阿里云
政务云

了解更多

文档版本：20181214

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。
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。	`swich` *`{stand | slave}`*

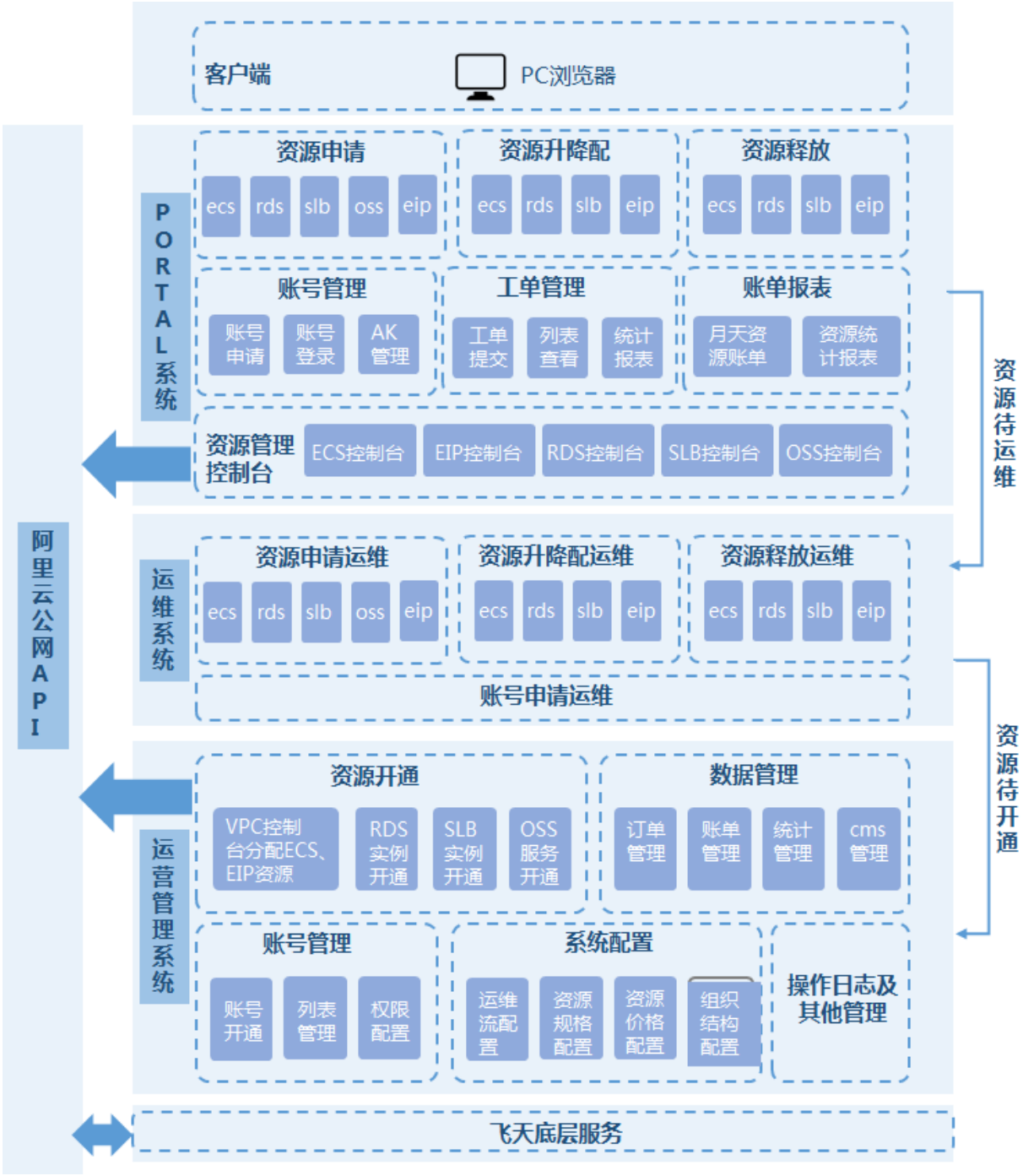
目录

1 阿里政务云架构

阿里政务云依托于阿里云业内顶尖技术，提供与其他机房完全物理隔离的专属高规格物理集群、高等级的安全防护，从平台系统架构、网络架构的设计层面开始，保障政务云的独立性、安全性、高可用性。

平台系统架构

阿里政务云基于飞天技术架构，提供完整的管控、运维、运营体系，以及多款阿里云核心产品。下图为某案例的系统技术架构。此案例包括：资源管理控制台、运维系统、运营管理系统、公网API几个主要模块。系统技术架构图如下所示。


客户端
PC浏览器
PORTAL系统
资源申请
ecs rds slb oss eip
资源升降配
ecs rds slb eip
资源释放
ecs rds slb eip
账号管理
账号申请 账号登录 AK管理
工单管理
工单提交 列表查看 统计报表
账单报表
月天资源账单 资源统计报表
资源管理控制台
ECS控制台 EIP控制台 RDS控制台 SLB控制台 OSS控制台
资源待运维
阿里云公网API
运维系统
资源申请运维
ecs rds slb oss eip
资源升降配运维
ecs rds slb eip
资源释放运维
ecs rds slb eip
账号申请运维
资源待开通
运营管理系统
资源开通
VPC控制台分配ECS、EIP资源
RDS实例开通
SLB实例开通
OSS服务开通
数据管理
订单管理 账单管理 统计管理 cms管理
账号管理
账号开通 列表管理 权限配置
系统配置
运维流配置 资源规格配置 资源价格配置 组织结构配置
操作日志及其他管理
飞天底层服务

2 安全合规

2.1 政务云等保现状及安全资质

阿里政务云平台已完成等保三级认证，其上的云产品均在满足等保三级要求之外，以更高的安全要求设计、完善产品功能，旨在为政务类用户提供更安全、更合规、更稳定的云服务。

国密加密安全保障

阿里政务云采用国密加密机服务，满足政务场景下对加密算法更安全、更合规的要求，保障政务云服务的安全性。

阿里云等保现状

2017年11月，政务云平台通过新的云计算安全等级保护三级要求的测评，是国内首个为政务类用户提供的、且满足等保三级要求的云计算平台。

按照新的云等保要求和监管部门的意见，在具体的云上应用等级保护合规和测评中，**涉及阿里云平台侧的相关要求不再进行单独测评，可以直接引用阿里云平台的测评结论。**

阿里云将提供以下材料，协助用户云上系统通过等保测评：

- 阿里云等保备案证明
- 阿里云测评报告封面及结论页
- 阿里云安全产品销售许可证（公安部）

政务云安全产品

政务云提供丰富的安全产品、完整的安全技术解决方案，相关的政务云安全产品及其满足的等保要求如下。

产品名称	产品描述
DDoS 基础防护	免费为阿里云用户提供最高5G的默认DDoS防护能力。阿里云在此基础上，推出了安全信誉防护联盟计划，将基于安全信誉分进一步提升DDoS防护能力，用户最高可获得100G以上的免费DDoS防护资源。
DDoS 高防	DDoS高防IP是针对互联网服务器（包括非阿里云主机）在遭受大流量DDoS攻击后导致服务不可用的情况下，推出的付费服务，用户可通过配置高防IP，将攻击流量引流到高防IP，确保源站的稳定可靠。

产品名称	产品描述
Web 应用防火墙#网络安全#	对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。
安骑士#服务器安全#	ECS贴身安全护卫：一款主机安全软件，为您提供主机漏洞检测、基线检查、病毒查杀、资产统一管理等功能，为您建立安全运维管理平台。
SSL 证书#应用安全#	SSL证书，在云上签发各品牌数字证书，实现网站HTTPS化，使网站可信，防劫持、防篡改、防监听。并进行统一生命周期管理，简化证书部署，一键分发到云上产品。
数据库审计#数据安全#	数据库审计服务，可针对数据库SQL注入、风险操作等数据库风险操作行为进行记录与告警。支持RDS云数据库、ECS自建数据库，为云上数据库提供安全诊断、维护、管理能力。
加密服务#数据安全#	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。
内容安全#业务安全#	内容安全基于深度学习技术， 提供图片、视频，文字等多媒体的内容风险智能识别服务，不仅能帮助用户降低色情、暴恐、涉政等违规风险，而且能大幅度降低人工审核成本。
态势感知#大数据安全#	态势感知支持病毒云查杀、异常登录提醒、肉鸡检测、数据外泄检测、Linux软件漏洞、弱口令、主机合规检测。提供ECS、RDS、SLB等云产品安全配置检测。帮助您扩大安全可见性，集中管理云上资产安全事件。
堡垒机#安全管理#	基于协议正向代理实现，对SSH、Windows远程桌面、SFTP等常见运维协议的 数据流进行全程记录，再通过协议数据流重组的方式进行录像回放，达到运维审计的目的。
安全管家#安全服务#	阿里云安全管家服务是阿里云安全专家基于阿里云多年安全最佳实践经验为云上用户提供的全方位安全技术和咨询服务，为云上用户建立和持续优化云安全防御体系，保障用户业务安全。
先知#安全众测#	先知平台提供私密的安全众测服务，可帮助企业全面发现业务漏洞及风险，按效果付费。企业加入先知平台后，可自主发布奖励计划，激励先知平台的安全专家来测试和提交企业自身网站或业务系统的漏洞，保证安全风险可以快速进行响应和修复，防止造成更大的业务损失。

产品名称	产品描述
云防火墙	云防火墙是业界首款公共云环境下的SaaS化防火墙，它统一管理互联网到业务的南北向访问策略和业务与业务之间的东西向微隔离策略，内置威胁入侵检测模块(IPS)，支持全网流量可视、业务间访问关系可视，是业务上云的第一个网络安全基础设施。
实人认证	依托活体检测、人脸比对等生物识别技术、证件 OCR 识别技术、阿里巴巴实人可信模型等进行的自然人真实身份的核验服务。
数据风控#业务安全#	数据风控由阿里聚安全提供，是基于阿里大数据计算能力，通过业内领先的风险决策引擎，解决企业账号、活动、交易等关键业务环节存在的欺诈威胁，降低企业经济损失。

2.2 安全合规

随着互联网业务的多维快速发展，网络安全事故也在各领域频发，法规制度对网络安全机制的建立、完善提出了更高、更明确的要求。政务类业务在拓展网络应用的同时，应当将安全合规作为业务发展的重点考虑内容之一。阿里政务云满足国家等保三级认证要求，为政务类用户提供更安全、更合规的云平台及云服务。

法规制度背景

2016年11月7日上午，十二届全国人大常委会第二十四次会议表决，正式通过了《中华人民共和国网络安全法》，网络安全法将于2017年6月1日起施行。

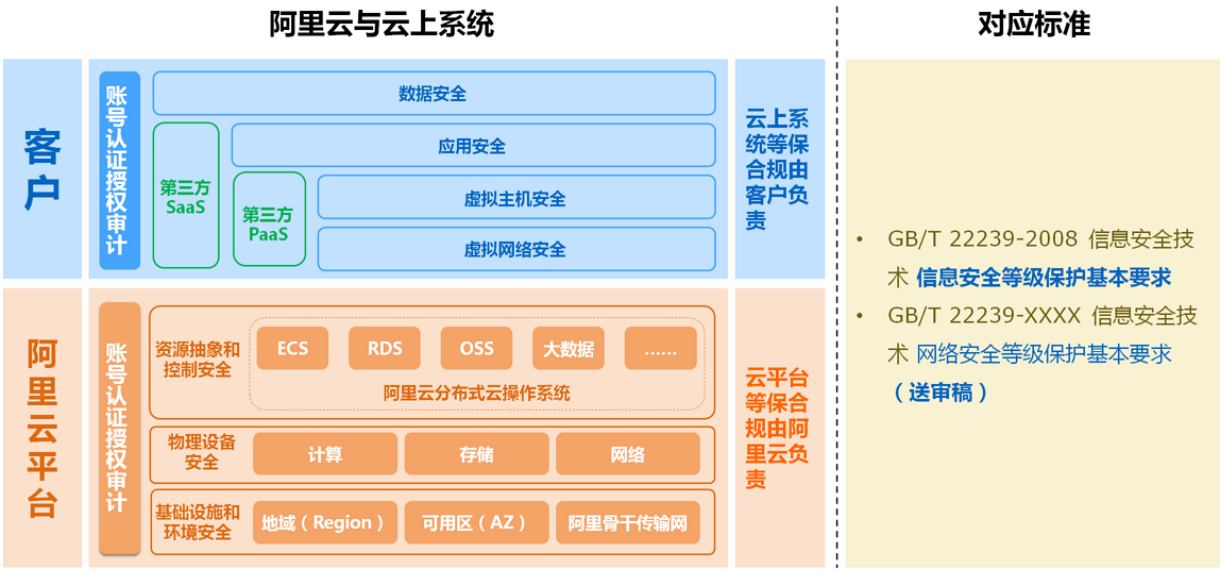
根据网安法，政企需履行一定的义务并承担网络安全相关责任，网安法的重点解读请参考 《网络安全等级保护基本要求》重点解读 章节。

其中，网安法第二十一条为：**国家实行网络安全等级保护制度**（下文简称：等保安全制度），等保安全制度适用于境内所有信息系统。政企需按照网络安全等级保护制度履行安全保护义务，按照等保安全制度申报完成网络安全等级评定，根据各级保护制度的要求整改、建设信息系统，是企业应履行的义务，同时可发现自身系统的安全隐患及不足，以及时整改，进而可提高企业整体的行业竞争力。更详细的等保安全制度介绍请参考 等保安全制度简介 章节。

云上系统责任共担

在评估是否达成安全合规要求时，政企使用的云平台及部署在云上的系统应用均需满足等保认证的要求，云上系统的合规性由阿里云与政企共同承担。

图 2-1: 云上系统责任共担



2.3 附录 1 网络安全法简介

《网络安全等级保护基本要求》重点解读

根据网安法，企业需关注：

- 义务：按照网络安全等级保护制度履行安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露、篡改。
- 责任：网络运营者应对保障用户信息安全负有主体责任。
- 措施：
  - 制定网络安全事件应急预案，及时处理系统漏洞、计算机病毒、网络攻击、网络入侵等安全风险、并按照规定向有关部门报告。
  - 加强对用户发布信息的管理，及时消除法律、行政法规禁发的信息，建立网络信息投诉、举报制度、并及时受理。
  - 对收集的用户严格保密，并建立健全用户信息保护制度，不得非法收集、提供、获取、 使用用户信息。
- 维护：做好公共通信和信息服务、能源、水利、金融、公共服务、电子政务等重要行业的数据备份、防篡改、防泄漏、容灾措施，尤其是国家关键信息基础设施系统。

2.4 附录 2 等级保护简介

等级保护是什么

- **制度要求**
  - 《中华人民共和国网络安全法》：“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。
  - 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。
  - 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）规定：“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度”。
- **工作依据**
  - 《警察法》规定：警察履行“监督管理计算机信息系统的安全保护工作”的职责。
  - 国务院令第147号规定：“公安部主管全国计算机信息系统安全保护工作”，“等级保护的具体办法，由公安部会同有关部门制定”。
  - 2008年国务院三定方案，公安部新增职能：“监督、检查、指导信息安全等级保护工作”。
- **监管范围与力度**
  - 信息安全等级保护的适用范围：中华人民共和国境内的计算机信息系统。
  - 监管力度：二级及以上系统均纳入公安机关监管范围，其中三级系统至少每年测评一次。
  - 三级系统对安全产品主要要求：境内独立法人、自主知识产权、信息安全产品认证证书。
- **地位和作用**
  - 国家信息安全保障工作的基本制度、基本国策。
  - 开展信息安全工作的基本方法。
  - 促进信息化、维护国家信息安全的根本保障。

等级保护分级说明

等级	等级定义	适用系统
第一级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益	不重要系统

等级	等级定义	适用系统
第二级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全	一般重要系统
第三级	信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害	比较重要系统
第四级	信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害	非常重要系统
第五级	信息系统受到破坏后，会对国家安全造成特别严重损害	极度重要系统

《网络安全等级保护基本要求》重点解读

网络与通信安全

表 2-1: 安全要求

类别	安全要求
网络架构	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
访问控制	• 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。 • 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。
通信传输	应采用校验码技术或加解密技术保证通信过程中数据的完整性。
边界防护	应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。
入侵防范	• 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。 • 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

表 2-2: 条款解读与应对政策

条款解读	应对政策
• 根据服务器角色和重要性，对网络进行安全域划分。 • 在内外网的安全域边界设置访问控制策略，并要求配置到具体的端口。 • 在网络边界处应当部署入侵防范手段，防御并记录入侵行为。 • 对网络中的用户行为日志和安全事件信息进行记录和审计。	• 推荐使用阿里云的VPC和安全组对网络进行安全域划分并进行合理的访问控制。 • Web应用防火墙防范网络入侵。 • 态势感知的日志功能对用户行为日志和安全事件进行记录分析和审计。 • 对于经常面临DDoS威胁系统，还可使用DDoS高防进行异常流量过滤和清洗。

设备与计算安全

表 2-3: 安全要求

类别	安全要求
身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性。
访问控制	应根据管理用户的角色建立不同账户并分配权限，仅授予管理用户所需的最小权限，实现管理用户的权限分离。
安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
入侵防范	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
恶意代码防范	应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

表 2-4: 条款解读与应对政策

条款解读	应对政策
• 避免账号共享、记录和审计运维操作行为是最基本的安全要求。 • 必要的安全手段保证系统层安全，防范服务器入侵行为。	• 推荐使用阿里云的堡垒机、数据库审计对服务器和数据的操作行为进行审计，同时为每个运维人员建立独立的堡垒机账号，避免账号共享。

条款解读	应对政策
	• 使用安骑士对服务器进行完整的漏洞管理、基线检查和入侵防御。

应用和数据安全

表 2-5: 安全要求

类别	安全要求
身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求。
访问控制	应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
安全审计	应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
数据完整性	应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性和保密性。
数据备份恢复	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

表 2-6: 条款解读与应对政策

条款解读	应对政策
• 应用是具体业务的直接实现，不具有网络和系统相对标准化的特点。大部分应用本身的身份鉴别、访问控制和操作审计等功能，都难以用第三方产品来替代实现。 • 数据的完整性和保密性，除了在其他层面进行安全防护以外，加密是最为有效的方法。 • 数据的异地备份是等保三级区别于二级最重要的要求之一，是实现业务连续最基础的技术保障措施。	• 在应用开发之初，就应当考虑应用本身的身份鉴别、访问控制和安全审计等功能。 • 对已经上线的系统，通过增加账号认证、用户权限区分和日志审计等功能设计满足等保要求。 • 数据的安全，推荐使用成熟的云盾CA证书服务实现HTTPS，确保数据在传输的过程中保持处于加密状态。 • 数据备份，推荐使用RDS的异地容灾实例自动实现数据备份，亦可以将数据库备份文件手工同步到阿里云其他地区的服务器。

安全管理策略

表 2-7: 安全要求

类别	安全要求
安全策略和管理制度	应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系。
安全管理机构和人员	应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。
安全建设管理	应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，并形成配套文件。
安全运维管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

表 2-8: 条款解读与应对政策

条款解读	应对政策
• 安全策略、制度和管理层人员，是保证持续安全非常重要的基础。策略指导安全方向，制度明确安全流程，人员落实安全责任。 • 等保要求提供了一种方法论和最佳实践，安全可以按照等保的方法论进行持续的建设和管理。	• 安全策略、制度和管理层人员，需要客户管理层根据本企业的实际情况，进行梳理、准备和落实，并形成专门的文件。 • 漏洞管理过程中需要用到的技术手段，推荐使用阿里云的安全管家和先知众测服务，快速发现云上系统漏洞，及时处理。

3 阿里政务云的隔离性

3.1 数据中心隔离

阿里政务云与阿里公共云的数据中心完全隔离，政务云采用独立的物理机房，为政务用户提供专属的云平台及云产品，保障政务用户在政务云上的业务数据不出政务云专属机房。

独立的物理机房

为了满足国家法律法规和等保要求，阿里政务云数据中心和阿里公共云数据中心进行隔离，即网络环境、设备设施完全物理隔离，给政务云用户提供独立的物理机房。

为了在数据层面满足用户业务数据不出政务云的专属机房，政务云的所有数据存储相关的数据都在政务云专属机房内落盘，这样确保在各个层面上用户数据无法出此机房。

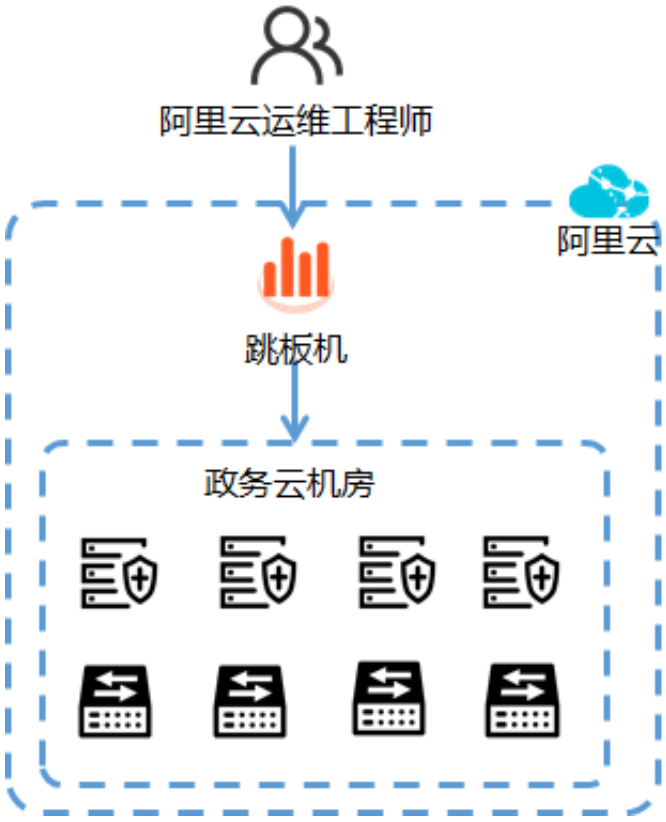
3.2 运维平台隔离

成为政务云的用户后，您仅需关注您的云资源的水位、利用率等基础运维事务，政务云平台的运维由阿里云运维工程师执行。

阿里云运维工程师通过飞天运维管理平台统一运维管理政务云平台，并采取严格的访问控制、职责分离、监控审计的运维策略，来确保政务云平台的运维安全。

访问控制

阿里云运维团队进行政务云平台的运维工作时，对政务云的访问受到严格的安全合规约束，阿里政务云内部网络与阿里云内网完全隔离，运维的必访问操作须使用特定的“跳板机”才能够进行底层资源的运维工作。



职责分离与权限管理

职责分离

阿里云对运维权限分角色进行职责分离，防止权限滥用和审计失效。

- 运维和审计职责分离，运维团队执行运维操作，安全团队负责审计。
- 数据库管理员和系统管理员职责分离。

账号管理和身份认证

阿里云使用统一的账号管理和身份认证系统管理员工账号生命周期：

- 每个员工存在唯一的账号。
- 集中下发密码策略，强制要求员工设置符合密码长度、复杂度要求的密码，并定期修改密码。
- 支持账号密码登录、一次性口令登录、数字证书登录等多种认证登录方式。

授权

阿里云基于员工工作岗位和角色，遵循最小权限和职责分离原则，授予员工有限的资源访问权限。

员工根据工作需要通过集中的权限管理平台申请VPN访问权限、堡垒机访问权限、管控平台以及生产系统访问权限，经主管、数据或系统所有者、安全管理员以及相关部门审批后，进行授权。

监控审计与变更管理

监控

阿里云使用自动化监控系统对云平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控。监控系统广泛使用仪表盘展示阿里云关键运营指标，并可配置告警阈值，当关键运营指标超过设置的告警阈值时，自动通知运维和管理人员。

审计

员工对生产系统的所有运维操作必须且只能通过堡垒机进行。所有操作过程完整记录下来实时传输到集中日志平台。阿里云根据《帐号使用规范》及《数据安全规范》里定义的违规事项定义审计规则，发现违规行为并通知安全人员跟进。

内部使用的B/S管理和支持系统按照阿里云日志审计规范详细记录敏感操作，并把日志发送到集中日志平台。

变更管理

阿里云依据ISO/IEC 20000建立了完整的变更管理流程，根据变更紧急程度进行变更等级划分；根据变更来源、对象等进行变更分类管理，明确了可能发生的变更结果的界定标准。整个变更以流程化或自动化的系统和工具来支撑，流程涵盖变更申请、评估、审批、测试、实施及复核等阶段，并明确了变更管理流程中各角色的职责。

变更申请阶段界定了需求提出、记录、接收和判定等关键节点。

变更执行阶段主要涵盖变更方案、变更计划、变更评估和变更实施等要求，所有的变更在获准执行之前，需经过测试，变更时间窗口和变更方案等需经过评审，同时阿里云会向可能受影响的客户发出变更通知。重要的变更操作要求双人复核。

变更验证阶段明确了变更验证、配置项复核和变更结果通知等要求。阿里云完整记录变更过程中的信息，并部署了自动化配置检查工具，可自动进行基础设施和信息系统的配置校验。

4 阿里政务云账号体系

阿里政务云建议您先申请一个全新的阿里云账号来申请阿里政务云政务用户的专属认证，完成政务云账号认证后，此账号将打上政务用户的标签，并与阿里公共云隔离开来以确保政务云环境的安全可控。

为保障政务云用户账号的安全性、账号资源的专属性，只有完成政务云认证的政务专属用户才能登录政务云管控台，查看政务云的相关资源。

说明：

- 完成政务云认证并成为政务云用户后，您将无法访问、查看、管理已经在阿里公共云中申购的云资源和服务。所以建议您申请一个全新的专属账号来注册阿里政务云。
- 如果您希望恢复查看公共云的资源，唯一的解决方法即是取消政务云标签。您可以通过提交工单申请取消政务云用户标签。成功取消后，您的公共云资源可重新查看到并继续使用，但您的政务云资源将无法查看使用。请谨慎操作，并提前做好账号规划。

成为政务云用户需进行如下几个步骤：

1. 注册一个政务云专属的账号。
2. 进入政务云认证页面进行政务云认证。
3. 开通MFA多因素认证，增强账号的安全性。
4. 根据业务需要使用RAM授权子账号。

详细的注册登录政务云的操作指导请参考 注册账号并认证、 登录阿里政务云 章节。

阿里政务云用户与普通官网用户的区别

- 政务云用户环境为VPC环境，不允许创建经典网络。
- 政务云用户购买云产品时，查看到的是“阿里政务云”节点的政务专属云产品，无法查看阿里公共云的云资源。
- 政务云用户购买云产品，实例将创建到阿里政务云专属的机房、地域、可用区和集群，此环境与阿里云公共云或其他环境保持隔离。
- 政务云用户通过公网可以访问管理控制台（www.aliyun.com），也可以通过专线或VPN管理控制台。
- 政务云用户可以通过使用MFA来加强登录认证，保障账号的安全性。

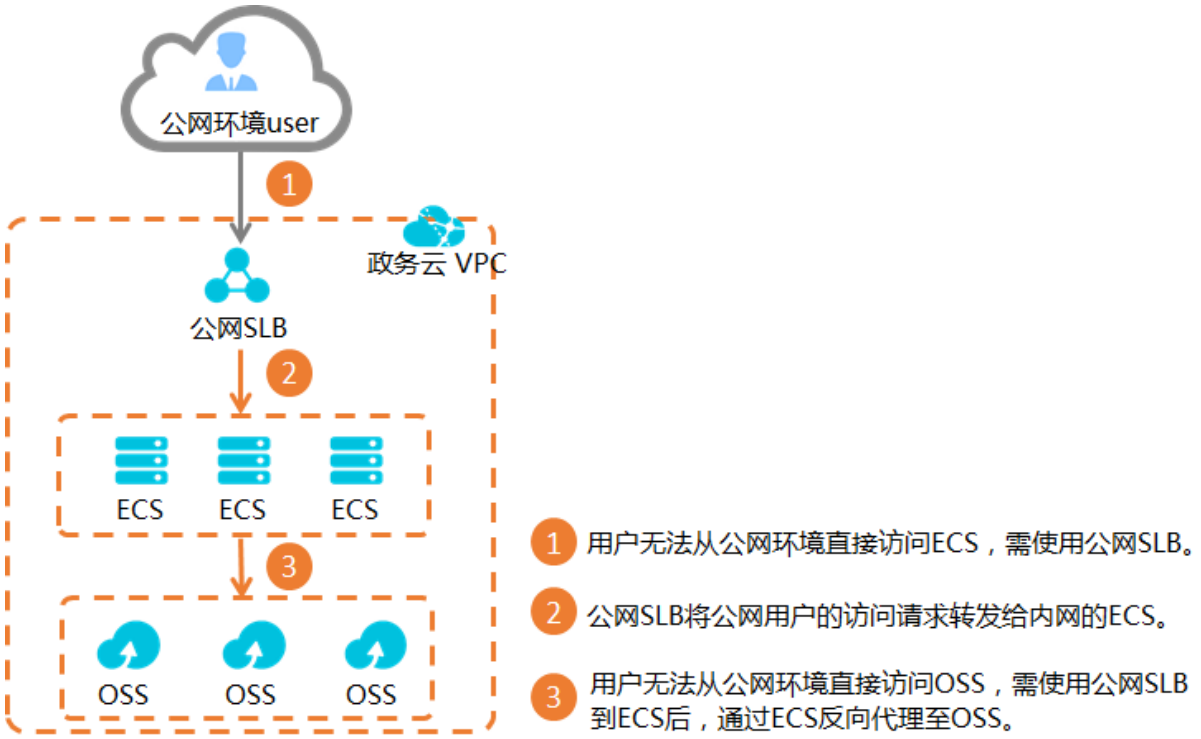
用户隔离

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。

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。

5 主要云产品的隔离

为保障政务云产品使用的安全性，用户无法直接通过互联网环境访问政务云内网环境中的业务。以ECS、OSS为例，您无法在互联网环境中直接访问ECS上的应用或者存储在OSS中的文件，如下图所示。



ECS

政务云ECS的EIP/公网IP 默认不对外提供服务（网络边界实现ACL阻断），政务云环境中 ECS 的公网IP 仅用于访问互联网资源的路由作用，比如，您购买了一台政务云ECS绑定了一个公网地址，这时，从购买的ECS机器上，是可以访问淘宝、百度等互联网资源的，但是，即便您的ECS启动了http服务绑定了公网地址的80端口，其他人从外部访问这个公网IP是访问不到的，因为产品做了限制。

EIP 直接对外服务被掐断。如果要对外提供服务，可以通过公网 SLB来实现。

SLB

政务云 SLB 也有特殊之处。公共云的SLB公网地址几乎可以开放任意端口到互联网，但是政务云分为两种模式，来面对不同的安全诉求。

白名单

政务云整体采用的是白名单机制，也就是说，对于所有公网 SLB 实例，在网络边界设置了ACL，只允许SLB的某几个端口被互联网访问。如果有用户的SLB 实例的其他端口想对外开放服务，需提交工单提交需求，经过政务云业务方和安全审核并通过后，由阿里云网络工程师做 ACL 变更，允许这几个 VIP SLB地址对外开放指定端口。

黑名单

为了更轻型的客户策略，政务云同样也可以为一些安全轻量级用户采取黑名单机制：安全列举一些会被经常攻击、渗透的服务端口，在集群上线时，网络ACL禁止这些端口开放在政务云SLB的公网地址段上。所以，当您在使用政务云SLB的时候，如果发现有些服务端口不通，很可能就是这些规则所导致的。

OSS

内网OSS

遵循政务行业的“指引”等规范，政务云 OSS 在设计之初，没有提供互联网下载/上传服务，也就说，政务云的用户的OSS bucket 只能在私网范围内被访问。通过政务云的ECS私网访问，或者是政务云用户的云下服务器通过专线来访问，互联网或者公共云用户的机器是不能访问的。

也就是说，如果您是一个政务云用户，您的OSS只能政务云私网访问，公共云ECS的私网到政务云OSS的私网主动访问是阻止的，但是政务云的ECS却可以主动发起到公共云 OSS的私网访问。

公网OSS

如果政务云OSS一定要对外提供服务，需要用户创建一个公网SLB，SLB挂载的若干台ECS，在ECS上配置OSS的反向代理，负责把OSS 访问请求转发到后端 OSS实例，

说明：

此场景下OSS的访问非常不安全，使用时请务必根据您的业务场景设置好ECS上往内部OSS代理的安全策略，否则可能会出现OSS访问安全事件。