阿里云安全白皮书

2016 年 8 月，版本 2.1

目录

第1章 简介

阿里云致力于打造公共、开放、安全的云计算服务平台。通过技术创新，不断提升计算能力与规模效益，将云计算变成真正意义上的基础设施。

阿里云竭诚为客户提供稳定、可靠、安全、合规的云计算基础服务，帮助客户保护其系统及数据的可用性、机密性和完整性。

本白皮书介绍了阿里云云安全体系，内容包括：

- 安全责任共担
- 阿里云平台安全
- 阿里云产品提供的安全功能
- 阿里云云盾安全服务
- 阿里云安全生态

帮助客户在其现有的 IT 控制框架下集成和使用阿里云服务。阿里云安全体系帮助客户更好地使用阿里云平台以及理解整体 IT 控制环境。

第2章 安全责任共担

基于阿里云的客户应用，其安全责任由双方共同承担：阿里云确保云服务平台的安全性，客户负责基于阿里云服务构建的应用系统的安全。

阿里云负责基础设施（包括跨地域、多可用区部署的数据中心，以及阿里巴巴骨干传输网络）、物理设备（包括计算、存储和网络设备）、飞天分布式云操作系统及之上的各种云服务产品的安全控制、管理和运营，从而为客户提供高可用和高安全的云服务平台。

阿里云基于阿里巴巴集团多年攻防技术积累，为客户提供云盾安全服务，保护客户的应用系统。

客户负责以安全的方式配置和使用云服务器（ECS）、数据库（RDS）实例及其他云产品，基于这些云产品以安全可控的方式构建自己的应用；客户可选择使用云盾安全服务或者阿里云安全生态里的第三方安全厂商的安全产品为其应用系统提供安全防护。

安全责任共担模式帮助客户减轻安全运营负担，使得客户能够更专注于核心业务。

2.1 阿里云安全责任

阿里云负责基础设施、物理设备、分布式云操作系统及云服务产品安全，并为客户提供保护云端应用及数据的技术手段。

阿里云保障云平台自身安全：

- 保障云数据中心物理安全；
- 保障云平台硬件、软件和网络安全，如操作系统及数据库的补丁管理、网络访问控制、DDoS 防护、灾难恢复等；
- 及时发现云平台的安全漏洞并修复，修复漏洞过程不影响客户业务可用性；
- 通过与外部第三方独立安全监管与审计机构合作，对阿里云进行安全合规与审计评估。

阿里云为客户提供保护云端信息系统的技术手段：

- 为客户提供多地域、多可用区分布的云数据中心以及多线 BGP 接入网络，使得客户可利用阿里云基础设施构建跨机房高可用的云端应用；
- 云账号支持主子账号、双因素认证、分组授权、细粒度授权、临时授权；
- 为客户提供安全审计手段；
- 为客户提供数据加密手段；
- 为客户提供云盾安全服务；
- 引入第三方安全厂商，为客户提供个性化的行业安全解决方案。

2.2 客户安全责任

客户基于阿里云提供的服务构建自己的云端应用系统，综合运用阿里云产品的安全功能、云盾安全服务以及安全生态提供的第三方安全产品保护自己的业务系统。

客户应保护阿里云账号，使用阿里云访问控制服务（RAM）为每个运维管理人员分配独立的 RAM 用户账号，授予完成运维管理工作需要的最小权限，通过群组授权实现职责分离。阿里云建议客户为重要账号启用双因素认证。使用阿里云操作审计服务（ActionTrail）记录管理控制台操作及 OpenAPI 调用日志。使用阿里云加密服务对敏感数据进行加密。

阿里云提供的云服务器（ECS）、专有网络（VPC）服务的实例完全由客户控制，客户应管理实例并进行安全配置。例如客户应加固租用的云服务器操作系统、升级补丁，配置安全组防火墙进行网络访问控制。

阿里云提供的其他服务，例如云数据库（RDS）、大数据计算服务（ODPS），客户不需要关心如何维护实例，也不需要关心操作系统、数据库的补丁升级、配置加固，只需要管理这些服务的账号及授权，并使用这些服务提供的安全功能，例如配置 RDS 服务的源 IP 白名单。

第3章 阿里云平台安全

3.1 安全合规

阿里云为客户提供经第三方权威测评及认证机构现场审核过的云服务。这些测评和认证可以为客户提供更多有关阿里云制定的安全策略、流程和程序，实施的安全控制措施以及安全运营的信息。

阿里云已经通过以下测评及认证：

- ISO/IEC 27001
- 云安全 STAR（CSA STAR）
- 信息安全等级保护三级
- 可信云服务认证
- CNAS 认可的云测评

3.2 高可用的基础设施

阿里云为客户提供全球部署、多地域多可用区的云数据中心；采用多线 BGP 网络提高网络访问体验；飞天分布式云操作系统为所有云产品提供高可用基础架构和多副本数据冗余；全球领先的热升级技术使得产品升级、漏洞修复都不会影响客户业务；高度自动化的运维及安全，国内领先的合规性；为客户提供高可用、安全、可信的云计算基础设施。

3.2.1 全球部署的基础设施

阿里云在全球部署数据中心，同地域支持多个可用区。客户业务跨地域、跨可用区部署，可实现高可用架构，例如同城应用双活、异地数据灾备。

国家	地域	可用区数量
中国	深圳	2
	青岛	2
	杭州	4
	香港	2
	北京	2
	上海	2
美国	硅谷	2
新加坡	新加坡	1

3.3 物理与环境安全

阿里云园区和办公区均设置入口管控，并划分单独的访客区，访客出入必须佩戴证件，且由阿里云员工陪同。阿里云数据中心建设满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心机房通信基础设施标准》中 T3+标准，包含以下物理与环境安全控制要求：

3.3.1 访问控制

阿里云数据中心仅向本数据中心运维人员授予长期访问权限，若运维人员转岗或离职，权限立即清除。其他人员若因为业务需求要进入数据中心，必须先提出申请，经各方主管审批通过后才能获取短期授权；每次出入需要出示证件，并进行登记，且数据中心运维人员全程陪同。

阿里云数据中心内部划分机房包间，测电区域，库房间等区域，各个区域拥有独立的门禁系统，重要区域采用指纹等双因素认证，特定区域采用铁笼进行物理隔离。

3.3.2 监控与审计

阿里云数据中心机房各区域设有安防监控系统，监控范围覆盖所有区域和通道，配有物业保安 7x24 小时巡逻。

所有视频监控和文档记录均会长期保存，且由专人定期复核。

3.3.3 火灾检测及应对

阿里云数据中心火灾探测系统利用热和烟雾传感器实现，传感器位于天花板和地板下面；在事件触发时，提供声光报警。数据中心采用整体气体灭火系统与手动灭火器，同时组织火灾检测与应对的培训和演练。

3.3.4 电力

为保障阿里云业务 7*24 小时持续运行，阿里云数据中心采用双路市电电源和冗余的电力系统，主、备电源和系统具备相同的供电能力。若电源发生故障，会由带有冗余机制的电池组和柴油发电机对设备进行供电，保障数据中心在一段时间内的持续运行能力。

3.3.5 温度和湿度

阿里云数据中心采用精密空调来保障恒温恒湿的环境，并对温湿度进行电子监控，一旦发生告警立即采取应对措施。空调机组均采用热备冗余模式。

3.3.6 设备安全

阿里云建立了对设备全生命周期（包含接收、保存、安置、维护、转移以及重用或报废）的安全管理。设备的访问控制和运行状况监控有着严格管理，并定期进行设备维护和盘点。

当设备重用或报废时，阿里云会对存储介质进行覆写、消磁或折弯等数据清除处理，数据清除技术满足行业标准，清除操作留有完整记录，确保客户数据不被未授权访问。

3.4 网络安全

3.4.1 网络隔离

阿里云对生产网络与非生产网络进行了安全隔离，从非生产网络不能直接访问生产网络的任何服务器和网络设备。

阿里云把对外提供服务的**云服务网络**和支撑云服务的**物理网络**进行安全隔离。通过网络 ACL 确保云服务网络无法访问物理网络。

阿里云采取网络控制措施防止非授权设备私自联到云平台内部网络，并防止云平台物理服务器主动外联。

3.4.2 云平台 DDoS 防护

阿里云使用自主研发的 DDoS 防护系统保护所有数据中心，自动检测、调度和清洗，从遭受攻击到开始清洗响应时间不超过 5 秒，保证云平台网络稳定。

3.5 分布式云操作系统安全

阿里云基于自主研发的飞天大规模分布式计算和存储平台提供云服务，为了保障飞天平台的安全性，阿里云对分布式云操作系统进行了定制和加固，针对入侵和逃逸风险设计了防御措施和监控手段，确保底层系统的安全。

3.6 安全开发（SDL）

阿里云严格按照安全开发生命周期方法开发云平台及云产品，目标是将信息安全融入到整个软件开发生命周期中。

在需求分析阶段，阿里云根据 FRD（功能需求文档）进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，形成《安全需求分析建议》，并与业务方、开发人员就其中建议达成共识；

在产品设计阶段，阿里云对系统进行攻击面分析、威胁建模，对产品设计中采用的技术进行安全评估，形成《产品设计安全建议》，并与开发人员就安全建议达成共识；

在编码阶段，阿里云设计了安全的开发框架供开发人员使用，同时要求开发人员严格遵循安全编码规范；

在测试阶段，阿里云通过渗透测试和代码审计发现漏洞；

在发布阶段，只有经过安全测试，并且得到《安全审核报告》许可后，系统才能发布到线上环境，以防止产品携带安全漏洞在生产环境运行；发布过程按照安全上线规范对系统进行整体加固。

3.7 安全运维

阿里云通过飞天运维管理平台进行统一管理，采取严格的访问控制、职责分离、监控审计来确保运维安全。

3.7.1 堡垒机

阿里云在生产网络边界部署了堡垒机，办公网内的运维人员只能通过堡垒机进入生产网进行运维管理。

运维人员登录堡垒机时使用域账号密码加动态口令方式进行双因素认证。堡垒机使用高强度加密算法保障运维通道数据传输的机密性和完整性。

3.7.2 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。

3.7.3 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。

3.7.3.1 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，由安全团队负责审计。

数据库管理员和系统管理员职责分离。

3.7.4 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。

3.7.5 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。

阿里云集中日志平台仅提供日志采集和查看接口，不提供修改和删除接口。

3.7.6 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。

3.8 数据安全

3.8.1 数据安全体系

阿里云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据生产、数据存储、数据使用、数据传输、数据传播、数据销毁）各环节进行数据安全管理管控，实现数据安全目标。

在数据安全生命周期的每一个阶段，都有相应的安全管理制度以及安全技术保障。

3.8.2 数据所有权

2015 年 7 月，阿里云发起中国云计算服务商首个“数据保护倡议”，这份公开倡议书明确：运行在云计算平台上的开发者、公司、政府、社会机构的数据，

所有权绝对属于客户；云计算平台不得将这些数据移作它用。平台方有责任和义务，帮助客户保障其数据的私密性、完整性和可用性。

3.8.3 多副本冗余存储

阿里云使用分布式存储，文件被分割成许多数据片段分散存储在不同的设备上，并且每个数据片段存储多个副本。分布式存储不但提高了数据的可靠性，也提高了数据的安全性。

3.8.4 数据传输加密

云平台提供标准的加密传输协议，以方便云平台与外界以及系统间传输敏感数据的需求。其中管理控制台以及 OpenAPI 网关均支持 HTTPS 数据加密传输协议，支持标准的 TLS 协议，可提供高达 256 位密钥的加密强度，完全满足敏感数据加密传输需求。

3.8.5 数据存储加密

对于云平台运行需要用到的敏感数据，例如授权凭证、用户密码、密钥，统一使用阿里云密钥管理中心提供的密钥管理及加密机制进行加密存储。

阿里云为客户提供加密服务，通过在阿里云中使用经国家密码管理局检测认证的硬件密码机，帮助客户满足数据安全方面的监管合规要求，保护云上业务数据的机密性。借助加密服务，客户可以实现对加密密钥的完全控制和进行加解密操作。

3.8.6 残留数据清除

对于曾经存储过客户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖。同时，任何更换和淘汰的存储设备，都将统一执行消磁处理并物理折弯之后，才能运出数据中心。

3.8.7 运维数据安全

阿里云运维人员未经客户许可，不得以任意方式访问客户未经公开的数据内容。

阿里云遵循生产数据不出生产集群的原则，从技术上控制了生产数据流出生产集群的通道，防止运维人员从生产系统拷贝数据。

第4章 阿里云产品安全

4.1 弹性计算

4.1.1 云服务器 ECS

4.1.1.1 租户隔离

CPU 隔离：阿里云 ECS 支持 Xen 和 KVM 两种 Hypervisor，基于硬件虚拟化技术 VT-x，hypervisor 运行在 vmx root 模式，虚拟机运行在 vmx non-root 模式，通过硬件机制进行隔离，有效地防止了虚拟机访问特权资源，同时也做到了虚拟机之间的有效隔离。

内存隔离：在虚拟化层，Hypervisor 隔离内存。云服务器运行时，使用硬件辅助的 EPT（Extended Page Tables，扩展页表）技术，确保云服务器之间无法互访对方内存。云服务器释放后，它的所有内存会被 Hypervisor 清零。这样防止云服务器关闭后释放的物理内存页内容被其他云服务器访问到。

存储隔离：在虚拟化层，Hypervisor 采用分离设备驱动模型实现 I/O 虚拟化，虚拟机所有 I/O 操作都会被 Hypervisor 截获处理；Hypervisor 保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。云服务器释放后，原有磁盘的内容在被删除的时候由宿主机的文件系统回收，当再次分配的时候，由宿主机的文件系统负责清空对应的磁盘内容。

网络隔离：ECS 实现了虚拟交换机（virtual switch）。发往某个虚拟机的报文只会送到这个虚拟机的虚拟网卡所对应的虚拟交换机端口，其他虚拟机看不到这个报文。在阿里云的实现方式下，运行在混杂（promiscuous）模式下的

虚拟实例也不可能接收或嗅探到应去往其他虚拟实例的流量。虽然可以把网络接口设置为混杂模式，但 hypervisor 不会传送任何到其他目的地址的流量给它们。即使同一个客户拥有的运行在同一台物理服务器上的两个虚拟实例之间也不能嗅探到对方流量。阿里云还采用 VPC 和安全组防火墙进行网络隔离。

4.1.1.2 安全组防火墙

安全组是阿里云提供的分布式虚拟化防火墙，具备状态检测包过滤功能。

安全组是一个逻辑上的分组，这个分组是由**同一个地域（Region）**内具有相同安全保护需求并相互信任的实例组成。使用安全组可设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分网络安全域。

每个实例至少属于一个安全组。

同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通，可以授权某个源安全组或某个源网段访问目的安全组。

4.1.1.3 防 IP/MAC/ARP 欺骗

在传统网络里，ip/mac/arp 欺骗一直是网络面临的严峻考验。通过 ip/mac/arp 欺骗，黑客可以扰乱网络环境，窃听网络机密。

阿里云云平台通过宿主机上的网络底层技术机制，彻底解决了这些问题：在宿主机数据链路层隔离由云服务器向外发起的异常协议访问并阻断云服务器 arp/mac 欺骗，在宿主机网络层防止云服务器 ip 欺骗。

4.1.1.4 高可用性

负载均衡：多台 ECS 云服务器可以使用 SLB 负载均衡服务组成集群，消除单点故障，提升应用系统的可用性。

数据高可靠性：云服务器镜像文件、快照文件均默认存储三份，分布在不同交换机下的不同物理服务器上，数据可靠性不低于 99.999%。

故障自动恢复：云服务器部署在宿主机（承载云服务器的物理服务器）上，宿主机可能因性能异常或者硬件原因导致故障，当检测到云服务器所在的宿主机发生故障时，系统会启动保护性迁移，把云服务器迁移到正常的宿主机上，自动恢复，保障应用的高可用性。

快照：快照是云服务器上的数据在某一个时间点的拷贝。云服务器可以按照用户事先设定的策略定时自动创建快照，也可以由用户创建自定义快照。用户可使用快照回滚来恢复以往磁盘数据，加强数据安全，提高系统可用性。常见快照使用场景：1）云服务器系统变更前做好快照，在变更出现问题后可以快速回退；2）对已安装应用软件包的云服务器打快照，从快照创建自定义镜像，可以批量创建服务器，简化用户管理部署工作。

4.1.1.5 安全镜像

阿里云镜像集成了所有已知的高危漏洞补丁，防止主机上线之后即处于高风险状态。

在发现新的高危安全漏洞后，阿里云会迅速更新镜像并提供给客户。

阿里云使用数据校验算法和单向散列算法确保镜像完整性，防止被恶意篡改。

4.1.1.6 漏洞热修复

漏洞热修复技术使得漏洞修复过程不需要重启系统，可以让客户的虚拟机彻底无感知，确保上层客户业务不受影响。

4.1.2 云引擎 ACE

阿里云应用引擎（以下简称 ACE）是阿里云计算推出一款基于弹性扩展的网络应用托管平台，采用多层沙箱保护提供安全运行环境，并且整合多种软件开发常用的扩展服务，帮助开发者快速开发和部署应用程序，将开发者从系统运维、技术钻研等工作中解放出来，集中于核心业务的开发和运营。目前支持 JAVA、PHP、Python、NODEJS 等开发语言。

4.1.2.1 高可用性

个别 ACE 实例故障不影响整体服务，具备健康检查机制，实例宕机后自动重启，硬件设备故障时应用实例将自动漂移。

云引擎支持多个应用实例负载均衡，消除单点故障。

4.1.2.2 沙箱隔离

Web 容器、操作系统、网络多层沙箱立体防护

- 资源层沙箱

资源层沙箱对用户和运行实例占有的资源进行隔离。

- 操作系统层沙箱

该沙箱控制文件的读写权限。仅允许读写用户自己的文件，禁止执行任何程序，禁止对敏感系统文件的读取。

- 运行实例沙箱

运行实例沙箱对开发语言的调用进行限制，禁止使用禁用的类、方法。

4.1.2.3 安全防御

云引擎对多租户进行安全隔离，保障客户数据安全。

在安全防护策略上，云引擎在阿里云云盾的防御体系下，提供抗网络入侵检测、DDoS 防御系统、防密码暴力破解、主机入侵防御、安全弱点分析功能，保障客户应用安全。

4.1.2.4 监控和审计

提供应用的性能数据的监控与分析，包括 JVM 的各项参数、网络流量数据。同时提供运行日志的查询和下载功能，方便用户调用。

4.2 网络

4.2.1 负载均衡 SLB

4.2.1.1 高可用性

采用 LVS 集群部署方式，采用全冗余设计，无单点，可用性不低于 99.99%。

根据应用负载进行弹性扩容，在流量波动情况下不中断对外服务。

4.2.1.2 健康检查

SLB 服务会检查云服务器池中 ECS 的健康状态，自动隔离异常状态的 ECS，该 ECS 恢复正常后自动解除屏蔽，从而解决了单台 ECS 的单点问题，同时提高了应用的整体服务能力。

4.2.1.3 抗 CC 攻击

在标准的负载均衡功能之外，SLB 服务还具备 TCP 与 HTTP 抗 DDoS 攻击的特性，在官方 LVS 基础上进行了定制化，新增 synproxy 等攻击 TCP 标志位 DDoS 攻击防御功能，增强了应用服务器的防护能力。

4.2.1.4 访问控制

SLB 可以屏蔽后端服务器 IP 地址，对外只提供 VIP。

SLB 提供源 IP 白名单功能，可限制仅允许可信的源 IP 访问客户通过 SLB 开放的服务。

4.2.1.5 https/ssl 负载均衡

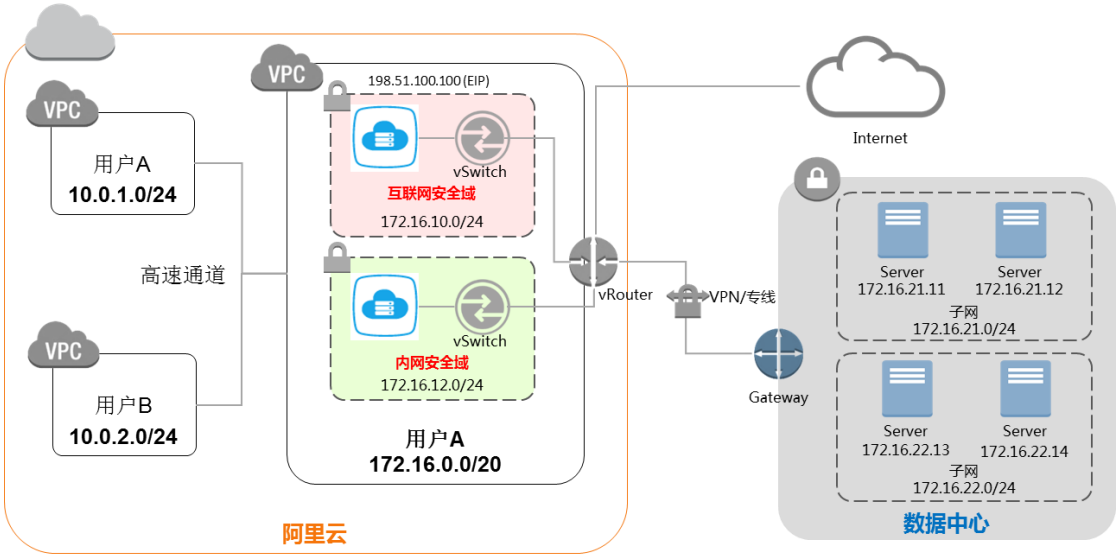
SLB 支持 HTTPS/SSL 负载均衡功能：

1. 对于需要进行证书认证的服务，可以集中、统一在 SLB 上管理证书和密钥。而无须部署在每台 ECS（Real Server）上。
2. 可配置密文卸载（Offload）功能，解密处理统一在 SLB 上进行，降低后端 ECS CPU 开销。

SLB 提供证书管理系统管理和存储用户证书和密钥，用户上传到证书管理系统的私钥都会加密存储。

4.2.2 专有网络 VPC

专有网络（AliCloud VPC），帮助客户基于阿里云构建出一个隔离的网络环境。客户可以完全掌控自己的虚拟网络，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等。此外客户也可以通过专线/VPN 等连接方式将 VPC 与传统数据中心组成一个按需定制的网络环境，实现应用的平滑迁移上云。典型的 VPC 网络架构如下图所示：



4.2.2.1 自定义网络

客户可以在 VPC 内自定义网络地址，划分子网，自定义路由。

4.2.2.2 网络安全域划分

可以通过具备状态检测包过滤功能的安全组防火墙进行网络安全域的划分。

4.2.2.3 网络边界控制

Internet 边界 :只有绑定了弹性公网 IP(EIP)的实例可以直接访问互联网。没有 EIP 的实例可以把默认路由指向有 EIP 且配置了 SNAT 的实例访问互联网。

VPN 接入 :VPC 里可以部署 SSL VPN 实例 ,通过互联网供远程拨号接入；或部署 IPSec VPN 实例 ,通过互联网与其他 VPC 或物理网络互联组成混合网络。

专线接入：阿里云提供专线接入点，通过专线可以把 VPC 与物理网络互联组成混合网络。专线接入不支持 VPN 隧道。

4.2.2.4 租户隔离

不同租户的云服务器在不同的 VPC 里。

不同 VPC 之间通过 VxLAN 隧道 ID 进行隔离。VPC 内部由于虚拟交换机和虚拟机路由器的存在，所以可以像传统网络环境一样划分子网，每一个子网内部的不同云服务器使用同一个虚拟交换机互联，不同子网间使用虚拟路由器互联。

不同 VPC 之间内部网络完全隔离，只能通过弹性公网 IP 互联。

4.2.2.5 网络访问控制

VPC 使用安全组防火墙进行三层网络访问控制。

4.3 数据库

4.3.1 云数据库 RDS

4.3.1.1 租户隔离

数据库实例隔离：RDS 通过数据库自身的实例隔离机制进行租户隔离，每个租户拥有自己实例的管理员权限 ;同时阿里云对数据库服务器进行了安全加固，例如禁止 RDS 用户通过数据库读写操作系统文件 ,保证 RDS 用户无法访问物理服务器上运行的其他用户的数据库实例。

4.3.1.2 访问控制

用户可设定 RDS 服务为内网连接模式，即只允许 ECS 云服务器从内网访问 RDS，可以防止数据库暴露在公网上。

RDS 用户可以设置 IP 白名单，仅允许指定源 IP 访问用户的 RDS 服务。

4.3.1.3 高可用性

每个 RDS 实例拥有两个物理节点进行主从热备，主节点发生故障，秒级切换至备节点，服务可用性高达 99.95%。

数据库数据存储在 Raid 5 磁盘阵列上，拥有多重备份，数据可靠性高达 99.9999%。

备份恢复：用户可随时进行数据备份，RDS 能够根据备份文件将数据库恢复至 7 日内任意时刻，提高了数据的可用性。

4.3.1.4 SQL 日志

RDS Proxy 记录所有发往 RDS 的 SQL 语句，内容包括连接 IP、访问的数据库名称、执行语句的账号、SQL 语句、执行时长、返回记录数、执行时间点等信息。

4.3.2 云数据库 Memcache 版

4.3.2.1 身份认证

云数据库 Memcache 版提供基于用户名、密码的身份认证机制。

4.3.2.2 *访问控制*

云数据库 Memcache 版仅允许 ECS 云服务器访问 ,并可以限制源服务器的 IP 地址，避免外部攻击。

4.3.3 云数据库 Redis 版

云数据库 Redis 版（AliCloudDB for Redis）是兼容开源 Redis 协议的 Key-Value 类型在线存储服务。云数据库 Redis 版支持字符串、链表、集合、有序集合、哈希表等多种数据类型，及事务（Transactions）、消息订阅与发布（Pub/Sub）等高级功能。

4.3.3.1 身份认证

云数据库 Redis 版提供基于实例 ID、密码的身份认证机制。

4.3.3.2 访问控制

云数据库 Redis 版仅支持阿里云内网访问，不支持外网访问，即只有在阿里云 ECS 上的应用才能与云数据库 Redis 版建立连接并进行数据操作。

4.3.3.3 高可用性

通过自动的故障检测和数据迁移，云数据库 Redis 版对应用屏蔽了机器和网络的硬件故障，提供 99.95%的高可用性。

云数据库 Redis 版通过存储多个数据备份及备份失效时的快速恢复，提供不低于 99.99%的数据可靠性。

4.3.4 分析型数据库 ADS

4.3.4.1 租户隔离

分析型数据库允许用户通过 MySQL 协议以及 MySQL 协议兼容的 JDBC、ODBC 方式连接数据库，连接时以用户 AccessKey ID 为用户名，AccessKey Secret 为密码。基于 MySQL 协议的要求，用户的 AccessKey Secret 在传输过程中，会基于随机的 Salt 进行加密，保证用户的密码安全。

分析型数据库以数据库作为租户隔离的基本单元，数据库的创建者云账号为数据库的 Owner。未经数据库创建者授权，任何其他云账号不能访问该数据库的数据。

用户的数据库在自己独享的进程级别实例上运行，从进程级别实现了数据库的隔离。

4.3.4.2 高可用性

可定制的数据多副本和动态资源管理机制提供不间断在线服务。

阿里云负载均衡产品（Load Balancer）保证了用户访问链路（从阿里云网络入口到分析型数据库产品访问入口）的负载均衡和高可用。

从分析型数据库产品内部设计的角度，多副本冗余、双活、主备的实例部署、热升级等，保证了实例级别的高可用。

4.3.4.3 访问控制

数据访问包括用户数据访问和元数据访问。

用户数据访问包括对用户数据库表的查询 SELECT、实时表的数据插入 INSERT 和删除 DELETE 等操作。

元数据从可见级别上，可以分为用户可见元数据和系统管理相关元数据（用户不可见）。用户对可见元数据可进行只读查询，但不能进行修改和删除，保证了用户元数据的完整性和安全性。用户无法访问系统管理相关元数据，保证了系统级别敏感数据的安全性。

分析型数据库提供符合主流数据库标准的 ACL 授权管理功能，数据库的 Owner 可以通过 GRANT/REVOKE 等命令，对用户进行数据对象的授权管理操作。

4.3.4.4 控制台访问控制

分析型数据库控制台为用户提供了对数据库的用户视角功能操作的统一界面。不同用户角色，在不同的数据库和权限体系下，有自己特定的操作视图。

4.3.4.5 系统内部信息保护

分析型数据库在系统内部储存在磁盘上的敏感信息，全部通过非对称加密方式加密后存储。从 ODPS 中进行数据装载时，访问用户在 ODPS 上的数据的系统云账号仅在特定的位置具有访问权限，并且在访问时会对数据装载的发起者再次校验，确保数据装载的发起者有对应 ODPS 表的访问权限。

4.4 存储与 CDN

4.4.1 对象存储 OSS

对象存储（Object Storage Service），是阿里云对外提供的海量、安全和高可靠的云存储服务。RESTFul API 的平台无关性，容量和处理能力的弹性扩展，按实际容量付费真正使您专注于核心业务。

4.4.1.1 身份验证

阿里云用户可以在管理控制台里自行创建 Access Key，Access Key 由 AccessKey ID 和 AccessKey Secret 组成，其中 ID 是公开的，用于标识用户身份，Secret 是秘密的，用于用户鉴别。

当用户向 OSS 发送请求时，需要首先将发送的请求按照 OSS 指定的格式生成签名字符串；然后使用 AccessKey Secret 对签名字符串进行加密（基于 HMAC 算法）产生验证码。验证码带时间戳，以防止重放攻击。OSS 收到请求以后，通过 AccessKey ID 找到对应的 AccessKey Secret，以同样的方法提取签名字符串和验证码，如果计算出来的验证码和提供的一样即认为该请求是有效的；否则，OSS 将拒绝处理这次请求，并返回 HTTP 403 错误。

4.4.1.2 访问控制

对 OSS 的资源访问分为拥有者访问、第三方用户访问。这里的拥有者指的是 Bucket 的拥有者，也称为开发者。第三方用户是指访问 Bucket 里资源的用户。 访问又分为匿名访问和带签名访问。对于 OSS 来说，如果请求中没有携带任何和身份相关的信息即为匿名访问。 带签名访问指的是按照 OSS API 文档中规定的在请求头部或者在请求 URL 中携带签名的相关信息。

OSS 提供 Bucket 和 Object 的权限访问控制。

Bucket 有三种访问权限：public-read-write，public-read 和 private。

- public-read-write：任何人（包括匿名访问）都可以对该 bucket 中的 object 进行 PUT，Get 和 Delete 操作。
- public-read：只有该 bucket 的创建者可以对该 bucket 内的 Object 进行写操作（包括 Put 和 Delete Object）；任何人（包括匿名访问）可以对该 bucket 中的 object 进行读操作（Get Object）。
- private：只有该 bucket 的创建者可以对该 bucket 内的 Object 进行读写操作（包括 Put、Delete 和 Get Object），其他人无法访问该 Bucket 内的 Object。

用户新创建一个 Bucket 时，如果不指定 Bucket 权限，OSS 会自动为该 Bucket 设置 private 权限。

Object 有四种访问权限：public-read-write, public-read, private, default。

- public-read-write：所有用户拥有此 Object 的读写权限。
- public-read： 非此 Object 的 Owner 拥有此 Object 的读权限，只有

此 Object 的 Owner 拥有此 Object 的读写权限。

- private：此 Object 的 Owner 拥有该 Object 的读写权限，其他的用户对此 Object 没有读、写权限。
- default：Object 遵循 Bucket 的访问权限。

用户上传 Object 时，如果不指定 Object 权限，OSS 会为 Object 设置为 default 权限。

4.4.1.3 RAM&STS

RAM (Resource Access Management) 是阿里云提供的资源访问控制服务。通过 RAM，主账号可以创建出子账号，子账号从属于主账号，所有资源都属于主账号，主账号可以将所属资源的访问权限授予给子账号。STS（Security Token Service）是阿里云提供的临时访问凭证服务，提供短期访问权限管理。STS 可以生成一个短期访问凭证给用户使用，凭证的访问权限及有效期限由用户定义，访问凭证过期后会自动失效。OSS 已经接入 RAM/STS 鉴权。

4.4.1.4 高可用性

OSS 服务可用性高达 99.9%。

OSS 数据三副本存储，可靠性达到 99.99999999%。

4.4.1.5 租户隔离

OSS 将用户数据切片，每片用户数据打上用户标签，离散存储在分布式文件系统中，并且用户数据和数据索引分离存储。OSS 用户认证采用 Access Key 对称密钥认证技术，对于用户的每个 HTTP 请求都验证签名。在用户验证通过后，根据用户标签，重组用户离散存储的数据。从而实现多租户间的数据存储隔离。

4.4.1.6 服务器端加密

OSS 支持在服务器端对用户上传的数据进行加密（Server-Side Encryption）。当用户上传数据时，OSS 对收到的用户数据加密，然后再将加密得到的数据永久保存下来；用户下载数据时，OSS 自动对保存的加密数据解密后把原始数据返回给用户，并在返回的 HTTP 请求 Header 中声明该数据进行了服务器端加密。

用户创建 Object 时，只需要在 Put Object 的请求中携带 x-oss-server-side-encryption 的 HTTP Header，并指定其值为 AES256，即可以实现该 Object 的服务器端加密存储。

4.4.2 表格存储 Table Store

表格存储（Table Store）是构建在阿里云飞天分布式系统之上的 NoSQL 数据库服务，提供海量结构化数据的存储和实时访问。表格存储（Table Store）以实例和表的形式组织数据，通过数据分片和负载均衡技术，实现规模上的无缝扩展。应用通过调用表格存储 API / SDK 或者操作管理控制台来使用表格存储服务。

4.4.2.1 身份验证

表格存储根据 AccessKey 对请求进行身份认证和鉴权，每个合法的表格存储请求都必须携带正确的 AccessKey 信息。表格存储对应用的每一次请求都进行身份认证和鉴权，以防止未授权的数据访问，确保数据访问的安全性。

4.4.2.2 高可用性

通过自动的故障检测和数据迁移，表格存储对应用屏蔽了机器和网络的硬件故障，提供 99.9%的高可用性。

表格存储通过存储多个数据备份及备份失效时的快速恢复，提供不低于99.99999999%的数据可靠性。

4.4.2.3 强一致性

表格存储保证数据写入强一致，写操作一旦返回成功，应用就能立即读到最新的数据。

4.4.2.4 监控集成

用户可以从表格存储控制台实时获取每秒请求数、平均响应延时等监控信息。

4.4.3 归档存储

归档存储(Archive Storage)作为阿里云数据存储产品体系的重要组成部分，致力于提供低成本、高可靠的数据归档服务，适合于海量数据的长期归档、备份。

数据以“Archive(文档)”的形式存储在归档存储中，是数据操作的基本单元。Archive 支持任意数据类型，如电影、音乐、文稿等。我们鼓励用户将多个数据文件进行打包、压缩、加密后，进行上传。单个 Archive 最大可达 40TB，在创建时都会分到一个唯一的 ID，内容无法修改。

Vault(目录)是归档存储提供给用户用于存放 Archive 的单元，相当于目录的作用，也是计费、权限控制等功能的管理单位。Vault 名称在每个用户的每个 Region 下唯一，用户在每个 Region 最多可以创建 10 个 Vault，Vault 不支持嵌套。

每个 Vault 里可以包含任意数量的 Archive。Vault 可以通过 Web 控制台、API 两种方式进行创建、删除等操作。

4.4.3.1 身份验证

阿里云用户可以在管理控制台里自行创建 Access Key，Access Key 由 Access Key ID 和 Access Key Secret 组成，其中 ID 是公开的，用于标识用户身份，Secret 是秘密的，用于用户鉴别。

归档存储服务仅对外提供 HTTPS 协议接口。

当用户向归档存储服务发送请求时 ,需要首先将发送的请求按照归档存储服务指定的格式生成签名字符串 ;然后使用 Access Key Secret 对签名字符串进行加密（基于 HMAC 算法）产生验证码。验证码带时间戳，以防止重放攻击。归档存储服务收到请求以后 通过 Access Key ID 找到对应的 Access Key Secret，以同样的方法提取签名字符串和验证码 ,如果计算出来的验证码和提供的一样即认为该请求是有效的；否则，消息服务将拒绝处理这次请求，并返回 HTTP 403 错误。

4.4.3.2 高可用性

归档存储服务数据多副本存储，可靠性达到 99.99999999%。

4.4.3.3 租户隔离

数据隔离：归档存储将用户数据切片，每片用户数据打上用户标签，离散存储在分布式文件系统中，并且用户数据和数据索引分离存储。用户认证采用 Access Key 对称密钥认证技术，对于用户的每个 HTTP 请求都验证签名。在用

户验证通过后，根据用户标签，重组用户离散存储的数据。从而实现多用户间的数据存储隔离。

4.4.3.4 数据完整性保护

数据文件在完成上传归档后，便不可修改，确保数据不可被篡改。每个文件会被分配终身唯一 ID。同样的文件多次上传，会得到不同的唯一 ID。

从初次上传开始，归档存储提供的树形校验码会贯穿始终。每 MB 数据都会进行独立的校验保护 ,在用户需要获取数据时 ,提供了局部的完整性校验功能。

4.4.4 消息服务 MS

消息服务（Message Service）是一种高效、可靠、安全、便捷、可弹性扩展的分布式消息与通知服务。消息服务能够帮助应用开发者在他们应用的分布式组件上自由的传递数据，构建松耦合系统。

4.4.4.1 身份验证

阿里云用户可以在管理控制台里自行创建 Access Key，Access Key 由 Access Key ID 和 Access Key Secret 组成，其中 ID 是公开的，用于标识用户身份，Secret 是秘密的，用于用户鉴别。

消息服务仅对外提供 HTTP 协议接口。

当用户向消息服务发送请求时 ,需要首先将发送的请求按照消息服务指定的格式生成签名字符串；然后使用 Access Key Secret 对签名字符串进行加密（基于 HMAC 算法）产生验证码。验证码带时间戳，以防止重放攻击。消息服务收到请求以后，通过 Access Key ID 找到对应的 Access Key Secret，以同样的方

法提取签名字符串和验证码，如果计算出来的验证码和提供的一样即认为该请求是有效的；否则，消息服务将拒绝处理这次请求，并返回 HTTP 403 错误。

4.4.4.2 访问控制

消息服务默认情况下，只支持队列创建者访问消息队列数据。同时，消息服务完全接入阿里云访问控制服务（RAM），支持主子账号和临时 AK 的访问方式。

子账号在主账号授权情况下可以访问主账号资源，其他用户也可以在资源所有者授权情况下，获取临时 AK 访问消息服务资源所有者的数据。

4.4.4.3 高可用性

消息服务可用性高达 99.9%。

消息服务数据三副本存储，可靠性达到 99.99999999%。

4.4.4.4 租户隔离

数据隔离：消息服务将用户消息数据切片，每片用户数据打上用户标签，离散存储在分布式文件系统中，并且用户数据和元数据分离存储。消息服务用户认证采用 Access Key 对称密钥认证技术，对于用户的每个 HTTP 请求都验证签名。在用户验证通过后，根据用户标签，重组用户离散存储的数据。从而实现多用户间的数据存储隔离。

4.4.5 内容分发网络 CDN

AliCloud CDN（内容分发网络）将源站内容分发至全国所有的节点，缩短用户查看对象的延迟，提高用户访问网站的响应速度与网站的可用性，解决网络带宽小、用户访问量大、网点分布不均等问题

4.4.5.1 身份验证

阿里云用户可以在管理控制台里自行创建 Access Key，Access Key 由 Access Key ID 和 Access Key Secret 组成，其中 ID 是公开的，用于标识用户身份，Secret 是秘密的，用于用户鉴别。

CDN 仅对外提供 HTTP 协议接口。

4.4.5.2 租户隔离

数据隔离：CDN 上用户的缓存数据，每片用户数据打上用户标签，存储系统中，并且用户数据和数据索引分离存储。用户认证采用 Access Key 对称密钥认证技术，对于用户按域名粒度请求区分。在用户验证通过后，根据用户域名，存储的数据。从而实现多用户间的数据存储隔离。

4.4.5.3 URL 鉴权

URL 鉴权功能旨在保护用户站点的内容资源不被非法站点下载盗用。采用防盗链方法添加 referer 黑、白名单方式可以解决部分盗链问题，但是，由于 referer 内容可以伪造，referer 防盗链方式还不能很好的保护站点资源，因此采用 URL 鉴权方式保护用户源站资源更为安全有效。

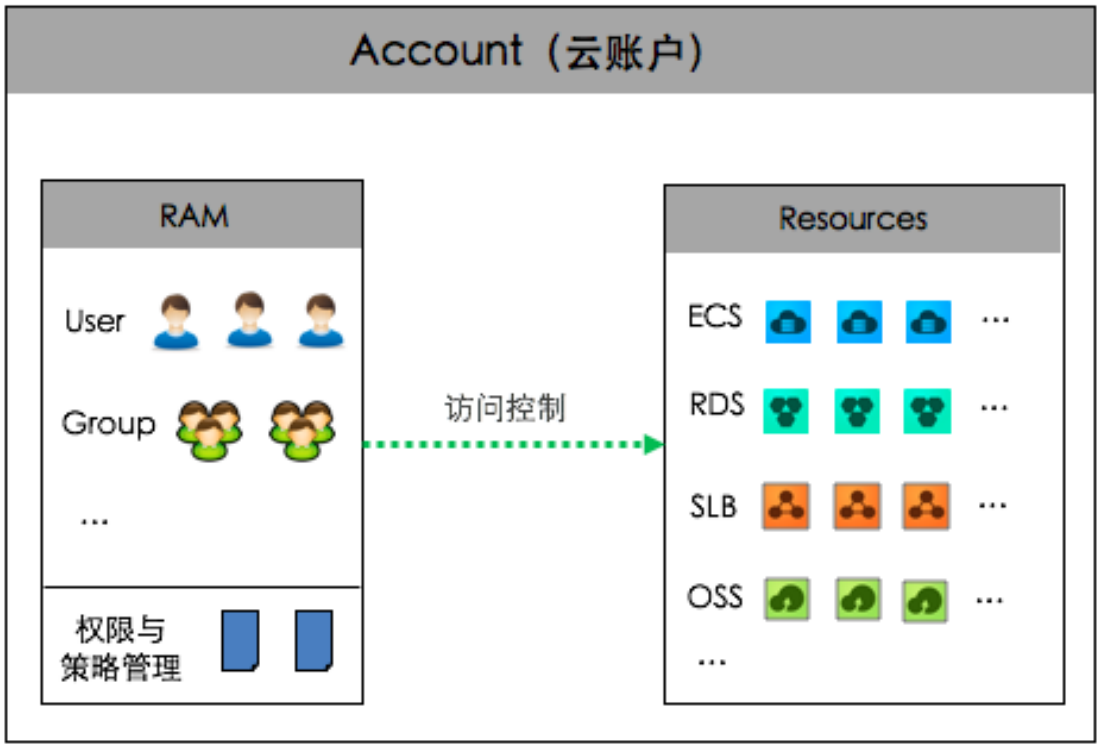
URL 鉴权功能是通过阿里云 CDN 加速节点与客户资源站点配合实现的一种更为安全可靠的源站资源防盗方法。由 CDN 客户站点提供给用户加密 URL（包含权限验证信息），用户使用加密后的 URL 向加速节点发起请求，加速节点对加密 URL 中的权限信息进行验证以判断请求的合法性，对合法请求给予正常响应，拒绝非法请求，从而有效保护 CDN 客户站点资源。

4.5 管理与监控

4.5.1 访问控制 RAM

阿里云访问控制服务（RAM）使得一个阿里云账户（主账户）可拥有多个子账户，支持分组授权（类似于角色）、双因素认证、强密码策略、控制台用户与 API 用户分离、临时授权、账户临时禁用等功能。授权可以细化到 API 粒度，支持时间段、源 IP 地址、资源标签等条件。

RAM 为客户提供的集中式用户身份与访问控制管理服务。与阿里云提供的其它服务类似，RAM 被抽象成云账户下的一种资源，但在每个云账户下只允许存在一个 RAM 实例，下图展现了 RAM 与其它云服务之间的关系：



RAM 是阿里云账户安全管理和安全运维的基础。通过 RAM 可以为每个子账户分配不同的密码或 AK，消除了云账户共享带来的风险；同时可为不同的子账户分配不同的权限，大大降低了因账户权限过大带来的风险。

4.5.1.1 账户安全管理

RAM 允许在云账户下创建并管理多个用户。RAM 用户是代表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。在云账户下，每个用户都有唯一的用户名、登录密码或访问密钥。通过 RAM，还可以控制 RAM 用户对基础设施云服务的访问权限，支持角色分离和最小特权的安全最佳实践。

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；从权限角度看，云账户与 RAM 用户是一种 root 与 user 的关系，Root 对资源拥有一切操作控制权限，而 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。

4.5.1.2 身份验证

使用云服务 API 访问资源：先为 RAM 用户创建 AccessKey，即可使用 AccessKey 来调用 API，或者使用客户端工具来调用 API；

使用管理控制台访问资源：为 RAM 用户创建登录密码，即可在 RAM 用户登录页面进行登录。

4.5.1.3 双因素认证

在使用控制台访问资源时，RAM 支持针对云账户和 RAM 用户启用多因素认证（Multi-Factor Authentication, MFA）。MFA 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。关于 MFA 的详细介绍，请参考章节：阿里云账户安全 - 多因素认证。

4.5.1.4 群组管理

RAM 提供了群组功能，如果多个用户的工作职责相同，那么建议通过创建群组的方式来进行用户权限管理。

一般情况下，不必对 RAM 用户直接绑定授权策略，更方便的做法是创建与人员工作职责相关的群组（如 admins、developers、accounting 等），为每个群组绑定合适的授权策略，然后把用户加入这些群组。群组内的所有用户共享相同的权限。这样，如果需要修改群组内所有人的权限，只需在一处修改即可。当组织人员发生调动时，只需更改用户所属的群组即可。

4.5.1.5 授权管理

授权策略是一组权限的集合，它以一种策略语言来描述。通过给用户或群组附加授权策略，用户或群组中的所有用户就能获得授权策略中指定的访问权限。RAM 支持两种类型的授权策略：系统授权策略和客户自定义授权策略。

系统授权策略

系统授权策略是阿里云提供的一组通用授权策略，主要针对不同产品的只读权限或所有权限。对于阿里云提供的这组授权策略，用户只能用于授权，而不能编辑和修改。对于这些系统授权策略，阿里云会自动进行更新或修改。

自定义授权策略

RAM 支持用户创建自定义授权策略，使用 Policy(授权策略)来描述授权的具体内容。授权内容主要包含效力(Effect)、资源(Resource)、对资源所授予的

操作权限(Action)以及限制条件(Condition)。举例来说，可以实现如下的细粒度授权：允许对 OSS 的 samplebucket 进行只读操作，条件是请求者的 IP 来源为 42.160.1.0，访问时间为早上 9 点至晚上 9 点，否则拒绝访问。

4.5.1.6 角色管理

角色是一种可以由子用户（RAM 用户）扮演的虚拟身份，主要用来解决**临时授权、跨云帐号授权以及为云服务授权**的问题。

区别于子用户，角色不可以设置密码和 AccessKey，但是可以设置可信实体。 可以在可信实体中定义哪些云服务或哪些云帐号下的子用户可以扮演此角色，即以此角色的身份和权限来访问您的云资源。

角色主要有两种：

用户角色：允许子用户扮演的角色，可以是自己的子用户，或者是其他帐号的子用户。服务角色主要用来解决跨帐号访问和临时授权的问题。

服务角色：允许云服务扮演的角色，授予一个云服务可以访问您其他云服务中的部分资源的权限。

4.5.1.7 安全令牌（STS）

阿里云 STS (Security Token Service) 是为阿里云账号（或 RAM 用户）提供短期访问权限管理的云服务。

有时存在一些用户（人或应用程序），他们并不经常访问您的云资源，只是偶尔需要访问一次，我们称这些用户为“**临时用户**”；**还有些用户，由于自身安全性不可控，不适合颁发长期有效的访问密钥。**这些情况下，可以通过 STS

(Security Token Service，它是 RAM 的一个扩展授权服务) 来为这些用户颁发访问令牌。颁发令牌时，并可以根据需要来定义令牌的权限和自动过期时间。

使用 STS 访问令牌给临时用户授权的好处是让授权更加可控，不必为临时用户和安全性较低的用户创建一个 RAM 用户账号及密钥，因为 RAM 用户密钥都是长期有效的。此外，也可以授权允许一个 RAM 用户使用 STS 服务颁发访问令牌，以实现对 RAM 用户的进一步分权。

4.5.1.8 账户安全管理最佳实践

- 为云账户和高风险权限 RAM 用户启用多因素认证（MFA）；
- 分离用户管理、权限管理与资源管理的 RAM 用户，分权制衡；
- 为云账户和 RAM 登录用户配置强密码策略；
- 不要为云账户（主账户）创建 AccessKey，避免 AK 泄漏的巨大风险；
- 定期轮转用户登录密码和 AccessKey；
- 将控制台用户与 API 用户分离，不建议给 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 AccessKey；
- 使用策略限制条件来增强安全性，比如访问源 IP，时间等；
- 员工换岗、离职时，及时调整和撤销 RAM 用户不再需要的权限；
- 遵循最小授权原则，不要过度授权。

4.5.2 云监控

云监控 CMS（Cloud Monitor System）是一个开放性的监控平台，可实时监控云上站点和服务器，并提供多种告警方式（短信，旺旺，邮件）以保证及时预

警，为站点和服务器的正常运行保驾护航。目前云监控提供站点监控、云服务监控和自定义监控三种服务。

4.5.2.1 站点监控

站点监控可以对目标站点服务的可用性以及响应时间进行监控。系统已经默认预置了 8 种监控类型，包括 http 监控、ping 监控、tcp 监控、udp 监控、DNS 监控、pop 监控、smtp 监控、ftp 监控。其中每种监控类型里面包含了两个监控项：status 和 responsetime。每个用户最多可以设置 200 个站点监控。

4.5.2.2 云服务监控

云服务监控是阿里云为用户提供的各种云产品的监控 ,当前对用户开放的包括 ECS、RDS、SLB、OCS、OSS、EIP、KVStore、MNS、ADS、CDN，其它云产品的监控会陆续加入进来。

4.5.2.3 自定义监控

自定义监控是提供给用户自由定义监控项及报警规则的一项功能。通过此功能，用户可以针对自己关心的业务进行监控，将采集到监控数据上报至云监控，由云监控来进行数据的处理 ,并根据结果进行报警。云监控当前允许至多 10 个自定义监控项，且上报监控数据的服务必须在阿里云的云服务器上。

4.6 大规模计算

4.6.1 开放数据处理服务 ODPS

4.6.1.1 安全体系

开放数据处理服务（Open Data Processing Service， 简称 ODPS）由阿里云自主研发，提供针对 TB/PB 级数据、实时性要求不高的分布式处理能力，应用于数据分析、挖掘、商业智能等领域。阿里巴巴的数据业务都运行在 ODPS 上。

ODPS 的安全体系有如下特点：

- 用户访问需要认证，用户操作需要鉴权，所有操作记录审计日志；
- 支持多租户的使用场景，同时满足多用户协同、数据共享、数据保密和安全的需要；
- 支持 ACL 授权、policy 授权、角色授权、跨 project app 授权多种权限管理方法，满足多种场景的需求；
- 开放的架构可以很方便的根据用户的需要添加新的安全功能。

4.6.1.2 身份验证

ODPS 认证使用消息签名机制，它不同于传统的基于用户名/密码的认证方法。消息签名机制可以保证消息在 HTTP 传输过程中的完整性(Integrity)和真实性(Authenticity)。 常用的消息签名算法有 HMAC-SHA1 和 RSA-SHA1。传统的基于用户名/密码的认证方法适合于人机交互模式，如浏览 Web 网站；而消息签名机制则适合于非交互模式 比如编写 APP 应用程序访问开放服务的 API。目前 ODPS 采用的消息签名算法是 HMAC-SHA1。

4.6.1.3 授权管理

项目空间(Project)是 ODPS 实现多租户体系的基础，是用户管理数据和计算的基本单位，也是计量和计费的主体。当用户申请创建一个项目空间之后，该用户就是这个空间的所有者（Owner）。也就是说，这个项目空间内的所有对象（eg, 表, 实例, 资源，UDF 等）都属于该用户。这就是说，除了 Owner 之外，任何人都无权访问此项目空间内的对象，除非有 Owner 的授权许可。

当项目空间的 Owner 决定对另一个用户授权时 ,Owner 需要先将该用户添加到自己的项目空间中来。只有添加到项目空间中的用户才能够被授权。

角色（Role）是一组访问权限的集合。当需要对一组用户赋予相同的权限时，可以使用角色来授权。基于角色的授权可以大大简化授权流程，降低授权管理成本。当需要对用户授权时，应当优先考虑是否应该使用角色来完成。

ODPS 可以对项目空间里的用户或角色 ,针对 Project、Table、Function、Resource Instance 四种对象，授予不同权限。

ODPS 支持两种授权机制来完成对用户或角色的授权 :ACL 授权 和 Policy 授权 。

ACL 授权是一种基于对象的授权。通过 ACL 授权的权限数据（即访问控制列表, Access Control List）被看做是该对象的一种子资源。只有当对象已经存在时，才能进行 ACL 授权操作；当对象被删除时，通过 ACL 授权的权限数据会被自动删除。ACL 授权支持类似于 SQL92 定义的 GRANT/REVOKE 语法，它通过简单的授权语句来完成对已存在的项目空间对象的授权或撤销授权。

Policy 授权则是一种基于策略的授权。通过 Policy 授权的权限数据（即访问策略）被看做是授权主体的一种子资源。只有当主体（用户或角色）存在时，

才能进行 Policy 授权操作；当主体被删除时，通过 Policy 授权的权限数据会被自动删除。Policy 授权使用 ODPS 自定义的一种访问策略语言来进行授权，允许或禁止主体对项目空间对象的访问权限。

4.6.1.4 跨项目空间的资源分享

假设你是项目空间的 Owner 或管理员（admin 角色），如果有人需要申请访问你的项目空间资源，但是这个申请人并不属于你的项目团队。那么你可以使用跨项目空间的资源分享功能。

Package 是一种跨项目空间共享数据及资源的机制，主要用于解决跨项目空间的用户授权问题。

使用 Package 之后，A 项目空间管理员可以对 B 项目空间需要使用的对象进行打包授权（也就是创建一个 Package），然后许可 B 项目空间安装这个 Package。在 B 项目空间管理员安装 Package 之后，就可以自行管理 Package 是否需要进一步授权给自己 Project 下的用户。

4.6.1.5 数据保护机制（Project Protection）

如果项目空间中的数据非常敏感，绝对不允许流出到其他项目空间中去，那么可以使用项目空间保护机制——设置 ProjectProtection，明确要求项目空间中“数据只能流入，不能流出”。

4.7 应用服务与中间件

4.7.1 日志服务 LOG

日志服务（Log Service，简称 LOG）是针对日志收集、存储、查询和分析的服务。LOG 可收集云服务和应用程序生成的日志数据并编制索引，提供实时查询海量日志的能力。

4.7.1.1 *高可用性*

LOG 日志数据存放在分布式文件系统上，提供三副本存储机制，保障文件存储的可靠性。

4.7.1.2 只读日志系统

日志服务有一个重要特性就是防篡改。LOG 提供的是一个 append only 的日志系统，只能追加日志，而不能修改已经写入的日志，从根本上解决了日志防篡改的问题。

4.7.1.3 离线归档

LOG 提供日志归档保存到 ODPS 的功能 ,以便用户利用 ODPS 做数据分析。

4.7.1.4 身份验证

LOG 认证采用由阿里云颁发给用户的访问服务的秘钥（Access Key），在认证时使用 HMAC-SHA1 签名算法。

4.7.2 开放搜索服务 Open Search

开放搜索服务（Open Search）是阿里云自主开发的用于解决用户结构化数据搜索需求的托管服务，支持数据结构、搜索排序、数据处理自由定制。

开放搜索服务（Open Search）将应用结构简单化、定制化，用户可以通过可视化界面，自由配置文档的字段及属性，支持 OSS、ODPS、RDS 数据源、API/SDK 数据上传、界面上传等多种接入方式，数据自动同步和定时索引重建。通过简单操作即可完成多表 join 和数据处理，同时支持两轮相关性排序定制，使搜索操作简单、灵活。

4.7.2.1 高可用性

开放搜索服务（Open Search Service）在支持单应用亿级别文档存储和搜索，毫秒级别查询延迟，单应用万级别 QPS 性能的基础上提供 99.9%的系统可用性，不低于 99.9999%的数据持久性，并提供自动检测故障与恢复功能，保障服务的最高可用性。

4.7.2.2 数据隔离与备份

开放搜索服务（Open Search Service）为用户导入后的数据提供用户级别的数据隔离、访问控制和权限管理机制。

用户上传的数据保存三份副本存储，为用户数据提供冗余备份措施。

4.7.2.3 数据配额

开放搜索服务(Open Search)提供针对存储容量大小、每秒访问量(QPS)的配额机制。

4.7.2.4 认证与授权

开放搜索服务（Open Search）与其他云产品一样，同样提供已认证的 API 和 SDK 的方式对服务进行调用操作，API 和 SDK 认证采用由阿里云颁发给用户的访问服务的秘钥（Access Key），在认证时使用 HMAC-SHA1 签名算法。

用户在不同请求间被要求使用不同的随机数值（建议使用 13 位毫秒时间戳+4 位随机数），以防止网络重放攻击。在请求调用 API 时，提供请求次数频率限制功能。

4.7.2.5 访问控制

开放搜索服务（Open Search）提供精细化的查询分析使用访问规则功能，用户在配置好查询分析后，可以自定义规则控制查询分析的适用范围。

4.7.3 媒体转码服务 MTS

媒体转码服务（Media Transcoding），是为多媒体数据提供的转码计算服务。它以经济、弹性和高可扩展的音视频转换方法，将多媒体数据转码成适合在 PC、TV 以及移动终端上播放的格式。

4.7.3.1 资源权限管理

媒体转码服务为用户提供工作流方式创建转码任务，用户转码文件需提前预处理上传到 OSS 的 bucket 里面，用户开通媒体转码服务后，在 云资源授权管理管理 中，通过 RAM（ Resource Access Management）管理授予 MTS 访问存储媒体文件的 OSS Bucket 及 消息通知功能 MNS 相关权限。

4.7.3.2 容错管理

媒体转码服务支持消息通知管理服务，用户可以及时了解转码任务执行状态，包括转码出现的报错信息和告警信息。

4.7.4 性能测试服务 PTS

性能测试服务（Performance Test Service，简称 PTS）是集测试机管理、测试脚本管理、测试场景管理、测试任务管理、测试结果管理为一体的性能云测试平台。PTS 基于阿里云计算平台研发，可提供超大规模并发压力，满足任意规模系统的性能测试需求。PTS 在工作时会通过施压机产生压测流量，用户如果对施压的流量、地域等有更多要求，PTS 施压机可动态扩展在全球范围进行部署。

4.7.4.1 权限控制

性能测试服务提提供已认证的 API 和 SDK 的方式对服务进行调用操作，API 和 SDK 认证方式采用由阿里云颁发给用户的访问服务的秘钥（Access Key），同时在认证时增加使用 HMAC-SHA1 签名算法。

性能测试服务在预处理前会根据用户自身云服务资源（主要为云服务器），添加到压测环境，才能进行性能测试任务的配置。

性能测试服务使用最小权限账号权限运行，防止越权操作。

4.7.4.2 安全隔离

阿里云安全团队对性能测试控制台进行定期的安全测试和规范要求，划分了水平权限和测试权限，用户仅能查看和访问自己的数据。

性能测试服务提供压测进程隔离措施，每个用户使用单独的压测进程进行测试。

利用 jvm 功能对开发语言的调用进行限制，禁止使用禁用或敏感的类、方法。

4.7.4.3 监控和审计

实施对性能测试集群进行实施监控，当用户在测试时，对用户测试任务进行监控告警，保障性能测试服务的可用性，监控告警措施包括旺旺、邮件和短信。

第5章 阿里云云盾

5.1 基础防护

云盾是阿里巴巴集团多年来安全技术研究积累的成果，结合阿里云云计算平台强大的数据分析能力，为客户提供如 DDoS 防护、主机入侵防护、Web 应用防火墙、安全漏洞检测、网页木马检测等一站式安全服务。

5.1.1 DDoS 基础防护

作为中国领先的云计算服务商，阿里云基于自主开发的大型分布式操作系统和十余年安全攻防的经验，为广大云平台用户推出基于云计算架构设计和开发的云盾 DDoS 攻击防御服务。云盾的 DDoS 攻击防御由云网络流量监控系统、DDoS 清洗系统和集中管控系统组成，分别负责 DDoS 攻击流量检测、DDoS 攻击过滤和集中策略管理功能。

阿里云为所有用户提供一定量免费的 DDoS 防护，免费防护阈值（即黑洞阈值）见产品规格，不同地域的黑洞阈值不同。

云盾 DDoS 攻击防御具有以下特点和优势：

全面覆盖常见 DDoS 攻击类型

云盾的 DDoS 清洗系统可帮助云用户抵御各类基于网络层、传输层及应用层的各种 DDoS 攻击(包括 CC、SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood、HTTP Get Flood 等所有 DDoS 攻击方式)，并能实时短信通知用户网站防御状态。

快速自动响应，5 秒内进入防护状态

云盾 DDoS 清洗系统采用全球领先的检测和防护技术，可以在 5 秒钟内完成攻击发现、流量牵引和流量清洗全部动作，大大减少了网络抖动现象。在防护触发条件上不仅仅依赖流量阈值，同时还对网络行为的统计判断，做到精准识别 DDoS 攻击，保障了在遇到 DDoS 攻击时客户业务的可用性。

高弹性、高冗余的 DDoS 防御能力

云盾 DDoS 清洗系统每个最小单元支持 10Gbps 的攻击流量过滤。得益于云计算架构的高弹性和大冗余特点，DDoS 攻击防御系统可在云环境中无缝扩容，实现 DDoS 攻击防御能力的高弹性。

双向防护，避免云资源被滥用

云盾 DDoS 攻击防御系统不仅仅能防护来自于云外的 DDoS 攻击，同时还能及时发现云内资源被滥用的非法行为。一旦发现云内有服务器被利用向外发起 DDoS 攻击，云网络流量监控系统会与主机安全防护系统联动，限制被滥用的云服务器的网络访问行为，并产生告警，实现对内部主机的有效管控。

5.1.2 安骑士（主机入侵防护）

阿里云云盾主机安全防护由 C/S 架构的主机防御系统和集中管控系统组成，其中云服务器上部署 Client 端负责异常检测和处置，由统一的 Server 端进行检测数据分析，集中管控系统负责整体策略管理和安全日志分析。主机安全防护服务提供：密码暴力破解防御、网站后门检测和处理、异地登录告警功能。

云盾安骑士服务属于可选服务，客户可自行决定是否使用。

云盾主机安全防护具有以下特点和优势：

海量的暴力破解防御能力

云盾主机安全防护基于阿里大数据处理能力，实时识别出暴力破解攻击行为，支持 SSH/RDP/MySQL/FTP/MS SQL 等常见应用的暴力破解防护。

精准的 Web 木马检测

- 利用动静结合的检测方式，对网页木马进行分析检测：
- 通过 HTML 和 javascript 引擎对可疑的代码进行解析，利用基于阿里云数百万量级的恶意文件特征库进行静态模式匹配识别。
- 同时通过模拟浏览器对被检测页面进行访问，动态地分析代码的恶意行为，从而发现未知木马，及时地主动隔离。

异常登录告警

据统计在服务器异地登录事件中，有超过半数事件是入侵或者攻击行为。异地登录告警功能基于用户的登录行为模型，准确识别出异地（精确到地市级）、异地登录行为，对疑似的非管理员登录系统行为通过手机短信进行告警。

5.1.3 绿网

绿网针对阿里云用户，提供信息内容安全管控及内容安全检测服务。当用户的网站内容涉及违规信息时，绿网会对用户进行消息提醒，并提供违规网页地址及快照查看功能。

绿网服务具有以下优势和特点：

检测种类丰富多样

提供多种违规内容的检测，如赌博、色情、枪支、毒品等违规内容的实时监控和检测。

消息订阅、灵活提醒

可选择分时段、分方式进行消息提醒，支持邮件和短信两种通知方式

操作简单、方便管理

提供了“疑似违规”及“违规记录”模块，方便用户快速查阅及操作进行处理。

5.2 高级防护

5.2.1 安全网络

安全网络是阿里云推出的一款集安全、加速和个性化负载均衡为一体的网络接入产品。用户通过接入安全网络，可以缓解业务被各种网络攻击造成的影响，提供就近访问的动态加速功能。

安全网络提供的所有节点均为 BGP 节点，可以通过节点的组合创建网络，通过 CNAME 或者 SDK 的方式快速接入需要保护的应用，从而使应用具备分布式抗攻击的能力。

弹性扩展接入节点：

用户可根据自身业务自定义应用，分组，节点个数，弹性扩展自由配置。

DDoS 防御：

安全网络为每个分布式节点提供基础攻击防护能力，并支持智能的攻击节点业务调度。同时支持高防 IP 付费防护方案。

集成网站防护：

安全网络集成网站防护功能，提供网站 WAF 和 CC 防护功能，每个分组最多支持 100 个域名防护。

全面详细防护报表：

安全网络提供实时精确的流量报表以及攻击详情，让你及时获得当前服务详情。

5.2.2 DDoS 高防 IP

云盾 DDoS 高防 IP 是针对互联网服务器（包括非阿里云主机）在遭受大流量的 DDoS 攻击后导致服务不可用的情况下，推出的付费增值服务，用户可以通过配置高防 IP，将攻击流量引流到高防 IP，确保源站的稳定可靠。

5.2.3 网络安全专家服务

网络安全专家服务是云盾 DDoS 高防 IP 服务的基础上，推出的安全代维托管服务。该服务由阿里云云盾的 DDoS 专家团队，为企业客户提供定制的 DDoS 防护策略优化、重大活动保障、人工值守等服务。

5.2.4 服务器安全托管

由阿里安全专家团队为您提供个性化云服务器安全托管服务，包含专家人工安全体检、清除木马、系统加固、人工安全技术支持、托管服务报告等服务。

5.2.5 渗透测试服务

云盾渗透测试服务是针对用户的网站或业务系统，通过模拟黑客攻击的方式，进行专业性的入侵尝试，评估出重大安全漏洞或隐患的增值服务。

5.2.6 态势感知

专为企业安全运维团队打造，结合云主机和全网的威胁情报，利用机器学习，进行安全大数据分析的威胁检测平台。可让客户全面、快速、准确地感知过去、现在、未来的安全威胁。

5.2.7 反欺诈服务

反欺诈服务是基于阿里大数据风控服务能力，通过领先的行为收集技术和机器学习模型，解决账号、活动、支付等关键业务环节存在的欺诈威胁，降低企业经济损失。

5.2.8 先知计划

先知计划是一个帮助企业建立私有应急响应中心的平台(帮助企业收集漏洞信息)。企业加入先知计划后，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，防止造成更大的安全损失。

5.2.9 加密服务

5.2.9.1 产品概述

加密服务（AliCloud Data Encryption Service）通过在阿里云上使用经国家密码管理局检测认证的硬件密码机，帮助客户满足数据安全方面的监管合规要求，保护云上业务数据的机密性。借助加密服务，用户可以进行安全的密钥管理，并使用多种加密算法来进行加密运算。

5.2.9.2 产品特点

安全的密钥存储

使用防篡改硬件密码机保护客户密钥。

安全的密钥管理

阿里云只能管理设备硬件，主要包括监控设备可用性指标、开通、停止服务等。密钥完全由客户管理，阿里云没有任何方法可以获取客户密钥。

合规

使用符合国家密码管理局（GM/T 0029-2014）和中国人民银行（PBOC1.0/2.0/3.0）要求的密码机设备，设计体系符合国家密码监管部门监管规范和使用要求。

方便的业务使用

加密服务部署在用户客户的 VPC 中，通过客户指定的私网 IP 地址进行管理和调用，可以很方便地与云服务器实例上的业务配合使用。

按需使用

以服务方式提供，客户可通过阿里云控制台按需开通或关闭服务。

第6章 阿里云安全生态

阿里云秉承开放资源，相互合作的态度，引入行业安全合作伙伴，共建云安全产业链生态，为客户提供业界领先的、和客户现有场内安全控制措施体验一致的安全解决方案。

阿里云安全市场已提供 VPN、下一代防火墙、IPS、UTM、堡垒机、日志审计、数据库审计等安全解决方案，供客户选择。

第7章 附录

7.1 术语和定义

7.1.1 地域

同一城市的多个数据中心构成了一个产品地域。

地域内的云服务内网间是可以互通的，不同地域之间的云服务内网不互通。

7.1.2 可用区

可用区（Zone）是指在同一地域内，电力和网络互相独立的物理区域。

同一可用区内的 ECS 实例网络延时更小。

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。如果您的应用需要较高的容灾能力，建议您将 ECS 实例部署在同一地域的不同可用区内；如果您的应用在实例之间需要较低的网络时延，则建议您将 ECS 实例创建在相同的可用区内。

7.1.3 CSP

Cloud Service Provider，云服务提供商

7.1.4 ECS

云服务器（Elastic Compute Service，简称 ECS）是一种处理能力可弹性伸缩的计算服务，其管理方式比物理服务器更简单高效。

云服务器帮助您快速构建更稳定、安全的应用，降低开发运维的难度和整体 IT 成本，使您能够更专注于核心业务创新。

7.1.5 SLB

负载均衡（Server Load Balancer，简称 SLB）是对多台云服务器进行流量分发的负载均衡服务。

SLB 可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

7.1.6 RDS

关系型数据库服务（Relational Database Service，简称 RDS）是一种稳定可靠、可弹性伸缩的在线数据库服务。RDS 采用即开即用方式，兼容 MySQL、SQL Server 两种关系型数据库，并提供数据库在线扩容、备份回滚、性能监测及分析功能。RDS 与云服务器搭配使用 I/O 性能倍增，内网互通避免网络瓶颈。

7.1.7 OSS

对象存储服务（Object Storage Service，简称 OSS）是支持任意数据类型的存储服务，支持任意时间、地点的数据上传和下载，OSS 中每个存储对象（object）由名称、内容、描述三部分组成。

7.1.8 ODPS

Open Data Processing Service，是基于阿里云完全自主知识产权的云计算平台构建的数据存储与分析的平台。ODPS 提供大规模数据存储与数据分析，用户可以使用 ODPS 平台上提供的数据模型工具与服务，同时也支持用户自己发布数据分析工具。

7.1.9 CC

CC 攻击（Challenge Collapsar）是 DDoS（分布式拒绝服务）的一种，也是一种常见的网站攻击方法，攻击者通过代理服务器或者肉鸡攻击网站动态页面，造成网站服务器资源耗尽。

7.1.10 ISO 27001

ISO 27001 是信息安全管理体系（ISMS）国际标准，为各类组织建立并运行信息安全管理体系提供了最佳实践指导。

按照标准要求，应：

- 基于业务风险的方法，建立、实施、运行、监控、评审、维护和改进信息安全；
- 为了确保信息的机密性、完整性和可用性，设立了相应的组织架构，建立了体系化的安全管理制度，并提供资源保障；
- 遵循 PDCA 方法，持续改进信息安全管理。

7.1.11 云安全 STAR 认证（CSA STAR）

云安全 STAR 认证(CSA Security, Trust & Assurance Registry ,简称 CSA STAR）由云安全联盟（Cloud Security Alliance，简称 CSA）和英国标准协会（简称 BSI）联合推出。该认证以 ISO/IEC 27001 认证为基础，结合云端安全控制矩阵（Cloud Controls Matrix，简称 CCM）的要求，运用成熟度模型和评估方法，为提供和使用云计算的任何组织，从沟通和利益相关者的参与；策略、计划、流程和系统性方法；技术和能力；所有权、领导力和管理；监督和测量等 5 个维度 ,综合评估组织云端安全管理和技术能力 ,最终给出独立第三方外审结论。

7.1.12 信息安全等级保护

信息安全等级保护是我国信息安全保障的一项基本制度，是国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

等级保护工作包含定级、备案、测评、整改、监督检查共五个工作环节。信息系统安全责任主体根据系统重要性负责对系统开展定级，并向地市所在的公共安全网络安全监管部门进行备案，委托具备资质的等级保护测评机构开展测评，依据测评结果开展安全建设整改。公安机关对单位的等级保护工作开展进行监督检查。

7.1.13 可信云

可信云认证由工信部数据中心联盟组织颁发。证明云服务协议已达到《云计算服务协议参考框架》和《可信云服务认证评估方法》的标准要求；满足用户数据持久保存、数据隐私、控制数据迁移、数据审查、数据销毁的数据安全要求；满足用户业务功能完备、业务可用性合理、故障恢复能力可靠、基本业务资源调配性能、网络接入性能达标、服务计量可信的业务质量要求；满足用户服务变更、终止条款、服务赔偿条款、用户约束条款、服务商免责条款的权益保障要求。

7.1.14 CNAS 认可的云测评

CNAS 认可的云测评是国内唯一一家基于云计算国家标准开展的标准符合性测试，目前覆盖了云计算 IAAS 领域的虚拟机管理平台、对象存储两大方面。CNAS 认可的云测评由工信部电子标准院基于国家标准 GB / T 31915-2015《信息技术 弹性计算应用接口》和 GB / T 31916.2-2015《信息技术 云数据存储和

管理 第 2 部分 基于对象的云存储应用接口》等开展，在打造中国云计算标准生态链，服务政府云采购方面发挥了积极的推动作用。

7.2 版本历史

2014 年 1 月：发布 1.2 版本。

2015 年 12 月：发布 2.0 版本。

2016 年 8 月：2.1 版本，阿里云品牌形象全新升级，更换阿里云 Logo