阿里云
阿里政务云

新手上路

文档版本：20190815

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

法律声明.....I
通用约定.....I
1 上云须知..... 1
2 注册账号并认证..... 3
3 登录阿里政务云..... 5
4 购买与使用..... 7
5 如何选用政务云产品.....8
5.1 如何选用云服务器.....8
5.2 如何选用存储类产品.....10
5.3 如何选用数据库类产品.....12
5.4 如何选用安全类产品.....15
6 政务云云产品使用安全规范.....21
6.1 ECS安全配置.....21
6.2 SLB安全配置.....23
6.3 RDS安全配置.....23
6.4 Memcache安全配置.....24
6.5 OSS安全配置.....24
6.6 CDN与视频服务安全加固.....25
主账号安全配置.....25

1 上云须知

阿里政务云主要服务于政务用户，基于合规需求和安全考虑，阿里政务云与公共云在使用上有部分区别，请在使用阿里政务云前仔细阅读本文档。

开放地域

阿里政务云采用独立机房集群部署，根据客户需求逐步开放，目前已经开放的地域有“华北2 阿里政务云1”地域，本地域：

- 包含两个可用区：华北2 阿里政务云1 可用区A（cn-north-2-gov-1a）和华北2 阿里政务云1 可用区B（cn-north-2-gov-1b）。
- 均使用VPC网络环境，支持用户自定义网络地址。
- 支持用户通过互联网访问政务云服务，或使用专线、SSL VPN接入政务云平台。

账号使用须知

成为政务云用户时，建议您注册专门的阿里云账号，并通过实名认证、政务云认证后成为政务云账号。此账号一旦完成政务云认证，将无法使用公共云资源。注册政务云账号请注意：

- 账号隔离：
  - 政务云平台支持通过账号隔离实现环境隔离，不同账号的云资源之间相互隔离。
  - 支持为不同环境（如生产环境、预生产环境、UAT测试环境、开发/集成测试环境）申请单独的阿里云账号。
- 政务云认证：
  - 同一个企业实体可以为多个政务云账号提供认证。
  - 成功认证为阿里政务云的客户账号将无法使用公共云的资源。
  - 使用公共云账号进行政务云认证时，需先释放公共云账号内的所有公共云资源。
  - 为了方便账号管理，建议申请新阿里云账号用于阿里政务云业务。

互联网访问限制

阿里政务云实行了严密的符合政务行业规范的风控措施，在互联网访问上，有以下访问限制：

- 访问控制台：阿里政务云客户访问网页控制台需要设定开通MFA，输入账户的用户名密码后，需再次对动态密钥进行验证。
- 远程运维操作：需MFA（多因素认证）并设置相应的安全组规则，才能对ECS进行远程运维操作。
- 访问RDS：不能使用阿里政务云分配的内网IP直接访问RDS，RDS仅对内网的ECS开放。

- **互联网访问云产品：阿里政务云在网络访问方向和端口上进行了限制，不支持目前公共云互联网访问：**
  - **ECS不能被外网直接访问，互联网用户只能通过负载均衡间接访问ECS，带宽在SLB上选取。**
  - **ECS需要主动发起互联网访问时，在ECS选取外网带宽，否则带宽选0。**
  - **负载均衡允许对互联网开放的端口为80、443、2800-3300、5000-10000、13000-14000、21234、22223和22225。**

2 注册账号并认证

成为政务云用户开始使用政务云产品时，需首先注册阿里云账号并完成相应的认证流程。

背景信息

- 注册账号：政务云账号无法使用阿里公共云资源，建议您注册一个全新的账号用于政务云业务。
- 实名认证：实名认证决定了阿里云账号归属，如果账号归属于某个企业/政府，请进行企业/政府实名认证。政务云场景下请使用企业/政府实名认证。

更多政务云账号注意点请参考 阿里政务云账号体系 章节。

操作步骤

1. 注册账号。
   a) 登录 阿里云官网：https://www.aliyun.com/。
   b) 在页面右上角单击 免费注册 。
   c) 根据页面提示，输入账号信息并完成账号注册。
   d) （可选）您可以根据界面提示进一步完成邮箱绑定，完善您的账号信息。

      绑定邮箱时建议使用企业邮箱。

      > 说明:
      > 请牢记您的用户名与密码，后续使用此用户名与密码登录阿里云官网页面进行控制台操作。

2. 实名认证。
   a) 使用上述注册的阿里云账号、密码登录 阿里云官网 。
   b) 单击您的账号名，进入阿里云 账号管理 页面： https://account.console.aliyun.com。
   c) 在左侧导航栏中选择 实名认证 页签，根据您的实际需求选择 个人实名认证 或者 企业/政府实名认证。
   d) 在右侧页面中选择合适的认证方式后单击 立即认证 。

      > 说明:
      > 如果选择企业银行卡信息认证，认证时需要提供公司对公账号等企业信息。阿里云会向您提供的对公账号打入一笔小的款项，将这个金额输入后续的步骤就可以完成认证。

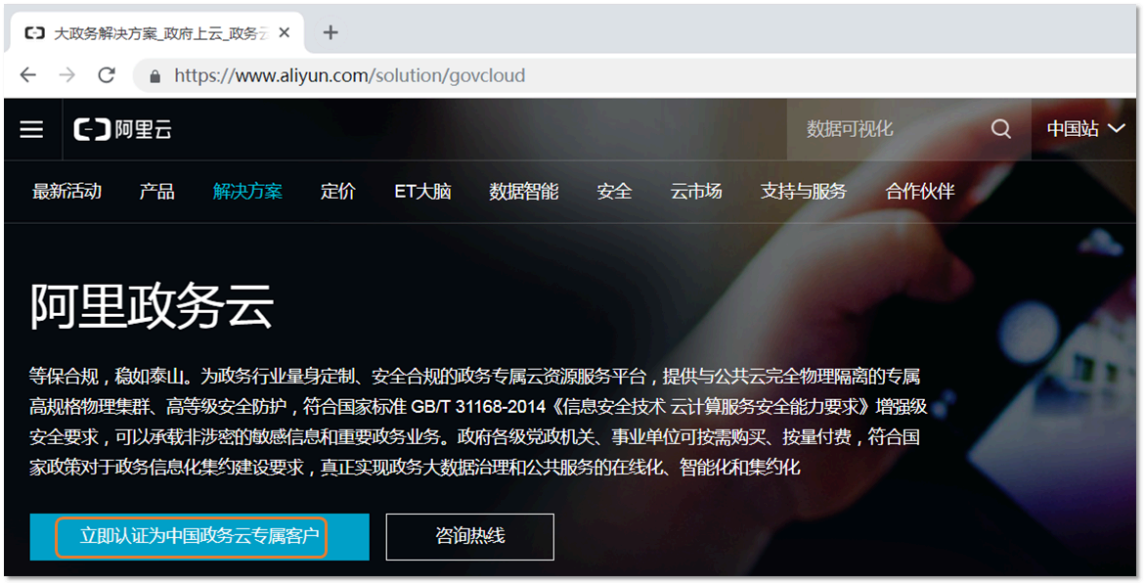
   e) 根据页面提示，完善认证信息。

3. 政务云认证。

a) 使用上述注册的阿里云账号、密码登录 阿里云官网 。

b) 鼠标悬浮于页面上方的解决方案，在下拉页面中选择行业解决方案 > 数字政府解决方案，进入阿里政务云详情页面。

c) 在政务云页面单击 立即认证为阿里政务云专属客户 。



d) 在弹出的页面中，根据实际情况填写阿里政务云平台入驻申请表，完成后单击 提交 。

3 登录阿里政务云

已完成政务云注册账号并认证后，您可以使用此账号登录政务云平台，用于后续购买使用政务云产品。

背景信息

- 登录阿里政务云平台前，请先确认已完成注册账号并认证。
- 为满足政务云安全等保要求，用户账号需绑定MFA（多因素认证），增强用户账号登录的安全性。

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）。双因素的安全认证将为您的账户提供更高的安全保护。

您可以使用阿里云APP（V4.6 及以上版本）绑定MFA认证，操作步骤请参考 如何进行 MFA 的绑定和使用文档，如果您使用例如“Google Authenticator”等APP绑定MFA认证，可参考以下步骤。

说明:

- 使用阿里云APP绑定MFA认证时，支持Android和iPhone类型的手机，且阿里云APP需使用V4.6及以上版本。
- 如果您此前已使用例如“Google Authenticator”等APP绑定MFA认证，可参考 如何完成 MFA 应用切换 章节切换为阿里云APP。

操作步骤

1. 登录阿里云官网后，单击您的账号名，进入阿里云 账号管理 页面： https://account.console.aliyun.com。

2. 在 安全设置 页签中找到 虚拟MFA，单击 设置 。

3. 在弹出的页面中，根据设置导航完成绑定。

   a) 验证身份：根据您的实际情况选择手机验证码验证或人工服务验证。

   b) 安装应用。

   虚拟MFA应用可安装于您的智能手机，请根据您的手机类型，在主流应用商店中搜索下载对应的虚拟MFA应用。

手机类型	MFA应用程序	logo样例
Android	谷歌动态口令	
iPhone	Google Authenticator	
Windows Phone	身份验证器	
Blackberry	Google Authenticator	

   c) 绑定TOTP：在智能手机上打开应用，扫描页面中的二维码。如果您需要在多台终端设备间共享安全码，则可在多个智能手机上安装 MFA 应用，并分别扫码条形码，确保每一个设备都添加相关用户并显示安全码（请检查各设备的动态口令是否一样）后再进行下一步骤。

   > 说明:
   > 此二维码中包含MFA密钥，仅有一次机会出现，请您务必不要泄露此二维码。

   d) 单击 下一步 绑定成功。

4. 重新登录。

   a) 退出管理控制台。

   b) 输入用户名、密码后单击 登录 。

   c) 打开智能手机中的MFA应用，查看动态动态口令并输入登录页。

   d) 完成登录。

4 购买与使用

完成政务云账号注册并认证后，正常登录政务云平台后，您可以根据您的业务需求购买并使用政务云产品。

政务云平台部署有多种类型云产品，可满足政务类客户的多种业务需求。政务云平台上的产品详细列表可参考 政务云产品全家福 章节。

政务云平台上产品与公共云产品技术和使用上基本保持一致。您可参考各产品的公共云帮助文档购买云产品并搭建您的政务业务。

5 如何选用政务云产品

5.1 如何选用云服务器

在阿里政务云上，云服务器有很多不同的规格型号，例如都是4核8G内存的云服务器，在不同应用场景下的性能跑分不同，价格也不同。本文为您介绍阿里云云服务的常见参数类别，帮助您根据不同的业务需求选择合适的云服务。

云服务器参数对比介绍

以下以云服务器的CPU使用率、数据盘、规格族三个参数为例，介绍说明不同的参数型号适合的业务场景。

- CPU使用率

  云服务器的CPU使用可分为共享型与独享型。

  - 共享型云服务器：根据租户业务需求及服务器的CPU忙闲状态，动态分配CPU给租户使用。
  - 独享型云服务器：租户完全独占此服务器的CPU，无论CPU的忙闲状态如何，此服务器在一段时间内专属某个租户，不会分配给其他租户使用。

CPU系列	规格族	优点	缺点	适合业务
共享实例	S,N,C,E,M等等系列，需以官网为准	价格便宜，资源丰富	有CPU积分，多少积分跑多少运算能力	学校，简单应用，冷业务（例如容灾）等
独享实例	主要为SN系列	独占虚拟CPU，稳定性高	资源有限，价格较贵	不能接受CPU波动影响的业务，数据库，中间件，核心服务器等

说明:

一般政务类客户建议选择独享实例，以保障业务的安全、稳定性。

- 数据盘

  在阿里政务云中，云服务器的数据盘（包括系统盘）一般会有三种选择：SSD云盘，高效云盘以及本地盘：

数据盘系列	最大容量	最大IOPS	最大吞吐量	访问时延	数据可靠性
SSD云盘	32768GB	20000+	256 MBps	0.5~2 ms	极高

数据盘系列	最大容量	最大IOPS	最大吞吐量	访问时延	数据可靠性
高效云盘	32768GB	3000+	80 MBps	1~3 ms	极高
本地盘	1456GB*2	240000+	2000 MBps	<0.2 ms	非持久型块存储，实例释放，数据丢失

- 规格族

  在阿里政务云中，云服务器的规格有通用型、计算型、内存型：

规格系列	处理器与内存配比	IPV6	I/O优化	云盘类型	建议配置	建议购买时长
通用型	1:4	√	√	SSD 高效	ecs.g5.xlarge 4C16G	包年包月/按量
计算型	1:2	√	√	SSD 高效	ecs.c5.xlarge 4C8G	按量
内存型	1:8	√	√	SSD 高效	ecs.r5.xlarge 4c32g	按量

说明:

裸金属和GPU类型的云服务即将在阿里政务云上线，敬请关注。

通过上述对比，建议政务类行业：

- 一般配置选择4C 8G / 4C 16G /4C 32G之间即可满足。
- 个别小型应用可以等比调低CPU CORE数至2CORE，但不建议1CORE，因为在1CORE的情况下运行部分操作系统会有卡顿，延迟，给业务带来不了更好的服务，价格相差也较少，通俗的说就是性价比不高。
- 海量采购时，需要精细的对此进行计算。

客户案例

某政府用户打算在阿里政务云上搭建属于自己的业务平台，其中包括政府网站，内部移动应用，数据分析平台以及视频直播平台。

在这个场景中，根据客户的需求进行区分，一般情况下，在日均访问量5000以内，产品搭配如下：

业务需求	CPU系列	数据盘	规格族	数目
网站服务器	独享型	高效云盘	通用型，4C 16G	2台
内部移动应用	独享型	数据盘为高效云盘，系统盘为SSD	通用型，4C 16G，	2台
数据分析平台	独享型	系统盘数据盘均为SSD	计算型，8C 16G	4台
视频直播平台	独享型	系统盘为SSD数据盘为SSD/高效云盘	内存型 4C 32G	2台
流量处理	独享型	不需要单独购置数据盘	通用型 4C 16G	2台

5.2 如何选用存储类产品

在阿里政务云上存储类产品可主要分为：块存储，对象存储，文件存储三个类别。本文为您介绍这三类存储产品区别，帮助您根据您的业务现状及需求选用合适的存储类产品，避免因不熟悉同类产品而采购不适宜的产品，给后续使用、购买、经费控制等带来不便。

存储类产品对比介绍

下面从主要的几个参数项对块存储、对象存储、文件存储进行对比介绍：

对比项	块存储	对象存储	文件存储
IO特点	随机读写	追加随机读	随机读写
应用访问接口	POSIX接口	SDK、RESTful	POSIX接口
并发客户端数	数十级别	千级别	千级别
容量	GB~12TB	GB~PB级别	GB~PB级别
吞吐量	GB/s	数十GB/s	数十GB/s
IOPS（4K随机）	百万级别	千级别	十万级别
访问时延	百US级别	几十MS级别	MS级别
文件级的授权	不支持	支持	支持

通过上述参数的对比可见各类存储产品的优势：

- 块存储（ECS）：

  在低延时高IOPS上有明显优势，特别适合数据库等高性能IO场景。

  购买链接：https://ecs-buy.aliyun.com/disk#/cloudDisk/cn-north-2-gov-1

- 对象存储（OSS）：

  在海量和吞吐上有明显优势，特别适合互联网图片、音视频处理场景。

  购买链接：https://www.aliyun.com/product/oss

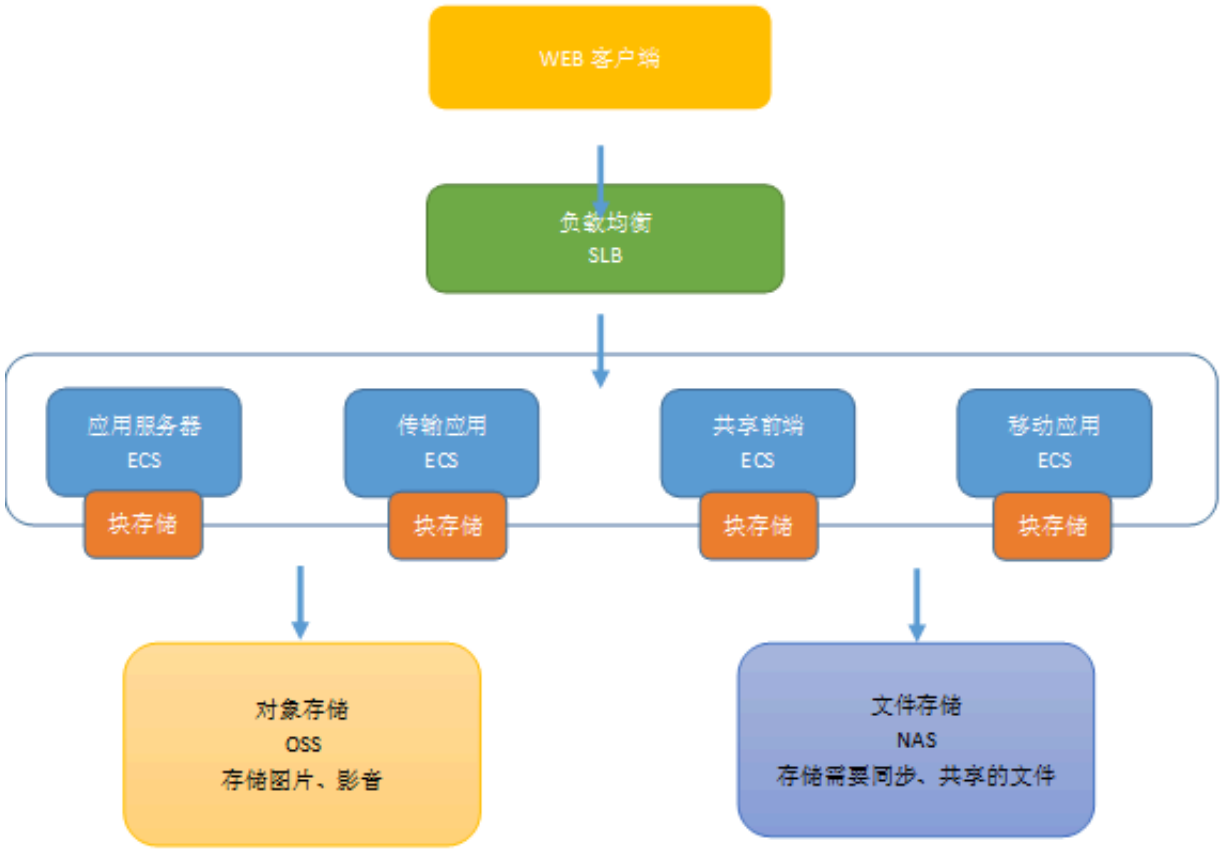
- 文件存储（NAS）：

  在吞吐和共享上有明显优势，特别适合高性能计算、以及数据共享场景。

  购买链接：https://www.aliyun.com/product/nas

客户案例

某政府单位提供了某项供社会群众访问和使用的业务应用，其应用可以对互联网用户提供音视频上传下载功能，也同时具备文件共享功能，对于这类场景我们可以采用以下架构：



5.3 如何选用数据库类产品

在阿里政务云上数据库类产品类型较多，其中关系型数据库包括：RDS系列、DRDS。NoSQL型数据库包括：Redis、MongoDB。本文为您介绍这几类数据库产品的区别，帮助您根据您的业务现状及需求选用合适的数据库类产品，避免因不熟悉同类产品而采购不适宜的产品，给后续使用、购买、经费控制等带来不便。

数据库类产品对比介绍

阿里政务云的数据库包括关系型数据库、NoSQL型数据库，其中每类数据库又分基础版、高可用版、集群版，分别可用于不同的政务场景。以RDS为例，下表为您对比介绍基础版、高可用版、集群版分别可用于什么样的政务类场景。

数据库系列	说明	适用政务场景
基础版	单节点实例，采用计算与存储分离的架构，可实现超高的性价比。 详细信息，请参见基础版。	· 政务数据库业务测试 · 小型政府网站后台数据库 · 政务开发环境
高可用版	采用一主一备的经典高可用架构，适合80%以上的用户场景。	· 大中型政府的内部数据库 · 面向广大民众，访问量较高的核心数据库

数据库系列	说明	适用政务场景
集群版	适用于SQL Server 2017 企业版，基于AlwaysOn技术实现，最大支持一主一备高可用架构和七个只读实例，支持横向扩展集群读能力。 说明: · 目前仅 SQL Server 2017 企业版支持集群版。 · 集群版基于SQL Server 源生 AlwaysOn 技术，实现计算与存储分离，并且可以通过独立购买只读实例实现读写分离。 · 集群版所有的只读实例可申请独立的只读连接实现业务读写分离。 · 同时每个只读实例默认也有独立的内网连接，以便基于独立只读实例的实现业务查询隔离。 详细信息，请参见集群版。	政务行业中高频率数据库读写

以下从价格、不同数据库系列适用的场景，为您对比介绍主流的关系型数据库和NoSQL数据库。

数据库类型	数据库名称	价格	适用场景
关系型数据库	RDS MySQL版	低	· 基础版：学习以及小型网站 · 高可用版：一定业务压力的中型数据库场景 · 集群版：业务不允许中断，访问压力较大
	RDS SQL server版	高	· 基础版：测试以及小型商业化网站 · 高可用版：企业级商业化网站 · 集群版：企业业务不允许中断，访问压力较大

数据库类型	数据库名称	价格	适用场景
	RDS PostgreSQL版	最低	· 基础版：学习以及小型网站 · 高可用版：一定业务压力的中型数据库场景 · 集群版：业务不允许中断，访问压力较大的场景，其性能较一般MySQL高
	RDS PPAS版	高	· 通用型：兼容oracle业务，但业务压力Udacity，虚拟化可以满足其需求 · 独享型：面对需要独享物理机的业务，一般为高并发oracle类业务
	DRDS	中	· 入门版本：4Core8G，价格亲民，适合中小型在线业务 · 企业版：16Core32G，复杂 SQL 响应好，适合超高并发在线业务 · 至尊版：32Core64G，复杂 SQL 执行响应最好，提供超大规格选择
NoSQL数据库	Redis	中	· 双机热备Redis：一般作为持久化数据库提高业务可用性 · 集群版本的Redis：一般作为缓存层，加速应用访问，解决一般数据库无法负载的读取压力
	MongoDB版	中	· 单节点实例单节点：适用于开发、测试及其他非企业核心数据存储的场景 · 副本集实例：适用于某些业务场景下对数据库有更高读取性能需求，如阅读类网站、订单查询系统等读多写少场景或有临时活动等突发业务需求 · 分片集群实例：基于多个副本集（每个副本集沿用三副本模式）组成的分片集群实例，提供更高的读取性能需求，为实时在线业务提供高速读取性能

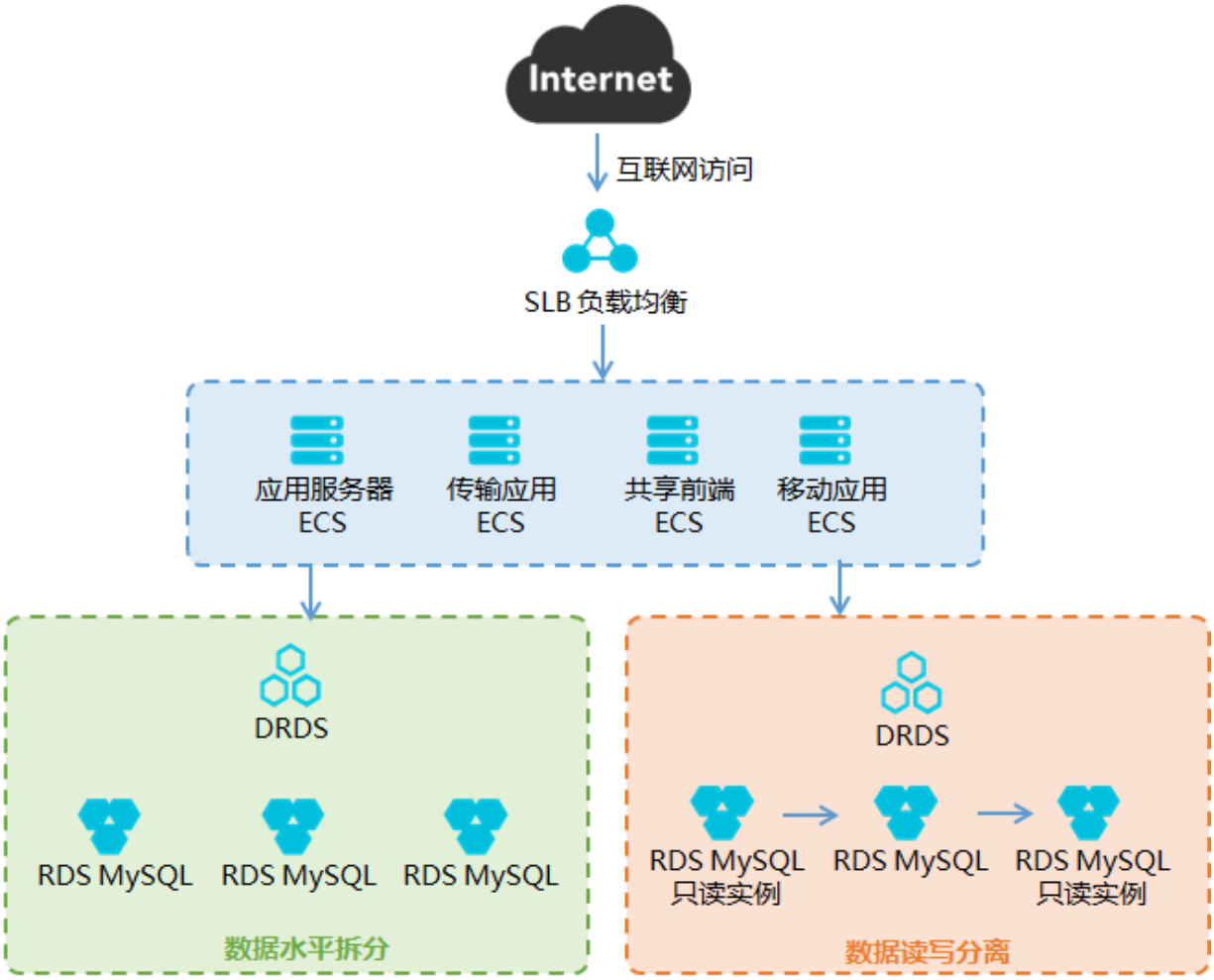
客户案例

某政府单位在面对互联网政务越来越多的业务场景时，经常遇到数据库卡死的情况，经过一番分析，认为数据库卡死有几个原因：

· 数据过多，数据库性能跟不上

· 查询并发较高，原数据库没有充分的并发能力

在这个场景下，此政府单位将多个MySQL服务器根据用途分为两组：应用以及移动，并将这两组通过DRDS产品部署成分布式架构，数据库的架构如下图所示。



按照此种架构，大大提升了数据库的并发能力，并升级原先老版本的MySQL至最新版，一举解决了问题。

5.4 如何选用安全类产品

在阿里政务云上安全产品众多，用户在面对众多安全产品时很难选择或匹配自己的场景，现将主要的安全产品进行对比分析，汇总介绍主要安全产品的描述和使用建议

安全类产品对比介绍

以下表格为各主要安全产品的对比介绍，您可仔细核对“设备及软件名称”栏中的描述是否和您的需求符合，如果符合则再参照优先级进行选择使用。其中优先级为：

- 必备：强烈推荐购买，如无此产品则可能存在较大安全隐患
- 极高：近期安全热点，如不选择则可能存在安全隐患
- 高：安全攻防重点，如果对系统架构较为熟练则可以自行配置

· 中：对业务本身没有影响，但缺少部分业务功能

表 5-1: 优先级：必备 云产品

序号	设备及软件名称	技术参数/配置/性能	优先级
1	态势感知（可视化分析，告警预警）	· 规格：支持云服务器总和40台。 · 能力：实现安全告警，病毒云查杀、网站后门查杀、异常登录提醒、肉鸡检测、数据外泄检测、安全可视化、日志分析、威胁情报。	必备
2	Web应用防火墙	· 正常业务请求QPS：5000 · 业务带宽（云外/云内）：130 Mbps / 200 Mbps · 支持10个域名防护	必备
3	云堡垒机（访问管理必备）	规格：支持50资产、50并发	必备
4	安骑士（云主机安全防护，安全防护核心）	· 防护云主机数量40台。 · 病毒查杀：多病毒检测引擎支持一键隔离网站后门、病毒文件，并已支持自动查杀部分主流勒索病毒、DDoS木马。 · 漏洞管理：覆盖Windows、Linux、Web-CMS漏洞,并支持一键修复。 · 基线检查：支持弱口令、系统、账户、权限、Web服务器等安全基线一键核查，提升主机安全加固防线。 · 入侵检测：大数据驱动，规则引擎结合机器学习算法、关联安全检测模型保障威胁检测能力。	必备

序号	设备及软件名称	技术参数/配置/性能	优先级
5	数据库审计（数据库业务必备）	· 支持5个数据库实例。 · 计策略的要素： - where：IP地址、用户名、端口号、数据库类型； - who:实例、schema； - what:表、字段、视图、包； - when：起始\结束时间、执行时长； - how：客户端工具； - Range：修改、删除或查询的行数 - ResultSet：返回结果集 - other：关键字、客户端工具和应用、错误码、关联表数等 · SQL注入检测与告警：检测SQL注入行为，并进行告警。 · 风险登录检测与告警：检测来自危险客户端IP、MAC、客户端程序并在可以时间使用可以数据库用户登录的行为，并进行告警。 · 风险操作检测与告警：检测来自特定用户（或用户组）、针对特定数据表的高危SQL操作，并进行告警。 · 敏感语句检测与告警：支持敏感对象检测，信任语句不告警、敏感语句告警。	必备

序号	设备及软件名称	技术参数/配置/性能	优先级
6	云防火墙（安全基础组件）	· 缺省支持ECS数量200台，最大支持扩展到5000台。 · 防护流量带宽200Mbps,支持扩展至2Gbps。 · 支持防火墙安全控制，同时控制入流量和出流量的访问。 · 支持基于域名的访问控制。 · 支持ECS颗粒度的微隔离，支持业务关系可视、可控、可管。 · 支持入侵防御（IPS）功能。 · 支持安全事件日志，流量日志和系统日志，保存6个月。 · 支持互联网到业务的访问流量分析。 · 支持业务主动外联分析。 · 支持被阻断访问的分析。	必备

表 5-2: 优先级：极高 云产品

序号	设备及软件名称	技术参数/配置/性能	优先级
1	DDoS高防（抗D是近期安全重点）	保底30G，弹性到300G	极高
2	网站威胁扫描（网站业务强推）	· 包含10个二级域名/IP的扫描授权。 · 内容风险每日周期性检测量10万URL。 · 支持网站深度漏洞检测和应急漏洞检测。 · 支持网页内容风险监控，包括网页篡改、垃圾广告、挂马暗链等，支持格式包括图片、文本、源码。	极高

序号	设备及软件名称	技术参数/配置/性能	优先级
3	加密服务（国密加密，政务业务数据加密必备）	· 加密服务基于国家密码局认证的硬件加密机，提供了云上数据加解密解决方案，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对云上业务的数据进行可靠的加解密运算 · 数据通讯协议：TCP/IP · 并发连接：64 · SM1加密运算性能：4000次/秒 · SM2签名运算性能：3000次/秒 · SM2验签运算性能：2000次/秒 · RSA2048公钥运算性能：3500次/秒 · RSA2048私钥运算性能：400次/秒 · 对称算法：SM1/SM4/DES/3DES/AES · 非对称算法：SM2、RSA(1024~2048) · 摘要算法：SM3、SH1/SHA256/SHA384	极高

表 5-3: 优先级：高 云产品

序号	设备及软件名称	技术参数/配置/性能	优先级
1	证书服务	HTTPS证书（推荐使用HTTPS增加安全性）	高
2	安全管家	应急版、护航版、企业版（根据业务规模选择不同类型）	高
3	渗透测试	阿里专家提供渗透测试（可以帮助客户监测出自己无法发现的漏洞）	高

表 5-4: 优先级：中 云产品

序号	设备及软件名称	技术参数/配置/性能	优先级
1	爬虫风险管理	有需求可考虑	中
2	实人认证	有需求可考虑	中
3	内容安全	有需求可考虑	中

客户案例一：基础安全案例

某政府单位部署了该单位的内部应用，用于处理内部工作事物，其应用通过VPN访问。对于这类场景我们可以采用以下思路来规划安全产品：

此业务所需云产品非常简单，仅2台虚拟机和1台负载均衡即可完成，访问流量每天不超过500DAU，且其上的内容并不属于保密和不可丢失范畴。

基础安全产品：Web应用防火墙、安骑士这两个安全产品即可满足需求，VPN可以采购阿里云VPN来满足需求。

客户案例二：互联网政务案例

某政府单位部署了该单位的对外职能网站，有互联网客户会对此网站上的应用访问和使用，且此功能具备一定的社会效应，故有较高的安全需求，对于这类场景我们可以采用以下思路：

此业务场景略微复杂，由虚拟机、数据库、对象存储、负载均衡等组成，所以我们需要将后台业务和前台业务做严格的安全区分，在划分不同的功能区后，后台通过堡垒机和VPN登录管理，前台着重注意防篡改和网络攻击。

- 基础安全产品：Web应用防火墙、安骑士、堡垒机
- 如果需要网站不被攻破和防篡改等则还可以加选：DDoS高防、网站威胁扫描、云防火墙
- 如果数据库有审计需求则可以加选： 数据库审计

客户案例三：高等级安全架构案例

某政府单位将业务核心应用部署在阿里政务云上，其中架构较为复杂，对安全性有极高的要求，并且要求不能有业务中断的场景，对于这类场景我们可以采用以下思路：

此客户使用阿里云产品超过20款，且用量较大，并且对安全有极高的需求。在这种情况下不能仅仅使用基础安全防护的产品，一定需要根据自身业务、架构等特点，从架构层面和流程层面做严格的规划。

安全产品基本属于全选，但更重要的是选择阿里云的专家服务：

- 专职售后团队：选择阿里云的至尊售后服务来做大客户售后支撑
- 专职安全团队：阿里云安全专家服务来对整体架构的安全性做评估
- 专职合规团队：阿里云合规团队为此类架构提供合规咨询和测评支撑
- 阿里政务云重保服务：阿里云关键客户重保业务可以让客户在关键时期（特殊时间段）得到全方位的安全保障

6 政务云云产品使用安全规范

6.1 ECS安全配置

ECS具备安全组的安全设置，通过安全组配置和阿里云提供丰富的云服务器及应用安全防护产品，可从多维度提高ECS的安全性。

安全组及安全产品

- 安全组：

  安全组是一种虚拟防火墙，具备状态检测和包过滤功能。安全组用于设置单台或多台实例的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。更多安全组的介绍请参考安全组 章节。

- 安骑士：

  安骑士是一款经受百万级主机稳定性考验的主机安全加固产品，拥有自动化实时入侵威胁检测、病毒查杀、漏洞智能修复、基线一键核查等功能，是构建主机安全防线的统一管理平台。更多安骑士的介绍请参考 什么是安骑士 章节。

- WAF：

  云盾Web应用防火墙（Web Application Firewall, 简称 WAF）基于云安全大数据能力，用于防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，并过滤海量恶意CC攻击，避免您的网站资产数据泄露，保障网站的安全与可用性。更多WAF的介绍请参考什么是Web应用防火墙 章节。

安全配置建议

使用场景	场景说明	安全配置建议
登录密钥	ECS远程登录账号及密钥。	建议设置为强密码形式：12位以上，同时包含数字、大小写字母、特殊符号
远程登录端口	22、3389端口分别用于ECS的Linux和Windows场景下的远程登录，需对这两端口进行安全限制。	· 利用安全组限制22、3389远程登录端口的访问来源IP。 · 无法设置白名单时，将远程登录的方式设置为SSH Key认证方式。

使用场景	场景说明	安全配置建议
MySQL、FTP等在ECS上安装的高危服务端口	由于MySQL和FTP的业务需求，需在ECS上开放对应的业务端口，这些端口需进行安全限制。	限制只允许本机访问或者利用安全组限制访问来源IP。
公网访问隔离	互联网访问本ECS实例。	建议: · ECS实例不直接对互联网暴露其IP地址，通过DNS、公网SLB、EIP等提供互联网服务。 · 在安全组配置时，IP段及端口不要全开放。只保留业务需要使用的端口和IP。
内网访问	VPC内部其他实例访问本ECS实例。	建议安全组配置时，IP段及端口不要全开放。只保留业务需要使用的端口和IP。
HTTP 证书	ECS的网络业务需加载HTTP证书。	· HTTP业务建议使用HTTPS协议，并加载HTTPS证书。 · HTTP服务的需要利用安全组限制访问来源IP。 · HTTP服务域名建议开通WAF防护。
云服务器防护	ECS实例自身的安全监控及防护可由阿里云提供的服务器安全防护产品安骑士保障。	建议每个ECS实例均安装使用安骑士，实时防护ECS实例。
应用防护	在ECS上部署了Web网站或其他应用，可对应用进行安全防护。	开通安全管家的网站安全体检功能、开通WAF。

其中:

· 密钥设置：请参考 创建实例 章节，在“系统配置”时，登录密码根据上述推荐，配置为高复杂度的强密码形式。
· 安全组配置：请参考#unique_18章节。其中“授权对象”根据上述安全配置建议进行修改。
· 安骑士安装使用：请参考 快速入门 章节。
· WAF部署使用：请参考 快速入门 章节。
· 证书服务：证书的购买、使用请参考 证书服务 章节。
· 安全管家：安全管家的使用请参考 使用手册 章节

6.2 SLB安全配置

阿里云提供5GB的免费DDoS基础防护功能，且SLB支持将HTTP重定向为HTTPS，提供更安全的传输协议。

- TLS安全策略：

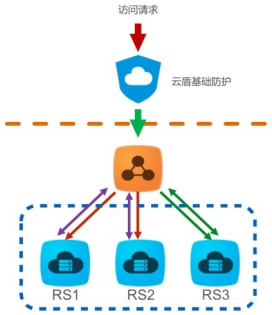
  SLB的HTTPS监听可配置选择不同的TLS协议版本和配套的加密算法套件。更多内容介绍请参考 管理TLS策略 章节。

- HTTP重定向至HTTPS：

  HTTPS是加密数据传输协议，安全性高。负载均衡支持将HTTP访问重定向至HTTPS，方便您进行全站HTTPS部署。负载均衡已经在全部地域开放了HTTP重定向功能。重定向配置请参考 HTTP重定向至HTTPS 章节。

- DDoS基础防护：

  阿里云免费为负载均衡服务提供最高5GB的DDoS基础防护。如下图所示。



所有来自Internet的流量都要先经过云盾再到达负载均衡，云盾会针对常见的攻击进行清洗过滤。云盾DDoS基础防护可以防御SYN Flood、UDP Flood、ACK Flood、ICMP Flood和DNS Flood等DDoS攻击。更多SLB的DDoS基础防护介绍请参考 DDoS基础防护 章节。

6.3 RDS安全配置

云数据库 RDS（Relational Database Service）提供了多样化的安全加固功能，从攻击防护、访问控制等维度给RDS数据库提供安全保障。

云数据库RDS提供了多样化的安全加固功能来保障用户数据的安全，其中包括但不限于：

- 网络：IP 白名单、VPC 网络、SSL（安全套接层协议）
- 存储：TDE（透明数据加密）、自动备份、手动备份，将备份数据存放于OSS，利用OSS的多副本功能提高高可用性
- 容灾：同城容灾（多可用区实例）、异地容灾（两地多中心）

- 密钥：RDS数据库的密码建议设置为强密码形式，要求为：12位以上，同时包含数字、大小写字母、特殊符号，密码设置请参考 创建账号和数据库 章节。

对数据库的各项业务防护包括：

- 攻击防护：针对DDoS攻击提供流量清洗、黑洞处理的安全防护措施。
- 访问控制：对数据库的访问用户名、密码及数据库访问，通过账号验证、白名单设置等进行安全防护。
- 网络隔离：通过VPC来获取更高程度的网络访问控制。
- 数据加密：RDS提供透明数据加密功能保障数据安全。

6.4 Memcache安全配置

MemcacheE提供白名单设置和高复杂度密码设置，提高其访问的安全性。

- 白名单：为了数据库的安全稳定，在开始使用 Memcache 实例前，需将访问数据库的 IP 地址或者 IP 段加到目标实例的白名单中。正确使用白名单可以让 Memcache 得到高级别的访问安全保护，建议您定期维护白名单。
- 密码设置：Memcache的访问密码建议设置为强密码形式：12位以上，同时包含数字、大小写字母、特殊符号

6.5 OSS安全配置

OSS适用于存储各种类型的静态资源，为防止OSS的资源被恶意盗用，OSS提供了几种安全防护功能，用户还可以集成安全类产品进行安全防护。

- 访问与控制：OSS支持设置ACL访问策略，限制对OSS的访问以提高存储资源的安全性。建议将应用的静态图片、css、js等资源放到OSS上面，设置bucket为public-read。其他资源设置bucket为private并使用AK认证。
- 安全管理：OSS支持各项安全管理设置，包括：
  - 设置访问日志记录
  - 设置防盗链
  - 设置跨域访问
  - 服务端加密编码
  - 客户端加密SDK介绍
- 安全产品：结合DDoS高防和WAF，可抵抗DDoS流量攻击、增强应用的安全防护。

6.6 CDN与视频服务安全加固

阿里云CDN支持防盗链、IP白名单、URL鉴权基础防护措施。

说明:

阿里云CDN是一款用于加速的产品，不具备抗攻击的能力。如果您需要抗DDoS和抗CC攻击的CDN加速功能，请使用阿里云高防服务。

下面介绍CDN的一些基本防护的配置：

- 防盗链功能：

  该功能是根据http请求的referer字段来对请求来源的域名进行筛选和链接。CDN支持三种防盗链设置：白名单、黑名单以及是否允许空refer。该方法主要通过URL过滤的方法对来源host的地址进行过滤，您可指定请求来源的域名。其中黑白名单同时只能有一种名单生效，通过该功能可以对请求来源最限制。 具体设置方法见： 设置防盗链。
- IP黑白名单：

  可以设置相应的IP黑白名单来针对来源IP进行限制。具体设置方法见： 设置IP黑白名单。
- URL鉴权：

  该功能可保护您安全需求较高的URL，它需要您按照指定的签名方式对于特定的URL增加鉴权认证。该功能适合安全密级较高的文件，并不建议一般的文件进行使用，因为每次的签名都需要通过客户端临时生成。相比于正常的访问会增加其访问时间。具体设置方法见：URL鉴权。
- CDN加速域名，不允许将*.XXX.com的泛域名解析到CDN的cname域名，存在域名劫持风险。
- 视频的直播服务，推流和拉流，必须强制开启鉴权，否则存在盗推和盗播风险。

6.7 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。