阿里云安全白皮书

2017 年9 月

版本3.0

阿里云

目录

1 白皮书介绍

数据安全和用户隐私是阿里云的最重要原则。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。

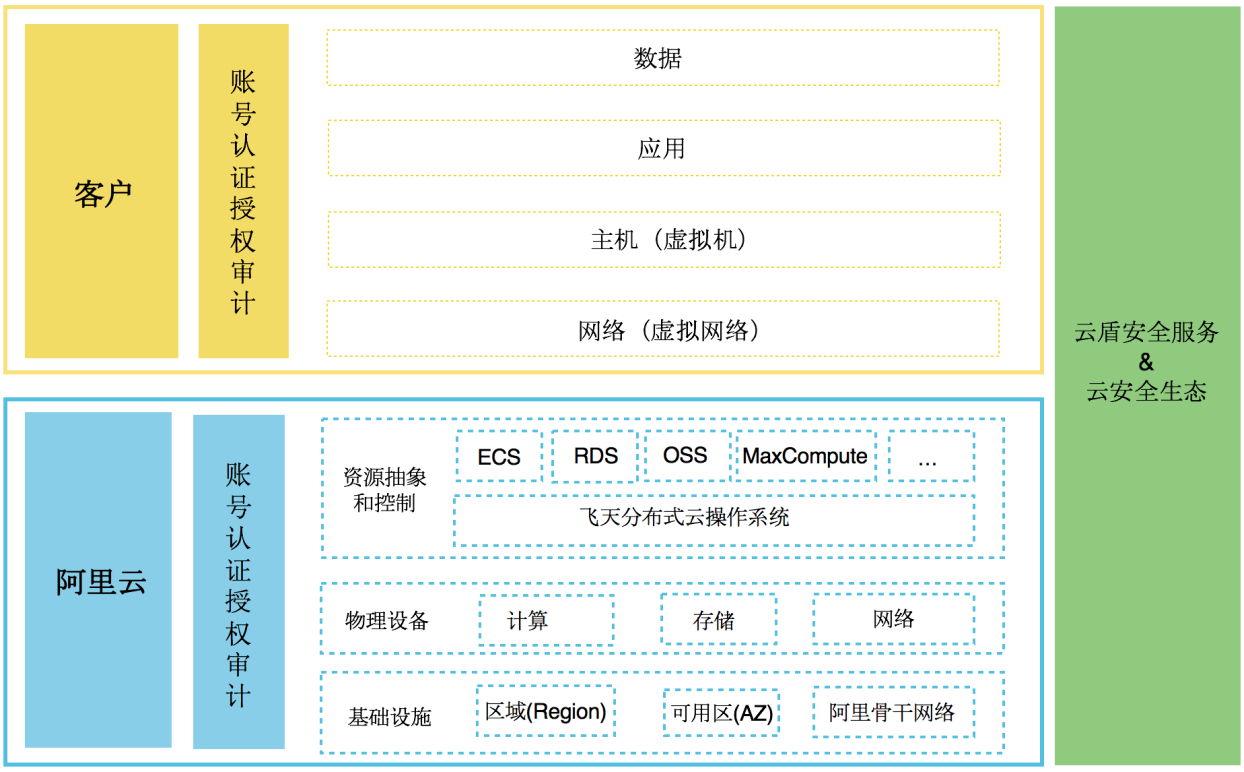
本白皮书介绍了阿里云云安全体系，内容包括：

- 安全责任共担
- 安全合规和隐私
- 阿里云基础设施
- 阿里云安全架构
- 阿里云产品提供的安全功能
- 阿里云云盾提供的安全服务
- 阿里云安全生态

同时，本白皮书提供了安全使用阿里云产品和云盾安全产品的最佳实践来帮助客户更好地使用阿里云平台以及理解整体安全控制环境。

2 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。

安全责任共担模式之下，阿里云提供并保障基础设施的安全，能够让用户降低 IaaS 层的安全性的顾虑，安心使用阿里云 IaaS 服务，更专注于核心业务发展 。

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；
- 云账户支持主子账号、多因素认证、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户，使用阿里云资源访问控制服务（Resource Access Management，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户启用多因素（MFA）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（MaxCompute），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户及授权，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。

3 安全合规和隐私

阿里云的安全流程机制已经得到国内外相关权威机构的认可，我们将基于互联网安全威胁的长期对抗经验融入到云平台的安全防护中，将众多的合规标准融入云平台合规内控管理和产品设计中，同时广泛参与各类云平台相关的标准制定并贡献最佳实践，并通过独立的第三方验证阿里云如何符合标准。至目前为止，阿里云一共拿到了海内外十余家机构的认证，是亚洲资质最全的云服务商。下表是阿里云具有的资质列表。

资 质	简 介
ISO 27001	信息安全管理体系国际认证，从数据安全、网络安全、通信安全、操作安全等各个方面证明阿里云平台履行的安全职责
CSA STAR	云安全管理体系国际认证，阿里云获得全球首个金牌
ISO 20000	IT 服务管理体系认证，意味着阿里云建立了标准的服务流程，并严格执行，云平台服务规范化，提高效率并降低 IT 整体风险
ISO 22301	业务连续性管理体系认证，进行业务连续性计划、灾备建设和定期演练，提升云平台稳定性
等级保护测评（4 级）	阿里云金融云成为全国首个通过云计算等级保护四级测评的云平台，意味着阿里云金融云正稳步成为国家关键信息基础设施
中央网信办党政部门云服务网络安全审查	阿里云是全国首批通过网信办云安全审查的社区云的服务商中，唯一增强级别审查（500 多项检查点）的
工信部云服务能力标准测试	工信部云服务能力标准测评是基于国家标准的，唯一公共云和专有云的服务能力认证
CNAS 云计算国家标准测试	云产品国家实验室认证是基于国家标准的唯一产品级分级认证
PCI DSS (支付卡行业数据安全标准)	PCI DSS 主要关注支付卡信息在组织范围内全生命周期的管理和控制，包括产生／进入、传输、存储、处理和销毁等
MTCS T3	新加坡云服务商安全最高等级认证，意味着阿里云可以参与新加坡政府项目
服务组织控制（SOC)审计	阿里云通过了 SOC1、2 的 TYPEI、TYPEII、SOC3 审计
TRUSTe	阿里云国际站通过美国企业隐私标准认证，标志着阿里云采集、使用、管理和销毁个人信息的合规性
HIPAA	阿里云支持 HIPAA 的业务伙伴协议以满足客户的需求，遵守美国健康保险可携性和责任法案，以保护健康信息的隐私和安全
MPAA	阿里云遵守美国电影协会(MPAA)的最佳实践指引
PDPA	阿里云遵守新加坡个人信息保护要求

Trusted Cloud 会员	阿里云成为德国联邦经济和能源部推动的 Trusted Cloud 会员
SCOPE 云守则创始会员	阿里云作为创始会员积极参与欧盟机构 SCOPE，为 GDPR 实施准备的云行为准则标准
发起“数据保护倡议”	中国云计算服务商首个“数据保护倡议”，明确数据所有权，以及阿里云的责任和义务
发布《阿里云数据安全白皮书》	通过完善的数据安全管理和先进的技术支撑实现对用户数据安全的承诺

3.1 合规

阿里云依据标准和行业最佳实践不断完善自身的管理与机制，并通过了一系列的标准认证、三方审计以及自评估，务求更好的向客户展示阿里云的合规实践。

同时，中小型企业客户在面对合规需求时，存在自身经验与资源的局限性。阿里云也希望借由审计报告、合规解决方案、以及合规架构咨询等诸多方式，来帮助中小企业开展合规工作，将阿里云合规实践的价值最大化。

阿里云面对不同角度、不同行业、不同地区的合规需求，整体合规工作可以划分为如下几类：

1) **管理体系合规**：旨在体现阿里云目前成熟的管理机制和遵从的行业最佳实践。

- ISO 27001：信息安全管理体系
- ISO 20000：IT 服务管理体系
- ISO 22301：业务可持续性管理体系
- CSA STAR：云服务安全的成熟度模型
- 等级保护测评（4 级）
- 中国 CNAS 云计算国家标准测试

2) **体系化合规报告**：旨在向客户展示云平台管控的完整性和有效性。 例如：体系控制是否持续有效，职责分离是否准确，运维操作审计等。

- PCI-DSS：支付卡行业数据安全标准
- MPAA：美国电影协会（MPAA）的最佳实践指引
- TRUSTe：TRUSTe 企业隐私认证
- SOC 1/2 TYPE II：服务组织控制 (SOC) 报告是阿里云请三方机构出具的一系列独立第三方检查报告，旨在阐述阿里云关键合规性控制和目标的持续有效性。这些报告的目的是帮助客户和客户的审计机构了解支持运营和合规性的控制措施。阿里云 SOC 报告分为三种类型：
    - SOC 1 TYPE II： 针对财报的内控报告
    - SOC 2 TYPE II：安全性、可用性与机密性报告

- SOC 3：安全性、可用性与机密性报告

3) **法务合规**：在不同地区开展云服务时，符合当地的法律法规是首要条件。但由于法务合规的独特性，无法通过证书或审计报告的形式来体现

- HIPAA – 阿里云支持 HIPAA 的业务伙伴协议（BAA）以满足客户的需求，遵守美国健康保险可携性和责任法案（HIPAA），以保护健康信息的隐私和安全。
- GDPR – 阿里云在努力满足欧盟数据保护法规的同时也致力于为阿里云的客户和伙伴提供支持。

4) **其他**：一些合规工作无法通过上述的三种形式展现，阿里云一直致力协助各个地区的监管机构建立和完善标准，分享阿里云的最佳实践。

- MTCS - 多层云安全 MTCS 是由新加坡政府的新加坡资讯通讯发展管理局发起，新加坡标准、生产力与创新局推出的云安全标准。其安全认证分为三个层次，其中阿里云得到第三级，为最高、最安全。

3.2 隐私保护

阿里云的个人信息处理原则：客户对所有提供给阿里云的个人信息拥有所有权和控制权。

每个客户在使用阿里云服务的时候，出于信任将最宝贵的个人信息托付给我们。阿里云也致力于保护每位客户的个人信息，并严格保障在客户期望范围内使用。阿里云在隐私政策方面对于公众完全透明，可以参考官网的隐私政策。同时，阿里云采用各种技术手段确保客户的个人信息仅存在于阿里云业务范围。

阿里云的信任中心提供了全面的合规信息，希望可以帮助客户更好地理解阿里云在合规方面的各种实践，并希望客户不仅可以一如既往地信任阿里云，也可以从阿里云的实践中获取合规方面的经验，与我们一起提高全球范围内的合规能力。同时，阿里云与 TrustArc 合作，为云上客户提供隐私合规服务。

在此，我们再一次声明，阿里云致力于保护世界各地客户的个人信息，并遵守经营业务市场所属国家或地区的适用法律。

阿里云的隐私政策可以在官方网站上找到， 任何隐私相关问题都可以通过我们的信任中心网页提交。

隐私政策官方网站： https://www.alibabacloud.com/help/faq-detail/42425.html。

3.3 透明度

与全球各国的其他大型互联网公司相似，阿里云有时会面临依法配合国家行政、司法机关执行公务的相关要求。当政府机构依法要求阿里云进行必要的数据披露时，我们会根据法律规定的义务进行规范化的配合与支持。此类场景可能包括配合公检法打击犯罪、侦破案件时进行取证，完成监管部门依照法律要求进行的安全检查，以及配合工商、知识产权部门查处各类打假、侵权案等。

对应每一种数据披露场景，阿里云都有严格的内部审核程序。在数据披露过程中，我们会要求数据需求方提供完备的证件与法律函件，对相关人员信息进行验证并记录。阿里云遵守依法提供、流程规范、风险可控、最小够用等原则，确保数据的调取和送达安全可控、有据可依。

4 阿里云基础设施

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； 高可用、安全、可信的云计算基础设施。

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、异地多活，两地三中心。

国家	地域	可用区数量
中国	华北 1	2
	华北 2	4
	华北 3	1
	华东 1	5
	华东 2	4
	华南 1	2
	香港区域	2
海外	亚太东南 1	2
	亚太东南 2	1
	亚太东北 1	1
	美国东部 1	1
	美国西部 1	2
	欧洲中部 1	1
	中东东部 1	1

5 阿里云安全架构

如上图所示，阿里云提供了共 11 个不同层面的安全架构保障，其中包括物理安全，硬件安全，虚拟化安全，云产品安全等 4 个云平台层面的安全架构保障；以及账户安全，主机安全，应用安全，网络安全，数据安全，安全运营，业务安全等 7 个云用户层面的安全架构保障。

本章在介绍整体安全架构时，会简要介绍各个架构层面中的关键特性，同时会覆盖多种阿里云产品，包括云盾安全产品。各种产品的详情请参见白皮书相关的章节内容。

5.1 云平台安全架构

阿里云云平台的安全架构如上图所示，主要包括了物理安全，硬件安全，虚拟化安全以及云产品安全四个重要组成部分。

5.1.1 物理安全

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，包含本章以下物理与环境安全控制要求。

5.1.1.1 机房容灾

- **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。

- **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。

- **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。

5.1.1.2 人员管理

- **访问管理**

  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。

- **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：

  - 每个员工持有唯一的账号；
  - 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。

- **授权管理**

  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。

- **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。

5.1.1.3 运维审计

- **监控**

  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。

- **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。所有操作过程会被完整记录下来并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。

  阿里云内部使用 B/S 结构的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。

5.1.1.4 数据擦除

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。特别是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。阿里云的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。

5.1.2 硬件安全

5.1.2.1 硬件固件安全

硬件固件是云计算安全依赖的安全基础，为了保障硬件固件安全，阿里云对底层硬件固件进行加固，其中包括硬件固件基线扫描，高性能 GPU 实例保护，BIOS 固件验签，BMC 固件保护。

- 硬件固件基线扫描： 定期对硬件和固件基本信息及相应版本进行扫描，检测可能的异常硬件固件信息。

- 高性能 GPU 实例保护：通过对开放给用户虚拟机的 GPU 关键寄存器保护，确保用户虚拟机除了进行高性能计算之外，无法篡改 GPU 的固件程序等重要资源。

- BIOS 固件验签：确保只有阿里云签名过的 BIOS 固件才可以被刷写在相关服务器上，从而避免了恶意的 BIOS 固件刷写。

- BMC 固件保护：确保在主机操作系统中，无法对 BMC 固件进行非授权的恶意刷写。

5.1.2.2 加密计算

阿里云平台的芯片级加密计算目前使用了处理器提供的硬件可信执行环境。用户可以通过使用软件建立一个可信执行环境，保护敏感数据和加解密密钥。通过支持硬件可信执行环境的售卖主机，用户可以通过自己编写支持可信执行环境技术的代码来保护用户自己的数据，从而确保只有用户编写的授权运行在可信执行环境内的代码可以访问和操作用户关键数据。通过阿里云加密计算技术，阿里云为用户数据安全上云提供了更强大的数据安全方案。

5.1.2.3 可信计算

阿里云在关键服务器上采用了基于 TPM 2.0 的可信计算技术，通过 TPM 2.0 的主动度量技术对基础软件的启动过程进行度量，基础软件包括了 BIOS，操作系统内核等。同时，阿里云的密钥管理服务也使用了 TPM 2.0 进行根密钥的保护。

5.1.3 虚拟化安全

虚拟化技术是云计算的主要技术支撑，通过计算虚拟化，存储虚拟化，网络虚拟化来保障云计算环境下的多租户隔离。 阿里云虚拟化安全技术主要包括租户隔离，补丁热修复，逃逸检测三大基础安全部分来保障阿里云虚拟化层的安全。

5.1.3.1 租户隔离

虚拟化层在租户隔离中起到至关重要的作用。基于硬件虚拟化技术的虚拟机管理将多个计算节点的虚拟机在系统层面进行隔离，租户不能访问相互之间未授权的系统资源，从而保障计算节点的基本计算隔离。同时虚拟化管理层还提供了存储隔离和网络隔离。具体租户隔离详情请见“云产品安全-弹性计算-ECS-租户隔离”一章。

- **计算隔离**

  阿里云提供各种基于云的计算服务，包括各种计算实例和服务，可自动伸缩以满足应用程序或企业的需求。这些计算实例和服务在多个级别提供计算隔离以保护数据，同时保障了用户需求

的配置灵活性。计算隔离中关键的隔离边界是管理系统与客户虚拟机以及客户虚拟机之间的隔离，这种隔离由 Hypervisor 直接提供。阿里云平台使用的虚拟化环境，将用户实例作为独立虚拟机运行，并且通过使用物理处理器权限级别强制执行此隔离，确保用户虚拟机无法通过未授权的方式访问物理主机和其他用户虚拟机的系统资源。

- **存储隔离**

  作为云计算虚拟化基础设计的一部分，阿里云将基于虚拟机的计算与存储分离。这种分离使得计算和存储可以独立扩展，从而更容易提供多租户服务。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，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。云用户实例服务器释放后，原有的磁盘空间将会被可靠的清零以保障用户数据安全。

- **网络隔离**

  为了支持 ECS 虚拟机实例使用网络连接，阿里云将虚拟机连接到阿里云虚拟网络。阿里云虚拟网络是建立在物理网络结构之上的逻辑结构。每个逻辑虚拟网络与所有其他虚拟网络隔离。这种隔离有助于确保部署中的网络流量数据不能被其它 ECS 虚拟机访问。

5.1.3.2 逃逸检测

虚拟机逃逸攻击主要包括两个基本步骤：首先将攻击方控制的虚拟机置于与其中一个攻击目标虚拟机相同的物理主机上，然后破坏隔离边界，以窃取攻击目标的敏感信息或实施影响攻击目标功能的破坏行为。

阿里云虚拟化管理程序通过使用高级虚拟机布局算法以防止恶意用户的虚拟机运行在特定物理机上。阿里云在虚拟化管理软件层面还提供了虚拟化管理程序加固、虚拟化管理程序下攻击检测、虚拟化管理程序热修复三大核心技术来防范恶意虚拟机的攻击。

5.1.3.3 补丁热修复

阿里云虚拟化平台支持补丁热修复技术，通过补丁热修复技术使得系统缺陷或者漏洞的修复过程不需要用户重启系统，从而不影响用户业务。

5.1.3.4 变更管理

虚拟化系统是云计算的重要基础，针对虚拟化系统的变更会直接影响业务运行。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。阿里云会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。

5.1.4 云产品安全

阿里云为用户提供了多种不同的云产品，其中包括云服务器 ECS，云数据库 RDS，对象存储 OSS，大数据计算服务 MaxCompute 等等。更多产品的安全特性和能力请参考“云产品安全”一章。

5.1.4.1 云产品安全生命周期（SPLC）

SPLC（Secure Product Lifecycle）是阿里云为云上产品量身定制的云产品安全生命周期，目标是将安全融入到整个产品开发生命周期中。SPLC 在产品架构审核、开发、测试审核、应急响应的各个环节层层把关，每个节点都有完整的安全审核机制确保产品的安全性能够满足严苛的云上要求，从而有效地提高云产品的安全能力并降低安全风险。

如上图所示，整个云产品安全生命周期可以分为六大阶段，分别是：产品立项、安全架构审核、安全开发、安全测试审核、应用发布、应急响应。

在产品立项阶段，安全架构师和产品方一同根据业务内容、业务流程、技术框架建立 FRD（功能需求文档）、绘制详细架构图，并在阿里云产品上云的所有安全基线要求中确认属于产品范围的《安全基线要求》。同时，本阶段会安排针对性的安全培训课程与考试给产品方人员，从而避免在后续产品开发中出现明显的安全风险。

在安全架构审核阶段，安全架构师在上一阶段产出的 FRD 和架构图的基础上对产品进行针对性的安全架构评估并做出产品的威胁建模。在威胁建模的过程中，安全架构师会对产品中的每一个需

要保护的资产、资产的安全需求、可能的被攻击场景做出详细的模型，并提出相对应的安全解决方案。安全架构师会综合《安全基线要求》和威胁建模中的安全解决方案，一并与产品方确认对于该产品的所有《安全要求》。

在安全开发阶段，产品方会根据《安全要求》在产品开发中遵守安全编码规范，并实现产品的相关安全功能和要求。为了保证云产品快速持续的开发，发布与部署效率，产品方会在本阶段进行自评确认《安全要求》都已经实现，并提供相对应的测试信息（如代码实现地址，自测结果报告等）给负责测试的安全工程师，为下阶段的安全测试审核做好准备。

在安全测试审核阶段，安全工程师会根据产品的《安全要求》对其进行架构、设计，服务器环境等全方位的安全复核，并对产品的代码进行代码审核和渗透测试。在此阶段发现的安全问题会要求产品方进行安全修复和加固。

在应用发布阶段，只有经过安全复核，并且得到安全审批许可后，产品才能通过标准发布系统部署到生产环境，以防止产品携带安全漏洞在生产环境运行。

在应急响应阶段，安全应急团队会不断监控云平台可能的安全问题，并通过外部渠道（如 ASRC 等）或者内部渠道（如内部扫描器、安全自测等）得知安全漏洞。在发现漏洞后应急团队会对安全漏洞进行快速评级，确定安全漏洞的紧急度和修复排期，从而合理分配资源，做到快速并合理的修复安全漏洞，保障阿里云用户、自身的安全。

5.2 云用户侧安全架构

阿里云在用户侧安全架构如上图所示，提供了 7 个层面的安全保障，其中包括了账户安全、主机安全、应用安全、网络安全、数据安全、安全运营及业务安全。

5.2.1 账户安全

阿里云提供多种安全机制来帮助客户保护账户安全以防止未授权的用户操作。这些安全机制包括云账户登录及 MFA 管理、创建子用户、集中管理子用户权限、数据传输加密、子用户操作审计。客户可以使用这些机制来保护其云账户安全。详情请见“云产品安全 – 管理与监控 – 身份与访问管理”一章。

5.2.1.1 账户认证

阿里云账户认证的基础是用身份凭证来证明用户的真实身份。身份凭证通常是指登录密码或访问密钥（Access Key，AK）。身份凭证是秘密信息，用户必须保护好身份凭证的安全。

通过阿里云的 RAM 资源访问控制服务，每个云账户可以独立开通一个 RAM 服务，并通过 RAM 创建子用户，为每个子用户分配不同的密码或访问密钥，消除了云账户共享带来的安全风险；同时可为不同的子用户分配不同的工作权限，大大降低了因账户权限过大带来的风险。用户可以通过 RAM 控制台为子用户创建密码策略，以保证各个子用户使用定期轮转的强密码从而提高整体账户的安全性。RAM 同时支持颁发 STS (Security Token Service) 安全令牌给在短时间内需要访问某些资源的临时用户，并根据需要来定义令牌的权限和自动过期时间（默认为 1 小时过期），从而避免颁发和防止泄露长期 AK。

- 登录密码(Password)
  云账户的密码规范、登录安全风控策略由阿里云统一管理。云账户下子用户(RAM 用户)的密码策略则可以由客户自己设定，比如密码字符组合规范、重试登录次数、密码轮转周期等策略。

- API 访问密钥(Access Key)
  Access Key 是阿里云服务 API 访问密钥，用户可以使用 Access Key 以程序方式操作阿里云 API。用户可以登录阿里云用户中心来管理 Access Key，包括创建、冻结、激活和删除操作。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。Access Key 是可以长期使用的 API 访问密钥，建议用户在使用时要考虑对 Access Key 的周期性轮转。

  阿里云强烈建议客户使用 RAM 用户的 Access Key，而不要使用云账户的 Access Key。云账户可以理解为根账号，它具有所有云产品的完全控制权限。根账号 Access Key 一旦泄露将可能造成极大风险，所以建议客户使用 RAM 用户进行资源操作并遵循最小授权原则。

- 密钥对管理(Key Pair)
  阿里云 RAM 服务在某些区域提供了密钥对管理功能。RAM 用户可以创建自己的 RSA 密钥对，

将公有密钥（Public Key) 上传到 RAM，私有密钥 (Private Key) 由用户自己保管。使用 Key Pair 访问 STS 服务可以获取当前用户的一个临时访问密钥 (Session Access Key)，用户可以使用临时访问密钥来访问某些区域的阿里云服务 API。

5.2.1.2 多因素认证(MFA, Multi-Factor Authentication)

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用户的账户提供更高的安全保护。阿里云可以支持基于软件的虚拟 MFA 设备。虚拟 MFA 设备是产生一个 6 位数字认证码的应用程序，它遵循基于时间的一次性密码 (TOTP) 标准(RFC 6238)。此应用程序可在移动硬件设备（包括智能手机）上运行。

5.2.1.3 访问控制

RAM (Resource Access Management) 是阿里云为客户提供的集中式用户管理与资源访问控制服务。使用 RAM，客户可以为其企业员工、系统或应用程序创建独立的用户账号，并可以控制这些用户对其云资源的操作权限。每个 RAM 用户可以拥有独立的登录密码或 Access Key，可以登录阿里云控制台，或以程序方式操作云服务 API。RAM 用户创建时默认没有任何资源操作权限，只有在获得显式授权的条件下 RAM 用户才能代表云账户进行资源操作。

使用 RAM，客户可以避免与其他用户共享云账户密钥，并根据最小权限原则为不同用户分配最小的工作权限，从而降低客户的企业信息安全管理风险。RAM 使得一个阿里云账户（主账号）可拥有多个子用户，并可以使用多因素认证、强密码策略、控制台用户与 API 用户分离、支持自定义细粒度授权策略，支持用户分组授权、临时授权令牌、账户临时禁用等功能。RAM 授权可以细化到对某个 API-Action 和 Resource-ID 的细粒度授权，还可以支持多种限制条件（源 IP 地址、安全访问通道 SSL/TLS、访问时间段、多因素认证等等）。

5.2.1.4 日志审计

用户认证凭证和权限控制是为了避免产生安全问题，而安全日志则可以帮助更好地理解和诊断安全状况。阿里云 ActionTrail 为客户提供统一的云资源操作安全日志管理，记录账户下的用户登录及资源访问操作，包括操作人、操作时间、源 IP 地址、资源对象、操作名称及操作状态。利用 ActionTrail 保存的所有操作记录，客户可以实现安全分析、入侵检测、资源变更追踪以及合规性审计。为了满足用户的合规性审计需要，用户往往需要获取主账户和其子用户的详细操作记录。ActionTrail 所记录的操作事件可以满足此类合规性审计需求。

5.2.2 主机安全

5.2.2.1 入侵检测

阿里云用户可以通过在主机上安装轻量级软件安骑士，实现与云端安全中心的联动，获取入侵检测的安全能力。主机的入侵检测包括异地登录提醒，识别暴力破解攻击，网站后门查杀，主机异常检测等功能。

5.2.2.2 漏洞管理

阿里云用户可以通过在主机上安装轻量级软件安骑士，实现与云端安全中心的联动，获取漏洞管理的安全能力。主机的漏洞管理综合了多套扫描引擎（网络端、本地端、PoC 验证），可以全面批量检测出系统存在的所有漏洞，并提供一键修复、生成修复命令、一键批量验证功能，实现漏洞管理的闭环。

5.2.2.3 镜像加固

镜像是云服务器 ECS 虚拟机实例运行环境的模板，一般包括操作系统和预装的软件。阿里云 ECS 租户可以使用镜像创建新的 ECS 实例和更换 ECS 实例的系统盘。阿里云官方公共镜像（支持 Linux 和 Windows 的多个发行版本）安全主要包括镜像基础安全配置，镜像漏洞修复，默认镜像主机安全软件三个部分，阿里云保持对阿里云公共镜像操作系统漏洞以及三方软件漏洞的实时监测，以确保所有阿里云公共镜像高危漏洞在第一时间得到修复，阿里云公共镜像默认进行主机最佳安全实践配置，并且所有阿里云公共基础镜像会默认添加阿里云主机安全软件以保障租户在实例启动时第一时间得到安全保障。

5.2.2.4 自动宕机迁移

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，恢复实例正常运行，保障应用的高可用性。

5.2.3 应用安全

5.2.3.1 Web 应用防护

Web 应用防火墙(Web Application Firewall, WAF),基于云安全大数据能力实现，通过防御 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，过滤海量恶意访问，避免网站资产数据泄露，保障网站的安全与可用性。

5.2.3.2 代码安全

在云产品安全生命周期（SPLC）中，阿里云的安全专家在各个开发节点中都会严格审核和评估代码的安全性，从而保障阿里云提供给用户的产品的代码安全质量。阿里云也会持续不断的对云市

场中的软件进行代码安全检测，从而有效降低安全风险。同时，阿里云强烈建议企业用户对其上线的应用进行黑白盒代码安全检测，务求上线后的应用不会存在安全漏洞，增加用户本身的业务的安全强壮性。

5.2.4 网络安全

5.2.4.1 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。阿里云也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。

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多因素认证。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。

5.2.4.2 虚拟专用网络（VPN）

VPN 网关（Virtual Pirvate Network Gateway）是一款基于 Internet，通过加密通道将企业数据中心，企业办公网络，阿里云专有网络（VPC）安全可靠连接起来的服务。阿里云 VPN 网关在中华人民共和国国家相关政策法规内提供服务，不提供访问 Internet 功能。

5.2.4.3 专有网络 （VPC）

专有网络（Virtual Private Cloud）可以帮助用户基于阿里云构建出一个隔离的网络环境，并可以自定义 IP 地址范围、网段、路由表和网关等；此外，也可以通过专线/VPN 等连接方式实现云上 VPC 与传统 IDC 的互联，构建混合云业务。

5.2.4.4 分布式防火墙

安全组是阿里云提供的分布式虚拟化防火墙，具备状态检测和包过滤功能。

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。

5.2.4.5 DDoS 防御

阿里云使用自主研发的 DDoS 防护系统保护所有数据中心，提供 DDoS 攻击自动检测、调度和清洗功能，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，保证云平台网络的稳定性。同时，阿里云的 DDoS 防护系统在防护触发条件上不仅仅依赖流量阈值， 还基于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。

5.2.5 数据安全

5.2.5.1 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。

5.2.5.2 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。

5.2.5.3 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。

5.2.5.4 全栈加密

阿里云对于数据安全提供了全栈的加密保护能力，其中包括从应用程序敏感数据加密，RDS 数据库透明加密，块存储数据加密，对象存储系统加密，硬件加密模块和网络数据传输加密。

对于应用程序敏感数据加密，阿里云支持使用处理器提供的硬件可信执行环境下的加密解决方案。

- **数据传输加密**

  阿里云为用户访问提供了 HTTPS 协议来保证数据传输的安全。如果用户通过阿里云控制台操作，阿里云控制台会使用 HTTPS 进行数据传输。所有的阿里云服务都为客户提供了支持 HTTPS 的 API 访问点，允许用户使用 Access Key 以程序方式来调用阿里云服务 API。阿里云的传输协议支持标准的 SSL/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。

- **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服务（KMS）提供的密钥管理及加密机制进行加密存储。同时，不同的云产品也支持数据加密以满足用户的要求（具体产品请参照产品对应章节）：

  - 在 RDS 数据库透明加密层，数据库数据可以被加密的形式存放到数据库系统中。
  - 块存储数据加密支持虚拟机内部使用的块存储设备的自动加密，确保块存储的数据在分布式系统中加密存放。
  - 对象存储(OSS)系统也直接支持加密能力，用户可以选择是否使用加密保存对象数据。
  - 在硬件层，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。

5.2.5.5 镜像管理

ECS 提供快照与自定义镜像功能，快照可以保留某个时间点上的系统数据状态，用于数据备份，便于用户可以快速灾难恢复。用户可以使用快照创建自定义镜像，将快照的操作系统、数据环境信息完整的包含在镜像中， 快照使用增量的方式，两个快照之间只有数据变化的部分才会被拷贝。

5.2.5.6 密钥管理

阿里云提供的密钥管理服务（Key Management Service，KMS）是一款安全易用的管理类服务。用户无需花费大量成本来保护密钥的保密性、完整性和可用性。借助 KMS 用户可以安全、便捷的使用密钥，并专注于开发中需要的加解密功能场景。

5.2.5.7 硬件加密模块（HSM）

HSM(硬件加密模块)会被用来提供硬件加密功能，将密钥保护在硬件加密模块内部。阿里云通过提供硬件加密模块的能力帮助用户提升数据安全保护等级。

5.2.5.8 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。

5.2.5.9 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。

5.2.6 安全运营

5.2.6.1 态势感知

态势感知利用大数据技术，从攻击者的角度，有效捕捉高级攻击者使用的 0day 漏洞攻击、新型病毒攻击事件、和正在发生的安全攻击行为有效的展示，帮助云上租户实现云上业务安全可视和可感知。态势感知区别于传统 IDC 和 SIEM（仅做了被识别的告警事件关联），是从海量的原始数据中分析信息并通过机器学习的模型完成对安全事件过程的完整还原 。同时，态势感知聚焦在“敌我态势”，对敌方的实体（黑客本人，黑客组织）进行长期的威胁情报监控和行动点技术手段观测，对我方薄弱环节进行实时感知，对安全决策具有重要参考意义。

5.2.6.2 操作审计

阿里云同时为客户提供操作审计(ActionTrail)服务。阿里云 ActionTrail 为客户提供统一的云资源操作安全日志管理，记录账户下的用户登录及资源访问操作，包括操作人、操作时间、源 IP 地址、资源对象、操作名称及操作状态。利用 ActionTrail 保存的所有操作记录，客户可以实现安全分析、入侵检测、资源变更追踪以及合规性审计。

5.2.6.3 应急响应

阿里云组建了专门的安全应急团队来应对云平台上可能的安全威胁，并对异常事件积极的进行响应和处理。

安全应急团队会不断监控云平台可能的安全问题，并会通过外部渠道（如 ASRC 等）或者内部渠道（如内部扫描器、安全工程师自测等）得知安全漏洞。一旦发现漏洞，应急团队会对安全漏洞进行快速评级并着手修复。同时，应急团队也会及时的发公告将安全问题第一时间通知用户。阿里云制定有严格的应急响应流程来确保每一次安全事件都进行严格而快速的处理。

为了确保安全应急响应流程技术有效，阿里云组建了专门的团队不定期的对阿里云进行攻击演练，以确保安全应急响应流程的有效性。阿里云还会定期邀请第三方团队对阿里云进行渗透测试，以验证阿里云安全防护体系的有效性和安全应急响应流程的流畅性。

5.2.6.4 安全众测

阿里云建有先知平台，提供私密的安全众测服务。先知可以帮助企业全面发现业务漏洞和风险信息。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。先知平台会为所有入驻企业的漏洞严格保密，从而避免漏洞被恶意宣传。

5.2.7 业务安全

业务安全服务是基于阿里大数据风控能力，通过海量风险数据和机器学习模型，解决账号注册、认证、交易、运营等关键业务环节存在的各种风险问题，保障企业业务健康发展。

5.2.7.1 防垃圾注册

阿里云提供垃圾注册防控服务，其中包括用户信息有效性验证，图形验证码防批量注册，实时风险处理服务等功能。通过对用户的信息、行为、软硬件环境信息、设备指纹等综合信息来判定用户注册账户的风险程度，并提供多样化的功能进行验证和处理。

5.2.7.2 防交易欺诈

阿里云提供防交易欺诈服务，对交易过程中出现的账户盗用，坏账资损，银行卡盗用，交易诈骗等欺诈行为进行有效防控。

5.2.7.3 活动防刷

在企业的运营活动中，如果有恶意用户通过虚假行为和作弊等手段批量的套取活动营销资金和物品等，就会造成正常用户无法享受权益和企业营销资金浪费，进而极大的影响运营活动的效果。阿里云提供活动防刷服务，使企业可以对这类作弊风险进行有效的防范。

5.2.7.4 实人认证

阿里云提供用户真实身份认证服务，为企业用户更高等级的业务发展提供实名制的基础。通过实名校验，生物识别，和风险防控的功能，当企业业务需要用户进一步认证身份时，可以采用如视频验证等功能，提升用户的认证等级。

6 云产品安全

6.1 弹性计算

阿里元提供了多种基于云的弹性计算服务，这些计算服务主要通过云服务器 ECS 来对外提供服务。

6.1.1 云服务器 ECS

阿里云云服务器 ECS 实例是一个虚拟的计算环境，包含了 CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件，是 ECS 提供给每个用户的操作实体。一个实例就等同于一台虚拟机，用户对所创建的实例拥有管理员权限，可以随时登录进行使用和管理。用户可以在实例上进行基本操作，如挂载磁盘、创建快照、创建镜像、部署环境等。

6.1.1.1 租户隔离

由于 ECS 的实例会分配给不同的用户，因此实例之间的隔离对各个用户是重要的安全保障。ECS 的租户实例隔离是基于硬件虚拟化技术的虚拟机管理，将多个虚拟机在系统层面进行隔离。实例不能访问相互之间未授权的系统资源，从而保障运算节点的基本计算资源的隔离。同时虚拟化管理层还提供了存储隔离和网络层隔离。

租户隔离中关键的隔离边界是虚拟机管理系统与客户虚拟机以及客户虚拟机之间的隔离。以下将从 CPU 隔离，内存隔离，存储隔离，和网络隔离 4 个层面介绍 ECS 实例间资源隔离的实现机制。

- **CPU 隔离**
  基于硬件虚拟化技术 Intel® VT-x，Hypervisor 运行在 VMX root 模式，而虚拟机运行在 VMX non-root 模式。通过使用物理处理器的不同权限级别，可以有效地防止虚拟机通过未授权的方式访问物理主机和其他的用户虚拟机的系统资源，同时也做到了虚拟机之间的有效隔离。Hypervisor 通过提供相互隔离的计算通道控制虚拟机与主机资源进行交互。这样可以防止用户获得对系统以及对其他租户的原始读/写/执行访问，并减轻共享系统资源所带来的风险，保障租户之间的计算隔离。

- **内存隔离**
  在虚拟化层，Hypervisor 负责隔离内存。ECS 实例运行时，使用硬件辅助的 EPT（Extended Page Tables，扩展页表）技术，可以确保虚拟机之间无法互访对方内存。实例释放后，它的所有内存会被 Hypervisor 清零，从而有效防止 ECS 实例关闭后释放的物理内存页内容被其他用户的实例访问到。

- **存储隔离**

  作为云计算虚拟化基础设计的一部分，阿里云将基于虚拟机的计算与存储分离。这种分离使得计算和存储可以独立扩展，从而更容易提供多租户服务。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，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。云用户实例服务器释放后，原有的磁盘空间将会被可靠的清零以保障用户数据安全。

  阿里云 ECS 虚拟机数据磁盘加密（以下简称 ECS 磁盘加密）是一种针对虚拟机内部使用的块存储设备的自动存储加密功能。ECS 磁盘加密为租户的数据磁盘提供卷加密，保障租户的数据安全。ECS 磁盘加密为租户提供了一种简单的安全的加密手段，能够对租户新创建的数据盘进行加密处理，满足租户的业务和认证需要。ECS 磁盘加密功能是一种透明加密，阿里云租户无需构建、维护和保护自己的密钥管理基础设施，无需更改任何已有的应用程序和运维流程，也无需做额外的加解密操作。

  ECS 磁盘加密是在 ECS 实例所在的网络控制节点上进行的，对从 ECS 实例传输到云盘的数据进行加密。ECS 实例对虚拟磁盘的读写最终都会被映射为对阿里云数据存储平台上的文件的读写，除用户自身，任何其他人无法读取其中的数据。阿里云数据存储平台会充分保障用户数据在后端存储的隔离性，和用户数据的可靠性以及安全性。

- **网络隔离**

  为了支持 ECS 虚拟机实例使用网络连接，阿里云要求将虚拟机连接到阿里云虚拟网络。阿里云虚拟网络是建立在物理网络结构之上的逻辑结构。每个逻辑虚拟网络与所有其他虚拟网络隔离。这种隔离有助于确保部署中的网络流量数据不能被其他 ECS 虚拟机访问。

  阿里云 ECS 虚拟机可以通过 Hypervisor 提供的虚拟网络进行相互之间的隔离以确保自身的流量不被随意转发,同时所有的 ECS 虚拟机均可利用阿里云 VPC 和安全组防火墙功能，以满足用户在各种场景下的网络访问权限切分。

  ECS 虚拟机实例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。

6.1.1.2 安全组防火墙

安全组是阿里云提供的虚拟化防火墙，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。

6.1.1.3 SSH 密钥对

SSH 密钥对是阿里云提供的新的远程登录 ECS 实例的认证方式，目前仅适用于 Linux 实例。相较于传统的用户名和密码认证方式，SSH 密钥对登录认证更为安全可靠，同时便于远程登录大量 Linux 实例。

SSH 密钥对是通过一种加密算法生成的一对密钥：一个对外界公开，称为“公钥”；另一个由用户自己保留，称为“私钥”。如果用户已经将公钥配置在 Linux 实例中，那么，在本地或者另外一个实例中，用户可以使用私钥通过 SSH 命令或相关工具登录之前有公钥配置的实例，而不需要输入密码。

6.1.1.4 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 MAC/ARP 欺骗，在宿主机网络层防止云服务器 IP 欺骗。

6.1.1.5 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。具体请见 SLB 负载均衡章节。

- **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 99.9999999%。

- **故障自动迁移恢复**

  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，恢复实例正常运行，保障应用的高可用性。

6.1.1.6 快照与镜像

ECS 提供快照与自定义镜像功能，快照可以保留某个时间点上的系统数据状态，用于数据备份，或者制作镜像。用户可以方便的创建磁盘的自动快照策略，定义自动快照的创建时间、重复时间和保留时间等参数。

用户可以使用快照创建自定义镜像，将快照的操作系统、数据环境信息完整的包含在镜像中。然后使用自定义镜像创建多台具有相同操作系统和数据环境信息的实例，非常方便的复制实例。快照使用增量的方式，两个快照之间只有数据变化的部分才会被拷贝。推荐用户在以下业务场景中使用快照：

- 系统盘、数据盘的日常备份，用户可以利用快照定期的对重要业务数据进行备份，来应对误操作、攻击、病毒等导致的数据丢失风险。

- 更换操作系统，应用软件升级或业务数据迁移等重大操作前，用户可以创建一份或多份数据快照，一旦升级、迁移过程中出现任何问题，可以通过数据快照及时恢复到正常的系统数据状态。

- 生产数据的多副本应用，用户可以通过对生产数据创建快照，从而为数据挖掘、报表查询、开发测试等应用提供近实时的真实生产数据。

用户还可以自己创建镜像导入阿里云 ECS 使用。

6.1.1.7 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。同时，阿里云会使用数据校验算法确保镜像完整性，防止被恶意篡改。

6.1.1.8 补丁热修复

阿里云的虚拟化平台支持补丁热修复技术，通过补丁热修复技术使得系统缺陷或者漏洞的修复过程不需要用户重启系统，从而不影响用户业务。

6.1.1.9 RAM 和 STS 支持

RAM 是阿里云提供的资源访问控制服务。ECS 用户可以通过 RAM 创建子用户账号和不同的群组来管理和控制用户资源的访问权限。

RAM 可以帮助管理用户对资源的访问权限控制。例如，为了加强网络安全控制，用户可以给某个群组附加一个授权策略，该策略规定：如果原始 IP 地址不是来自特定的企业网络，则拒绝此类访问请求。

用户可以给不同群组设置不同权限来管理 ECS 资源，例如：

- SysAdmins：该群组需要创建和管理 ECS 镜像、实例、快照、安全组等权限。用户可以给 SysAdmins 组附加了一个授权策略，该策略授予组成员执行所有 ECS 操作的权限。

- Developers：该群组只需要使用 ECS 实例的权限。用户可以给 Developers 组附加一个授权策略，该策略授予组成员调用 DescribeInstances、StartInstance、StopInstance、CreateInstance 和 DeleteInstance 等 API 的权限。

如果某开发人员的工作职责发生转变，成为一名系统管理人员，用户可以方便的将其从 Developers 群组移到 SysAdmins 群组。

ECS 同时通过接入 STS 来支持 ECS 实例 RAM 角色的功能。实例 RAM 角色属于 RAM 角色的一种，它的目的是让 ECS 实例扮演具有某些权限的角色，从而赋予实例一定的访问权限。

实例 RAM 角色允许用户将一个 RAM 角色关联到 ECS 实例，在实例内部基于 STS 临时凭证（临时凭证将周期性更新）访问其他云产品。这样，一方面可以保证 Access Key 安全，另一方面也可以借助 RAM 实现权限的精细化控制和管理。

6.1.1.10 最佳实践

- **创建 ECS 实例的安全配置**
    - 网络类型选择：专有网络。专有网络是指逻辑隔离的私有网络，用户可以自定义网络拓扑和 IP 地址，支持通过专线连接，网络可扩展性强。适合于对网络有个性化定制及高级定制需求的客户。
    - 网络安全组选择：默认安全组（自定义端口），仅允许 22、3389 端口的访问。22 端口用于 Linux SSH 登录，3389 端口用于 Windows 远程桌面登录。
    - 镜像选择：按需选择官方提供镜像，并选中安全加固功能，即可免费加载云服务器安全组件，获得网站后门检测、异地登录提醒、暴力破解拦截等安全功能。
    - 安全设置，密钥对登陆设置：选择创建后设置，在 ECS 实例创建完成后至 ECS 控制台，密钥对中创建密钥对，选中新创建的密钥对，绑定刚创建的实例。

- **防火墙-网络安全组设置**
  网络安全组是 ECS 提供的免费的网络防火墙，如若配置不当可能导致业务的端口或者 IP 暴露在互联网，造成安全威胁。利用安全组限制，禁止私网访问，公网安全组和私网安全组都只保留业务需要使用的端口。

- **创建快照**
  快照可以保留某个时间点上的磁盘数据状态，用于数据备份或者制作自定义镜像。建议用户对重要的 ECS 实例设置快照备份功能。也可以开启自动快照策略，定时的备份重要业务数据。快照备份功能可以在 ECS 管理控制台 -> 选中某地域 -> 选中要设置的 ECS 实例按照提示进行设置。

- **实例登陆使用 SSH 密钥对**
  ECS 实例已支持 SSH 的 key 登陆，用户可以在 ECS 实例创建完成后至 ECS 控制台，密钥对中创建密钥对，选中新创建的密钥对，绑定刚创建的实例。

- **系统安全漏洞升级**
  系统的安全漏洞是不可避免的，需要用户定期关注其使用到的操作系统版本对应的漏洞，并定期升级。其中，Windows 系统需要开启 Windows 的安全更新，而 Linux 类系统可采用 yum 等工具来检查更新。建议用户通过开启安装安骑士，使用安骑士的漏洞补丁管理来升级系统漏洞。

- **使用安骑士保护 ECS 实例安全**
  安骑士是阿里云云盾推出的一款服务器安全运维管理产品。通过安装在服务器上的轻量级 Agent 插件与云端防护中心的规则联动，实时感知和防御入侵事件，保障服务器的安全。

6.1.2 块存储

阿里云块存储（Block Storage），是阿里云为云服务器 ECS 提供的低时延、持久性、高可靠的数据块级随机存储。块存储支持在可用区内自动复制用户的数据，防止意外的硬件故障导致数据不可用，以保护用户的业务免于组件故障的威胁。就像对待硬盘一样，用户可以对挂载到 ECS 实例上的块存储做格式化、创建文件系统等操作，并对数据持久化存储。

6.1.2.1 数据加密

块存储支持虚拟机内部使用的块存储设备的自动加密，确保块存储的数据在分布式系统中加密存放。

6.1.2.2 高可用性

块存储采用三副本的分布式机制，为 ECS 实例提供 99.9999999% 的数据可靠性保证。

6.1.3 文件存储

阿里云文件存储（Network Attached Storage，NAS）是面向阿里云 ECS 实例、HPC 和 Docker 的文件存储服务，提供标准的文件访问协议，用户无需对现有应用做任何修改，即可使用具备无限容量及性能扩展、单一命名空间、多共享、高可靠和高可用等特性的分布式文件系统。

6.1.3.1 访问控制

NAS 支持文件系统标准的目录/文件权限操作，并支持用户/组的读/写/执行权限。NAS 支持 VPC 挂载点和经典网络挂载点，并只允许同一 VPC 内或同一账号下的 ECS 实例访问其文件系统。
NAS 同时提供了 IP 级别的权限组进行细粒度的访问权限控制。

6.1.3.2 RAM 支持

NAS 接入了 RAM 服务，支持控制台设置 RAM 进行主子账号授权。

6.1.3.3 高可用性

NAS 提供 99.99999999%的数据可靠性，相比自建 NAS 存储，可以大量节约维护成本，降低数据可靠性风险。

6.1.4 弹性伸缩

阿里云弹性伸缩（Auto Scaling），是根据用户的业务需求和策略，经济地自动调整弹性计算资源的管理服务。弹性伸缩不仅适合业务量不断波动的应用程序，同时也适合业务量稳定的应用程序。

弹性伸缩用于可以监控用户的集群，随时自动替换不健康的实例，节省运维成本；也可以用于管理用户的集群，在高峰期自动增加 ECS 实例，在业务回落时自动减少 ECS 实例，节省基础设施成本。弹性伸缩同时与 SLB/RDS 紧密集成，自动管理 SLB 后端服务器和 RDS 白名单，节省用户的操作成本。

6.1.4.1 身份认证

弹性伸缩会对每个访问的请求进行身份认证，所以无论使用 HTTP 还是 HTTPS 协议提交请求，都需要在请求中包含签名（Signature）信息。弹性伸缩通过使用 Access Key ID 和 Access Key Secret 进行对称加密的方法来验证请求的发送者身份。Access Key ID 和 Access Key Secret 由阿里云官方颁发给访问者（可以通过阿里云官方网站申请和管理），其中 Access Key ID 用于标识访问者的身份；Access Key Secret 是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密，只有阿里云和用户知道。

6.1.4.2 RAM 支持

弹性伸缩服务接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.1.5 资源编排

阿里云资源编排服务 (Resource Orchestration Service，ROS)是一种简单易用的云计算资源管理和自动化运维服务。用户通过 ROS 模板描述多个云计算资源的依赖关系、配置细节等，并自动完成所有资源的创建和配置，以达到自动化部署、运维等目的。编排模板同时也是一种标准化的资源和应用交付方式，并且可以随时编辑修改，使基础设施即代码（Infrastructure as Code）成为可能。

6.1.5.1 RAM 支持

ROS 接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.2 网络

6.2.1 负载均衡 SLB

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

6.2.1.1 高可用性

采用全冗余设计，无单点，支持同城容灾。搭配 DNS 可实现跨地域容灾，可用性高达 99.95%。同时 SLB 可以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。

6.2.1.2 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。

6.2.1.3 抗 CC 攻击

阿里云对开源四层负载均衡 LVS 的管理软件 Keepalived 进行了全面优化，使得基于 LVS 的四层负载均衡具备接近于实时防御的能力。结合云盾，可提供 5G 以下的防 DDOS 攻击能力。

采用 Tengine 作为负载均衡基础模块的七层负载均衡具备多维度的 CC 攻击防御能力。

6.2.1.4 访问控制

SLB 可以屏蔽后端服务器 IP 地址，对外只提供虚拟 IP（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。

6.2.1.5 HTTPS

SLB 支持 HTTPS/SSL/TLS 负载均衡功能：

- 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。

- 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。

6.2.1.6 日志功能

负载均衡提供日志管理功能，用户可以查看某个实例的操作日志和健康检查日志。

6.2.1.7 RAM 和 STS 支持

用户通过自己云帐号创建的 SLB 实例，都是该帐号拥有的资源。默认情况下，帐号对自己的资源拥有完整的操作权限。

SLB 已支持 RAM 服务。用户可以将用户云账户下负载均衡资源的访问及管理权限授予 RAM 中子用户。SLB 同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

6.2.1.8 最佳实践

- 在使用 SLB 的时候，需要检查勿将后端 ECS 实例的管理端口通过 SLB 转发至公网，比如 ECS 的 22、3389、3306、6379 等高危端口端口。

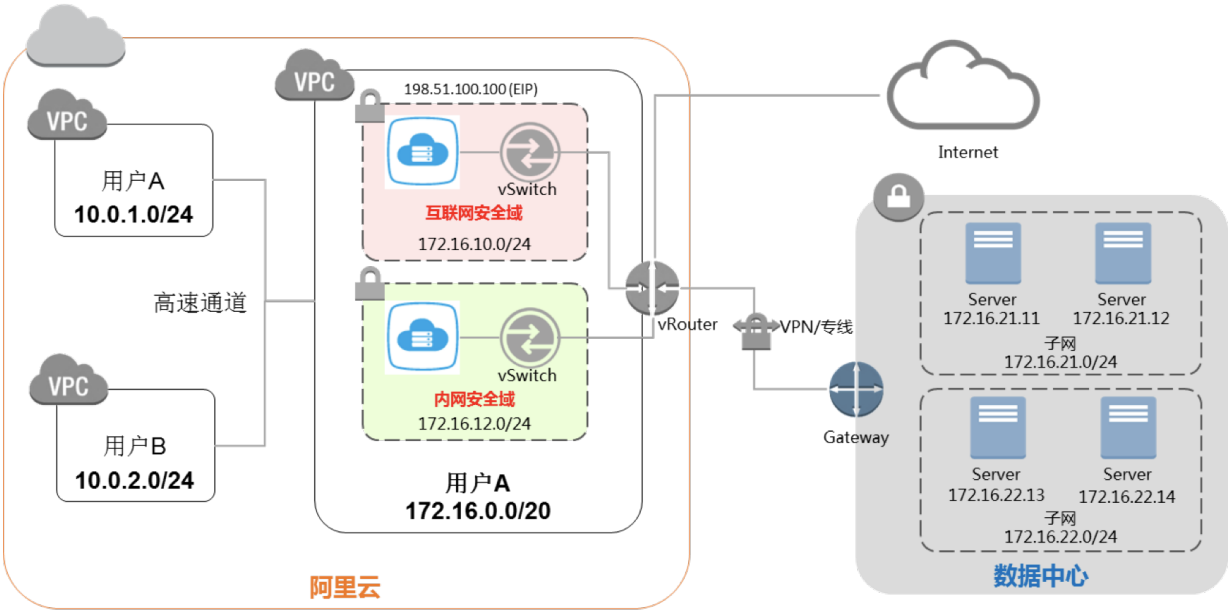
- 如果仅仅是做私网负载均衡，用户可以选择私网 SLB 实例。公网实例和私网实例的不同：
    - 公网实例：负载均衡实例仅提供公网 IP，可以通过 Internet 访问的负载均衡服务。
    - 私网实例：负载均衡实例仅提供阿里云私网 IP 地址，只能通过阿里云内部网络访问该负载均衡服务，Internet 用户无法访问。

- SLB 提供了 HTTPS 监听，支持单向和双向认证，建议使用。

6.2.2 专有网络 VPC

用户可以使用阿里云提供的专有网络（Virtual Private Cloud，VPC）构建出一个隔离的网络环境，并可以自定义 IP 地址范围、网段、路由表和网关等；此外，也可以通过专线/VPN 等连接方式实现云上 VPC 与传统 IDC 的互联，构建混合云业务。

典型的 VPC 网络架构如下图所示：



6.2.2.1 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。

6.2.2.2 防火墙

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。

6.2.2.3 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。

- 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。

6.2.2.4 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。

6.2.2.5 租户隔离

不同租户的云服务器 ECS 部署在不同的 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。

6.2.2.6 弹性公网 IP

弹性公网 IP（Elastic IP Address，EIP），是可以独立购买和持有的公网 IP 地址资源，能动态绑定到不同的 ECS 实例上，绑定和解绑时无需停机。

EIP 是一种 NAT IP。它实际位于阿里云的公网网关上，通过 NAT 方式映射到了被绑定 ECS 实例的私网网卡上。因此，绑定了 EIP 的 ECS 实例可以直接使用这个 IP 进行公网通信，但是在网卡上并不能看到这个 IP 地址。EIP 可以用于不同 VPC 之间的互联。

6.2.2.7 VPN 网关

VPN 网关（VPN Gateway）是一款基于 Internet，通过加密通道将企业数据中心和阿里云专有网络（VPC）安全可靠连接起来的服务。阿里云 VPN 网关在中华人民共和国国家相关政策法规内提供服务，不提供访问 Internet 功能。

- **快速构建混合云**
  VPN 网关是基于 Internet 建立加密隧道进行通信，比建立专线的方式更简单，耗时更短，可以非常快速地将企业数据中心和云上 VPC 连接起来，构建混合云。

- **专线接入验证**
  用户对 IDC 和云上 VPC 的连接有非常高的质量要求，希望通过阿里云高速通道的专线接入功能使用专线构建混合云。但专线接入耗时较长，此时，可以使用 VPN 网关先进行相关的验证工作。

- **异地容灾和数据备份**
  对于质量要求相对不高的异地容灾，以及数据流相对较小的异地备份，可以通过 VPN 网关将用 IDC 和云上 VPC 建立的加密通信隧道进行，安全便捷。

6.2.2.8 高速通道

高速通道（Express Connect）是一款基于 IP VPN 的便捷高效的网络服务，用于在云上的不同网络环境间实现高速、稳定、安全的私网通信，包括跨地域/跨用户的 VPC 内网互通、专线接入等场景。可以有效的帮助用户提高网络拓扑的灵活性和跨网络通信的质量和安全性。

- VPC 间内网通信
  高速通道支持位于相同地域或不同地域，同一账户或不同账户的 VPC 之间进行内网互通。阿里云通过在两侧 VPC 的路由器上分别创建虚拟路由器接口，以及自有的骨干传输网络来搭建高速通道，实现两个 VPC 之间安全可靠，方便快捷的通信。

- 物理数据中心和阿里云上 VPC 间内网通信
  通过物理专线在物理层面上连接用户的数据中心到阿里云，然后建立虚拟边界路由器和虚拟路由器接口来连接数据中心与阿里云 VPC。

6.2.2.9 RAM 和 STS 支持

VPC 已支持 RAM 服务。用户可以将用户云账户下 VPC 资源的访问及管理权限授予 RAM 中子用户。VPC 同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

6.2.2.10 NAT 网关

阿里云 NAT 网关（NAT Gateway）是一款企业级的 VPC 公网网关，提供 NAT 代理（SNAT、DNAT）、10Gbps 级别的转发能力以及跨可用区的容灾能力。

NAT 网关作为一个网关设备，需要配置公网 IP 和公网带宽才能正常工作。NAT 网关上的公网 IP 和公网带宽，被抽象为共享带宽包。一个共享带宽包由一份公网带宽和一组公网 IP 组成，这些公网 IP 共享带宽。

NAT 网关与共享带宽包需要配合使用，组合成为高性能、配置灵活的企业级网关。

6.3 数据库

6.3.1 云数据库 RDS 版

阿里云关系型数据库（Relational Database Service，RDS）是一种稳定可靠、可弹性伸缩的在线数据库服务。基于阿里云分布式文件系统和高性能存储，RDS 支持 MySQL、SQL Server 等数据库引擎，并且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案 。

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/TLS（安全套接层协议）

- **存储**：TDE（透明数据加密）、自动备份

- **容灾**：同城容灾（多可用区实例）、异地容灾（容灾实例）

6.3.1.1 租户隔离

RDS 通过虚拟化技术进行租户隔离，每个租户拥有自己独立的数据库权限。同时阿里云对运行数据库的服务器进行了安全加固，例如禁止用户通过数据库读写操作系统文件，确保用户无法接触其他用户的数据。

6.3.1.2 高可用性

高可用版 RDS 实例拥有两个数据库节点进行主从热备，主节点发生故障可以迅速切换至备节点，月服务可用性承诺为 99.95%。

用户可以随时发起数据库的备份，RDS 能够根据备份策略将数据库恢复至任意时刻，提高了数据可回溯性。

6.3.1.3 访问控制

- **数据库账户**

  当用户创建实例后，RDS 并不会为用户创建任何初始的数据库账户。用户可以通过控制台或者 Open API 来创建普通数据库账户，并设置数据库级别的读写权限。如果用户需要更细粒度的权限控制，比如表/视图/字段级别的权限，也可以通过控制台或者 Open API 先创建超级数据库账户，并使用数据库客户端和超级数据库账户来创建普通数据库账户。超级数据库账户可以为普通数据库账户设置表级别的读写权限。

- **IP 白名单**

  默认情况下，RDS 实例被设置为不允许任何 IP 访问，即 127.0.0.1。用户可以通过控制台的数据安全性模块或者 Open API 来添加 IP 白名单规则。IP 白名单的更新无需重启 RDS 实例，因此不会影响用户的使用。IP 白名单可以设置多个分组，每个分组可配置 1000 个 IP 或 IP 段。

6.3.1.4 网络隔离

- **VPC 网络**

  除了 IP 白名单外，RDS 还支持用户使用 VPC 来获取更高程度的网络访问控制。VPC 是用户在公共云里设定的私有网络环境，通过底层网络协议严格地将用户的网络包隔离，在网络 2 层完成访问控制；用户可以通过 VPN 或者专线，将自建 IDC 的服务器资源接入阿里云，并使用 VPC 自定义的 RDS IP 段来解决 IP 资源冲突的问题，实现自有服务器和阿里云 ECS 同时访问 RDS 的目的。

  使用 VPC 和 IP 白名单将极大程度提升 RDS 实例的安全性。

- Internet

  部署在 VPC 中的 RDS 实例默认只能被同一个 VPC 中的 ECS 实例访问。如果有需要也可以通过申请公网 IP 的方式接受来自公网的访问（不推荐），包括但不限于：

  - 来自 ECS EIP 的访问。
  - 来自用户自建 IDC 公网出口的访问。

  IP 白名单对 RDS 实例的所有连接方式生效，建议在申请公网 IP 前先设置相应白名单规则。

6.3.1.5 数据加密

- SSL/TLS

  RDS 提供 MySQL 和 SQL Server 的安全套接层协议。用户可以使用 RDS 提供的服务器端根证书来验证目标地址和端口的数据库服务是否为 RDS 提供，从而有效避免中间人攻击。除此之外，RDS 还提供了服务器端 SSL/TLS 证书的启用和更新能力，以便用户按需更替 SSL/TLS 证书以保障安全有效性。

- TDE

  RDS 提供 MySQL 和 SQL Server 的透明数据加密功能。RDS for MySQL 的 TDE 由阿里云自研，RDS for SQL Server 的 TDE 基于 SQL Server 企业版的功能改造而来。TDE 加密使用的密钥由 KMS 服务加密保存，RDS 只在启动实例和迁移实例的动态读取一次密钥。用户可自行通过 KMS 控制台对密钥进行更替。

6.3.1.6 SQL 审计

RDS 提供查看 SQL 明细功能，用户可定期审计 SQL，及时发现问题。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。

6.3.1.7 备份恢复

为了保证数据完整可靠，数据库需要常规的自动备份来保证数据的可恢复性。RDS 提供两种备份功能，分别为数据备份和日志备份。

6.3.1.8 实例容灾

阿里云为全世界多个地域提供云计算服务，每个地域（Region）都包含多个可用区（Zone）。

为了提供比单可用区实例更高的可用性，RDS 支持多可用区实例（也叫做同城双机房或者同城容灾实例）。多可用区实例将物理服务器部署在不同的可用区，当一个可用区（A）出现故障时流量可以在短时间内切换到另一个可用区（B）。整个切换过程对用户透明，应用代码无需变更。

为了提供更高的可用性，RDS 还支持跨地域的数据容灾。用户可以将地域 A 的 RDS 实例 A’通过数据传输（Data Transmission）异步复制到地域 B 的 RDS 实例 B’（实例 B’是一个完整独立的 RDS 实例，拥有独立的连接地址、账号和权限）。

6.3.1.9 软件升级

RDS 为用户提供数据库软件的新版本。在绝大多数情况下版本升级都是非强制性的。只有用户主动重启了 RDS 实例的时候，RDS 才会将被重启实例的数据库版本升级到新的兼容版本。在极少数情况下（如致命的重大 Bug、安全漏洞），RDS 会在实例的可运维时间内发起数据库版本的强制升级。需要注意的是，强制升级的影响仅仅是几次数据库连接闪断，在应用程序正确配置了数据库连接池的情况下不会对应用程序造成明显的影响。用户可以通过控制台或者 Open API 来修改可运维时间，以避免 RDS 在业务高峰期发生了强制升级。

6.3.1.10 RAM 和 STS 支持

用户通过云账户创建的 RDS 实例，都是该账户自己拥有的资源。默认情况下，云账户对自己的资源拥有完整的操作权限。

RDS 已支持 RAM 服务。使用阿里云的 RAM 服务，用户可以将云账户下 RDS 资源的访问及管理权限授予 RAM 中子用户。RDS 同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

6.3.1.11 最佳实践

- **网络设置**
  RDS 支持公网的访问和私网的访问，如果仅在阿里云内部使用，建议设置为私网访问。如果再 VPC 内访问，建议选择 VPC 实例。

- **IP 白名单设置**
  通过 RDS 控制台，设置 RDS 连接 IP 白名单为对应的 ECS 私网 IP 或者云服务的私网 IP。

- **数据加密**
  - SSL/TLS：RDS 提供 MySQL 和 SQL Server 的安全套接层协议。用户可以使用 RDS 提供的服务器端证书来验证目标地址和端口的数据库服务是否为 RDS 提供，从而有效避免中间人攻击。
  - TDE：RDS 提供 MySQL 和 SQL Server 的透明数据加密功能。RDS for MySQL 的 TDE 由阿里云自研，RDS for SQL Server 的 TDE 基于 SQL Server 企业版的功能改造而来。

6.3.2 云数据库 Memcache 版

阿里云云数据库 Memcache 版（ApsaraDB for Memcache）是一种高性能、高可靠、可平滑扩容的分布式内存数据库服务。基于飞天分布式系统及高性能存储，并提供了双机热备、故障恢复、业务监控、数据迁移等方面的全套数据库解决方案。

6.3.2.1 高可用性

云数据库 Memcache 版由 Proxy 服务器（服务代理）、分片服务器和配置服务器三个组件组成。

- Proxy 服务
  单节点配置，集群版结构中会由多个 Proxy 组成，系统会自动对其实现负载均衡及故障转移。

- 分片服务器
  每个分片服务器均是双副本高可用架构，主节点故障之后，系统会自动进行主备切换保证服务高
  可用。
- 配置服务器
  用于存储集群配置信息及分区策略，目前采用双副本高可用架构，保证高可用。

6.3.2.2 身份认证

云数据库 Memcache 版支持 SASL(全称 Simple Authentication and Security Layer)鉴权，即用户需要输入正确的用户名和密码才能对数据进行操作。

云数据库 Memcache 版默认通过 SASL 访问，为了方便用户使用，云数据库 Memcache 也支持免密方式登录，前提必须开启 IP 白名单后才能开启此功能，在 IP 白名单中的 IP 可访问 Memcache 实例。

6.3.2.3 访问控制

- IP 白名单
  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。在开始使用 Memcache 实例前必须将访问 Memcache 的实例 IP 或者 IP 段添加到 IP 白名单中方可正常访问实例。

- VPC
  云数据库 Memcache 全面接入 VPC，可基于阿里云构建出一个隔离的网络环境。

6.3.2.4 备份恢复

云数据库 Memcache 版提供了备份存档功能， 为用户免费保存 7 天内的备份文件，7 天外的备份文件将会自动删除。

6.3.2.5 RAM 支持

云数据库 Memcache 版接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.3.3 云数据库 Redis 版

阿里云云数据库 Redis 版（ApsaraDB for Redis）是兼容开源 Redis 协议标准的、提供持久化的内存数据库服务，基于高可靠双机热备架构及可无缝扩展的集群架构，满足高读写性能场景及容量需弹性变配的业务需求。

6.3.3.1 高可用性

云数据库 Redis 版在支持单节点架构的同时，更支持双机热备架构和集群架构来达到故障时系统自动切换保障系统服务的高可用性。

- **单节点架构**
  单节点架构适用于纯缓存场景，支持单节点集群弹性变配，满足高 QPS 场景，提供超高性价比。

- **双机热备架构**
  系统工作时主节点（Master）和备节点（Slave）数据实时同步，主节点发生故障可以迅速切换至备节点，全程自动且对业务无影响，主备架构保障系统服务具有高可用性。

- **集群架构**
  集群（Cluster）实例采用分布式架构，每个分片都采用一主一备的高可用架构，自动容灾切换、故障迁移，多种集群规格可适配不同的业务压力，线性扩展数据库性能。

6.3.3.2 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。

6.3.3.3 访问控制

- **内网访问**
  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。

- IP 白名单
  在开始使用 Redis 实例前，需要将访问数据库的 IP 地址或者 IP 段加到目标实例的白名单中方可正常访问。

6.3.3.4 备份恢复

云数据库 Redis 版提供了备份存档功能，为用户免费保存 7 天内的备份文件，7 天外的备份文件将会自动删除。

6.3.3.5 RAM 支持

云数据库 Redis 版接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.4 存储与 CDN

6.4.1 对象存储 OSS

阿里云对象存储服务（Object Storage Service，OSS），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，按实际容量付费等特点使用户能专注于其核心业务。

6.4.1.1 身份认证

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 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。OSS 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，OSS 将拒绝处理这次请求，并返回 HTTP 403 错误。

6.4.1.2 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：任何人（包括匿名访问）都可以对该 Bucket 中的 Object 进行读/写/删除操作；所有这些操作产生的费用由该 Bucket 的 Owner 承担，**请慎用该权限**。

- public-read：只有该 Bucket 的 Owner 或者授权对象可以对存放在其中的 Object 进行写/删除操作；任何人（包括匿名访问）可以对 Object 进行读操作。

- private：只有该 Bucket 的 Owner 或者授权对象可以对存放在其中的 Object 进行读/写/删除操作；其他人在未经授权的情况下无法访问该 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：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，其他的用户没有权限操作该 Object。

- 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。

6.4.1.3 RAM 和 STS 支持

OSS 已支持 RAM 服务。使用阿里云的 RAM 服务，用户可以将云账户下 OSS 资源的访问及管理权限授予 RAM 中子用户。OSS 同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

6.4.1.4 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%。

6.4.1.5 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。

6.4.1.6 访问日志

OSS 提供自动保存访问日志记录功能。Bucket 的拥有者可以通过 OSS 控制台为其所拥有的 Bucket 开启访问日志记录功能。当一个源 Bucket（ Source Bucket）开启访问日志记录功能后，OSS 自动将访问这个 Bucket 的请求日志，以小时为单位，按照固定的命名规则，生成一个 Object 写入用户指定的目标 Bucket（ Target Bucket）。

6.4.1.7 防盗链

OSS 是按使用收费的服务，为了防止用户在 OSS 上的数据被其他人盗链，OSS 支持基于 HTTP header 中表头字段 referer 的防盗链方法。用户可以通过 OSS 管理控制台或者 API 的方式对一个 Bucket 设置 referer 字段的白名单和是否允许 referer 字段为空的请求访问。例如，对于一个名为 oss-example 的 Bucket，设置其 referer 白名单为 http://www.aliyun.com/。则所有 referer 为 http://www.aliyun.com/的请求才能访问 oss-example 这个 Bucket 中的 Object。

6.4.1.8 跨域访问

跨域访问，或者说 JavaScript 的跨域访问问题，是浏览器出于安全考虑而设置的一个限制，即同源策略。当来自于 A 网站的页面中的 JavaScript 代码希望访问 B 网站的时候，浏览器会拒绝该访问，因为 A、B 两个网站是属于不同的域。

在实际应用中，经常会有跨域访问的需求，比如用户的网站 www.a.com，后端使用了 OSS。在网页中提供了使用 JavaScript 实现的上传功能，但是在该页面中，只能向 www.a.com 发送请求，向其他网站发送的请求都会被浏览器拒绝。这样就导致用户上传的数据必须从 www.a.com 中转。如果设置了跨域访问的话，用户就可以直接上传到 OSS 而无需从 www.a.com 中转。

6.4.1.9 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编码（Server-Side Encryption）。用户上传数据时，OSS 对收到的用户数据进行加密编码，然后再将编码得到的数据永久保存下来；用户下载数据时，OSS 自动对保存的编码数据进行解码并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编码。换句话说，下载一个进行服务器端加密编码的 Object 和下载一个普通的 Object 没有多少区别，因为 OSS 会为用户管理整个编解码过程。

OSS 的服务器端加密编码是 Object 的一个属性。用户创建一个 Object 的时候，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 的服务器端加密编码存储。

6.4.1.10 客户端加密

客户端加密是指用户数据在发送给远端服务器之前就完成加密，而加密所用的密钥明文只保留在用户本地，从而可以保证用户数据安全，即使数据泄漏别人也无法解密得到原始数据。

6.4.1.11 最佳实践

- **数据访问控制**

  OSS 提供 Bucket 级别的权限访问控制，一般将应用的静态图片、CSS、JS 等资源放到 OSS 上面，应当设置 Bucket 为 public-read。

  如果是用户业务中的敏感数据，用户应请将 Bucket 设置为 private 并使用 AK 认证。

- **数据传输完整性**

  数据在客户端和服务器之间传输时有可能会出错。OSS 现在支持对各种方式上传的 object 返回其 CRC64 值，客户端可以和本地计算的 CRC64 值做对比，从而完成数据完整性的验证。

6.4.2 表格存储 Table Store

阿里云表格存储（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。

6.4.2.1 身份认证

表格存储根据 Access Key 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 Access Key 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。

6.4.2.2 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。

6.4.2.3 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。

6.4.2.4 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。

6.4.2.5 RAM 和 STS 支持

表格存储已支持 RAM 服务。使用阿里云的 RAM 服务，用户可以将云账户下表格存储资源的访问及管理权限授予 RAM 中子用户。表格存储同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

6.4.2.6 VPC 支持

当前表格存储已支持 VPC 内访问，可以进入表格存储控制台进行开通并绑定 VPC。

6.4.3 归档存储

归档存储（Archive Storage）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。

6.4.3.1 身份认证

归档存储服务使用 Access Key 进行身份认证。

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。

6.4.3.2 高可用性

归档存储服务数据多副本存储，可靠性达到 99.99999999%。

6.4.3.3 租户隔离

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。

6.4.3.4 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。

6.4.4 内容分发网络 CDN

阿里云内容分发网络（Content Delivery Network，CDN）是建立并覆盖在承载网之上、由分布在不同区域的边缘节点服务器群组成的分布式网络，替代传统以 WEB Server 为中心的数据传输模式。CDN 能将源内容发布到边缘节点并配合精准的调度系统；也能将用户的请求分配至最适合他的节点，使用户可以以最快的速度取得他所需的内容，有效解决 Internet 网络拥塞状况，提高用户访问的响应速度。

6.4.4.1 身份认证

阿里云 CDN 使用 Access Key 进行身份认证。

CDN 提供了 HTTP 和 HTTPS 协议对外提供服务。

当用户向 CDN 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。

6.4.4.2 租户隔离

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。

6.4.4.3 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。

阿里云 CDN 兼容并支持多种鉴权方式，用户可以根据自己的业务情况，选择合适的鉴权方式，来实现对源站资源的有效保护。

6.4.4.4 HTTPS 安全加速

HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer）安全超文本传输协议，是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。即将 HTTP 用 SSL/TLS 协议进行封装，HTTPS 的安全基础是 SSL/TLS。

HTTPS 加速优势：

- 传输过程中对用户的关键信息进行加密，防止类似 Session ID 或者 Cookie 内容被攻击者捕获造成的敏感信息泄露等安全隐患。

- 传输过程中对数据进行完整性校验，防止 DNS 或内容遭第三方劫持、篡改等中间人攻击（MITM）隐患，还可使用 HTTPS 来防止流量劫持。

阿里云 CDN 提供 HTTPS 安全加速方案，仅需开启安全加速模式后上传加速域名证书/私钥，并支持对证书进行查看、停用、启用、编辑操作。

6.4.4.5 防盗链

阿里云 CDN 提供防盗链功能。

防盗链功能基于 HTTP 协议支持的 Referer 机制，通过 referer 跟踪来源，对来源进行识别和判断，用户可以通过配置访问的 referer 黑白名单来对访问者身份进行识别和过滤，从而限制 CDN 资源被访问的情况。

目前防盗链功能支持黑名单或白名单机制，访客对资源发起请求后，请求到达 CDN 节点，CDN 节点会根据用户预设的防盗链黑名单或白名单，对访客的身份进行过滤，符合规则可以顺利请求到资源；若不符合规则，该访客请求被禁止，返回 403 响应码。

6.4.4.6 IP 黑名单

阿里云 CDN 提供 IP 黑名单功能，支持黑名单规则，添加了黑名单的 IP，表示此 IP 无法访问当前加速域名。

6.4.4.7 HTTPDNS

传统的 DNS 解析是通过访问运营商 Local DNS 获得解析结果，这种方式容易引发域名劫持、域名解析错误、流量跨网等问题，从而导致网站无法访问或访问缓慢。

HTTPDNS 是域名解析服务，通过 HTTP 协议直接访问阿里云 CDN 的服务器，由于绕过了运营商的 Local DNS，因此可以避免 DNS 劫持并获得实时精确的 DNS 解析结果。

客户端发起请求，通过 HTTP 协议访问阿里云 CDN 指定 HTTPDNS 服务端，该服务端依托遍布各地的二级 DNS 节点解析域名，获得域名解析结果并最终返回给客户端。

6.4.4.8 RAM 支持

通过用户云帐号开通 CDN 服务，创建加速域名，所有服务和加速域名都是该帐号自己拥有的资源。默认情况下，云帐号对自己的资源拥有完整的操作权限。

CDN 接入了阿里云的访问控制 RAM 服务，用户可以将云账户下 CDN 资源的访问及管理权限授予 RAM 中子用户。

6.5 数据与智能

6.5.1 大数据计算服务 MaxCompute

6.5.1.1 安全体系

阿里云大数据计算服务（MaxCompute，原名 ODPS）是一种快速、完全托管的 GB/TB/PB 级数据仓库解决方案。MaxCompute 为用户提供了完善的数据导入方案以及多种经典的分布式计算模型，能够更快速的解决海量数据计算问题，有效降低企业成本，并保障数据安全。

6.5.1.2 身份认证

MaxCompute 支持两种账号体系：阿里云账号体系和 RAM 账号体系。

请注意在默认情况下，MaxCompute 项目只能够识别阿里云账号系统。

6.5.1.3 授权管理

项目空间(Project)是 MaxCompute 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。

MaxCompute 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。

MaxCompute 支持两种授权机制来完成对用户或角色的授权：

- 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 MaxCompute 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。

6.5.1.4 跨项目空间的资源分享

假设一个用户是项目空间的 Owner 或管理员（admin 角色），如果有人需要申请访问用户的项目空间资源，但是这个申请人并不属于用户的项目团队，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。

6.5.1.5 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”。

6.5.2 分析型数据库 AnalyticDB

阿里云分析型数据库（AnalyticDB），是阿里巴巴自主研发的海量数据实时高并发在线分析（Realtime OLAP）云计算服务，可以在毫秒级针对千亿级数据进行即时的多维分析透视和业务探索。分析型数据库对海量数据的自由计算和极速响应能力，能让用户在瞬息之间进行灵活的数据探索，快速发现数据价值，并可直接嵌入业务系统为终端客户提供分析服务。

6.5.2.1 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 Access Key ID 为用户名，Access Key Secret 为密码。基于 MySQL 协议的要求，用户的 Access Key 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户为数据库的 Owner。未经数据库创建者授权，任何其他云账户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。

6.5.2.2 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（Server 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。

6.5.2.3 用户与权限

分析型数据库用户基于阿里云帐号进行认证，用户建立的数据库属于该用户，用户也可以授权给其他用户访问其数据库下的表。

分析型数据库支持基于数据库表的层级权限管理模型，提供类似 MySQL 的 ACL 授权模式。一个 ACL 授权由被授权的用户、授权对象和授予的对象权限组成。

类似 MySQL，分析型数据库中的数据库创建者可以使用 GRANT/REVOKE 语句进行授权和权限回收。

6.5.2.4 RAM 支持

在 0.8.43 或 0.9.7 以后的版本的阿里云分析型数据库中，支持通过阿里云 RAM 服务创建的子账号登录分析型数据库，并管理子账号在不同条件下是否有使用分析型数据库的权限。

主账号在阿里云访问控制的控制台中，可以新建多个子账号，通过授予对应的授权策略，使子账号在一定条件下可以访问分析型数据库。子账号访问分析型数据库的 MySQL 协议端时需要使用其的 Access Key ID/Secret 作为用户名和密码。若在访问控制中允许子账号登录阿里云控制台，子账号也可登录分析型数据库的控制台 DMS。

6.6 应用服务与中间件

6.6.1 日志服务

阿里云日志服务（Log Service，简称 Log）是针对日志类数据的一站式服务，在阿里巴巴集团经历大量大数据场景锤炼而成。用户无需开发就能快捷完成日志数据采集、消费、投递以及查询分析等功能，提升运维、运营效率，建立 DT 时代海量日志处理能力。

6.6.1.1 高可用性

Log 服务的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。

6.6.1.2 只读日志系统

Log 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。

6.6.1.3 离线归档

Log 服务除了本身提供的实时查询与分析功能外，还提供日志归档保存到 MaxCompute 与 OSS 的功能，以便用户利用 MaxCompute 以及开源大数据软件做数据分析。

6.6.1.4 身份认证

Log 服务认证采用由阿里云颁发给用户的访问服务的密钥（Access Key），在身份认证时使用 HMAC-SHA1 签名算法。

6.6.1.5 RAM 支持

Log 服务接入了阿里云的访问控制 RAM 服务，用户可以将云账户下 Log 资源的访问及管理权限授予 RAM 中子用户。

6.6.2 开放搜索服务 Open Search

阿里云开放搜索服务（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 MaxCompute、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。

6.6.2.1 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。

6.6.2.2 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。

6.6.2.3 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。

6.6.2.4 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密钥（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。

6.6.2.5 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。

6.6.2.6 RAM 支持

用户通过云账户创建的 OpenSearch 应用，都是该账户自己拥有的资源。默认情况下，账户对自己的资源拥有完整的操作权限。

开放搜索服务接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.6.3 媒体转码

媒体转码（ApsaraVideo for Media Transcoding）是为多媒体数据提供的转码计算服务。媒体转码服务提供了经济、弹性和高可扩展的音视频转换方法，适用于音视频网站、在线教育、金融视频、电商视频等多种场景。

6.6.3.1 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，在云资源授权管理中，通过 RAM 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。

6.6.3.2 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。

6.6.3.3 RAM 支持

媒体转码服务接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.6.4 消息队列

消息队列（Message Queue， MQ）是阿里巴巴集团中间件技术部自主研发的专业消息中间件。产品基于高可用分布式集群技术，提供消息发布订阅、消息轨迹查询、定时（延时）消息、资源统计、监控报警等一系列消息云服务，是企业级互联网架构的核心产品。MQ 历史超过 9 年，为分布式应用系统提供异步解耦、削峰填谷的能力，同时具备海量消息堆积、高吞吐、可靠重试等互联网应用所需的特性，是阿里巴巴双 11 使用的核心产品。

6.6.4.1 多协议接入

支持 HTTP 协议：支持 RESTful 风格 HTTP 协议完成收发消息，可以解决跨语言使用 MQ 问题。

支持 MQTT 协议：支持主动推送模型，多级 Topic 模型支持一次触达 1000 万+ 终端，可广泛应用于物联网和社交即时通信场景。

支持 TCP 协议：区别于 HTTP 简单的接入方式，提供更为专业、可靠、稳定的 TCP 协议的 SDK 接入。

6.6.4.2 RAM 支持

消息队列默认情况下，只支持队列创建者访问消息队列数据。同时，消息服务接入了阿里云的访问控制 RAM 服务，用户可以将云账户下消息服务资源的访问及管理权限授予 RAM 中子用户。

6.6.4.3 高性能

同一网络内，消息传输网络时延在 10 毫秒之内，性能测试下，网卡可被打满。

默认单 Topic 发送消息上限为每秒 5000 条，最高可申请扩展至 10W 以上。

默认单条消息大小最大支持 256KB，华北 2 地域支持 4MB 大消息。

6.6.4.4 独立部署

支持专有云独立输出，支持物理机和虚拟机，仅几台机器便可搭建完整消息云服务。

专有云配套 mqadmin 命令集和管理类 Open API，方便运维人员实时监控系统状态。

支持混合云架构，允许用户通过专线的方式接入服务。

6.6.5 性能测试服务 PTS

性能测试服务（Performance Test Service，PTS）是阿里巴巴集团中间件技术部自主研发的一套 SaaS 化性能测试平台。产品内部名称为“全链路压测平台”，是阿里巴巴用于保障每年双 11 稳定性的最重要武器。

PTS 集脚本管理、场景管理、过程监控、压测报告为一体，压测流量从全国不同的地域发起，具备强大的分布式压测能力。通过模拟海量用户真实的业务操作场景，用户可以提前对站点进行业务高压力测试，全方位探测站点的性能瓶颈，确保平稳地应对业务峰值。

6.6.5.1 权限控制

性能测试服务提供已认证的 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密钥（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户权限运行，防止越权操作。

6.6.5.2 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。

6.6.5.3 监控和审计

性能测试服务对被测试集群进行实时监控。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。

6.6.5.4 RAM 支持

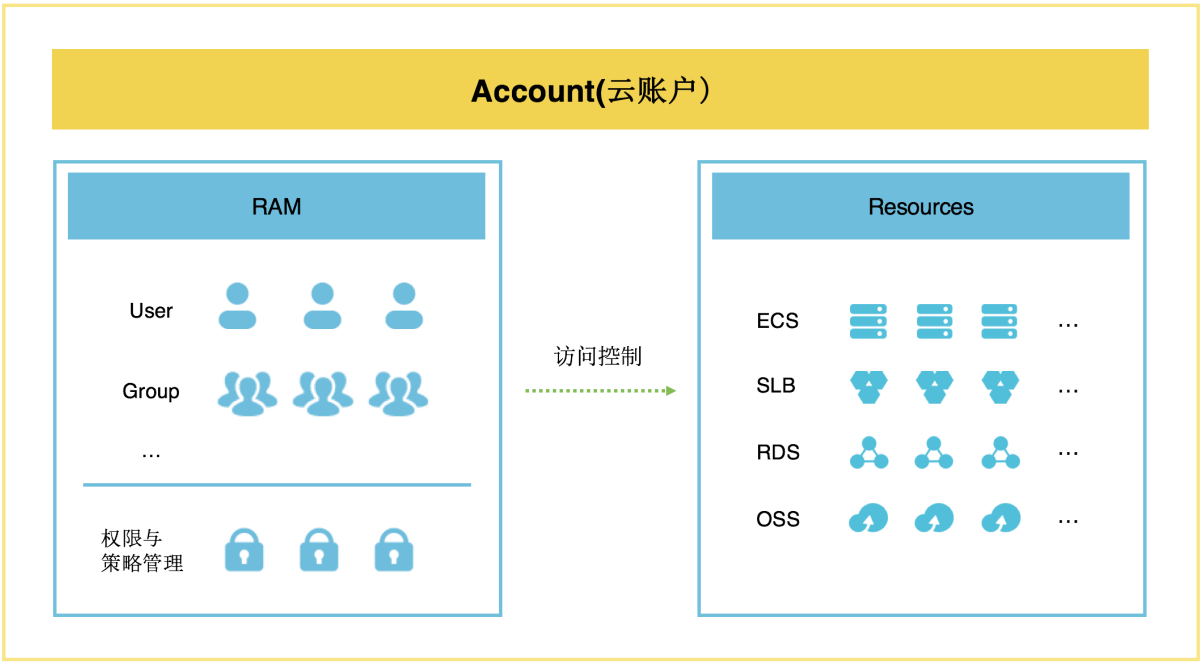
性能测试接入了 RAM 服务，用户可通过开启 RAM 功能来完成授予 RAM 子用户访问权限。

6.7 管理与监控

6.7.1 身份与访问管理

阿里云为客户提供了多种工具和功能，用来帮助客户在各种情况下授权资源的使用权力。其中，阿里云为客户提供 RAM (Resource Access Management)资源访问控制服务，用于用户身份管理与资源访问控制。RAM 使得一个阿里云账户（主账号）可拥有多个独立的子用户（子账号），多因素认证、强密码策略、控制台用户与 API 用户分离、支持自定义细粒度授权策略，支持用户分组授权、临时授权令牌、账户临时禁用等功能。RAM 授权可以细化到对某个 API-Action 和 Resource-ID 的细粒度授权，还可以支持多种限制条件（源 IP 地址、安全访问通道 SSL/TLS、访问时间段、多因素认证等等）。

RAM 为客户提供集中式用户身份与访问控制管理服务，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 可以为每个子用户分配不同的密码或 API 访问密钥(Access Key)，消除了云账户共享带来的安全风险；同时可为不同的子用户分配不同的工作权限，大大降低了因账户权限过大带来的风险。

6.7.1.1 用户管理

一个云账户可以通过 RAM 服务来创建一个或多个独立的子用户。云账户与 RAM 子用户的关系如下：(1) 从资源归属关系上来看，云账户是阿里云资源归属、资源使用计量计费的基本主体，而 RAM 用户只能存在于某个云账户下的 RAM 中。RAM 用户不拥有资源，在被授权操作时所创建的资源归属于云账户；RAM 用户不拥有账单，被授权操作时所发生的费用也计入云账户账单。(2) 从权限关系上来看，云账户与 RAM 用户是一种类似 Linux 下 Root 与 User 的关系，云账户对资源拥有一切操作控制权限，而 RAM 用户只能拥有被云账户所授予的某些权限，而且云账户在任何时刻都可以撤销 RAM 用户身上的权限。同时，云账户也可以授权 RAM 用户使其拥有 RAM 资源本身的操作权限。

每一个 RAM 用户应当对应到某一个主体，如操作员或应用程序。如果有新的用户或应用程序需要访问云账户下的云资源，则需要创建 RAM 用户并授权其访问相关资源。对云账户下有多个 RAM 用户的情况，为更好的管理用户及其权限，建议使用群组（Group）来为职责相同的 RAM 用户创建群组进行归类，并在授权时选择给群组授权。

管理员通过 RAM 还可以创建一种称为"RAM 角色"的用户。RAM 角色与普通 RAM 用户类似，都是 RAM 中管理的身份主体。与 RAM 用户相比，RAM 角色更像是一种虚拟用户，它没有长期的身份认证密钥，且需要被一个受信的真实用户身份扮演才能正常使用。

6.7.1.2 身份凭证

身份凭证是用于证明用户真实身份的凭据，它通常是指登录密码或访问密钥（Access Key，AK）。身份凭证是秘密信息，用户必须保护好身份凭证的安全。

RAM 用户支持如下的身份凭证：

- **登录密码(Password)**
  云账号的密码规范、登录安全风控策略由阿里云统一管理。云账号下子用户(RAM 用户)的密码策略则可以由客户自己设定，比如密码字符组合规范、重试登录次数、密码轮转周期等策略。

- **多因素认证(MFA, Multi-Factor Authentication)**
  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用户的账户提供更高的安全保护。阿里云可以支持基于软件的虚拟 MFA 设备。虚拟 MFA 设备是产生一个 6 位数字认证码的应用程序，它遵循基于时间的一次性密码 (TOTP) 标准(RFC 6238)。此应用程序可在移动硬件设备（包括智能手机）上运行。

- **API 访问密钥(Access Key)**
  Access Key (AK)是阿里云服务 API 访问密钥，用户可以使用 Access Key 以程序方式操作阿里云 API。Access Key 包括访问密钥 ID（AK ID）和秘密访问密钥（AK Secret）。RAM 用户在调用资源时会传入访问密钥 ID，并使用秘密访问密钥对请求进行签名。用户可以登录阿里云用户中心来管理 Access Key，包括创建、冻结、激活和删除操作。Access Key 是可以长期使用的 API 访问密钥，建议用户在使用时要考虑对 Access Key 的周期性轮转。

  阿里云强烈建议客户使用 RAM 用户的 Access Key，而不要使用云账号的 Access Key。云账号可以理解为根账号，它具有所有云产品的完全控制权限。根账号 Access Key 一旦泄露将可能造成极大风险，所以建议客户使用 RAM 用户进行资源操作并遵循最小授权原则。

- **密钥对管理(KeyPair)**
  阿里云 RAM 服务在某些区域提供了密钥对管理功能。RAM 用户可以创建自己的 RSA 密钥对，将公有密钥 (Public Key) 上传到 RAM，私有密钥 (Private Key) 由用户自己保管。使用 KeyPair 访问 STS 服务可以获取当前用户的一个临时访问密钥 (Session Access Key)，用户可以使用临时访问密钥来访问某些区域的阿里云服务 API。

6.7.1.3 群组管理

对云账户下有多个 RAM 用户的情况，为更好的管理用户及其权限，建议使用群组（Group）。为职责相同的 RAM 用户（如 Admins、Developers、Accounting 等）创建群组进行归类，并在授权时选择给群组授权。这样，在具体用户职责发生变化时，只用将其移动到相应职责的群组下，不会对其他用户产生影响；当群组的权限发生变化时，只用修改群组的授权策略，可以直接应用到与该群组关联的所有 RAM 用户身上。

6.7.1.4 权限和授权策略管理

1) 权限

阿里云使用权限来描述一个操作主体（如用户、用户组、RAM 角色）对具体资源的访问能力。权限指在某种条件下允许 (Allow)或拒绝 (Deny)对某些资源执行某些操作。

- **云账户（又称主账号/根账号/资源 Owner）控制所有权限**
  - 每个资源有且仅有一个属主（资源 Owner）。该属主必须是云账户，是对资源付费的人，对资源拥有完全控制权限。
  - 资源属主不一定是资源创建者。比如，一个 RAM 用户被授予创建资源的权限，该用户创建的资源归属于云账户，该用户是资源创建者但不是资源属主。

- **一个新创建的 RAM 用户默认无任何权限**
  - RAM 用户代表的是操作员，其所有操作都需被显式授权。
  - 新建 RAM 用户默认没有任何操作权限，只有在被授权之后，才能通过控制台和 API 操作资源。

- **RAM 用户不会自动拥有对其所创建资源的任何权限**
  - 如果 RAM 用户被授予创建资源的权限，用户将可以创建资源。
  - 但是 RAM 用户不会自动拥有对所创建资源的任何权限，除非资源 Owner 对该用户有显式的授权。

2) 授权策略（Policy）

权限的载体是授权策略。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（默认拒绝优先）。

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，比如对 ECS 的只读权限、对 ECS 的完全权限等。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。

6.7.1.5 RAM 角色管理

RAM 角色可以被看成一种虚拟 RAM 用户，它没有长期的身份认证密钥（如登录密码或 Access Key），它需要被一个授信的真实 RAM 用户扮演才能正常使用。RAM 角色可以用来解决跨云帐号的资源授权、不同云服务之间的资源访问授权、给移动 App 颁发临时授权令牌等场景。

RAM 角色主要有两种:

- **用户角色**
  允许子用户扮演的角色。角色扮演者可以是客户自己云账户下的子用户，或者是其他帐号的子用户。用户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其他云服务资源的权限。

相比于 RAM 用户，在使用方法上 RAM 角色需要被一个授信的实体 RAM 用户扮演，扮演成功后实体 RAM 用户将获得 RAM 角色的 STS 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。需要注意的是，当 RAM 用户切换到 RAM 角色身份后，将只能执行该角色身份被授权的所有操作，而登录时实体身份所对应的访问权限被隐藏。当 RAM 用户切回登录身份时，将拥有 RAM 用户的实体身份所对应的访问权限，而不再拥有角色身份所拥有的权限。

6.7.1.6 STS 安全令牌服务

阿里云 STS (Security Token Service) 是为 RAM 用户提供短期访问资源的权限凭证的云服务。有时存在一些用户（人或应用程序），他们并不经常访问客户云账户下的云资源，只是偶尔需要访问一次，这些用户可以被称为“临时用户”；还有些用户，比如运行在不可信移动设备上的 App，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 来

为这些用户颁发临时权限凭证。颁发令牌时，管理员可以根据需要来定义令牌的权限和自动过期时间（默认为 1 小时过期）。

STS 访问令牌是一个三元组，它包括一个安全令牌（Security Token）、一个访问密钥 ID（Access Key ID） 和一个秘密访问密钥 （Access Key Secret）。用户在调用资源 API 时会传入安全令牌和访问密钥 ID，并使用秘密访问密钥对请求进行签名。STS 颁发的安全令牌不会与其他访问密钥一起使用。

使用 STS 安全令牌服务使得资源授权更加可控， 不必再为临时用户和安全性较低的用户创建并管理一个长期的 RAM 用户账号及密钥。此外，STS 颁发的权限凭证为自动颁发，所以不用被嵌入在用户端代码等不安全的位置，同时默认情况下每小时令牌会自动轮换以增加安全性。

6.7.1.7 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）**
  建议用户为根账户绑定 MFA，每次使用根账户时都强制使用多因素认证。如果用户创建了 RAM 用户，并且给用户授予了高风险操作权限（比如，停止虚拟机，删除存储桶），那么建议用户给 RAM 用户绑定 MFA。

- **授权予高风险特权操作时，使用带 IP 和 MFA 限制条件的授权策略进行授权**
  同时可以考虑账号密码和多因素认证设备交给不同的人员分开保管，这样可以做到必须两人同时在场时才能完成某些操作。

- **分离用户管理、权限管理与资源管理的 RAM 用户，分权制衡**
  一个好的分权体系应该支持权力制衡，尽可能地降低安全风险。在使用 RAM 时，用户应该考虑创建不同的 RAM 用户，其职责分别是 RAM 用户管理、RAM 权限权限、以及各产品的资源操作管理。

- **使用群组给 RAM 用户分配权限**
  一般情况下，用户不必对 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，如果用户需要修改群组内所有人的权限，只需在一处修改即可。当用户的组织人员发生调动时，用户只需更改用户所属的群组即可。

- **善用 STS 安全令牌服务，为临时用户提供短期访问资源的权限凭证**

使用 STS 安全令牌服务使得资源授权更加可控，不必再为临时用户和安全性较低的用户创建并管理一个长期的 RAM 用户账号及密钥。此外，STS 颁发的权限凭证为自动颁发，所以不用被嵌入在用户端代码等不安全的位置，同时默认情况下每小时令牌会自动轮换以增加安全性。

- **为云账户和 RAM 登录用户配置强密码策略**
  如果用户允许用户更改登录密码，那么应该要求他们创建强密码并且定期轮换。用户可以通过 RAM 控制台为 RAM 用户创建密码策略，如最短长度、是否需要非字母字符、必须进行轮换的频率等等。

- **不要为云账户（主账号）创建 Access Key，避免 AK 泄漏的巨大风险**
  由于云账户对名下资源有完全控制权限，所以为了避免因访问密钥泄露所带来的灾难性损失，不建议用户创建云账户访问密钥并使用该密钥进行日常工作。创建云账户的访问密钥需要通过登录阿里云控制台才能完成，该操作需要多因素认证，并且还支持严格的风控检查。只要云账户不主动创建访问密钥，就可以更好的控制账户名下的资产安全风险。

- **定期轮转用户登录密码和 Access Key**
  建议用户或 RAM 用户要定期轮换登录密码或访问密钥。在用户不知情的时候，如果出现凭证泄露，那么凭证的使用期限也是受限制的。用户可以通过设置密码策略来强制 RAM 用户轮换登录密码或访问密钥的周期。

- **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 Access Key。通常只给员工创建登录密码，给系统或应用程序只创建访问密钥。

- **使用策略限制条件来增强安全性，比如访问源 IP，时间等**
  建议用户给用户授权时设置策略限制条件，这样可以增强安全性。比如，授权用户 Alice 可以关停 ECS 实例，限制条件是 Alice 必须在指定时间、并且用户公司网络中执行该操作。

- **及时调整和撤销 RAM 用户不再需要的权限**
  当一个用户由于工作职责变更而不再使用权限时，用户应该及时将该用户的权限进行撤销。这样，如果在不知情的时候，当用户的访问凭证泄露时对用户带来的安全风险最小。

- **遵循最小授权原则，不要过度授权**
  最小授权原则是安全设计的基本原则。当用户需要给用户授权时，请授予刚好满足他工作所需的权限，而不要过渡授权。比如，在用户的组织中，如果 Developers 组员（或者一个应用系统）的工作职责只需要读取 OSS 存储桶里的数据，那么就只给这个组（或应用系统）授予

OSS 资源的只读权限，而不要授权 OSS 资源的所有权限，更不要授予对所有产品资源的访问权限。

6.7.1.8 授权管理典型场景

- **企业员工子账号管理与分权**

  云账号 A 代表某企业的超级管理员，它拥有企业购买的所有云产品的绝对控制权限。为了尽可能地避免云账号密码或 AK 泄露所导致的风险不可控，通常不建议企业员工直接使用云账号(root 权限)进行日常的资源操作。更好的做法是开通 RAM 服务，为企业员工分配不同的子账号，然后给不同子账号分配不同的工作权限，遵循最小授权原则，尽可能做到责权一致，降低企业上云的信息安全管理风险。

- **跨企业(租户)的资源授权管理**

  假设云账号 A 和云账号 B 分别代表不同的企业。A 购买了多种云资源（如 ECS 实例/ RDS 实例/ SLB 实例/ OSS 存储空间/…）来开展业务。企业 A 希望能专注于其业务系统研发，而将云资源运维监控管理等任务委托（或授权）给企业 B。企业 B 还可以进一步将 A 的资源权限分配给一个或多个员工进行管理，而且 B 希望能精细控制其员工对 A 的资源的操作权限。如果 A 和 B 的这种代运维关系终止，那么企业 A 随时可以撤销对企业 B 的授权。通过 RAM 提供的跨账号角色授权，企业 A 可以轻松实现对企业 B 的授权管理。

- **针对移动 App 的临时权限令牌管理**

  企业 A 开发了一款移动 App，通常移动 App 会运行在不可信的用户设备上，这些设备并不受 A 的控制。如果 App 需要操作 A 的云上资源，如何保证 App 的安全将是一个非常大的挑战，它要求 App 端不能保存持续有效的密钥，因为 App 是运行在不可信设备上，它可能被恶意人员完全控制。为此，用户需要授权协议能支持给 App 授予最小的临时权限，即使临时权限令牌被恶意人员控制，其带来的损失应该控制在最小。为了解决这个问题，RAM 提供的角色令牌管理可以满足 A 实现给不同设备上运行的 App 颁发不同的最小临时权限。

- **管理不同云服务之间的访问权限**

  阿里云平台上支持售卖多款云产品，比如 ECS(弹性计算), OSS(对象存储)等。在云平台中，不同云产品之间的云资源是完全隔离的，未经资源属主(购买云资源的客户)的授权，任何一方（包括云产品自身）是没有权限操作客户的云资源。比如，企业 A 购买了云产品 ECS 和 OSS，如果 A 在 ECS 上部署的应用程序需要访问 OSS 上的数据，默认是没有任何操作权限的，除非有 A 显式授权允许其 ECS 实例访问 OSS 数据。类似的场景非常多，比如授权 MTS(媒体转码服务)访问 OSS 数据、绿网服务读取 OSS 数据、EMR 服务创建或释放 ECS 虚拟机、FC(函数计算)服务操作 OSS 数据、等等。客户可以通过 RAM 来实现授权一个服务操作另一个服务上的资源，从而确保所有云资源的操作权限由资源属主的完全控制。

6.7.2 密钥管理服务

密钥管理服务（Key Management Service, KMS）是一款安全易用的管理类服务。用户无需花费大量成本来保护密钥的保密性、完整性和可用性，借助密钥管理服务用户可以安全、便捷的使用密钥，从而专注于开发用户真正需要关心的加解密功能场景。

KMS 实现了多种严格的安全保护措施，来保障用户的数据安全。

6.7.2.1 认证与访问控制

- **用户端认证**

  KMS 与其他阿里云服务一样，需要用户使用 Access Key ID 和 Access Key Secret 保护请求（基于 HMAC 消息验证码算法）。服务端通过验证消息验证码确保消息的完整性同时验证用户身份。KMS 通过 HTTPS 协议对外提供服务，因此客户端可以通过验证服务端证书的方式验证服务身份。用户与服务通信的数据保密性，也由 HTTPS 协议提供保护。

- **访问控制**

  KMS 通过集成阿里云访问控制服务（RAM）提供访问控制功能。

6.7.2.2 安全信道

- **内部通信安全**

  密钥管理服务（Key Management Service）内部由多组不同身份的进程协同工作。密钥管理服务的内部通信全部使用双向认证的 TLSv1.2 协议，保护内部节点的通信安全。

6.7.2.3 数据安全性

- **域主密钥**

  KMS 中的域主密钥是整个服务的核心主密钥，它由一个专门的分布式系统（Virtual HSM，VHSM）持有和使用，域主密钥的明文仅存在于 VHSM 节点的内存以及他们之间通信的加密信道中。

  VHSM 的节点使用硬件设备来加密保护存储于本地的数据。VHSM 会定期轮转域主密钥，轮转完成后，旧的域主密钥仅用于解密之前生成的用户主密钥。

- **用户主密钥**

  用户通过 KMS 服务的 API 或者控制台可以创建和管理用户主密钥（CMK），用户主密钥无法从 KMS 服务中导出。用户主密钥在 VHSM 产生后会由域主密钥加密，并保护相关的上下文数据（例如用户主密钥的所属用户，用户主密钥 ID 等等）。加密后的用户主密钥存储在高可靠的存储服务中。

当用户需要使用用户主密钥时，KMS 服务会取出密文的用户主密钥，结合用户的请求输入到 VHSM 中，VHSM 解密出用户主密钥明文，再使用明文的用户主密钥完成用户请求的操作。整个过程中，用户主密钥的明文仅会出现在 VHSM 的内存中。使用后立即被释放。

6.7.2.4 管理、运维安全性

- **多人管控机制**

  KMS 除了符合阿里云运维的安全规范以外，还实现了多人管控机制。对于重要的操作（包括但不限于：内部节点的证书签发，重要的管理 API 调用），必须由多人输入密码审核后才能成功操作。

6.7.2.5 可信计算技术

- **本地可信存储**

  KMS 使用本地可信存储保护本地落盘文件，每个文件有独立的文件密钥，该密钥由可信平台模块（TPM 2.0）的存储密钥（Storage Key）加密保护。这些文件只能在当前可信平台模块（TPM 2.0）管理的运行环境中被解密。

- **远程可信证明**

  KMS 所依托的阿里云底层运维系统支持基于远程可信证明的机器管理。密钥管理服务所在的集群开启了该功能，当且仅当机器能够出示远程可信证明时，机器才能成功加入集群，并部署相应的程序。

6.7.2.6 最佳实践

- **加密与解密实践**

  用户可以直接调用 KMS 的 API，使用指定的用户主密钥（CMK）来加密、解密数据。这种场景适用于少量（少于 4KB）数据的加解密，用户的数据会通过安全信道传递到 KMS 服务端，对应的结果将在服务端完成加密、解密后通过安全信道返回给用户。

- **信封加密**

  用户可以直接调用 KMS 的 API，使用指定的用户主密钥（CMK）来产生、解密数据密钥，并自行使用数据密钥在本地加解密数据。这种场景适用于大量数据的加解密，用户的数据无需通过网络传输大量数据，可以低成本的实现大量数据的加解密。

6.7.3 操作审计

操作审计(ActionTrail)会记录用户的云账户资源操作，提供操作记录查询，并可以将记录文件保存到指定的 OSS 存储空间。利用 ActionTrail 保存的所有操作记录，用户可以实现安全分析、资源变更追踪以及合规性审计。

ActionTrail 收集云服务的 API 调用记录（包括用户通过控制台触发的 API 调用记录），规格化处理后将操作记录以文件形式保存到指定的 OSS 存储空间。用户可以使用 OSS 提供的所有管理功能来管理这些记录文件，比如授权，开启生命周期管理，归档管理等等。同时用户还可以使用 OSS 数据加密以及权限管理功能来确保事件记录的数据安全。ActionTrail 支持从操作时段、用户名、资源类型、资源名称、操作名称等维度来查询操作事件，可以帮助用户快速诊断问题或追踪安全事故。

一般情况下，当用户通过控制台或 SDK 发起操作调用之后，ActionTrail 会在 5 分钟内传送操作记录到用户指定的 OSS Bucket。用户可以通过 ActionTrail 控制台查看最近 7 天的操作记录；如果要查看更多的记录，需要去用户设置的 OSS Bucket 中查看。

ActionTrail 的审计场景主要包括：

- **安全分析**
  当用户云账号或资源存在安全问题时，ActionTrail 所记录的日志将能分析原因。比如，ActionTrail 会记录用户所有账号登录操作，何时、从哪个 IP、是否使用多因素认证登录，都有详细记录，通过这些记录用户可以判断其账号是否存在安全问题。

- **资源变更追踪**
  当用户云端资源出现异常变更时，ActionTrail 所记录的操作日志将能帮助用户找到原因。比如，当用户发现一台 ECS 实例停机了，可以通过 ActionTrail 找到是谁、何时、从哪个 IP 发起的停机操作。

- **合规性审计**
  如果用户的组织有多个成员，而且已经使用阿里云的 RAM 服务来管理这些成员的身份，那么为了满足所在组织的合规新审计需要，用户往往需要获取每个成员的详细操作记录。ActionTrail 所记录的操作事件可以满足此类合规性审计需求。

6.7.4 云监控

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。云监控服务可用于收集获取阿里云资源的监控指标，探测互联网服务可用性，以及针对指标设置警报。云监控服务能够监控云服务器 ECS、云数据库 RDS 和负载均衡等各种阿里云服务资源，同时也能够通过 HTTP,ICMP 等通用网络协议监控互联网应用的可用性。用户可以全面了解在阿里云上的资源使用情况、性能和运行状况。借助报警服务，用户可以设置不同的报警规则，在监控数据达到报警阈值时发送报警信息，让用户可以及时做出反应，保证应用程序顺畅运行。

6.7.4.1 访问控制

云监控支持通过 RAM 访问控制实现子账号对云服务监控的监控数据、管理报警规则、管理联系人和联系人组的权限控制。注意，RAM 系统权限中的“只读访问云监控(CloudMonitor)的权限”包含监控、报警服务、应用组、报警联系人组“等监控相关的只读权限。

云监控除基本的子账号权限控制外，目前支持时间、MFA、IP 三种鉴权类型。

7 阿里云云盾

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、态势感知、加密服务等一站式安全服务。

云盾的以下所有产品都已支持接入 RAM 服务，支持通过 RAM 创建子用户并进行授权。

7.1 基础防护

7.1.1 DDoS 基础防护

阿里云免费为用户提供最高 5G 的默认 DDoS 防护能力。

在此基础上，阿里云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。

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。

7.1.2 最佳实践

对于不常受到攻击的初创/小体量用户来说，加入安全信誉防护联盟计划并根据联盟建议，维护平台安全，提升安全信誉分，从而获得更高的免费 DDoS 防护能力是一个行之有效的方案。

DDoS 基础防护产品的防护阈值可以自动设置也可以手动设置。当选择自动设置后，系统会根据云服务器的流量负载动态调整清洗阈值。当选择手动设置后，用户可以手动对流量和报文数量的阈值进行设置。当超过此阈值后云盾便会开启流量清洗。请注意，防护阈值的设置需要设置成略高于实际访问值。阈值设置过高，起不到防御效果；而设置过低，DDoS 基础防护触发流量清洗可能会影响正常的访问。

7.2 高级防护

7.2.1 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。

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。

7.2.1.1 最佳实践

用户开通高防 IP 服务需要把域名解析到高防 IP 清洗中心上。对于非 Web 业务，把业务 IP 换成高防 IP 服务，配置源站 IP。对于 Web 业务，用户需要通过域名 DNS 服务商修改域名对应的 A 记录，指向高防 IP。

举例来说：www.aliyun.com 源站 IP 为 42.120.158.67，分配的高防 IP 为 115.29.203.183。用户需要去 DNS 服务商将 www.aliyun.com 的域名解析 A 记录从 42.120.158.67 修改为 115.29.203.183。

完成域名解析的修改后，所有公网流量都会通过高防 IP 服务的清洗中心，通过端口协议转发的方式将用户的访问通过高防 IP 服务转发到源站，同时将恶意攻击流量在高防 IP 清洗中心进行清洗过滤后将正常流量返回给源站，从而确保源站业务可持续和稳定访问。

同时高防 IP 服务和云盾 Web 应用防火墙（WAF）、阿里的 CDN 是完全兼容的。因此最佳的部署架构是将高防 IP，CDN，和 WAF 结合在一起为用户的源站部署提供保护和加速：

- 高防 IP（入口层，DDoS 防护）-> CDN（静态资源加速） -> Web 应用防火墙（中间层，应用层防护）-> 源站（ECS/SLB/VPC/IDC…）

7.2.2 移动安全

移动安全（Mobile Security）为移动应用（APP）提供全生命周期的安全服务，能够准确发现应用的安全漏洞，恶意代码，仿冒应用等安全风险；通过应用加固和安全组件等功能，大幅提高应用反逆向、反破解能力。护航手机淘宝，支付宝等超级应用，历经多次双 11 实战考验。
移动安全服务提供以下功能：

1）**漏洞扫描**

该功能通过对 Android 应用进行扫描，快速定位漏洞位置，并提供完整修复方案。采用静态扫描和动态扫描结合的方式最大限度覆盖应用中潜在的安全漏洞：

- 静态扫描采用污点分析技术，通过精确回溯变量值，能够在寄存器的粒度对漏洞进行分析跟踪。
- 动态扫描采用模糊测试方法，通过还原真实的 Android 环境，得到精确结果。

2) 恶意代码扫描

该功能针对使用第三方插件、委托第三方开发或应用分发渠道型的企业用户，通过对 Android 应用进行扫描，准确识别植入到应用中的恶意代码。

- 自主研发的扫描引擎，在国际权威测试 AV-Test 中多次获得满分。
- 采用先进的机器学习算法和大数据技术，自动提取特征码。

3) 仿冒检测

该功能是企业品牌风险识别的重要工具，能够精准识别出仿冒 Android 应用的传播渠道，帮助企业遏制仿冒应用的传播，降低对品牌的伤害。覆盖范围包括：

- 全球 300 多个应用分发渠道。
- 网盘、论坛、企业网站、钓鱼网站等非典型渠道。

4) 应用加固

应用加固通过对 Android 应用进行重新编译、加壳保护、修改指令调用顺序等手段来增强应用反破解能力。应用加固功能注重加固强度与兼容性并重，避免一般加固功能盲目追求加固强度导致加固后完全不可用。 应用加固核心功能包括：

- 反主流静态分析工具: 能够有效的防止黑客通过 APKTool，dex2jar，JEB 等静态分析工具来分析应用的 java 层代码。
- SO 加壳: 通过对 SO 文件进行加壳保护，能够有效的防止恶意者通过 IDA，readelf 等工具对 SO 里面的逻辑进行分析。
- DEX 加壳: 通过对 DEX 文件进行加壳保护，以及动态运行时加载修复等技术手段，能够有效的防止黑客对 java 层代码的内存 dump。

- 常量加密: 对 DEX 文件中的明文常量字符串进行加密，运行时通过解密函数动态解密，增大了逆向分析的难度。
- Java 指令翻译: 修改 java 层业务逻辑的调用关系链，即便黑客得到 Java 层的代码，也无法完整的分析整个业务逻辑。
- Java 模拟执行: 通过将 DEX 文件中的指令抽离,并使用一个自定义的执行环境进行模拟执行，能够有效防止恶意者对 Java 层代码进行指令级别的 dump。

5) 安全组件

安全组件以客户端 SDK 的形式，保证应用完整、数据安全和执行环境可信，针对性解决移动应用的常见问题如外挂、重打包、网络请求仿冒、机密数据泄露、核心逻辑破解、运行环境不可控等。安全组件提供的核心功能包括:

- 安全存储: 安全存储功能在安全沙箱内实现了对于用户数据的安全加密与本地存储，保护用户的隐私数据不被泄露。
- 安全加密: 安全加密功能在安全沙箱内实现密钥管理与加解密过程，保证密钥的安全性。
- 安全签名: 安全签名功能在安全沙箱内实现了客户端请求的签名处理，保证客户端与服务端通信请求不被伪造。
- 模拟器检测: 检测应用是否运行在模拟器上，防止被黑客动态调试破解，进而引发刷单、抢红包等业务安全问题。
- 白盒加密：最新加密技术，采用复杂的数学运算取代密钥，即使应用被破解，也无法找到密钥。
- 白盒签名：使用白盒加密的技术进行签名，继承了白盒加密高安全性。

7.2.3 Web 应用防火墙

Web 应用防火墙(Web Application Firewall, WAF),基于云安全大数据能力实现，通过防御 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，过滤海量恶意访问，避免网站资产数据泄露，保障网站的安全与可用性。

Web 应用防火墙功能	子功能	特性描述
业务配置	支持协议	• 支持对网站的 HTTP、HTTPS（高级版及以上）流量进行 Web 安全防护。
Web 应用安全防护	常见 Web 应用攻击防护	• 防御 OWASP 常见威胁：SQL 注入、XSS 跨站、Webshell 上传、后门隔离保护、命令注入、非法 HTTP 协议请求、常见 Web 服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。

Web 应用防火墙功能	子功能	特性描述
		• 网站隐身：不对攻击者暴露站点地址、避免绕过 Web 应用防火墙直接攻击。 • 0day 补丁定期及时更新：防护规则与淘宝同步，及时更新最新漏洞补丁、第一时间全球同步下发最新补丁，对网站进行安全防护。 • 友好观察模式：针对网站新上线的业务开启观察模式、对于匹配中防护规则的疑似攻击只告警不阻断、方便统计业务误报状况。
Web 应用安全防护	CC 恶意攻击防护	• 对单一源 IP 的访问频率进行控制、重定向跳转验证、人机识别等。 • 针对海量慢速请求攻击、根据统计响应码及 URL 请求分布、异常 Referer 及 User-Agent 特征识别，结合网站精准防护规则进行综合防护。 • 充分利用阿里云大数据安全优势、建立威胁情报与可信访问分析模型、快速识别恶意流量。
Web 应用安全防护	精准访问控制	• 提供友好的配置控制台界面，支持 IP、URL、Referer、User-Agent 等 HTTP 常见字段的条件组合，打造强大的精准访问控制策略，可支持盗链防护、网站后台保护等防护场景。 • 与 Web 常见攻击防护、CC 防护等安全模块打造多层综合保护机制、轻松依据需求，识别可信与恶意流量。
Web 应用安全防护	虚拟补丁	• 在 Web 应用漏洞补丁发布和修复之前，通过调整 Web 防护策略实现快速防护。
管理	攻击事件管理	• 支持对攻击事件、攻击流量、攻击规模的集中管理统计
可靠性	支持负载均衡	• 以集群方式提供服务，多台机器负载均衡（多种负载均衡策略）
可靠性	支持平滑扩容	• 可根据实际流量情况，缩减或增加集群机器的数量，进行服务能力弹性扩容

Web 应用防火墙功能	子功能	特性描述
可靠性	无单点问题	• 单台机器宕机或者下线维修，均不影响正常服务。

WAF 的工作方式是通过修改 DNS 记录，将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测，过滤，清洗后再代理转发到应用服务器，完成整个 WEB 应用防护。

7.2.3.1 最佳实践

- **配置源站 ECS 安全组或 SLB 白名单,可以防止黑客直接攻击源站 IP**
  注意：源站保护不是必须的，不配置不会影响正常业务转发，但不做源站保护可能导致攻击者在源站 IP 暴露的情况下绕过 WAF 防护直接攻击源站。

- **使用 WAF 来防止敏感信息泄露**
  防泄漏功能主要覆盖包括网站存在敏感信息泄漏，尤其是手机号、身份证、信用卡等信息的过滤。本功能可以防御 URL 未授权访问；通过越权查看漏洞访问；网页存在敏感信息被恶意爬虫爬取访问等场景。

- **使用 WAF 有效防御 WordPress 反射攻击防御**
  WAF 高级版及以上版本用户可以通过精准访问控制规则有效防御 WordPress 反射攻击。

7.2.4 安骑士（主机安全）

安骑士是一款主机安全软件，通过安装在云服务器上的轻量级软件，与云端安全中心的联动，提供漏洞管理、基线检查和入侵检测等功能，帮助客户看清楚“系统弱点”，查出来“入侵事件”，加快事件“响应速度”。

1) 漏洞管理

综合多套扫描引擎（网络端、本地端、PoC 验证），全面批量检测出系统存在的所有漏洞，提供一键修复、生成修复命令、一键批量验证功能，实现漏洞管理的闭环。

- **系统软件 CVE 漏洞**
  通过检测服务器上安装软件的版本信息，与 CVE 官方的漏洞库进行匹配，检测出存在漏洞的软件并给用户推送漏洞信息（可检测如：SSH、OpenSSL、Mysql 等软件漏洞）

- **Windows 系统漏洞**

通过订阅微软官方更新源，若发现用户服务器存在高危的官方漏洞未修复，将为用户推送微软官方补丁（如“SMB 远程执行漏洞”等。注意系统将只推送高危漏洞，安全更新和低危漏洞需要用户手动更新）

- **Web 漏洞**
  通过网络端 Web 扫描完成，可检测 SQL 注入、XSS 等业务逻辑漏洞
- **CMS 漏洞**
  共享阿里云安全情报源，通过目录及文件的检测方案，检出 Web-CMS 软件漏洞，并给用户提供云盾自研补丁（可修复如：Wordpress、Discuz 等软件漏洞）
- **其他高危漏洞**
  可检测出配置型、组件型的漏洞，无法通过版本匹配和文件判断的漏洞（如：redis 未授权访问漏洞等）

2) 基线检查

- **账户安全检测**
  深度检测服务器上是否存在黑客入侵后留下的账户，以及影子账户、隐藏账户和克隆账户。
- **弱口令检查**
  收集常用的弱口令字典，检测 SSH、RDP 等服务是否使用了弱密码。
- **配置风险检测**
  对常见登录配置、进程配置、注册表配置进行检查，以达到企业级服务器安全准入标准。

3) 入侵检测

- **异地登录提醒**
  记录所有登录记录，对于非常用登录的行为进行实时提醒，可自由配置常用登录地。
- **暴力破解**
  对非法破解密码的行为进行识别，并上报到阿里云处罚中心进行拦截，避免被黑客多次猜解密码而入侵。
- **网站后门查杀**
  自研网站后门查杀引擎，拥有本地查杀加云查杀体系，同时兼有定时查杀和实时防护扫描策略，支持常见的 php、jsp 等后门文件类型
- **主机异常检测**
  对反弹 Shell、对外 DDoS、挖矿等恶意进程，以及 C&C 肉鸡检测、恶意源下载等异常连接进行实时检测和告警

7.2.5 态势感知

态势感知区别于传统 IDC 和 SIEM（仅做了被识别的告警事件关联），是从海量的原始数据中分析信息并通过机器学习的模型完成对安全事件过程的完整还原 。同时，态势感知聚焦在“敌我态势”，对敌方的实体（黑客本人，黑客组织）进行长期的威胁情报监控和行动点技术手段观测，对我方薄弱环节进行实时感知，对安全决策具有重要参考意义。

态势感知利用大数据技术，从攻击者的角度，有效捕捉高级攻击者使用的 0day 漏洞攻击、新型病毒攻击事件、和正在发生的安全攻击行为有效的展示，帮助云上租户实现云上业务安全可视和可感知。

态势感知具有以下功能：

- **安全告警集中化**
  快速了解云上业务的安全态势，如攻击，漏洞，入侵，防御效果，自身业务弱点，主机对外提供服务的安全状态等态势。

- **安全事件关联调查**
  安全事件的自动化分析，对历史事件回溯关联，帮客户发现事件的成因，过程，目的，对黑客行为进行全链路取证。

- **漏洞扫描和风险评估**
  资产暴露面分析和暴露风险评估，并支持 web 漏洞，主机漏洞，配置隐患，弱口令的实时检测。

- **安全可视化操作**
  最多 10 块电视屏幕进行安全可视化展示，是企业向上汇报，或接受参观的最佳实践。

- **实时日志检索**
  支持逻辑检索，支持 50 个维度的数据逻辑组合，日志类型：HTTP 流量，网络 session 连接，DNS 解析日志。

7.2.5.1 最佳实践

阿里云云盾-态势感知拥有资产管理、安全监控、入侵回溯、黑客定位、情报预警等功能特性。在以下场景建议使用态势感知为用户的云上业务提供安全天生可视和可感知。

- **安全态势感知**

  全面了解云上业务的安全态势，如攻击情况，漏洞情况，入侵情况，防御效果，自身业务弱点，主机对外提供服务的安全状态等。态势感知可提供网络攻击和主机攻击识别，网络异常连接检测，APT 攻击识别，业务层安全威胁识别，以及安全日报发送等功能。

- **入侵行为对策**

  当用户的云上业务遭到入侵，如主机负载突然增加，收到告警短信主机 ECS 被入侵；或存在对外攻击行为，或网站页面出现各种恶意广告链接；或数据被加密，黑客要求给比特币赎金时，态势感知可提供以下功能：

  - 入侵检测：可识别 WannaCry 勒索软件，后门 shell，一句话木马，软件病毒，主机连接中控源等数十种入侵行为
  - 入侵行为分析：如分析入侵原因，入侵过程，黑客全链路行为取证
  - 安全事件详情：如 DDoS 攻击协议分析，后门地址，进程地址，攻击防御效果

- **日志分析**

  态势感知提供全 SaaS 化的日志检索平台，免安装免维护，即开即用，支持逻辑（布尔表达式）检索，支持 50 个维度的数据逻辑组合，秒级出结果的检索引擎等功能来达到以下效果：

  - 日志分析：通过日志证据进行调查，评估资产受损范围和影响
  - 操作审计：对主机服务器的操作日志进行审计，对高危操作做排查
  - 业务统计：对 web 访问日志进行统计和分析，追踪来访者的环境和状态

- **大屏实时监控**

  态势感知为用户提供 9 块可视化大屏界面，可实时监控云上安全态势，提升团队工作效率，并进行对外形象展示和汇报。

- **代码外泄感知**

  态势感知情报采集系统，可以通过网络爬虫，抓取代码托管网站，对企业相关的情报进行实时监控和通知，避免了企业因为管理问题导致的数据外泄（如公司源码上传至 Github 等代码托管平台，导致企业的数据库连接地址和密码，服务器登陆密码，在代码中直接外泄）。提供企业客户相关的情报内容，包括数据泄露情报，用户名密码泄露情报，暗网相关情报，IM 群攻击预谋情报等。

7.2.6 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，邀请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。相比传统渗透测试，先知具有测试效率高、测试人员多、测试效果好、性价比高等优势。

先知平台可以帮助企业及时发现现有业务的安全问题，包括业务逻辑漏洞、权限问题等安全工具无法有效检测的漏洞等，尽早的发现存在的漏洞可以有效的减少公司可能的损失。先知平台会为所有入驻企业的漏洞严格保密，从而避免漏洞被恶意宣传。

先知平台提供以下服务：

- **实时安全测试和漏洞收集**
  先知平台可以帮助企业及时发现现有业务的安全问题，包括业务逻辑漏洞、权限问题等安全工具无法有效检测的漏洞等，尽早的发现存在的漏洞可以有效的减少公司可能的损失。先知平台会为所有入驻企业的漏洞严格保密，从而避免漏洞被恶意宣传。测试发现的漏洞实时展示在控制台，方便客户最快速度响应漏洞。

- **漏洞生命周期管理服务，协助客户在最短时间内修复漏洞，及时对高危严重漏洞进行响应**
  阿里保障过 G20 的安全专家为用户量身定制测试范围、奖励计划、邀请测试人员进行测试；并为用户提供漏洞修复建议、漏洞复测服务及定期的漏洞报告。

- **可信众测**
  阿里云培训并授权合作伙伴测试；提供 VPN 及测试行为审计，与国家信息技术安全研究中心合作，权威可靠。安全测试过程透明、测试日志全部保留可追溯、提供测试过程审计报告。

- **国内最好的测试效果**
  截止到 2017 年 9 月，先知平台上的测试人员平均为入驻的企业提交 91 个漏洞（目前这个数据还在持续上升），其中 50%的漏洞被确认（平均一次测试约 45 个）；严重、高危漏洞占比为 40%（平均一次测试约 18 个）。

7.2.6.1 最佳实践

- **金融行业**：行业内经常出现敏感信息泄露的情况，被监管部门通报批评、责令整改。可采购先知提前发现能导致敏感信息泄露的漏洞。

- **视频直播行业**：行业内经常主播信息或其他敏感信息被泄露，流入黑产、被黑产骚扰用户的情况；另外黑客可以无限制刷礼物、开关房间；利用漏洞薅企业营销活动的羊毛，浪费企业的营销资源。可采购先知提前发现能导致敏感信息泄露、业务资损的漏洞。

- **政府/央企客户**：数据泄露会引发公信力危机。可采购先知提前发现能导致敏感信息泄露的漏洞。

- **媒体/社区客户**：行业内经常出现某站被黑客漏洞利用成功后，发布不当内容，承受巨大的监管压力。客户可采购先知提前发现能导致业务或数据被篡改的漏洞。

7.2.7 云盾混合云

云盾混合云是云盾的线下输出版本，完全部署在客户本地，实时从云端获取威胁情报，本地数据不会上传到阿里云。能够在用户自有 IDC、专有云、公共云、混合云等多种业务环境为用户建设涵盖网络安全、应用安全、主机安全、安全态势感知的全方位互联网安全攻防体系。

云盾混合云提供以下功能：

1) 态势感知

- **安全监控**
  全面包含企业漏洞监控、开放端口监控、黑客入侵监控、web 攻击监控、DDoS 攻击监控、威胁情报监控、企业安全舆情监控等安全态势。
- **入侵分析**
  通过建模分析方法，从流量特征、主机行为、主机操作日志等获取关键信息，识别无法单纯通过流量检测或文件查杀发现的入侵行为。
- **威胁分析**
  借助阿里云端分析模型输入并结合情报数据，发现业务当前攻击威胁来源和行为，评估威胁程度。
- **弱点分析**
  扫描 SQL 注入、XSS 等各种 Web 漏洞和第三方开源程序漏洞，并对主机 ECS 漏洞、配置项问题做到实时监控与发现。
- **安全数据运营**
  建立用户自控的安全数据分析引擎，用户可利用收集的泛安全数据与云端情报进行数据关联分析，进一步增强场景化的安全态势感知能力。

2) DDoS 防御

- **双向全量流量 DDoS 检测能力**
  同时对出方向、入方向流量同时进行全量流量的 DDoS 攻击检测，不仅能够发现外对内的攻击行为，也能发现内部被控制的肉鸡信息。检测类型包括 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood、SSDP Flood、DNS Flood、HTTP Flood 等。
- **海量 DDoS 清洗检测/清洗能力**

结合云端高防 IP 资源，可提供 1000G + 的 DDoS 清洗能力。

3) 入侵防御

- **检测/防御 OWASP 常见威胁**
  针对 GET、POST 常见 HTTP 请求，进行 SQL 注入、XSS 跨站、Webshell 上传、命令注入、远程文件包含、路径遍历、常用 Web 服务器漏洞攻击等安全防护。

4) 主机防护

- **登录安全，识别异常和非法登录**
  基于登录记录，对非常用登录地、登录源 IP 的行为进行实时提醒，并针对非法暴力密码的行为进行识别，防御暴力破解攻击。
- **网站后门木马查杀**
  基于阿里云自研的后门查杀引擎，定时查杀和扫描本地文件，发现后门后立即预警/清除。
- **补丁管理**
  能够针对常见 Web 软件漏洞、重要 Windows 操作系统漏洞进行一键发现、修复及回滚，避免黑客利用。
- **安全运维**
  支持远程脚本执行，用户可通过安全运维通道实现 Linux 服务器的 shell 脚本、Windows 服务器的 dos 命令的批量下发执行。

7.2.8 安全管家

安全管家服务是安全代维托管服务。该服务由阿里云云盾安全技术专家团队，为企业客户提供私家定制的安全防护策略优化、重大活动保障、人工值守等服务，让企业客户在日益严重的安全攻击下高枕无忧。

安全管家服务包括以下服务内容：

1) 咨询与方案设计

- 调研用户云上业务，分析用户云上系统安全状况；
- 基于最佳安全实践，结合云上业务现状，量身定制云安全保障体系；
- 建立 VIP 专属钉钉群，随时指导用户安全建设与运营。

2) 评估与加固指导

- 全面评估客户云上业务的资产信息、漏洞信息、威胁信息；
- 建立资产的分类、分级保护方案，安全效益最大化；
- 指导用户进行安全风险管理，合理控制安全风险。

3) 安全漏洞管理

- 定期扫描系统、应用层安全漏洞，及时发现安全隐患；
- 漏洞修复指导，保证漏洞修复效果；
- 高危 0day 漏洞预警，第一时间了解漏洞信息，防患于未然。

4) 安全威胁管理

- 自动监控客户安全攻击态势，高危攻击及时告警；
- 定期分析安全攻击态势与安全趋势，指导安全建设方向；
- 根据安全威胁信息及时调整安全防御策略。

5) 云盾产品支持

- 协助用户进行云盾产品部署，实现产品的快速上线；
- 根据业务特点优化云盾产品策略，防护效果最大化；
- 定期分析云盾产品使用效果，安全态势一目了然。

6) 安全应急响应

- 快速响应、及时处置，将黑客攻击的影响降到最低；
- 分析黑客入侵手法与入侵后行为，评估入侵损失；
- 提供安全加固与安全防范指导，防止重复发生安全事件。

7.2.8.1 最佳实践

云上安全保障需要采取技术加管理相结合的方式才能取得效果，在缺乏专业安全人员的情况下，安全建设是很难取得理想效果的。

安全管家服务由经验丰富的安全专家提供的专业安全管理服务，在用户投入安全建设之前， 建议客户首先通过安全管家服务进行安全咨询，由安全专家来帮助定制安全防护方案，并根据方案进行安全建设，即能获得良好的安全保障效果，也能节约安全投入。

安全管家服务同时也提供包括安全检测扫描、安全产品托管、安全加固、定期巡检、安全应急响应等一系列服务内容，能够通过服务从技术、产品、管理等角度提升客户系统的整体安全防御能力和运营管理能力；帮助客户更好地发现安全隐患，及时改进安全措施，防御黑客攻击和破坏，保障客户业务的稳定运行。

7.2.9 数据风控

数据风控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，解决解决账号注册、认证、交易、运营、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。

数据风控服务具备以下功能：

1) 验证码服务

提供滑动验证码服务，通过生物特征判定操作计算机的是人还是机器，从而取代传统验证方式。

- WEB 网页：页面引入 JS 脚本，服务端调用验证码 API 获得校验结果。
- 移动端 HTML5 页面：页面引入 JS 脚本，服务端调用验证码 API 获得校验结果。
- Android/iOS： 客户端集成 SDK 组件，服务端调用验证码 API 获得校验结果。

2) 防垃圾注册

阿里云提供垃圾注册防控服务，其中包括用户信息有效性验证，图形验证码防批量注册，实时风险处理服务等功能。通过对用户的信息，行为，软硬件环境信息，和设备指纹等综合信息来判定用户注册账户的风险程度，并提供多样化的功能进行验证和处理。

- **信息有效性验证**：对用户提交的邮箱和手机等信息进行有效性验证，确保信息真实可信。包括但不限于邮箱激活、手机短信验证、语音下行等验证功能
- **图形验证码服务**：通过风控模型智能分析，可以动态选择输出图形验证码服务，有效控制批量攻击规模
- **实时风险处理服务**：基于阿里的黑名单数据和关系网络模型等识别结果，提供对高风险的垃圾账户进行实时拦截处理功能。

3) 防交易欺诈

阿里云提供防交易欺诈服务，对交易过程中出现的账户盗用，坏账资损，银行卡盗用，交易诈骗等欺诈行为进行有效防控。

- **用户分层模型**：基于阿里大数据，对不同的用户进行分层定义，可以选择与之对应权限、额度等。
- **多种验证功能**：通过多种方式，验证账户、银行卡等持有人身份，包括但不限于短信、语音下行、密码保护问题、Miro Charge、3DS 等。
- **风控智能引擎**：通过阿里自建的风控智能引擎，实时识别交易过程中的各种风险，及时介入处置，包括但不限于二次验证、KYC、拦截等，将风险影响控制到最低。

4) 活动防刷

在企业的运营活动中，如果有恶意用户通过虚假行为和作弊等手段批量的套取活动营销资金和物品等，就会造成正常用户无法享受权益和企业营销资金浪费，进而极大的影响运营活动的效果。阿里云提供活动防刷服务，使企业可以对这类作弊风险进行有效的防范。

- **活动评审**：对营销活动的方案设计提供专业的评审建议，避免出现原则性漏洞。
- **用户风险评估**：通过阿里海量数据，对每个用户进行风险评估（邮箱、手机、身份 ID 等）。基于不同的用户，可以设计活动准入和权益分级等限制。
- **防刷拦截活动资格**：通过生物特征判定操作计算机的是真实的用户，并及时拦截机器作弊行为，以防止批量作弊攻击。同时，通过对用户行为分析虚假操作可能性，取消作弊用户活动资格。

5) 实人认证

阿里云提供用户真实身份认证服务，为企业用户更高等级的业务发展提供实名制基础。实人认证服务提供有实名校验，生物识别，和风险防控的功能。

- **实名校验**：证件信息验证，核实身份证号码和姓名是否真实匹配。
- **生物识别**：通过人脸认证、视频验证，鉴别用户照片、视频是否本人。
- **风险防控**：基于风险记录，识别虚假认证的证件，手机，其它设备等等手段。

7.2.9.1 最佳实践

数据风控可以极大地减少业务中的用户异常行为，以登录为例：

- 在配置数据风控后，初始登录页面并不会出现任何可见的验证信息，减少了用户干扰。
- 当用户输入帐密进行登陆时，业务先通过业务风险防控进行风险判定：1）无风险，进入帐密校验等登录业务处理；2）有风险，返回登录页面，弹出验证码，进行风险验证拦截。

业务安全服务可以极大地减少企业在各个业务中的风险，保障企业健康发展：

- 在部署垃圾注册防控后，用户基本信息的真实性有了保障。对于批量攻击本服务提供图形验证码拦截，同时确保正常用户的操作流程不会被打断。
- 当用户进行业务操作时，风控智能引擎会提供实时分析保护：
    - 如果有风险出现，通过短信验证等方式确保操作安全。
    - 如果没有风险，用户操作不被打扰，同时积累数据记录用户成长，享受更多权益。

7.2.10 内容安全

内容安全基于深度学习技术及阿里巴巴多年的海量数据支撑， 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，解决广告推广，谩骂等用户体验痛点，而且能大幅度降低人工审核成本。

内容安全服务提供以下功能：

1）站点监测服务：

内容安全针对阿里云网站类用户，提供信息内容安全检测及管控服务。当用户的网站内容涉及违规信息时，会提前预警，并提供违规网页地址及快照查看功能，免去用户手动检测网站内容的负担 。

2）OSS 图片鉴黄服务：

通过人工智能技术对用户存储在 OSS 上的图片进行识别以及色情程度的打分，并提供便捷易用的结果展示平台。通过删除、忽略等快捷操作，方便用户对图片作快速处理，减少审核人力，有效降低涉黄风险。

3）内容检测 API：

内容检测 API 基于阿里巴巴多年的技术沉淀和海量的数据支撑，提供文本、图片、视频等多媒体内容安全检测的开发接口服务。该服务可不依赖于阿里云其他服务，只要是公网可访问的图文信息均可过滤。

- 图片智能鉴黄服务
  通过神经网络算法和实时更新的亿级图像样本库，可对图片和视频进行识别以及色情程度量化。智能学习用户审核标准，逐渐降低人工审核成本。
- 视频智能鉴黄服务
  采用截帧画面、声音、文字多维度综合决策视频结果，最大限度避免因为截图模糊而导致误判。并且在结果中返回证据画面，协助审核人员判断。
- OCR 图文识别服务
  拥有国内顶尖 OCR 算法团队，上亿字符样本积累，可精准定位图片中文字位置，准确识别斜排字，艺术字等字体。
- 图片暴恐涉政识别服务
  深度学习算法结合独有的情报、舆情、预警和分析体系及实时更新的样本图库，能够快速定位暴恐旗帜、人物和场景以及敏感政治人物。
- 图片敏感人脸识别服务
  提供包括政治人物、敏感人物、以及名人明星等人物的面部识别，能够避免业务的违规和侵权风险。
- 图片广告识别服务
  有效识别带二维码的广告图片，并且采用独创的牛皮癣算法，能够通过判断图片中文字是否后期加入来有效识别广告图片。
- 文本反垃圾
  采用 NLP 自然语言理解算法有效识别色情、暴恐涉政、广告、辱骂等文本垃圾，并且能够结合行为策略有效管控灌水、刷屏等恶意行为。

7.2.11 加密服务

加密服务（Alibaba Cloud 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。

云盾加密服务具有以下特点：

1) 安全的密钥存储

使用防篡改硬件密码机保护客户密钥。

2) 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。

3) 安全的加密算法

全面支持国产算法以及部分国际通用密码算法，满足用户各种加密算法需求。

- 对称密码算法：支持 SM1、SM4、DES、3DES、AES
- 非对称密码算法：支持 SM2、RSA（1024-2048）
- 摘要算法：支持 SM3、SHA1、SHA256、SHA384

4) 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。

5) 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。

6) 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。

7) 金融行业支持

符合中国人民银行标准和规范的金融行业定制加密需求，全面支持金融支付领域的加解密需求。

- PIN 码的产生/加密/转加密/验证等
- ARQC 的生成/验证、脚本加密、脚本 MAC 等

- MAC1 计算及验证、MAC2 计算及验证、TAC 验证等
- 外部认证、更新密钥、内部认证等
- 敏感数据加密、转加密、报文 MAC 计算及验证等
- CVV/CVN 产生及校验、PVV/PVN 的产生及校验

7.2.11.1 最佳实践

加密服务的主要使用场景包括云上金融业务系统、政务系统、企业财务系统等敏感数据保护。

- 金融业务系统的加密服务使用场景主要包括银行卡号，身份证，PIN 码等敏感信息的存储。

- 政务系统的加密服务使用场景主要包括涉密业务的敏感信息存储。

- 企业财务系统的加密服务使用场景主要包括合同，财务等敏感信息存储。

7.2.12 证书服务

证书服务（Alibaba Cloud Certificates Service），可以在云上签发 Symantec、GlobalSign、GeoTrust 证书，实现网站 HTTPS 化，使网站可信，防劫持、防篡改、防监听。并对云上证书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。

证书服务提供如下功能：

- 实现网站 HTTPS 化，加密用户与网站间的交互访问，强化网站用户侧可信展示程度，防劫持、防篡改、防监听。

- 提供受信任 CA 认证中心颁发的数字证书。经过 CA 认证中心审核认证后，颁发各等级的数字证书。

- 提供证书生命周期管理功能，可以在多个渠道下统一管理数字证书的功能，用户可以在统一的平台下查看各个云业务所使用的证书情况以及管理自己的证书订单。

- 提供在云平台上一键部署数字证书到其他已经开通的阿里云产品（如 CDN、SLB、高防和 WAF）的功能，帮助用户实现低成本部署数字证书。

- 按照标准的证书吊销流程，经过 CA 认证中心审核后，安全地吊销服务器数字证书。

7.2.12.1 最佳实践

通过 SSL 数字证书部署在 WebServer 或者其它云资源（SLB、CDN 等等 ）上，实现网站的 HTTPS 访问，大幅提高了站点的安全性，使得用户在机场、咖啡馆、网吧等的公开环境也能实现网站的安全、可信访问，降低的敏感数据泄漏的风险。

证书服务更贴合阿里云用户购买习惯，提供简洁的证书购买流程的同时，也提供了安全的证书和密钥存储方案，避免还需使用其他密钥存储方案的负担。

证书服务中的证书和阿里云产品联通，实现一键部署数字证书到阿里云产品，为用户免去了繁琐的部署过程。

7.2.13 堡垒机

云盾堡垒机是一款专门针对云上 IT 运维人员、运维行为进行管理和控制的安全产品。主要解决多人使用相同 ECS 账号登录 ECS，难以定位责任人；ECS 密码管理复杂，密码泄露严重；运维人员的操作不透明，越权导致数据泄漏；法律法规要求严格，云安全运维管理风险突出等云运维安全问题。

堡垒机提供以下功能：

1) 操作审计

多面记录运维人员的操作行为，作为追溯的保障和事故分析的依据。

- **运维操作记录**
  详细记录操作失误、恶意操作、越权操作。
- **Linux 命令审计**
  可提取命令字符审计，命令定点回放
- **Windows 操作录像**
  远程桌面的操作，全程录像，包括：键盘操作、鼠标操作、窗口打开等
- **文件传输审计**
  支持远程桌面文件传输、FTP/SFTP 的原文件审计

2) 权限管控

进行账号管控和权限组管理，分职权进行人员和资产管理。

- **账号管控**
  确保人员运维账号唯一性，解决共享账号、临时账号、滥用权限等问题

- **权组管理**
  按照人员、部门组织、资源组，建立人员职责与资源分配的授权管理

3) 安全认证

引入多因子认证机制，防止运维人员身份冒用和复用。

- **账号多因子认证**
  支持多因子认证机制，通过短信认证、动态令牌等技术，控制账号密码泄露风险

4) 高效运维

从架构、工具、ECS 接入等多方面提升运维效率。

- **C/S 架构运维接入**
  支持 SSH、RDP、TELNET、SFTP 协议
- **支持各种运维工具**
  PuTTY、SecureCRT、Xshell、WinSCP、mstsc 等
- **ECS 高效接入**
  一键同步并导入云服务器 ECS

7.2.14 数据库审计

云数据库审计服务是一款专业、主动、实时监控数据库安全的审计产品。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。云数据库审计支持 RDS 云数据库、ECS 自建数据库，将数据库监控、审计技术与公有云环境相结合，为云端数据库提供安全诊断、维护、管理能力。

云数据库审计服务符合等级保护三级标准，帮助用户满足合规性要求。政策相关要求：

1. 中国银监会、工业和信息化部、公安部、国家互联网信息办公室制定了《网络借贷信息中介机构业务活动管理暂行办法》中第十八条指出需要进行信息安全检查和审计。
2. 符合网络安全法
   - 第二十一条 （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
   - 第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

1) 用户行为发现审计

- 关联应用层和数据库层的访问操作
- 可溯源到应用者的身份和行为

2) 多维度线索分析

- 风险和危害线索：高中低的风险等级、SQL 注入、黑名单语句、违反授权策略的 SQL 行为
- 会话线索：根据时间、用户、IP、应用程序、和客户端多角度分析
- 详细语句线索：提供用户、IP、客户端工具、访问时间、操作对象、SQL 操作类型、成功与否、访问时长、影响行数等多种检索条件

3) 实时告警

异常操作、SQL 注入、黑白名单实时告警

- 异常操作风险：通过 IP、用户、数据库客户端工具、时间、敏感对象、返回行数、系统对象、高危操作等多种元素细粒度定义要求监控的风险访问行为
- SQL 注入：系统提供了系统性的 SQL 注入库，以及基于语义的 SQL 注入描述，发现异常立即告警
- 黑白名单：提供准确而抽象的方式，对系统中的特定访问 SQL 语句进行描述，使这些 SQL 语句出现时能够迅速报警

4) 详尽报表

针对各种异常行为的精细化报表：

- 会话行为：登录失败报表、会话分析报表
- SQL 行为：新型 SQL 报表、SQL 语句执行历史报表、失败 SQL 报表
- 风险行为：告警报表、通知报表、SQL 注入报表、批量数据访问行为报表
- 政策性报表： 塞班斯报表

8 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。

9 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。
2017 年 9 月：3.0 版本，阿里云安全架构和产品相关全面描述更新。