、数据或个人信息的内容。
   e. 以公共利益、公德、公共秩序、公共安全、国家和谐为理由，或者被适用法律禁止的内容。
   f. 与个人信息相关，包括但不限于个人信息、设备信息、电子邮件等。
4. 内容提交处理规定。

   如果阿里云决定使用您提交的材料，阿里云将在最快时间将你的意见发布到网站上的文档。

如果您发现阿里云内容违反了以上规定，或者发现其它内容滥用问题，可以报告至以下E-mail地址：*ApsaraDoc@alibaba-inc.com*，阿里云将优先调查和处理该类报告，并及时进行反馈。

1.2.2 编辑开源文档

如果您在浏览阿里云官方文档的时候发现任何需要修正或者改进的内容，请根据本文的操作步骤，提交变更内容到GitHub上。提交的内容被阿里云采纳后，您将成为该篇内容的编辑者之一显示在阿里云文档中心该篇文档的页面上。

前提条件

- 阿里云文档开源在*GitHub*上，您需要登录GitHub账号后才能编辑和提交内容。如果您还没有GitHub账号，请访问*Join GitHub*注册账号。
- 在编辑和提交内容之前，请阅读内容开源规定并在编辑过程中遵循规范中的约定。

背景信息

阿里云对外发布的文档以MarkDown格式开源在*GitHub*上。

操作步骤

1. 当您需要编辑文档内容时，只需要单击文档页面右上角的编辑按钮，打开GitHub上对应文档，如图 *1-1:* 编辑开源文档所示。

   图 1-1: 编辑开源文档

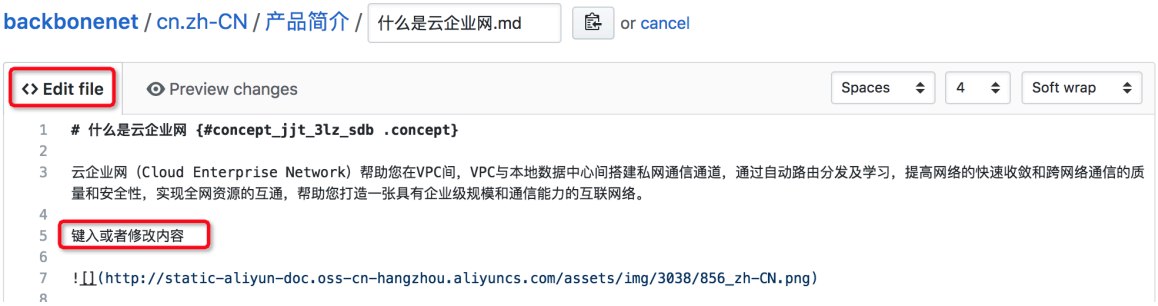
2. 在GitHub页面，单击 进入编辑状态。

   此时系统会为您创建一个分支，供您编辑和保存文件副本。

3. 在编辑框Edit file中修改文档内容，如图 1-2: 编辑内容所示。

   您可以单击上方或底部的Cancel取消保存。

   图 1-2: 编辑内容

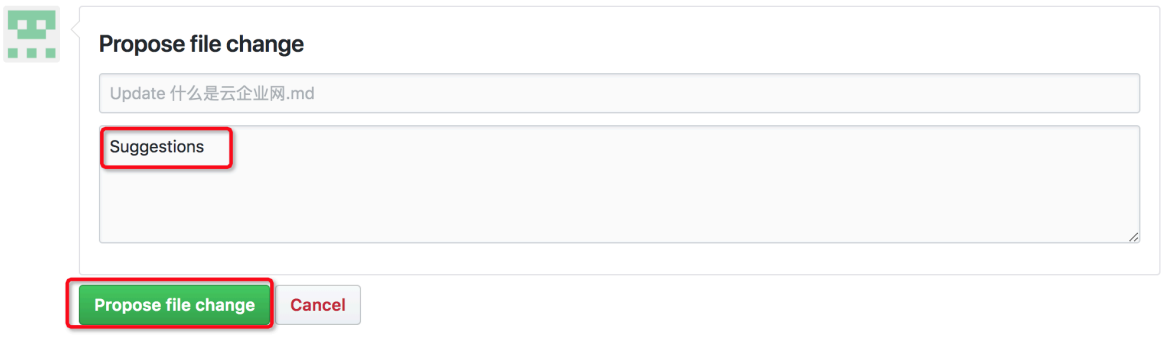


4. 在预览框Preview changes中确认修改结果，如图 3所示。

   图 1-3: 预览结果

5. 确认无误后，在Propose file change框中填写修改意见后，单击Propose file change提交修改建议，如图 1-4: 提交修改所示。

   图 1-4: 提交修改



预期结果

阿里云会根据内容开源规定审核和处理您所提交的修改建议。

感谢您对阿里云文档的支持和帮助。

2 使用阿里云管理控制台

欢迎使用阿里云管理控制台。本指南简要介绍如何使用阿里云管理控制台。如果您需要了解控制台提供的具体服务功能，请参见具体的产品文档。 本指南主要内容包括：

- 初步了解阿里云管理控制台
- 开始使用产品与服务
- 添加或删除快捷菜单
- 修改密码
- 获取计费信息
- 设置消息接收
- 备案
- 帮助与文档
- 提交工单
- 使用移动终端设备
- 浏览器兼容性

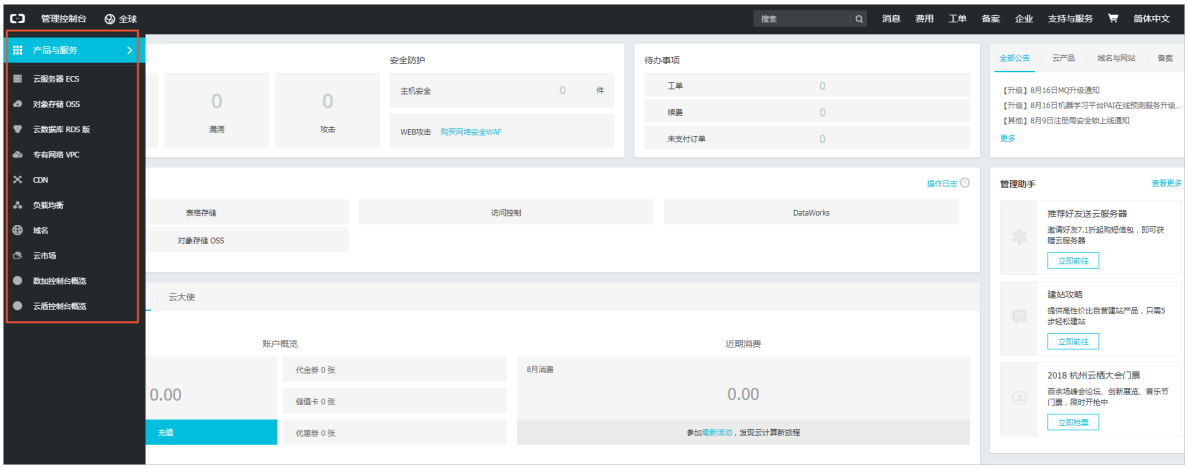
初步了解阿里云管理控制台

阿里云管理控制台是用于管理阿里云云产品的Web应用程序。该控制台提供直观的用户界面。您可通过该控制台管理阿里云产品，如启动并连接到ECS实例、使用OSS存储空间、设置报警监控等。您可以从阿里云管理控制台进入到各个产品或服务的控制台，也可以通过产品详情页面进入到该产品或服务的控制台进行访问。控制台还提供有关您的账户和账单的信息。

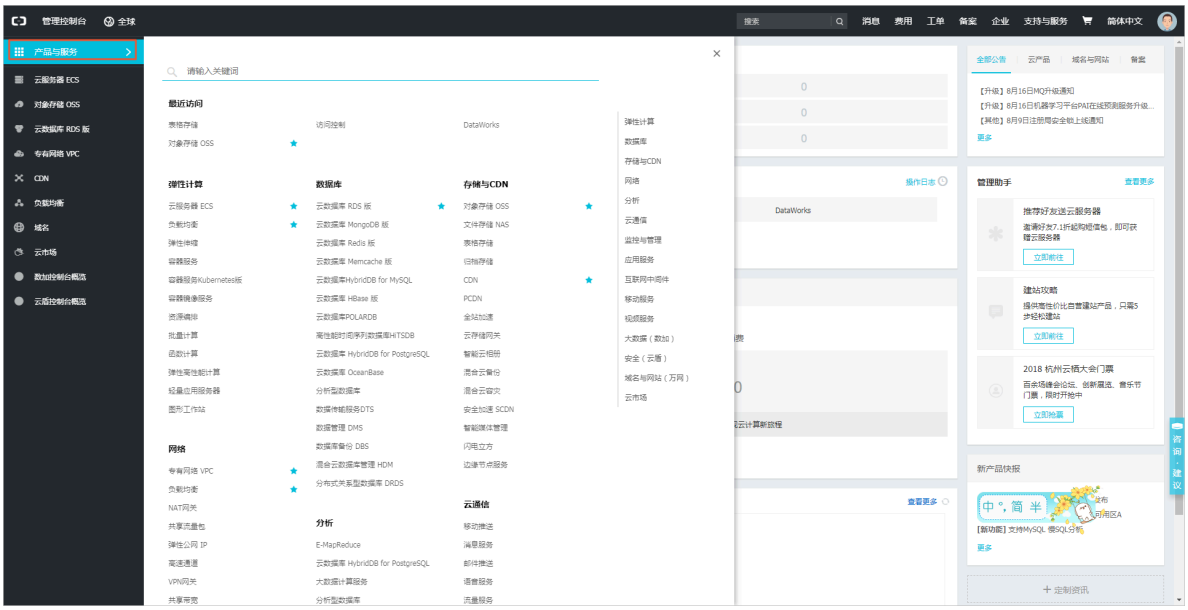
开始使用产品与服务

您可以在控制台中访问产品与服务。

1. 阿里云管理控制台左侧的产品快捷入口导航中列出了常用的产品与服务项目。



2. 单击左侧导航栏中的产品与服务可打开完整的产品和服务列表。

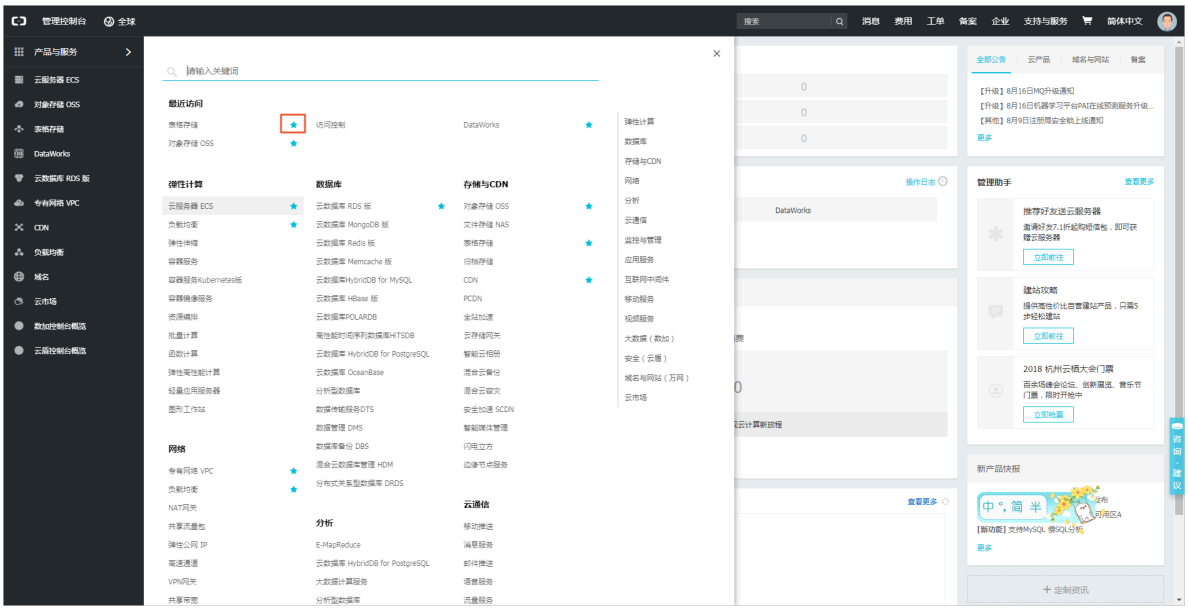


3. 单击某个产品或服务名称可打开该产品或服务的控制台。

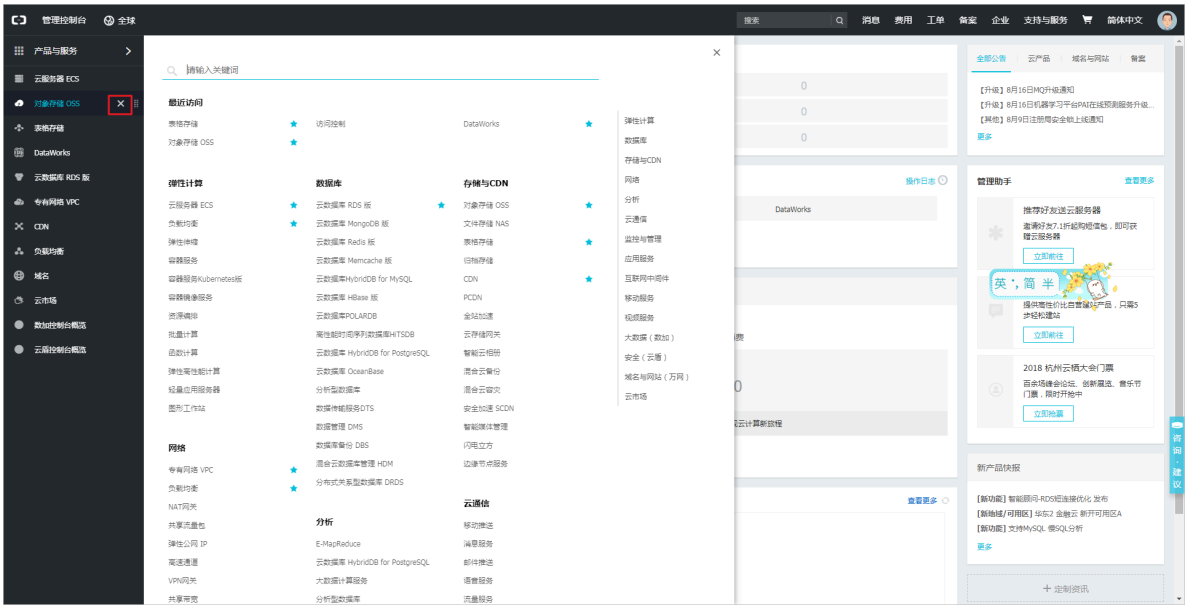
添加和删除快捷方式

您可以为常用的控制台添加快捷方式或者删除已有的快捷方式。

- 单击左侧导航栏中的产品与服务打开完整的产品和服务列表，单击任意产品右侧的对应图标 ★ 可将该产品添加到常用的控制台列表中。



- 从已添加到左侧导航栏的产品与服务中，单击图标 × 可将该产品从左侧导航栏中删除。



修改密码

您可以在控制台修改您的阿里云账户密码。

1. 在阿里云管理控制台顶部导航栏中，单击您的账号。

2. 在安全设置页面，单击登录密码对应的修改链接。

3. 在验证身份页面，选择身份验证方式。
   - 如果选择通过手机验证码，请确保您的手机还在正常使用，单击立即验证。然后进入步骤4。
   - 如果选择通过人工服务，单击立即申请，然后进入步骤5。
4. 通过手机验证码修改密码。
   a. 在验证码框中，单击免费获取，然后输入您收到的6位数字验证码。单击确定。
   b. 输入当前登录密码和新的登录密码并确认，然后单击确定。
5. 通过人工服务修改密码。
   a. 填写基本资料，包括登录账户名称、联系人名称、联系邮箱、联系手机、申诉原因等，单击下一步。
   b. 按要求上传账号所有人的证件信息，然后单击提交申诉。系统会在3个法定工作日内将申诉结果以短信和邮件的形式发送到您填写的联系手机和联系邮箱。
   c. 审批通过后，您填写的联系手机将被更新到您的账户绑定上，您可以使用联系手机自助找回密码。

获取账单信息

您可以从控制台获取您的阿里云账单信息。

1. 在阿里云管理控制台顶部导航栏中，单击费用。
2. 在费用中心页面，您可以查看账户总览、收支明细、消费记录、订单管理、代金券和优惠券管理等信息。

设置消息接收

您可通过控制台设置消息接收，包括接收人和接收方式等。

1. 在阿里云管理控制台顶部导航栏中，单击消息，进入消息中心页面。
2. 单击左侧菜单中的消息接收管理。系统列出所有的消息类型以及对应的接收人和接收方式。
3. 修改各类消息的接收方式，包括邮箱和短息。系统默认的消息接收人为账号联系人，您可以单击修改添加或删除消息接收人。

备案

备案是指向主管机关报告事由存案以备查考。在中华人民共和国境内提供非经营性互联网信息服务，必须办理备案。

您可以通过控制台注册并登录阿里云代备案管理系统。在阿里云管理控制台最上方的导航栏选择备案。

帮助与文档

控制台提供了各种帮助资源的入口，包括产品文档、阿里云开发者论坛、以及云栖社区的入口。

在阿里云管理控制台顶部导航栏中选择支持与服务 > 帮助与文档。

提交工单

您可以通过控制台的工单系统提交咨询类和技术类的问题，阿里云将尽快为您解答。

1. 在阿里云管理控制台顶部导航栏中选择 工单 > 提交工单。
2. 在提交工单页面，您可以选择咨询类问题和技术类问题提问。针对您的问题类型，单击对应的提问按钮。
3. 选择您遇到的具体问题类型。系统将列出针对这一类型的热点问题。
   - 如果您的问题已经在列表中，请单击此问题查阅解决方案。如果此解决方案无法解决您的问题，请单击提交工单。
   - 如果您的问题不在列表中，请单击以上没有包含您遇到的问题。在弹出的搜索框中输入您的问题并单击搜本产品或搜全部。系统将列出所有与您的问题相关的内容，如果您仍然无法找到满意的答案，请单击提交工单。
4. 在提交工单页面，选择问题的优先级，输入您的服务器IP地址，留下您的联系方式，也可简单描述您的问题并上传附件。完成后单击提交。

    说明:
   阿里云会对用户设置的工单优先级进行审核。审核确认为紧急的工单，阿里云将在两小时内进行回复。
5. 提交工单后，您可以在我的工单中查看工单处理进程。

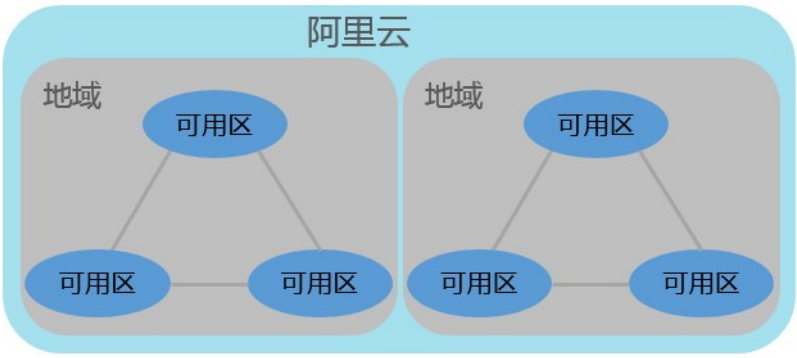
浏览器兼容性

建议使用IE9.0+、Chrome 53+、 firefox50+等版本浏览器访问阿里云官网。通过其他版本浏览器访问可能会出现功能（包括支付等功能）显示不完整。若您使用非以上浏览器访问阿里云官网遇到问题时，建议您及时更换或更新浏览器版本。

3 地域和可用区

本文提供完整的阿里云地域和可用区列表。

每个地域完全独立。每个可用区完全隔离，但同一个地域内的可用区之间使用低时延链路相连。地域和可用区之间的关系如下图所示。



地域（Region）

地域是指物理的数据中心。资源创建成功后不能更换地域。当前所有的地域、地域所在城市和 Region ID 的对照关系如下表所示。

> 说明:
> 不同产品可选择的地域有所不同，请您查看阿里云全球基础设施 确认各产品可选择的地域列表。

- 中国大陆

地域名称	所在城市	Region ID	可用区数量
华北 1	青岛	cn-qingdao	2
华北 2	北京	cn-beijing	7
华北 3	张家口	cn-zhangjiakou	2
华北 5	呼和浩特	cn-huhehaote	2
华东 1	杭州	cn-hangzhou	8
华东 2	上海	cn-shanghai	6
华南 1	深圳	cn-shenzhen	5

- 其他国家和地区

地域名称	所在城市	Region ID	可用区数量
香港	香港	cn-hongkong	2

地域名称	所在城市	Region ID	可用区数量
亚太东南 1	新加坡	ap-southeast-1	3
亚太东南 2	悉尼	ap-southeast-2	2
亚太东南 3	吉隆坡	ap-southeast-3	2
亚太东南 5	雅加达	ap-southeast-5	2
亚太南部 1	孟买	ap-south-1	2
亚太东北 1	东京	ap-northeast-1	2
美国西部 1	硅谷	us-west-1	2
美国东部 1	弗吉尼亚	us-east-1	2
欧洲中部 1	法兰克福	eu-central-1	2
英国（伦敦）	伦敦	eu-west-1	2
中东东部 1	迪拜	me-east-1	1

选择地域时，您需要考虑以下几个因素：

· 地理位置

您需要根据您以及自己的目标用户所在的地理位置选择地域。

- 中国大陆

一般情况下建议选择和您目标用户所在地域最为接近的数据中心，可以进一步提升用户访问速度。不过，在基础设施、BGP 网络品质、服务质量、云服务器操作使用与配置等方面，阿里云中国大陆地域没有太大区别。中国大陆 BGP 网络可以保证中国大陆全部地域的快速访问。

- 其他国家及地区

其他国家及地区提供国际带宽，主要面向非中国大陆地区用户。如果您在中国大陆，使用这些地域会有较长的访问延迟，不建议您使用。

■ 对香港、东南亚有需求的用户，可以选择香港地域、亚太东南 1 地域、亚太东南 3 地域或亚太东南 5 地域。

■ 对日、韩有需求的用户，可以选择亚太东北 1 地域。

■ 对印度有需求的用户，可以选择亚太南部 1 地域。

■ 对澳大利亚地区有需求的用户，可以选择亚太东南 2 地域。

■ 对美洲有需求用户，可以选择美国地域。

■ 对欧洲大陆有需求的用户，可以选择欧洲中部 1 地域。

■ 中东用户，可以选择中东东部 1 地域。

- 阿里云产品之间的关系

  如果多个阿里云产品一起搭配使用，需要注意：

  - 不同地域的云服务器 ECS、关系型数据库 RDS、对象存储服务 OSS 内网不互通。
  - 不同地域之间的云服务器 ECS 不能跨地域部署负载均衡，即在不同的地域购买的 ECS 实例不支持跨地域部署在同一负载均衡实例下。

- 资源的价格

  不同地域的资源价格可能有差异，请参见阿里云产品定价页面。

- 关于经营许可证备案

  选择地域时您需要考虑某些地区的特殊要求。如您在中国大陆地域购买了 ECS 实例，并用于 Web 服务器，您需要完成经营许可证备案。

  如您有办理经营许可证备案的需求，请您重点关注：

  - 北京地区企业，请选择购买的地域为华北 2。
  - 广东地区企业，请选择购买的地域为华南 1。

  > 说明：
  > 各省通信管理局对经营性备案的审批要求不同，如有变化，请以当地管局经营性备案网站公示内容为准。请参考《各省经营性备案网站链接》。

可用区（Zone）

可用区是指在同一地域内，电力和网络互相独立的物理区域。同一可用区内实例之间的网络延时更小。

在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求。

- 如果您的应用需要较高的容灾能力，建议您将实例部署在同一地域的不同可用区内。
- 如果您的应用要求实例之间的网络时延较低，则建议您将实例创建在同一可用区内。

有关地域和可用区的更多信息，请参见阿里云全球基础设施。

4 产品使用限制

在选购和使用阿里云产品之前，建议您阅读相关的使用限制和说明，包括实例规格、实例的使用约束和功能限制、带宽、云盘容量等。

各产品使用限制相关链接请参见下表。

弹性计算

产品	限制
云服务器ECS	· *ECS*使用须知 · 使用限制
弹性伸缩	使用限制
容器服务	· *Swarm* 使用限制 · *Kubernetes* 使用限制
批量计算	使用限制
函数计算	使用限制
专有宿主机	使用限制

数据库

产品	限制
云数据库RDS版	· *MySQL*使用限制 · *SQL Server*使用限制 · *PostgreSQL*使用限制 · *PPAS*使用限制
云数据库MongoDB版	使用限制
HybridDB for MySQL	使用限制
HybridDB for PostgreSQL	使用限制
云数据库 Redis 版	使用限制
云数据库 Memcache 版	使用限制

网络

产品	限制
负载均衡	使用限制
高速通道	使用限制
专有网络VPC	使用限制
NAT网关	使用限制

存储与CDN

产品	限制
对象存储OSS	使用限制
表格存储	使用限制
CDN	使用限制
文件存储	NFS 文件系统不支持特性

安全

产品	限制
SSL证书	使用限制

视频服务

产品	限制
媒体处理	使用限制
视频直播	使用限制

互联网中间件

产品	限制
消息队列 MQ	使用限制

5 主账号安全实践

阿里云主账号相当于您的所有云资源管控的 root 账号。一旦主账号的登录密码或 API 访问密钥丢失或泄露，将会对您的企业造成不可估量的损失。

那么，在使用阿里云服务时，如何保护您的主账号安全呢？请参考本文提供的主账号安全实践若干原则。

原则 1：给主账号开启多因素认证

- 给主账号开启多因素认证(MFA)，不要与他人共享 MFA 设备。
- 给授予特权操作的RAM 用户也开启多因素认证。特权操作通常指管理用户、授权、停止/释放实例、修改实例配置、删除数据等。

原则 2：不要使用主账号进行日常运维管理操作

- 给员工创建 RAM 用户账号，进行日常的运维管理操作。
- 为财务人员创建独立的 RAM 用户账号。
- 创建独立的 RAM 用户账号来作为 RAM 管理员。

原则 3：不要为主账号创建 AccessKey

AccessKey 与登录密码具有同样的特权，AccessKey 用于程序访问，登录密码用于控制台登录。由于 AccessKey 通常以明文形式保存在配置文件中，泄露的风险更高。

给所有的应用系统配置 RAM 用户身份，并在 为 *RAM* 用户授权 时遵循最小授权原则。

原则 4：使用带 IP 限制条件的授权策略进行授权

授予所有的特权操作 必须受 *IP* 条件限制*#acs:SourceIp#*。

那么，即使 RAM 用户的登录密码或 AccessKey 泄露，只有攻击者没有渗透进入您的可信网络，那么攻击者也无能为力。

原则 5：使用带 MFA 限制条件的授权策略进行授权

授予所有的特权操作 必须受 *MFA* 条件限制*#acs:MFAPresent#*。

那么，即使 RAM 用户的登录密码或 AccessKey 泄露，只要 MFA 设备没有丢失，攻击者也无能为力。

更多限制条件，请参考 *Policy*语法结构。

没有绝对的安全，只有最佳的实践。只有遵循最佳安全实践原则，综合利用这些保护机制，相信可以极大提高对您的账号资产的保护。

6 RAM 企业上云安全实践

本文为您介绍当企业上云之后，通过 RAM 进行安全管控，帮助您实现简单管理账号、统一分配权限、集中管控资源，建立安全完善的资源控制体系。

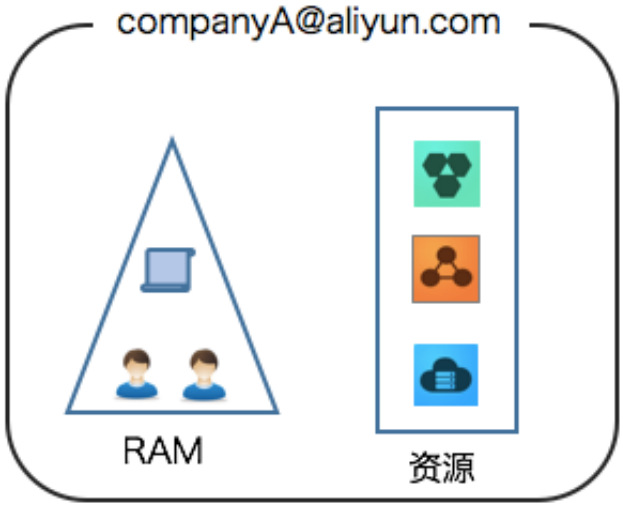
背景信息

某些公司使用 RAM 初期，对 RAM 的优势不够了解，也对云资源的安全管理要求不高。但是当初创企业成长为大型公司，或大型企业客户迁移上云，他们的组织结构更加复杂，对云资源的安全管理需求也更加强烈，需要建立安全完善的资源控制体系。

- 存在多用户协同操作，RAM 用户分工不同，各司其职。
- 主账号不想与其他 RAM 用户共享主账号密钥，密钥泄露风险较大。
- RAM 用户对资源的访问方式多种多样，资源泄露风险高。
- 某些 RAM 用户离开组织时，需要收回其对资源的访问权限。

解决方案

使用 RAM，您可以创建、管理 RAM 用户，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时，使用 RAM 可以让您避免与其他用户共享主账号密钥，按需为用户分配最小权限，管理更加方便，权限更加明确，信息更加安全。



安全管理实施方案

- 创建独立的 RAM 用户

  企业只需使用一个主账号。通过 RAM 为名下的不同操作员创建独立的 RAM 用户，进行分权管理，不使用主账号进行日常运维管理。

  详情请参考：创建 RAM 用户。

- 将控制台用户与 API 用户分离

  不建议给一个 RAM 用户同时创建用于控制台操作的登录密码和用于 API 操作的访问密钥。

  - 对于应用程序账号，只需要通过 OpenAPI 访问云资源，只需要给它创建访问密钥即可。
  - 对于员工账号，只需要通过控制台操作云资源，只需要设置登录密码即可。

  详情请参考：创建 RAM 用户。

- 创建用户并进行分组

  当主账号下有多个 RAM 用户时，可以通过创建用户组对职责相同的 RAM 用户进行分类并授权。

  详情请参考：创建 RAM 用户组#可选#。

- 给不同用户组分配最小权限

  您可以使用系统策略为用户或用户组绑定合理的权限策略，如果您需要更精细粒度的权限策略，也可以选择使用自定义策略。通过为用户或用户组授予最小权限，可以更好的限制用户对资源的操作权限。

  详情请参考：权限策略管理。

- 为用户登录配置强密码策略

  您可以通过 RAM 控制台设置密码策略，如密码长度、密码中必须包含元素、密码有效期等。如果允许子用户更改登录密码，那么应该要求他们创建强密码并且定期轮换登录密码或访问密钥。

  详情请参考：RAM 初始设置。

- 给主账号开启多因素认证

  开启 MFA（Multi-factor authentication，多因素认证）可以提高账号的安全性，在用户名和密码之外再增加一层安全保护。启用 MFA 后，用户登录阿里云时，系统将要求输入两层安全要素：

  - 第一安全要素：用户名和密码。
  - 第二安全要素：来自其虚拟 MFA 设备的可变验证码。

  详情请参考：设置 MFA#可选#。

- 为用户开启SSO单点登录功能

  开启SSO单点登录后，企业内部账号进行统一的身份认证，实现使用企业本地账号登录阿里云才能访问相应资源。

  详情请参考：阿里云用户 SSO 的 SAML 配置。

- 不要为主账号创建访问密钥

  由于主账号对名下资源有完全控制权限，AccessKey 与登录密码具有同样的权力，AccessKey 用于程序访问，登录密码用于控制台登录。为了避免因访问密钥泄露带来的信息泄露，不建议您创建主账号访问密钥并使用该密钥进行日常工作。

  详情请参考：管理访问密钥。

- 使用策略限制条件来增强安全性

  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。

  详情请参考：Policy 基本元素。

- 集中控制云资源

  阿里云默认主账号是资源的拥有者，掌握完全控制权。子账号对资源只有使用权，没有所有权。这一特性可以方便您对用户创建的实例或数据进行集中控制。

  - 当用户离开组织：只需要将对应的账号移除，即可撤销所有权限。
  - 当用户加入组织：只需创建新的账号，设置登录密码或访问密钥并为 RAM 用户授权。

  详情请参考：为 RAM 用户授权。

- 使用 STS 给用户授权临时权限

  STS （Security Token Service）是 RAM 的一个扩展授权服务，使用 STS 访问令牌可以给用户授予临时权限，您可以根据需要来定义访问令牌的权限和自动过期时间，可以让授权更加可控。

  详情请参考：#unique_52。

操作结果

遵循最佳安全实践原则，企业上云之后，综合利用这些保护机制，建立安全完善的资源控制体系，可以更有效的保护账号及资产的安全。

更多信息

企业上云以后通过 RAM 进行运维划分，根据不同的职责，划分不同的运维人员，方便管理和控制。详情请参考：RAM 对多运维人员的权限管控。

7 创建AccessKey

访问密钥AccessKey（AK）相当于登录密码，只是使用场景不同。AccessKey用于程序方式调用云服务API，而登录密码用于登录控制台。如果您不需要调用API，那么就不需要创建AccessKey。

您可以使用AccessKey构造一个API请求（或者使用云服务SDK）来操作资源。AccessKey包括AccessKeyId和AccessKeySecret。

- AccessKeyId用于标识用户。
- AccessKeySecret是用来验证用户的密钥。AccessKeySecret必须保密。

 警告:

禁止使用主账号AK，因为主账号AK泄露会威胁您所有资源的安全。请使用子账号AK进行操作，可有效降低AK泄露的风险。

操作步骤

1. 登录*RAM*管理控制台。
2. 在左侧导航栏，单击用户管理。
3. 单击需要创建AccessKey的用户名，进入用户详情页面。
4. 在用户AccessKey区域，单击创建AccessKey。
5. 在弹出的对话框中，展开AccessKey详情查看AcessKeyId和AccessKeySecret。然后单击保存AK信息，下载AccessKey信息。

 注意:

请您妥善保存AccessKey，谨防泄露。

8 备案

备案是中国大陆的一项法规，使用大陆节点服务器开办网站的用户，需要在服务器提供商处提交备案申请。

关于备案的详细介绍和流程指导，请您参见备案。