ALIBABA CLOUD

阿里云

安全白皮书

2020 年 1 月

版本：4.1

阿里云

法律声明

阿里云提醒您在阅读或使用《阿里云安全白皮书》（“本文档”）之前仔细阅读、充分理解本法律声明（“本声明”）各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本文档内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的本文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的本文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 本文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“Alibaba Cloud”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

目录

1. 概述

数据安全和用户隐私是阿里云最重要的原则。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机密性、完整性、和可用性。

本白皮书介绍了阿里云的公共云安全体系，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产品服务
- 阿里云的云上数据安全体系

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：阿里云要保障云平台自身安全并提供安全产品和能力给云上客户；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）和物理设备（包括计算、存储和网络设备）的物理和硬件安全，并负责运行在飞天分布式云操作系统之上的虚拟化层和云产品层的安全。同时，阿里云负责平台侧的身份管理和访问控制、监控和运营，从而为客户提供高可用和高安全的云服务平台。

客户负责以安全的方式配置和使用各种云上产品，并基于这些云产品的安全能力以安全可控的方式构建自己的云上应用和业务，保障云上安全。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，保护客户的云上业务和应用系统。阿里云建议客户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云上应用和业务系统提供全面的安全防护。

安全责任共担模式之下，阿里云保障云平台层面的安全并提供一方集成的云产品安全能力

和云盾安全服务给客户使用，让客户降低对安全性的顾虑，更专注于核心业务发展。请注意，专有云的安全责任模型与上述公共云模型有所不同，具体请参见《阿里云专有云安全白皮书》。

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，包括但不限于：

- 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，包括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，包括但不限于：

- 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。
- 为客户提供安全的硬件基础设施和设备。
- 为客户提供云上账户安全管理能力，包括但不限于云账号支持主子账号、多因素认证、分组授权、细粒度授权、临时授权等账户安全管控手段。
- 为客户提供安全监控和运营能力，包括安全审计手段。
- 为客户提供数据加密手段。

- 为客户提供各类安全服务。
- 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

客户应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。

客户应对云上产品进行安全配置管理，保障云上业务的基础安全和数据安全。请注意，客户在阿里云上如果使用的是基础类服务（例如，阿里云提供的云服务器（ECS）），那么相关服务实例完全由客户控制，客户应管理实例并进行安全配置，并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；但如果客户在阿里云上使用的是非基础类服务（例如，平台类或云原生类等服务），那么客户的安全责任会相应上移，不再需要关心如何维护实例，也不需要关心操作系统的补丁升级、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，MaxCompute 服务为客户提供了不同维度的权限控制能力，客户只需要根据业务需求妥善配置类似产品中的安全功能即可。

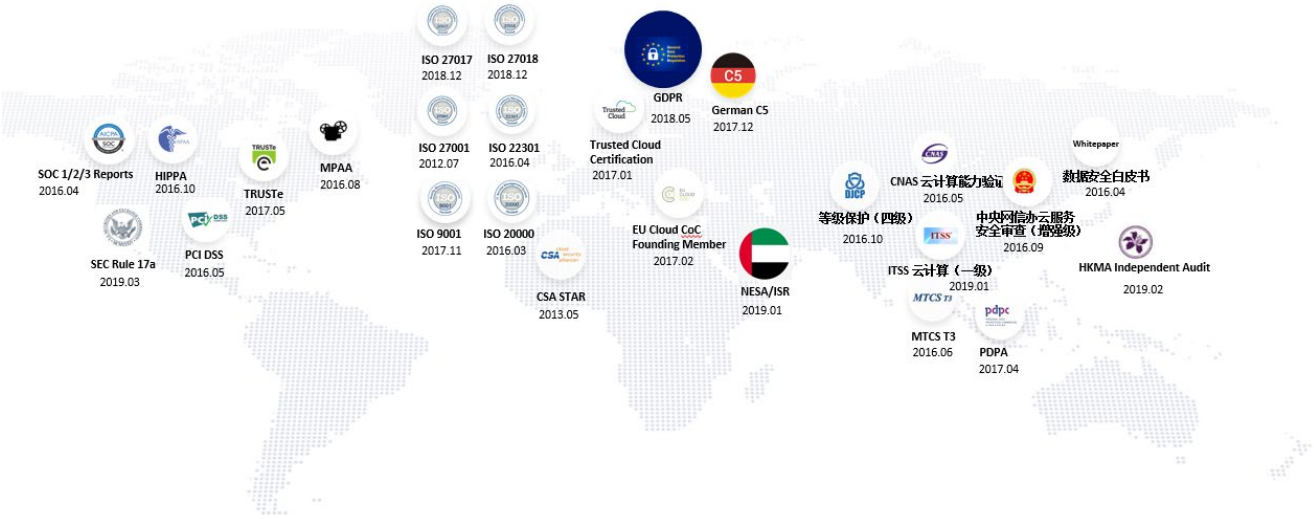
客户也应使用阿里云产品的原生加密能力或云盾加密服务对敏感数据进行加密，并对加密密钥进行妥善管理（例如，使用密钥管理服务（KMS）的托管 HSM 能力）。

客户在阿里云上的应用和业务系统需要通过使用云盾安全服务以及安全生态提供的第三方安全产品来保护。客户也可使用云盾安全服务对云上应用和业务系统，包括云上资源进行有效的安全监控和运营。在账户安全层面，客户应保护阿里云账户认证凭证（例如，开启多因素认证功能），并在账号设置上遵循最小权限原则，通过如群组授权等手段实现职责分离。客户也应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，对账号操作进行审计。

整体而言，阿里云为客户提供各种安全能力和产品服务，而客户负责正确的配置和使用上述安全能力和服务来构建其云上应用和业务系统的安全。

3. 安全合规

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计算服务相关的标准制定并贡献最佳实践，通过独立的第三方验证阿里云如何符合标准。



至目前为止，阿里云先后通过了海内外数十家权威机构的认证和审计，下表中列出了阿里云具有的合规资质。

资质		简介
全球认可	ISO 27001	ISO 27001 信息安全管理体系国际认证是被广泛采用的全球安全标准，阿里云作为首家在国内审核通过此项认证的云计算服务提供商，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。

	ISO 27017	ISO 27017 提供了一套使用云服务的相关信息安全控制指引，包含与 ISO/IEC 27002 相关控制的额外实施指引，以及与云服务特性相关的额外控制以及相应实施指引。
	ISO 27018	ISO 27018 针对云服务商对云上个人数据的安全防护国际标准认证，为云上个人身份信息处理者提供一套守则，以保护公共云中的个人身份信息（PII）不受侵犯，是目前国际上最权威、最严格、也是最被广泛接受和应用的信息安全体系认证。
	CSA STAR	CSA STAR 由英国标准协会（BSI）和国际云安全权威组织云安全联盟（CSA）联合推出，阿里云作为全球首家获得 CSA STAR 云安全金牌认证企业。
	ISO 9001	ISO 9001 质量管理体系用于证实组织具有提供满足用户要求和适用法规要求的产品能力的权威认证。
	ISO 20000	ISO 20000 是国际上首个公认的 IT 服务管理标准，阿里云是国内首家获得新版 ISO/IEC 20000-1:2011 认证的云计算服务商，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	ISO 22301 业务连续性管理体系是国际公认能够衡量企业服务连续性能力是否满足社会责任和客户承诺的唯一标准，阿里云通过全球首个最新版 ISO/IEC 22301 业务连续性国际认证。
	SOC1/2/3	SOC 报告是美国注册会计师协会创造的一套给服务提供商的报告称为：

		服务性机构控制体系鉴证（SOC - Service Organization Controls）报告。SOC 报告的目的是给服务提供商选项，方便他们提供更多的相关报告给客户。
国内权威	中央网信办云服务安全审查	阿里云电子政务云平台成为全国首批通过中央网信办云计算网络安全审查（增强级）的云计算服务。
	公安部网络安全等级保护 2.0	阿里云作为全国唯一一个云计算等级保护 2.0 示范单位，金融云是通过云计算等级保护四级测评的首个云平台，政务云是通过等保 2.0 国标测评的首个云平台。
	工信部云计算服务能力评估	阿里云（公共云和专有云）成为全国首批通过工信部云计算服务能力评估一级（最高级）的云服务商。
	云计算服务认证	阿里云云主机、对象存储、云数据库、内容分发等多款产品和服务获得可信云全国首批云服务认证，对数据可销毁性、数据可迁移性、数据私密性、数据知情权等进行了规范。
	大数据服务认证	阿里云大数据产品作为全国首批通过大数据系统通用规范最高等级测评，首批获得 CNAS 云产品（数加）国家实验室认证，多款产品达到业界最高大规模集群能力。
	安全服务能力认证	阿里云系列安全产品作为全国首家云计算安全综合防御产品获得公安部销售许可，并成为多行业云计算安全产品标准最佳实践。
	安全技术支撑	阿里云先后荣获 CNCERT 网络安全应急服务支撑单位（国家级）、CNVD

		（国家信息安全漏洞共享平台）技术组成员单位、国家网络与信息安全信息通报中心技术支持单位（多年优秀技术支持单位称号）、国家重大活动网络安全保卫技术支持单位等称号，成为为国家级安全工作提供技术支撑最多的云服务商。
行业及区域认可	C5	阿里云遵循 C5 标准，显示了云计算在控制和安全方面实现最高合规性的承诺，该标准不仅作为德国市场的基准，也越来越成为整个欧洲机构的基准。德国的客户可以利用 C5 审核来满足严格的本地要求，并使用阿里云服务来运行安全的工作负载。C5 主要面向专业云服务提供商，其审计人员和云服务提供商的客户。它有 17 个不同的控制要求，云提供商必须遵守或达到定义的最低标准。这是与德国公共部门合作的必要评估，并且越来越多地被私营部门采用。
	MTCS	新加坡认证机构 Certification International 向阿里云颁发了新加坡多层云安全 MTCS 最高安全评级 T3 认证。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（Infocomm Development Authority，IDA）发起，新加坡标准、生产力与创新局（SPRING Singapore）推出的云安全标准。其安全认证分为三个层次，其中第三级为最高、最安全。
	NESA/ISR	国家电子安全局（National Electronic Security Authority，简称 NESA）是阿拉伯联合酋长国（UAE）内，负责境内关键信息基础设施以及强化国家网络安全的政府机关。阿里云已依循该机关所制定的一系列信息安全指引，并完成 P1 级别的第三方合规审计。 信息安全规范（Information Security Regulation，简称 ISR）是由迪拜当

		地政府制定，此规范与国际标准 ISO27001 相似，囊括了数个信息安全领域，并依照迪拜政府的需求纳入特别适用于当地的信息安全要求规范。阿里云已由合格的第三方完成合规审计，确认阿里云遵循 ISR 相应的规范与具体要求。
	PCI-DSS	PCI-DSS 是一项重要的支付卡业务质素认证，评测支付卡数据的安全性，包括信用卡号、CVV2 号等，同时关注账号或密码传输与储存的安全性，阿里云是全国首家通过 PCI-DSS 安全认证的云计算服务商。
	SEC Rule-17a	阿里云完成了对象存储服务 OSS 解决方案能力相关的评估，以满足美国证券交易委员会（SEC）规则 17a-4(f)和金融业监管局（FINRA）颁布的经纪人经销商媒体要求规则 4511。通过这项评估阿里云能够服务更多国际金融行业客户，因为这些要求被更广泛的被很多美国以外的国家所采用，作为一个产品的金融要求支持能力衡量的一部分。
	TRUSTe	阿里云国际站通过 TRUSTe 企业隐私认证，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	阿里云通过第三方评估，确保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 会员并得到 Trusted Cloud 的认证。
	EU Cloud Code of Conduct	阿里云作为欧盟云守则（EU Cloud Code of Conduct）的创始会员和大会成员，积极参与制定为符合 GDPR Article 40 要求下的欧盟云服务的

	云守则 创始会员	守则，与欧盟数据保护部门进行建设性的合作，以确保他们对 GDPR 的期望和未来指导在撰写守则的同时得到考虑。阿里云致力于为整个阿里云生态系统保持高水准的数据保护，并为整个科技行业的健康发展做出贡献。 阿里云支持提高云计算行业透明度，并帮助云客户了解云服务提供商如何解决数据保护问题。

3.1. 监管合规

阿里云积极履行法律法规及贯彻相关政策，推动企业利用云计算技术加快数字化、网络化、智能化转型，按照《网络安全法》相关要求，在企业内部建立云计算服务相关安全管理流程和制度，通过系统化的方式确保合规要求内部落地。

阿里云按照国家互联网信息办公室、国家发展和改革委员会、工业和信息化部和财政部联合发布的《云计算服务安全评估办法》要求，阿里电子政务云平台在 2016 年全国首批通过云服务审查增强级要求，为党政机关、关键信息基础设施运营者提供安全可控的云计算服务。

阿里云按照网络安全等级保护制度，不断提升云计算服务的主动防御、动态防御、整体防控和精准防护能力，在 2019 年 5 月等保 2.0 系列标准正式发布后，成为全国首家通过等保 2.0 正式标准测评的云服务商。

阿里云在自身云平台满足监管合规要求外，致力于帮助用户以更小成本、更快捷方式、更高安全防护能力达到监管合规要求，推出了系列合规解决方案。其中，在阿里云等保合规安全解决方案（https://www.aliyun.com/solution/security/compliance）中，一方面在等保要求中的安全防护、数据审计、数据备份、数据加密以及安全管理等方面提供完善的能力，另一方面通过甄选和联合各地服务质量优异的咨询和测评机构，提供一站式、全流程合规方案，大大降低用户运营单位的投入，帮助用户快速、省心的通过等保测评。

3.2. 个人信息保护

长期以来，阿里云坚持致力于保护每位客户的个人信息，保证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。与此同时，阿里云积极响应国家监管部门对企业承担个人信息保护责任的号召，持续完善内部的个人信息管理和保护体系。阿里云设置了专业的个人信息保护团队，在隐私权政策、用户权利保障等方面持续优化，建立了内部整体的数据安全管理体系，落地数据安全保护的核心技术，为用户个人信息提供了全生命周期的安全可靠的保护能力。

阿里云通过大量权威机构的认证证明个人信息保护能力/数据安全保护能力，详细信息请见ISO 27017、PCI DSS、可信云云服务数据保护认证等。阿里云将持续建设阿里云整体的个人信息保护管理体系，除了关注阿里云作为控制者角色时云平台自身的个人信息保护能力之外，会进一步投入力量建设阿里云作为数据处理者的角色时相应的产品/服务中的个人信息保护能力。

阿里云的隐私权政策可以在阿里云官网查看，同时所有历史的隐私权政策也都可在官网找到，详细信息请参见法律声明及隐私权政策（https://help.aliyun.com/document_detail/103075.html），有任何隐私相关的问题都可以通过阿里云的工单系统、在线或电话客服进行反馈。

3.3. 透明度

阿里云长期致力于通过多种渠道向客户透明云服务商相关的情况。

客户一般可通过阿里云的工单系统提出对阿里云相关的资质、说明报告等信息，对于客户合理的要求，阿里云均会及时响应客户的需求。同时，阿里云也在探索更多增加透明度的方式，通过将与特定客户相关的内部操作透传给客户的方式，进一步消除客户对阿里云内部“黑盒”的疑虑。这种突破了静态展示的界限而主动将动态的信息传递给客户的方式，将是阿里云“透明度”的长期方向。

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，国内外相关权威机构的认可的合规性；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。具体信息，请参见阿里云全球基础设施（https://m.aliyun.com/markets/aliyun/about/global）。

地域		可用区数量
中国大陆	华北 1	2

	华北 2	8
	华北 3	2
	华北 5	2
	华东 1	8
	华东 2	6
	华南 1	5
	西南 1	2
其它国家和地区	中国香港	2
	亚太东南 1	3
	亚太东南 2	2
	亚太东南 3	2
	亚太东南 5	2
	亚太南部 1	2
	亚太东北 1	2
	美国东部 1	2

	美国西部 1	2
	欧洲中部 1	2
	英国（伦敦）	2
	中东东部 1	1

5. 阿里云安全架构

阿里云安全架构

阿里云提供了五横两纵的 7 个维度的安全架构保障。两个纵向维度分别为账户安全（身份和访问控制），以及安全监控和运营管理。请注意这两个纵向包括了租户侧和云平台侧的不同实现。在五个横向维度中，包括了从最底层的云平台层面安全，到对外租户层面的基础安全、数据安全、应用安全和业务安全。

本章在介绍整体安全架构时，将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，包括云盾安全产品的相关信息。各产品的相关能力详情，请参见本白皮书相关章节内容。

5.1. 云平台安全

云平台安全中的架构层面包含了阿里云作为云平台默认提供的基础安全能力，尤其是两纵的云平台内部身份与访问控制以及云平台安全监控运营两个维度，是云平台内部自身的安全管理和运营，客户并不直接感知；与之相似，在物理安全、硬件安全和虚拟化安全层面，客户也无需任何设置即可享受阿里云本身的高安全等级能力；而云产品安全能力这一层包含了云平台在各个产品中为客户提供的安全能力和安全保障，其中部分能力（如租户隔离）是产品本身默认的保障，部分能力（如数据加密）是产品提供能力的同时需要客户的开启和正确设置。

5.1.1. 物理安全

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，其中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；当触发事件时，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，一旦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。

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。

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，具体请参见云平台安全-云平台内部身份和访问控制章节。

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 7*24 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 架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. 数据销毁

安全擦除

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。阿里云建立废弃介质上数据安全擦除流程，处置数据资产前，检查含有敏感数据和正版授权软件的媒介是否已被覆写、消磁或折弯等数据清除处理，且不能被取证工具恢复。当因业务或法律原因，不再需要某些硬拷贝材料时，将其物理破坏，或取得数据处理第三方的损坏证明，以确保数据无法重建。

云服务客户数据处置

阿里云在终止为云服务客户提供服务时，及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。阿里云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。

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。

5.1.1.5. 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。

5.1.2. 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

阿里云平台提供了以 Intel® Software Guard Extensions（Intel® SGX）可信执行环境作为基础的硬件可信执行环境。在加密计算的硬件可信执行环境中，可以通过软件建立一个可信执行环境，进而保护敏感数据（例如，加解密密钥）。由于加密计算的信任根基于处理器芯片，而非基于底层软件，因此所有加密信息只能在可信执行环境中计算和运行，从而提供基于硬件的高等级的数据保护能力。

5.1.2.3. 可信计算

阿里云在关键服务器上采用了系统可信和应用可信功能，通过度量和验证保证云平台运行环境的安全，以及通过对白名单应用的监测管理确保应用的运行安全。

系统可信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 以及 vTPM 技术对物理机、虚拟机上基础软件栈的启动过程进行度量，并通过可信服务对度量结果进行验证。被度量的基础软件包括了 BIOS、BootLoader、操作系统内核以及加载的系统模块和应用等。安全运维人员可以通过验证结果对系统可信状态做判断，并采取相应的安全应对措施（例如，重新安装正确的软件或业务迁移）。

应用可信通过对应用执行环节如进程启动、文件访问、网络访问等行为进行记录、分析，获取其行为白名单和模型，当应用在运行时通过动态度量采集到的应用行为，并将动态度量结果通过行为白名单验证来判断应用是否可信。安全运维人员可以通过验证结果对应用进行处理重新安装载正确的版本等。

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、安全加固、逃逸检测、补丁热修复、数据清零等五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，请参见云产品安全-弹性计算-ECS-租户隔离章节。

- 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。

- 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. 安全加固

安全加固是指通过各种技术手段减少虚拟化管理程序中可能的被攻击面。阿里云使用轻量

级和专门为云上场景开发的虚拟化管理程序（以 KVM 为基础的 Hypervisor），并在设计之初即做到软硬件场景结合，专注于只支撑垂直的云上基础设施的硬件虚拟化。同时，为减少可能受到 0day 漏洞的影响，阿里云虚拟化管理程序会在不影响功能和性能的基础上限制系统级别的动态函数库的调用。简而言之，阿里云会最大限度的从虚拟化管理程序中裁剪一些与云上设备无关的代码来降低攻击面，此外，所有虚拟化软件必须编译和运行在一个可信的执行环境上才能保障每个二进制文件在执行时不被恶意篡改和替换。阿里云采用了一系列可信计算技术来保障整个链路的安全，也有一整套完善的控制机制来保障这些虚拟化二进制文件不被外部恶意获取分析利用。

在此之外，阿里云还对虚拟化管理程序和宿主机 OS/内核级别进行相应安全加固。例如，对虚拟化管理程序在动态运行时进行降权，并阻止内核执行用户空间代码以增加逃逸后提权的难度；开启内存地址随机化特性，并开启内核符号限制访问功能和内存保护页功能以增加内存溢出类攻击的难度。阿里云不断引入新的安全特性到虚拟化管理程序和宿主机 OS/内核中，这其中包括内部研发的和外部开源社区的最新安全功能。

5.1.3.3. 逃逸检测

虚拟化层面的入侵事件主要体现为在虚拟机上的逃逸攻击，其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。

在阿里云平台中，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，且虚拟机无法主动探测自身所处的物理主机环境。此外，阿里云在 Hypervisor 层面会对虚拟机异常行为进行检测，例如对 Coredump 文件实时分析监控、对 Hypervisor 加载和执行可疑代码段进行实时检测、对虚拟机的系统函数调用和 VM Exit 异常行为进行审计、以及对宿主机的进程执行行为和网络行为等可能的异常场景进行实时监控和分析，

及时发现对虚拟化平台的恶意攻击事件。

当检测到恶意攻击时，阿里云会定位和处置发起恶意攻击的虚拟机，并对整个攻击链条进行及时的采样还原，并对找到的漏洞进行补丁热修复。

5.1.3.4. 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。

5.1.3.5. 数据清零

作为存储虚拟化的延伸，云用户实例服务器释放后，其原有的磁盘和内存空间将会被可靠的进行数字清零以保障用户数据安全。

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，其中包括计算类产品（如云服务器 ECS）、存储类产品（对象存储 OSS）、网络类产品（如专有网络 VPC）、数据库类产品（如云数据库 RDS）、大数据类产品（如大数据计算 MaxCompute）等。更多产品的安全特性和能力，请参见云产品安全章节。

5.1.5. 云平台内部身份和访问控制

5.1.5.1. 身份管理

阿里云针对正式员工、实习生、外包、合作伙伴等内部用户使用身份认证系统进行账号生命周期管理。所有用户按照“一人一账号”、“公私数据分离”原则进行账号分配和使用，账号一旦分配，不得共享账号并对账号做统一的登录管理、账号密码管理和访问控制。一旦内部用户离职、转岗或工作内容发生变更，其所使用或管理的各项账号资源，必须回收或移交。

5.1.5.2. 密码管理

阿里云遵循一人一账号原则，每个账号都有明确的持有者。所有用户集中下发密码策略，强制要求设置符合密码长度、复杂度要求的密码，并定期修改密码且不能与上一次密码相同。同时，阿里云支持账号密码登录、一次性口令登录、数字证书登录等多种认证登录方式。

5.1.5.3. 权限管理

阿里云根据业务需要合理分配权限，按照权限、角色、用户组、部门和用户进行权限统一管理，每个内部用户通过权限管理系统实行权限申请、使用和回收。阿里云为了加强内部系统权限使用管理，降低权限使用风险，根据风险将权限和角色设置为不同等级，并根据等级进行不同层级的申请审批机制，对于超过一定时间未使用的权限，系统则自动冻结权限；对于离职用户，系统自动冻结账号，回收权限；对于转岗用户，系统自动回收其权限。

5.1.6. 云平台安全监控和运营

5.1.6.1. 云产品安全生命周期（SPLC）

云产品安全生命周期（Secure Product Lifecycle，简称 SPLC）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、应急响应六大阶段。

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。

5.1.6.2. 云平台安全监控

云平台侧的安全监控，主要目的是及时发现平台自身的应用和主机、网络等资源被恶意攻击的安全事件，并在发现安全事件之后，触发云平台内部应急响应流程进行妥善处置，及时消除影响。

安全监控主要分为日志收集、异常分析检测和告警展示三个部分。日志收集主要是将平台侧的主机日志、网络日志、应用层和云产品的日志进行收集，并分别导入实时计算平台和离线计算平台。异常分析检测会在各个计算平台中，通过安全监控算法模型，对日志进行处理和分析，进而完成风险的发现与监控。一旦发现异常安全事件，会在阿里云内部的安全监控平台上进行告警展示，并通过钉钉，短信，邮件通知等方式通知安全应急人员在第一时间进行响应处置。

5.1.6.3. 云平台侧蓝军渗透测试

阿里云在云平台侧红蓝对抗计划，通过组织具备黑客能力的专家成立蓝军队伍，充分施展黑客攻击技术和渗透思路（不限时间、不限技术、不限范围），以周期实战性质的攻防对抗方式找出云平台最脆弱的环节，客观检验阿里云安全防御能力、威胁检测能力的水位，提升阿里云核心安全能力，完善平台防御体系。

通过有组织的实战对抗演练，来检验云平台安全现状：

- 当前的防御措施是否有效
- 当前的入侵检测措施是否有效

- 当前的防御措施存在哪些技术盲点
- 当前的安全水位处于什么状态，需要在哪些方面增加投入

5.1.6.4. 云平台安全应急响应

云平台的应急响应是指阿里云对于内部监控发现的和外部上报的漏洞和安全事件做出应急处置。云平台侧通过日志收集和异常分析检测等手段发现可能的安全事件，并进行告警。外部上报的途径包括 ASRC 应急响应中心和阿里云先知漏洞平台、外部的开源三方组件对外通报的 CVE 漏洞信息和来自三方的威胁情报信息。

一旦发现安全事件和漏洞，阿里云会进行相应的安全应急响应。应急响应的第一步骤是对上报的漏洞和安全事件的真实性进行排查确认。一旦确认，阿里云平台安全人员会启动应急响应流程，并按照标准步骤进行处置。漏洞类事件会先确认漏洞的安全等级和影响范围，并保证阿里云的产品能在对应的 SLA 时间内完成相关漏洞的修复并发布上线。安全事件类的处置则主要包含事件影响范围确认，事件影响消除，和事后复盘改进等主要步骤。 同时，应急团队也会及时的通过线上公告等方式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。

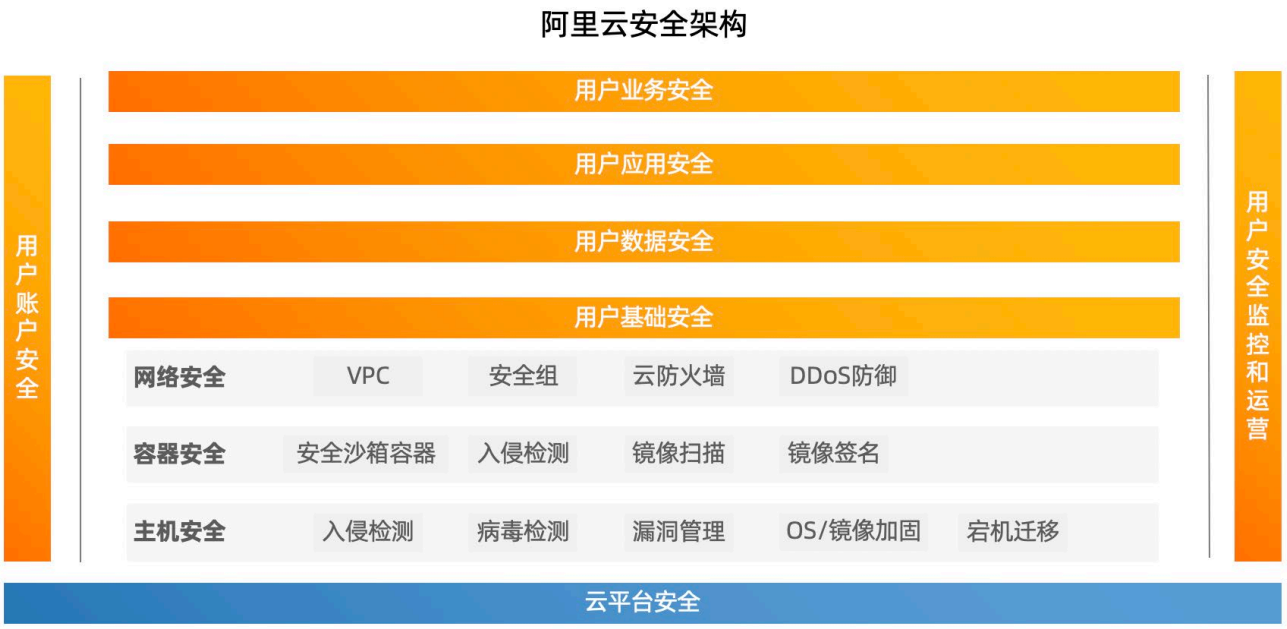
5.1.6.5. 变更管理

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。

5.2. 用户基础安全



云上用户的基础安全能力和要求主要体现在主机安全、容器安全和网络安全三个方面，即用户使用的最主要的计算资源和连通计算资源的网络方面的安全防护和隔离。对于云上用户来说，其云上应用和业务都是直接或者间接（通过上层云服务）的构建和运行于计算（主机和容

器）和网络服务的基础模块之上，因此用户基础安全和上一章的云平台安全能力就像地基一样，一起为用户的云上上层业务安全提供了坚实的基础。

当然，在计算和网络资源之外，存储资源对于用户来说也是至关重要的，尤其是在对于用户数据的保护方面，会在后文中用户数据安全章节中详细阐述。同时，在用户侧安全架构设计中，有两个纵向安全层面，即“用户账户安全”和“用户安全监控和运营”。这两个纵向安全层面对于各个用户侧横向层面均有涉及，如安全监控中对主机的配置安全检测、账户安全中对各种云上资源的权限管控等，因此统一到其独立章节阐述。

5.2.1. 主机安全

5.2.1.1. 入侵检测

阿里云用户可以使用云安全中心高级版（安骑士）的服务，通过在主机上安装轻量级云安全中心 Agent（原安骑士 Agent），实现和云端安全中心联动，为用户提供实时的入侵检测的安全能力。主机的入侵检测中主要包括了异常登录检测、网站后门查杀（Webshell）、主机异常行为检测（进程异常行为和异常网络连接检测）、主机系统及应用的关键文件篡改检测和异常账号检测等功能。同时，云安全中心还提供智能学习应用白名单的能力，识别可信和可疑/恶意程序形成应用白名单，防止未经白名单授权的程序悄然运行，可避免主机受到不可信或恶意程序的侵害。

5.2.1.2. 病毒检测

云安全中心高级版（安骑士）服务同时提供对主流勒索、挖矿、DDoS 木马等病毒的实时拦截能力。在系统内核层面实现云上文件和进程行为的全局监控和实时分析，有效绕过顽固木马和恶意程序的反查杀能力；还可以基于程序行为分析，挖掘出黑名单未能辨识的恶意威胁，实现主动拦截；其云端病毒库实时更新，集成了国内外主流杀毒引擎、阿里云自研沙箱和机器学

习引擎等前沿技术，可以避免因病毒库更新不及时而造成的损失。

5.2.1.3. 漏洞管理

阿里云用户可以使用云安全中心高级版（安骑士）的服务，通过在主机上安装轻量级云安全中心 Agent（原安骑士软件），实现和云端安全中心联动，为用户提供最新的漏洞扫描的安全能力。安骑士基于自主研发的跨平台漏洞扫描及修复引擎，能够帮助用户实现同时对多个系统和应用进行扫描和修复的安全运维工作。目前已支持主流 Windows 系统漏洞、Linux 软件漏洞、Web-CMS 漏洞、应用漏洞，同时还能提供针对网络上突然出现的紧急漏洞的应急检测和修复服务。

5.2.1.4. OS 和镜像加固

阿里云自研的 Aliyun Linux 2 OS 已经发布了经过国际第三方 Cyber Internet Security（CIS）组织认证的 OS Benchmark。用户可以遵循 CIS Benchmark 中的安全最佳实践（Remediation）操作规范来对 OS 进行安全加固，也可以通过遵循 CIS Benchmark 中最佳实践的加固脚本（Remediation Kit）来对 Aliyun Linux 2 OS 进行自动加固。CIS Benchmark 文档和加固脚本可以通过 CIS 官方网站获取。

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，包括阿里云自研的 Aliyun Linux 2 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，并且所有阿里云公共基础镜像会默认添加（用户可以主动选择不勾选）云安全中心 Agent 软件以保障租户在实例启动时第一时间得到安全保障。

5.2.1.5. 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。

5.2.2. 容器安全

5.2.2.1. 安全沙箱容器

容器服务 ACK 提供基于阿里云神龙的安全容器版本，整套技术基于阿里云安全沙箱技术实现，不同于传统的 Docker 共用内核架构，每个安全容器都有独享的内核，对内存、网络、IO 等实现了更强的隔离，用户可以基于这套框架，在单宿主机上更好的保障用户的多租户安全隔离。

5.2.2.2. 入侵检测

阿里云容器服务当前已经支持基于云安全中心的入侵检测，当前云安全中心在容器服务产品支持容器内 Web-CMS 漏洞检测和修复、Webshell 检测和修复、云查杀、进程异常行为、异常网络连接、进程启动日志、网络连接日志的功能。

5.2.2.3. 镜像扫描

针对基于 Linux 的部分基础镜像，阿里云容器镜像服务已经提供了镜像安全扫描的功能。本功能可以发现与被扫描镜像相关的最新 CVE 安全漏洞信息，同时在适用的情况下会向用户提出漏洞修复建议。

5.2.2.4. 镜像签名

容器镜像的签名和校验可确保仅在 ACK 上部署经过容器使用方签名确认的容器镜像。借助镜像签名和二进制授权校验，容器使用者可以要求在开发过程中由可信授权方对镜像进行签名，然后在部署时强制执行签名验证。通过强制执行验证，可以确保仅将经过验证的镜像集成到构

建和发布流程中，从而对容器环境实施更严格的安全控制。同时也可以依赖二进制授权校验进行进一步的安全策略配置。

5.2.3. 网络安全

5.2.3.1. VPC

阿里云的专有网络（Virtual Private Cloud，简称 VPC）可以帮助用户基于隧道技术，实现数据链路层的隔离，为每个用户提供一张独立隔离的安全网络环境。在 VPC 内部，用户可以自定义 IP 地址范围、网段、路由表和网关等；此外，用户可以通过 VPN 网关、高速通道物理专线、智能接入网关等服务将本地数据中心和云上 VPC 打通，也可以通过云企业网实现全球网络互通，在 VPC 间以及 VPC 与自有数据中心间搭建私网通信通道，从而形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

5.2.3.2. 安全组

安全组是阿里云提供的实例级别虚拟化防火墙，具备状态检测和数据包过滤功能，可用于在云端划分各个 ECS 实例（在容器服务中，即各个容器集群）间的安全域。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，普通安全组可以通过安全组规则授权两个安全组之间的互访，但企业安全组不支持安全组之间的授权。

5.2.3.3. 云防火墙

阿里云提供的云防火墙是业界首款公共云环境下的 SaaS 化防火墙，可以统一管理互联网

到业务的南北向访问策略和业务与业务之间的东西向微隔离策略。这是因为在云上环境中，用户不但需要管理进出互联网的边界，也需要在云产品之间、VPC 之间、乃至虚拟机实例之间进行网络边界管理。通过云防火墙，用户可以对南北向和东西向访问的网络流量进行分析，并支持全网流量（互联网访问流量，安全组间流量等）可视化，并支持对主动外联行为的分析和阻断。

在流量分析基础上，云防火墙提供全网各个层次的隔离管控能力，包括统一的公网 IP 地址管控，基于域名的访问控制，和基于 VPC 的隔离管控及阿里云与 IDC 专线之间的隔离管控。

云防火墙还集成了集成了入侵检测（IPS）功能和威胁情报能力，并支持入侵检测分析。同时，云防火墙支持网络流量及安全事件日志存储功能，默认保存 6 个月的安全事件日志和网络流量日志及防火墙操作日志， 满足网安法和等保 2.0 的相关要求。

5.2.3.4. 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，支持防护全类型 DDoS 攻击，并通过 AI 智能防护引擎对攻击行为进行精准识别和自动加载防护规则，保证网络的稳定性。同时，阿里云的 DDoS 防护系统支持通过安全报表，实时监控风险和防护情况。阿里云的 DDoS 防护系统，不仅仅能够支持客户的云上业务，也可支持云下企业客户使用阿里云在全球部署的大流量清洗中心资源，结合 AI 智能防护引擎，通过全流量代理的方式实现大流量攻击防护和精细化 Web 应用层资源耗尽型攻击防护。

5.3. 用户数据安全

用户的云上数据安全，是用户的生命线，也是云上安全整体能力的一个最重要具象表现。早在 2015 年 7 月，阿里云就发起了中国云计算服务商首个“数据保护倡议”，并在公开倡议书明确：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机密性、完整性和可用性。

数据安全的要求，可以用信息安全基本三要素 “CIA”来概括，即机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。机密性专指受保护数据只可以被合法的（或预期的）用户可访问，其主要实现手段包括数据的访问控制，数据防泄露，数据加密和密钥管理等手段；完整性是保证只有合法的（或预期的）用户才能修改数据，主要通过访问控制来实现，同时在数据的传输和存储中可以通过校验算法来保证用户数据的完整性；数据的可用性主要体现在云上环境整体的安全能力，容灾能力，可靠度，以及云上各个相关系统（存储系统、网络通路，身份验证机制和权限校验机制等等）的正常工作保障。阿里云的数据安全能力能够帮助用户防

止数据泄露，并满足个人信息保护、等保 2.0 以及 GDPR 等合规要求。

5.3.1. 数据保护

5.3.1.1. 数据分类

云上环境中，时时刻刻都会有海量数据的产生。而在对这些数据进行处理和保护之前，如何从海量数据中发现并分类出各种需要被保护的敏感数据是后续数据保护机制能够有效运作的前提条件。数据分类的第一步是对数据中的敏感信息，如个人验证信息（Personal Identifiable Information，简称 PII），进行发现和检测。数据分类的第二步是针对数据中的敏感信息，根据用户的使用场景、合规需求和安全要求，对数据进行分类分级，从而达到自知数据资产，并后续进行针对性保护的作用。

阿里云的敏感数据保护（Sensitive Data Discovery and Protection，简称 SDDP）产品，可以对用户云上数据进行发现和分类分级功能。SDDP 可在得到云上用户授权后，自动扫描和发现授权范围内的新增实例/库/表/列、对象存储文件桶/文件对象等不同级别数据信息。通过关键字、规则、机器学习模型算法，精准识别云环境内的敏感数据，并支持根据用户自身业务规则进行敏感数据自定义。SDDP 根据敏感数据识别结果，可实现云上数据基于业务内容的分类以及基于敏感程度的分级，以供后续根据敏感分类分级结果在云上系统中对用户数据实现相关的保护机制。

5.3.1.2. 数据脱敏

在发现和分类敏感数据后，为保护数据隐私，用户往往需要根据不同的业务场景对相关敏感数据进行脱敏后的使用。例如，用户往往希望能够在不改变数据结构和特征分布的情况下，对生产数据进行脱敏，并用于测试、开发、分析和三方数据交换等场景中。

阿里云的敏感数据保护产品，提供 Hash、加密、遮盖、替换、洗牌、变换等六大类近 30 种

内置脱敏算法并同时支持客户自定义脱敏算法或者自定义脱敏参数，确保脱敏后的数据无需改变相应的业务系统逻辑，保留原有数据特征和分布，确保数据的有效性和可用性。用户可以低成本、高效率、安全地使用脱敏数据完成业务需求。

5.3.1.3. 数据防泄露

用户数据的防泄露，主要体现在对数据的权限控制的完整度和数据使用中的监控和检测能力。如果想要防止数据泄露，首先需要实现对云上存储产品和传输产品权限的有效管控。阿里云的敏感数据保护产品支持“数据、人、权限”三要素的即时查询，支持角色背后主账号权限映射解析，和全局数据权限统一查询。SDDP 服务可以针对云上环境内不符合安全最佳实践的数据权限配置、权限使用异常进行告警。

其次，需要对用户数据的流转和操作过程有全面的监控和检测能力，及时发现数据使用中可能的异常行为。SDDP 服务能针对数据流转过程中的异常情况进行有效监控，实现数据流转链路动态展示，确保数据导出/数据传输合规有序。根据日志聚类分析，SDDP 服务能有效识别人工操作与应用接口调用。基于机器学习和大数据分析能力，SDDP 服务能针对环境内各类数据流转、数据操作中产生的异常行为进行监控告警。

最后，在发现数据泄露告警后，SDDP 服务支持对异常事件进行分析以供后续的处理响应。其中，事件分析支持集中归集各类告警事件，并通过使用时序分析技术还原责任主体行为基线，动态展示历史基线轨迹，从而有效的提升分析效率。同时，SDDP 服务支持各租户事件隔离处理，并支持处理结果自动回流机器学习样板库，从而使得异常检测能力日趋准确。

5.3.1.4. 数据完整性

在数据传输和存储层面，阿里云的云产品提供了全链路数据校验功能，且会定期对存储介质中的数据进行完整性扫描，以确保数据传输和存储过程中的数据可靠性需求。例如，对象存

储 OSS 服务支持对各种方式上传的 object 返回其 CRC64 值，用户在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。同时，在数据存储时也会有对应的校验码贯穿始终，达到对数据进行细粒度的完整性校验保护。

数据的完整性也通过阿里云的访问授权功能得到保障，具体请参见用户账户安全-访问授权章节。

5.3.1.5. 数据高可用

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。同时，阿里云的云产品，根据产品形态和用户业务需求，会为客户提供多副本、系统备份、故障热迁移、负载均衡、DDoS 防御等多重保护，保证用户在使用数据时的高可用性。例如，对象存储 OSS 服务提供同城数据冗余功能，可以为客户数据在 3 个不同可用区（AZ）进行备份，从而保证 12 个 9（99.9999999999%）的数据持久性和 99.95%的高可用性。

5.3.2. 全链路加密

阿里云对于数据安全提供了全链路的加密保护能力，包括传输加密（Encryption in Transit）、存储加密（Encryption at Rest），以及提供在运行态通过基于 Intel® Software Guard Extensions（Intel® SGX）的硬件加密计算环境。同时，阿里云提供了基于硬件加密机的加密服务和 SSL 证书服务，为用户提供数据加密的完整解决方案。

5.3.2.1. 传输加密

传输加密是指云产品为用户访问（包括读取和上传）数据提供了 SSL/TLS 协议来保证数据传输的安全。例如，用户如果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。所有的阿里云产品都为客户提供了支持 HTTPS 的 API 访问点，并提供高达 256 位密钥的传

输加密强度，满足敏感数据加密传输需求。

阿里云的网关产品也提供传输链路的加密功能。VPN 网关（VPN Gateway）服务，可通过传输链路加密通道将企业本地 IDC 和阿里云 VPC 安全可靠的连接起来。VPN 网关可建立 IPsec-VPN，将本地 IDC 网络和云上 VPC 连接起来；也可建立 SSL-VPN，将本地客户端远程接入 VPC。阿里云也提供智能接入网关（Smart Access Gateway，简称 SAG）服务，企业用户可通过智能接入网关实现就近加密接入，并在传输过程中通过使用 IKE 和 IPsec 协议对传输数据进行加密，保证数据安全。阿里云 VPN 网关和智能接入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。

5.3.2.2. 存储加密

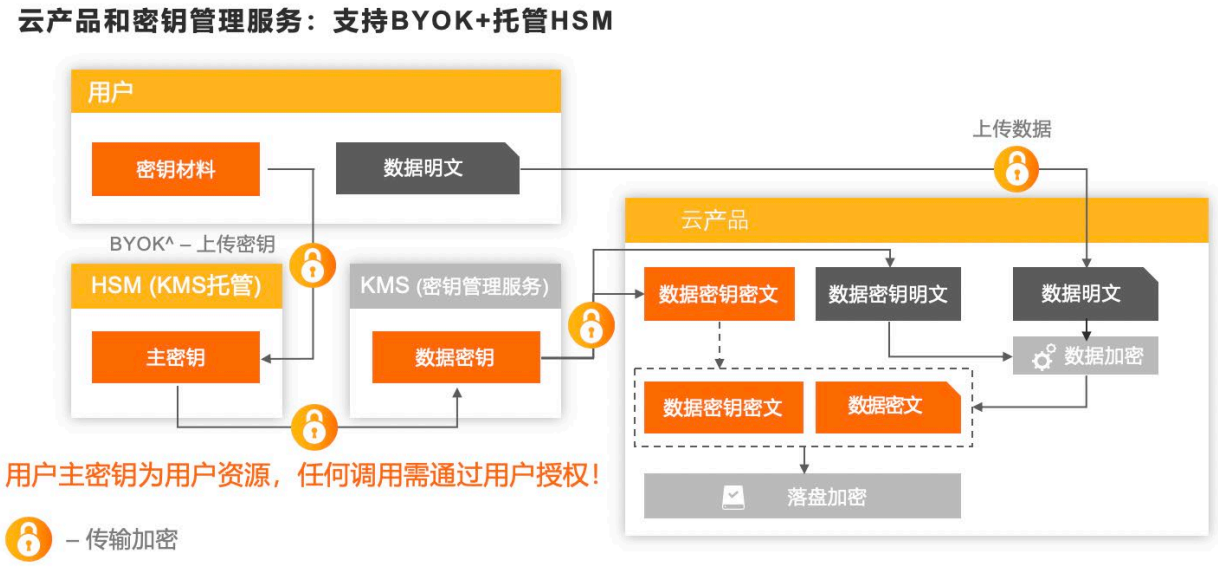
阿里云提供云产品落盘存储加密能力给用户，并统一使用阿里云密钥管理服务（Key Management Service，简称 KMS）进行密钥管理。阿里云的存储加密提供 256 位密钥的存储加密强度（AES256），满足敏感数据的加密存储需求。

不同产品基于业务形态和客户需求，其存储加密的具体设计略有不同，但大体而言，存储加密中密钥层次会至少分为两层，并通过信封加密的机制实现对数据的加密。第一层为客户主密钥（Customer Master Key，简称 CMK），第二层为数据密钥（Data Encryption Key，简称 DEK），其中 CMK 为 DEK 进行加解密操作和保护，DEK 为真实数据进行加解密操作和保护。在数据落盘存储时，云产品会将数据密钥密文（通过 KMS 使用 CMK 加密）在数据写入的时候，与密文数据（云产品在存储链路上使用 DEK 加密）一同写入永久性存储介质中。顾明思义，信封加密中的“信封”指的是在概念上数据密钥的密文和数据密文被打包在一个“信封”（Envelope）中。在读取加密数据时，数据密钥的密文也会一同被读取，并先于数据进行解密。只有在数据密钥被解密后，密文数据才能够被正常读取。

在信封加密机制中，客户主密钥 CMK 受阿里云 KMS 提供的密钥管理基础设施的保护，实施强逻辑和物理安全控制以防止未经授权的访问。阿里云的密钥管理基础设施符合（NIST）800-57 中的建议，并使用了符合合规要求的密码算法和硬件加密机（Hardware Security Module，简称 HSM）。在整个信封加密过程中，CMK 的明文从不会在 KMS 托管的 HSM 之外进行存储和使用。KMS 也支持软件密钥托管，通过软件密码模块（Software Cryptographic Module）对密钥进行保护。KMS 通过加固软件密码模块，保护软件密钥的明文材料不会离开软件密码模块的边界，仅能在模块边界内被加载于内存中。同时，数据密钥 DEK 明文仅会在用户使用的服务实例所在的宿主机的内存中使用，永远不会以明文形式存储在任何永久介质上。

云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。具体而言，当用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥管理服务（KMS）中的使用地域自动创建一个专为该服务使用的用户主密钥（CMK）。本密钥会作为服务密钥且其生命周期是托管给云服务的。具体表现为用户可以在密钥管理服务控制台上查询到该用户主密钥，但不能删除。

在存储加密功能中，阿里云也有多个产品支持用户自选密钥功能，包括支持用户自上传的 CMK（Bring Your Own Key，简称 BYOK，也称 Customer Supplied Key）或用户自己在 KMS 中生成的用户主密钥（CMK）作为主密钥对数据进行加密，并允许客户对 CMK 的生命周期进行全程管理。需要强调的是，用户自选的 CMK 是用户的资产，云产品必须得到用户的授权（通过 RAM）才可以使用其对数据进行加解密操作。用户也可以随时取消相对应的 CMK 授权，达到对数据加解密操作的可控。



请注意，为了表达的简单扼要，在本白皮书中，如无特别说明，后续会使用“用户自选密钥”来泛指使用用户自上传到 KMS（BYOK）或用户在 KMS 自生成的 CMK 作为主密钥进行存储加密的功能。

阿里云已拥有不同的云产品支持数据存储加密功能（具体产品请参见产品对应章节）：

- 块存储 EBS：支持虚拟机内部使用的块存储设备（即云盘）的数据落盘加密，确保块存储的数据在分布式系统中加密存放，并支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。
- 对象存储 OSS：支持服务端和客户端的存储加密能力。在服务端的加密中，支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。在客户端的加密中，支持使用用户自管理密钥进行加密，也支持使用用户 KMS 内的主密钥进行客户端的加密。
- RDS 数据库的数据加密：RDS 数据库的多个版本通过透明加密（Transparent Data Encryption，简称 TDE）或云盘实例加密机制，支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。

- 表格存储 OTS：支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。
- 文件存储 NAS：支持使用服务密钥作为主密钥进行数据加密。
- MaxCompute 大数据计算：支持使用服务密钥作为主密钥进行数据加密。

还有更多产品也支持了存储加密功能，包括支持使用服务密钥和用户自选密钥作为主密钥进行数据加密，具体情况请参见各云产品官网信息（www.aliyun.com）。

5.3.2.3. 加密计算

阿里云平台提供了以 Intel® Software Guard Extensions（Intel® SGX）可信执行环境作为基础的硬件可信执行环。用户可以通过软件建立一个可信执行环境，并保护敏感数据（如加解密密钥、账户凭证信息等）。通过支持加密计算能力的 ECS 主机（神龙机型），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，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，阿里云为用户数据在执行态环境中提供了更强大的数据加密保护能力。

5.3.2.4. 加密服务

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。

5.3.2.5. SSL 证书服务

证书服务（Alibaba Cloud Certificates Service），可以在云上签发第三方知名 CA 证书颁发机构的 SSL 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，一键分发到其它阿里云的产品（包括 CDN、SCDN、DCDN 和 SLB 等服务）。

5.3.3. 密钥管理

密钥管理服务（Key Management Service，简称 KMS）是一款安全易用的密码类服务，提供密钥的安全托管、密码运算等基本功能，内置密钥轮转等安全实践，同时支持其他云产品通过一方集成的方式对云产品管理的用户数据进行加密保护。KMS 的安全可靠的密钥管理功能是云产品数据加密功能的重要前提条件。

5.3.3.1. 托管 HSM

在支持用户托管密钥在 KMS 的软件密码模块之外，阿里云的 KMS 服务支持用户将密钥托管在硬件安全模块（Hardware Security Module，简称 HSM）之中，并可利用 HSM 进行密码运算和安全托管等功能，为用户的主密钥提供更高层次的保护。

用户可以将密钥托管在硬件安全模块（HSM）中，利用硬件机制来保护密钥的明文密钥材料不会离开 HSM 的安全边界。用户使用 HSM 密钥进行运算时，密码运算的过程也只会发生在 HSM 中，从而保证了用户密钥的私密性。HSM 托管密钥可以满足用户的高级别安全和合规需求，同时通过 KMS 内建的管理能力，极大地减少用户的管理开销。

5.3.3.2. 自选密钥

各个云产品可以在用户的 KMS 服务中为用户托管一个默认的“服务密钥”，并可以通过使用服务密钥实现数据加密功能，同时可以对云产品调用 KMS 加解密数据的行为进行适当的审计。但是，虽然云产品托管的服务密钥可以帮助用户获得最基本的数据保护能力，但是对于有明确诉求的用户，还可能存在一些密钥管理的短板，例如不能自主管理密钥的生命周期、不能设定自动轮转、保护级别仅仅为软件密钥等。

因此，用户可以通过在支持的云产品中选择自己创建或上传用户主密钥（CMK）到 KMS 中，并直接管理自选密钥的生命周期。通过 RAM 的授权后，自选密钥也可用于云产品的数据加密功

能，并赋能用户更多的安全能力：

- 用户可以禁用或者启用密钥，控制云产品加解密数据的能力。
- 用户可以配置授权策略，控制云产品加解密数据的能力。
- 用户可以通过在 KMS 中导入自带密钥（Customer Supplied Key，即 BYOK），进一步增强密钥的生命周期管理能力和控制云产品的数据加解密能力。

请注意，当使用自选密钥和上述安全能力时，也意味着，用户需要更多的考虑己方的责任，管理好密钥的授权和生命周期。

5.3.3.3. 密钥轮转

KMS 内建了密钥的版本管理能力，同时在多版本的基础上，支持通过配置的方式对用户主密钥进行自动轮转。自动轮转允许用户主密钥下周期性产生新的密钥版本作为加密密钥，而老版本仅能用作解密历史数据，从而降低针对密钥和受保护数据的攻击面。

在某些场景下，用户亦可针对老数据进行重加密，从而将主密钥下老密钥版本产生的密文数据转换为新密钥版本加密的密文数据。

用户也可以在自动轮转周期之外，针对特定的需要，一次或者多次手动轮转密钥的版本。

5.4. 用户应用安全

用户在阿里云上构建的应用也需要得到妥善的安全保护。在应用安全层面，阿里云为用户提供了应用环境安全、应用配置安全和应用自身保护的三个维度的安全功能。

5.4.1. 应用环境安全

5.4.1.1. 漏洞扫描

阿里云漏洞扫描服务是对用户在数字化转型中的最佳互联网扫描实践，可帮助用户自动发现其网站的关联资产，并进行高效精准的自动化漏洞渗透测试和敏感内容监测等，保障上线前和线上应用环境的安全性。同时，针对扫描的的结果会形成专业的风险扫描报告。对扫出来的安全漏洞进行归类，并提出修复建议，并可以提供安全专家级辅助漏洞验证和漏洞修复指导。

5.4.1.2. 代码托管

云上用户，尤其是在云上直接开发应用的用户，其上云后代码的安全保护是资产保护的重要部分。阿里云的云效服务提供了存放源代码等内容的 Git 库，并提供了严格的权限控制机制。通过云效权限管理功能，可以查看当前用户自己在特定 Git 库/组上的权限。当用户在特定 Git 库

/组上有 Master 或 Owner 角色权限时，还可以查看和修改该 Git 库/组的其他成员的权限，对其他成员的权限进行有效管理，并应用最小权限原则。

5.4.1.3. 代码审计

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。

阿里云提供代码审计服务，在驻场审计中检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞并提供代码修订措施和建议。审计过程中，通过人工和自动化工具结合的审计方式，审计 Java、PHP、ASP、ASPX、JSP、Python 等程序源码，并提供专业代码审计报告和修复后的复查报告。本服务由阿里云认证的合作伙伴提供专业服务。

5.4.1.4. 安全加固

阿里云也提供为用户的应用环境进行安全加固服务。在获得客户授权委托的情况下，远程登录到客户的业务系统服务器上，根据用户的资产情况和安全需求，对其外网或内网主机进行全方位的基线加固和组件升级，提前修补系统潜在的各种高危漏洞和安全威胁。本服务由阿里云认证的合作伙伴提供专业服务。

5.4.2. 应用配置安全

5.4.2.1. ACM 配置加密

应用配置管理（Application Configuration Management，简称 ACM），前身为淘宝内部配置中心 Diamond，现已作为 Nacos 的配置中心模块开源。ACM 是一款在分布式架构环境中

对应用配置进行集中管理和推送的产品。利用 ACM，用户可以在微服务、DevOps、大数据等场景下极大减轻配置管理的工作量，并增强配置管理的服务能力。为了确保敏感配置（数据源、Token、用户名、密码等）的安全性，降低用户配置的泄露风险，ACM 提供了创建加密配置的功能。ACM 提供的配置加密方法包括：

- KMS 加密：配置内容不可超过 6 KB。配置内容的明文数据会传输到 KMS 系统。
- KMS AES-128 加密：配置内容可以超过 6 KB，建议不超过 10 KB，最大不超过 100 KB。配置内容的明文数据不会传输到 KMS 系统，安全性更高。

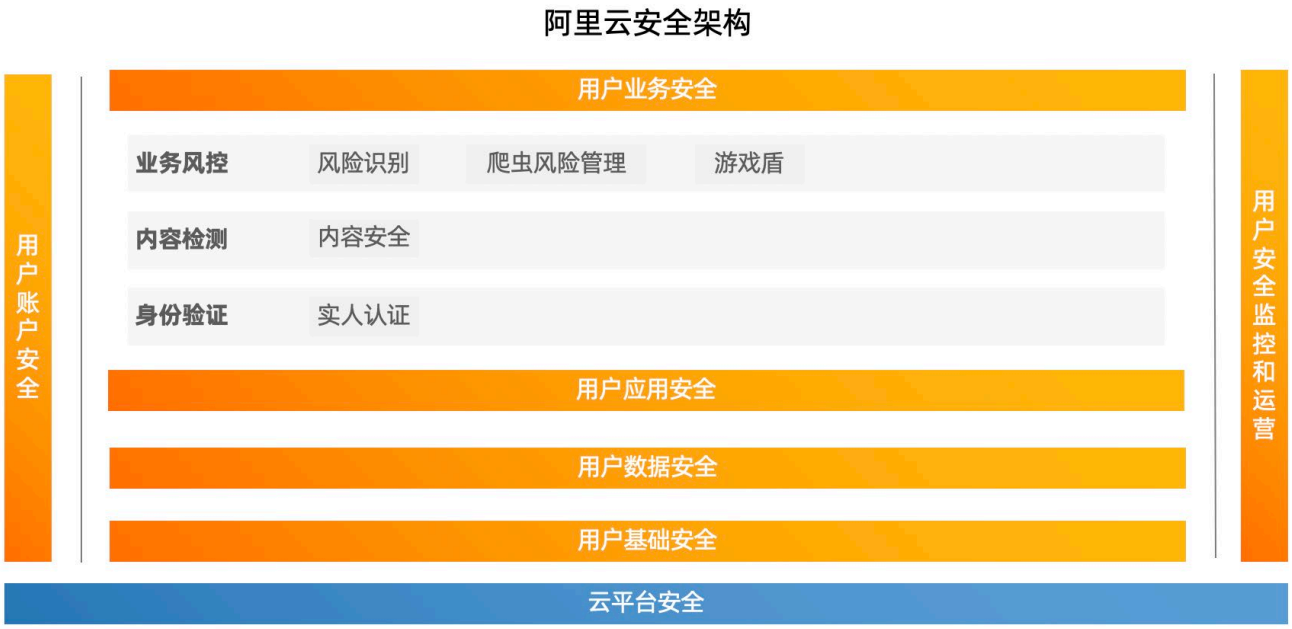
5.4.3. 应用保护

5.4.3.1. WAF

阿里云提供 Web 应用防火墙（Web Application Firewall，简称 WAF）服务，基于云安全大数据和智能计算能力，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 web 攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站应用的安全性与可用性。

值得一提的是，Web 应用防火墙依托阿里云强大的计算和数据处理能力，通过业界领先的 AI 深度学习方法，在降低误报率的同时有效地提高了检出率。同时，可以基于用户业务访问端上的模型收集和大数据分析能力准实时处理高危请求。Web 应用防火墙还提供自动报警和全局响应规则的同步下发和升级功能。

5.5. 用户业务安全



当用户的应用已经构建并运行于阿里云平台上后，对于用户的不同业务场景，阿里云也提供了相对应的安全能力。在业务安全层面，阿里云为用户提供了身份认证、内容检测和业务风控的三个维度的安全功能。

5.5.1. 身份验证

5.5.1.1. 实人认证

阿里云提供用户真实身份验证（实人认证）服务，为企业级用户的更高等级的业务发展提供实名制的基础。依托活体检测、人脸比对等生物识别技术、证件 OCR 识别技术等进行的自然人真实身份的核验服务。实人认证服务提供有源比对、无源比对等在线认证服务，也支持离线授权 SDK 在弱网或离线环境下的人脸认证应用。实人认证操作过程中采集到的活体照片，以及姓名和身份证号，与权威数据源进行核身比对，核身是同人和本人。实人认证服务目前仅支持对拥有中华人民共和国第二代居民身份证的居民进行认证。

5.5.2. 内容检测

5.5.2.1. 内容安全

阿里云为用户提供内容安全服务。基于深度学习技术及阿里巴巴多年的海量数据支撑，内容安全服务提供图片、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。内容安全服务依托阿里云线上计算和处理能力，能够做到实时自动化精准识别。

5.5.3. 业务风控

5.5.3.1. 风险识别

阿里云为用户提供风险识别服务。风险识别服务基于大数据、机器学习算法、流式计算等阿里巴巴的业务风控最佳实践，为用户提供从 API 服务、到决策引擎平台的一站式智能风控解决方案。尤其解决企业类客户在用户注册、运营活动、交易、信贷审核等关键业务中面临的欺诈问题。风险识别服务提供 API 服务，同时提供风控引擎平台供用户使用个性化业务场景事件管理，可视化编排复杂决策，丰富的特征变量与场景识别服务等功能。

风险识别服务在技术上依托阿里云线上大数据计算能力，可以实现 PB 级别的运算和模型建设能力，从而提供实时处理请求并提供风险识别结果的能力。通过采用 server-client 模式，安全专家通过统一的控制台配置专家策略和模型，实时动态地推送到执行引擎，实现一处配置全部执行、有效实现实时对抗。风险识别还集成了多款一方产品（云市场、MaxCompute、Log Service，OSS，RDS，Redis 等），实现零代码即插即用。

5.5.3.2. 爬虫风险管理

在云上业务中，防止恶意爬虫（Bot）可以有效降低和解决外部恶意自动化工具对用户网站的业务影响，主要防护场景包括航空占座、电商黄牛、恶意撞库、核心接口被刷、刷票刷积分

等。阿里云的爬虫风险管理服务提供对 Web 网页端/H5 页面/APP/API 全方位防护，并通过云端共享海量的威胁情报做到对爬虫类攻击的快速响应。同时无需改动用户服务端代码，通过 CNAME 的改动即可无缝接入爬虫风险管理服务，所有恶意爬虫流量都将在云端被检测、过滤，最终将正常的流量返回给源站服务器，从而确保源站业务免受恶意爬虫流量引发的数据泄露、业务欺诈等安全问题的影响。

5.5.3.3. 游戏盾

针对云上游戏类业务，阿里云提供了游戏盾（GameShield）服务。游戏盾是阿里云针对游戏行业面对的 DDoS 攻击推出的针对性的网络安全解决方案，相比 DDoS 高防，除了能针对大流量 DDoS 攻击（T 级别）进行有效防御外，还具备彻底解决游戏行业特有的 TCP 协议资源耗尽型攻击（L4-CC 攻击）问题能力，防护成本更低、效果更好。

5.6. 用户账户安全

在整体的云上安全架构设计中，用户的账户安全是贯穿始终的一个重要维度。云上用户的账户安全主要体现在五个方面，包括身份认证（Authentication）、访问授权（Authorization）、

账号管理（Account）、操作审计（Audit）和应用管理（Application），即账户安全中的 5A 要素。需要注意的是，在云上服务中，往往会有一个云服务或云产品（如 RAM 服务）实际提供了 5A 中的多个维度能力。由于本章着重介绍的是阿里云作为云平台提供给用户的不同维度的账户安全能力，因此在本章中会就 5A 维度进行阿里云相对应安全功能的介绍。各种产品的相关能力详情请参见本白皮书相关的章节内容。

5.6.1. 身份认证

身份认证是指通过凭证信息认证用户的真实身份。它通常是指通过登录密码或访问密钥（Access Key，简称 AK）来进行认证。请注意，用于身份认证的凭证信息对于用户来讲是秘密信息，用户必须妥善保护好身份凭证信息的安全。

5.6.1.1. 账号密码认证

用户可以使用其云账号（即主账号）或其云账号下 RAM 用户的密码登录阿里云控制台并对其云上资源进行操作。阿里云的账号密码规范、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，如密码字符组合规范、重试登录次数、密码轮转周期等策略。例如，用户可以通过 RAM 控制台为 RAM 用户创建密码策略，以保证各个子用户都使用定期轮转的强密码从而提高整体账户的安全性。

5.6.1.2. Access Key（AK）认证

阿里云的 Access Key（AK）是用户调用云服务 API 的身份凭证，用于在用户通过 API 访问阿里云资源时对用户身份进行认证。API 凭证相当于登录密码，只是使用场景不同。前者用于程序方式调用云服务 API，而后者用于登录控制台。

Access Key 包括访问密钥 ID（AK ID）和秘密访问密钥（AK Secret）。AK ID 用于标识用户，而 AK Secret 用来验证用户身份的合法性。用户在调用资源时会传入 AK ID，并使用 AK Secret

对请求进行签名（HMAC-SHA1 算法）。用户可以登录阿里云用户中心或 RAM 控制台来管理 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。

请注意，出于有效权限分割和降低风险的考虑，云上最佳安全实践中不建议用户为其云账号（即主账号）创建 AK 凭证，而建议为其下属的 RAM 用户各自创建 AK 凭证。

5.6.1.3. STS 认证

阿里云 Security Token Service（STS）是为 RAM 用户、阿里云服务、身份提供商等受信实体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号下的云资源，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，例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（和上述 AK 签名机制相同）。

5.6.1.4. MFA 认证

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。

5.6.1.5. SSO 认证

阿里云支持基于 SAML 2.0 的单点登录（Single Sign On，简称 SSO），可以支持企业客户使用企业自有身份系统（作为 Identity Provider）的登录服务登录访问阿里云（作为 Service Provider）。

为了满足不同企业客户的登录场景需求，阿里云提供了以下两种基于 SAML 2.0 协议的 SSO 机制：

- 用户 SSO：阿里云通过身份提供商 IdP 颁发的 SAML 断言（SAML Assertion）确定企业用户与阿里云 RAM 用户的对应关系。企业用户登录后，使用该 RAM 用户访问阿里云资源，对应的访问权限由 RAM 用户的授权策略所限制。
- 角色 SSO：阿里云通过身份提供商 IdP 颁发的 SAML 断言（SAML Assertion）确定企业用户在阿里云上可以使用的 RAM 角色。企业用户登录后，使用 SAML 断言中指定的 RAM 角色访问阿里云资源，对应的访问权限由 RAM 角色的授权策略所限制。

5.6.1.6. SSH 密钥对

针对 ECS Linux 实例，阿里云提供了 SSH 密钥对作为认证方式。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。SSH 密钥对默认采用 RSA 2048 位的加密方式，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。同时，阿里云容器服务也支持通过 SSH 密钥对的方式远程登录集群。

5.6.2. 访问授权

5.6.2.1. RAM

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 Resource Access Management（RAM）资源访问控制服务，用于用户身份管理与资源访问控制。RAM 使得一个阿里云账号(主账号)可拥有多个独立的子用户(RAM 用户），从而避免与其他用户共享云账号密钥，并可以根据最小权限原则为不同用户分配最小的工作权限，从而降低用户的信息安全管理风险。RAM 授权策略可以细化到对某个 API-Action 和 Resource-ID 的细粒度授权，还可以支持多种限制条件（例如，源 IP 地址、安全访问通道 SSL/TLS、访问时间、多因素认证等）。

RAM 是阿里云账号安全管理和安全运维的基础。通过 RAM 可以为每个 RAM 用户分配不同的密码或 API 访问密钥（Access Key），消除云账号共享带来的安全风险；同时可为不同的 RAM 用户分配不同的工作权限，大大降低了因用户权限过大带来的风险。

5.6.3. 账号管理

5.6.3.1. 阿里云账号

Resource Access Management（RAM）是阿里云为客户提供的集中式用户管理与资源访问权限控制服务。每个资源有且仅有一个属主（资源 Owner）。该属主必须是一个阿里云账号（又称主账号、根账号、资源 Owner），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。例如，一个 RAM 用户被授予创建资源的权限，该 RAM 用户创建的资源归属于云账号，因此该 RAM 用户只是资源创建者但不是资源属主。

5.6.3.2. RAM 用户

通过使用 RAM，用户可以在其云账号下为其企业员工、系统或应用程序创建独立的 RAM 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 使得一个阿里云账号（主账号）可拥有多个独立的子用户（RAM 用户），并支持多因素认证、强密码策略、控制台用户与 API 用户分离、自定义细粒度权限策略，用户分组授权、临时授权令牌等功能。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 用户才能代表云账号进行资源操作。

5.6.3.3. RAM 角色

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凭证（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、进行角色 SSO 登录等场景。

5.6.3.4. Resource Directory（多账号管理）

云账号是阿里云资源隔离和计量计费的最小管理单元。为了资源隔离或成本管理的需要，企业往往需要使用和管理多个云账号。为此，阿里云面向企业客户提供的一套基于多账号的分级管理服务，即资源目录（Resource Directory）。

资源目录支持按照基于企业的业务或生态环境，让管理员方便地创建体现业务关系的资源目录结构，并将企业多个账号分布到这个目录结构中的相应位置，从而形成资源间的多层级关系。企业可依赖设定的组织关系进行资源的集中管理，满足企业资源在财资、安全、审计及合规方面的管控需要。

5.6.4. 操作审计

5.6.4.1. ActionTrail

用户认证凭证和权限控制是为了避免产生安全问题，而操作日志则可以帮助更好地理解和诊断安全状况。阿里云 ActionTrail 为用户提供统一的云资源操作日志管理，记录云账号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，用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。

5.6.4.2. 堡垒机

用户的云上 IT 运维往往也需要相对应的详细运维操作日志和审计功能，而阿里云的堡垒机服务就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。堡垒机服务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，越权导致数据泄露；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。

堡垒机服务集中了运维身份鉴别、账号管控、系统操作审计等多种功能。基于协议正向代理实现，通过正向代理的方式实现对 SSH 、Windows 远程桌面、及 SFTP 等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维操作审计的目的。

5.6.5. 应用管理

5.6.5.1. 应用身份服务

今天的云上用户，往往在上云后仍然会有一部分应用或系统运行在云下（传统 IDC 或云下专有云），因此用户的云上和云下应用需要一个统一的身份、权限、账户、审计管理服务。阿里

云的应用身份服务（ID as a Service，简称 IDaaS）是一个集中式身份管理服务，为政企客户提供统一的应用门户、用户目录、单点登录、集中授权、以及行为审计等中台服务。应用身份服务可以为用户整合部署在本地或云端的内部办公系统、业务系统及三方 SaaS 系统的所有身份，实现一个账号打通所有应用服务。

应用身份服务支持多种账户数据源，如 AD、LDAP 以及任何提供 SCIM 标准 API 的应用，可快速导入企业既有账户体系。同时，应用身份服务也支持 SAML、OIDC、OAuth、CAS 等所有主流标准单点登录协议，对于未支持标准协议的应用，也支持采用 API、SDK、密码代填等方式进行快速集成。整体而言，应用身份服务在支持多种账户数据源和登录标准的同时，做到了云上应用一方预集成，即集成了市面上常见的公有云服务，并可对接阿里云 RAM 服务，为用户提供了统一的应用管控环境。

5.7. 用户安全监控和运营

当用户在云上的资源、应用、业务和账户都得到了应有的保护后，在后续的使用中用户需要云平台为其提供相应的安全监控和运营能力，使得用户可以做到感知安全态势，监控其云资源的配置安全正确性，对云上日志进行完整的监控，并在适宜的情况下针对客户整体业务环境的

进行安全测试、响应和咨询服务，让阿里云的安全监控和运营能力切实输出到用户的业务层面并为用户保驾护航。

5.7.1. 威胁检测和响应

5.7.1.1. 云安全中心

阿里云的云安全中心是一个实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地主机并满足监管合规要求。

云安全中心高级版（安骑士）服务提供基于威胁情报的威胁检测能力。依托阿里云海量网络基础数据、主机异常行为、黑客组织画像等基础能力，通过协议特征分析、机器学习异常网络和主机行为检测、DGA 恶意域名检测等方案，输出威胁情报指标（IOC）供检测模型使用。基于威胁情报数据，配合主机异常行为检测模型，实现多维度检测异常进程和恶意行为。

云安全中心的能力除了在用户基础安全-主机安全章节中提到的主机入侵检测、病毒检测、漏洞管理等功能，也包括云平台层面的配置检测和主机基线检查（请参见用户安全监控和运营-配置监控-云安全中心章节）、威胁检测、调查响应、日志分析和威胁可视化等功能。

5.7.1.2. 应急响应

阿里云提供安全应急响应服务，即由阿里云与授权安全合作伙伴提供的黑客入侵事件处理服务。应急响应服务目标是帮助用户正确应对黑客入侵事件，清理木马后门、分析入侵原因，降低安全事件带来的损失，并帮助客户快速恢复业务。整体而言，应急响应分为四个阶段：

- 准备阶段：了解安全事件概况、做好数据备份
- 应急处理阶段：对攻击进行抑制，清理恶意程序，恢复系统正常运行

- 入侵原因分析：分析系统和日志，查找入侵原因
- 报告阶段：总结应急相关过程，提供应急响应报告

5.7.2. 配置检查

5.7.2.1. 配置审计

配置审计（Cloud Config）是面向云上资源的审计服务，为用户提供跨区域的资源清单和检索能力，记录资源的历史配置快照，形成配置时间线。用户可以把企业的云上合规要求在配置审计设置为合规规则，当资源发生配置变更时，自动触发合规评估，并针对“不合规”配置发出告警。使用户能够实现对于海量云上资源合规性的自主监控，应对企业内部和外部合规的需要。

5.7.2.2. 云安全中心

用户可以使用云安全中心对其云服务器 ECS 进行基线检查。本服务通过任务下发模式，对主机进行安全配置扫描，包括账号安全、系统配置、数据库风险、合规对标要求等方面，对未符合标准的项目进行提醒。除此之外，用户还可以自定义检测策略，设置检测项目、检测周期、应用的服务器组等。

同时，云安全中心也提供云平台配置检查，包括身份认证、网络访问控制、数据安全、日志审计、基础安全防护五个维度的最佳安全配置实践检测。同时由于云安全中心和云平台的深度集成，可以帮助用户看到在从云主机到云平台等各个维度的安全隐患，从而降低因云环境和云产品配置错误导致的风险隐患。

5.7.3. 日志审计

5.7.3.1. 日志监控

除前文介绍过的 ActionTrail 和堡垒机日志功能（用户账户安全-操作审计章节）之外，阿里

云的日志服务（LogService）也提供各个云产品的日志收集和处理的功能，支持采集弹性计算、存储服务、数据库服务、网络服务、安全服务等多种类型的云产品日志数据（例如 ECS、OSS、SLB 等），记录云产品的操作信息、运行状况、业务动态等数据信息。整体而言，日志服务产品提供了各个云产品日志的实时采集和消费，查询和实时分析，以及投递数据仓库、三方 SIEM 的全栈功能，可以使用户对不同的日志实时进行监控和审计。

5.7.3.2. 平台侧操作日志透明化

传统上，云平台侧的内部运维操作，对用户是不可见的黑盒子，即用户不可感知也不可监控或审计。虽然阿里云已经获得了业界领先的三方合规认证资质，但用户在其数据上云后，对数据在云平台内部是否得到了妥善的保护和管理仍然应当能让用户直观地感受。因此，阿里云的部分云产品（如 OSS）对用户提供了平台侧的内部操作透明化能力，让阿里云的相关内部操作事件对用户可见透明，使得用户可以对云平台内部操作事件也可以进行审计监控等操作，让用户使用阿里云的时候更加安心。

5.7.4. 安全测试

5.7.4.1. 渗透测试

用户的业务系统，包括其业务逻辑和流程，都可能存在安全权限问题和漏洞，尤其是当企业级客户的云上系统未经过模拟攻击等深入的安全测试的时候。阿里云提供渗透测试服务，以攻击者思维，阿里云安全团队会模拟黑客对业务系统进行全面深入的黑盒安全测试。阿里云的安全团队会根据渗透测试标准和阿里渗透测试的经验对目标测试系统定制测试方案和用例，帮助企业用户挖掘出正常业务流程中的安全缺陷和漏洞，助力企业先于黑客发现安全风险，防患于未然。渗透测试服务的测试范围包括：用户业务系统、Web 应用、移动 App、网络/IoT/智能设备。渗透测试专业版为企业客户量身定制的测试计划，更包含了社会工程学、Web2.0 漏洞、开源软件 0day 漏洞等测试手段。

5.7.4.2. 安全众测

阿里云同时对用户提供先知安全众测平台，借助三方白帽子和阿里巴巴应急中心安全专家资源和能力，为企业客户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。企业在加入先知平台后，可自主发布奖励计划，激励先知平台的安全专家来测试和提交企业自身网站或业务系统的漏洞，保证安全风险可以快速进行响应和修复，防止造成更大的业务损失。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。

5.7.5. 安全咨询

5.7.5.1. 安全管家

安全管家服务是安全代为托管服务。该服务由阿里云安全技术专家团队，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、人工值守等评估和咨询服务，并为客户业务环境进行实时监控检测、加固指导、漏洞管理、应急响应等全方位安全保障工作，使得企业客户哪怕没有一支专门的安全工程师团队也能一样做好安全管理。

5.7.5.2. 等保咨询

阿里云整合云上安全产品的技术优势，并联合阿里云在各地的等保咨询合作机构，为企业客户提供等保 2.0 测评的专业咨询指导和量身定制的一站式合规解决方案，帮助客户更快地完成等保整改工作。

5.7.5.3. PCI-DSS 合规咨询

Payment Card Industry Data Security Standard（简称 PCI-DSS），是对于所有涉及支付卡行业的安全方面作出标准的要求。其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，目标是全面保障交易安全。阿里云联合产业内具备完整 PCI 资质的合作伙伴为企业客户提供咨询指导、弱点扫描、安全评估等一站式的 PCI-DSS 合规咨询服务，可面向亚太、

欧洲、美国和加拿大提供专业信息安全服务。

6. 云产品安全

由于篇幅有限，本章节只会覆盖较典型的产品和其安全功能，如需了解更多阿里云产品和服务请参见阿里云官网（www.aliyun.com）。

6.1. 弹性计算

阿里云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 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、和网络隔离四个层面介绍 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它用户虚拟机的系统资源，同时也实现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，使用硬件辅助的扩展页表（Extended Page Tables，简称 EPT）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。

阿里云云服务器 ECS 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，也提供通过对镜像加密来为租户的系统磁盘进行加密，从而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，能够对租户的磁盘进行对称加密（AES256）的加密处理，满足租户的业务和认证需求。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 磁盘加密支持使用 KMS 管理的服务密钥和用户自选密钥作为主密钥进行数据加密。用户自选密钥是指阿里云密钥管理服务（KMS）提供安全生成用户主密钥能力（Customer Master Key，简称 CMK），也支持 BYOK 模式（即由用户上传密钥材料生成 CMK，并托管在 KMS 中）。

ECS 磁盘加密支持端到端的传输加密，对从 ECS 实例传输到云盘的数据默认进行加密。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它虚拟网络隔离。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。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

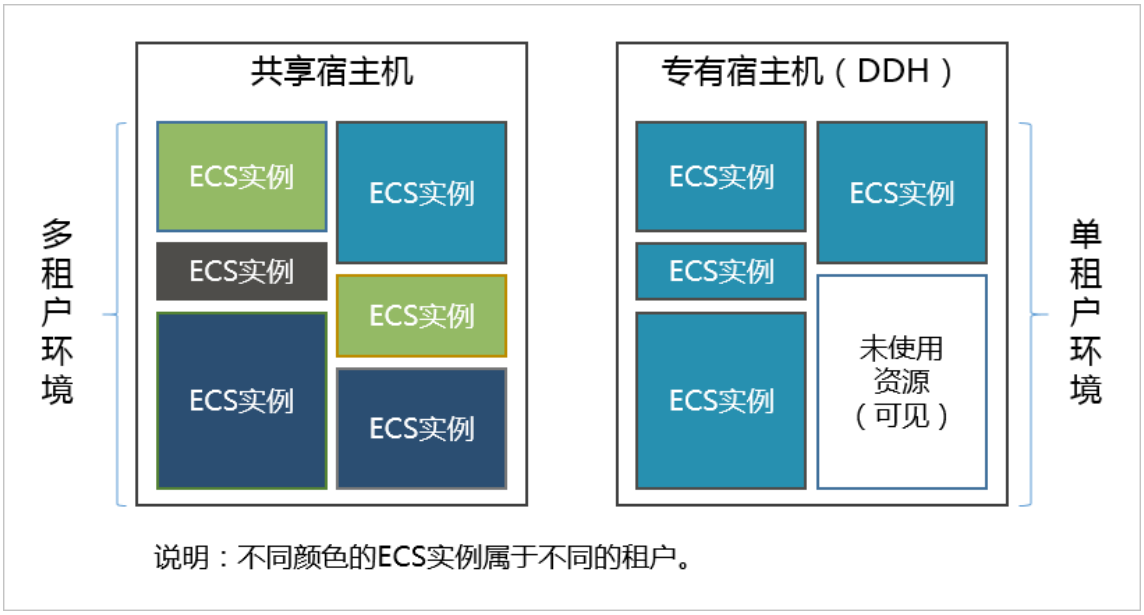
流量给它们。即使同一个客户拥有的运行在同一台物理服务器上的两个虚拟实例之间也不能嗅探到对方流量。

上述四项虚拟化隔离的技术解决了多租户共享物理资源时的租户隔离需求。在此之外，租户隔离的需求也可以通过单租户独享物理资源来达到目的，即专有宿主机形式。

专有宿主机

阿里云专有宿主机（Dedicated Host，简称 DDH）是指由一个租户独享物理资源的云主机。作为该云主机的唯一租户，用户不需要与其他租户共享云主机所有物理资源。用户还可以获得这台物理服务器的物理属性信息，包括 CPU 数量（Socket 数）、物理 CPU 核数、内存大小，并根据宿主机规格创建指定规格族的 ECS 实例。

DDH 与共享宿主机的区别如下图所示。



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，具备状态检测和数据包过滤功能，可用于在云端划分安全域。

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，普通安全组可以通过安全组规则授权两个安全组之间的互访。

安全组分为普通安全组和企业安全组两种，其特点有所不同。普通安全组适用于对网络精细化控制要求较高、需要使用多种 ECS 实例规格、以及网络连接数适中的用户场景。企业安全组适用于对运维效率、ECS 实例规格以及计算节点的规模有更高需求的用户场景。

功能对比	普通安全组	企业安全组
是否支持所有实例规格	是	否，实例规格必须同时支持 IPv6 功能
是否支持专有网络 VPC	是	是
是否支持经典网络	是	否
是否支持设置规则优先级	是	否
是否支持授权给其他安全组	是	否
是否支持手动设置允许访问的安全组规则	是	是
是否支持手动设置拒绝访问的安全	是	否，企业安全组默认拒绝任何访问请

组规则		求
支持的弹性网卡数量	受安全组内 ECS 实例数量限制	50000
是否支持绑定弹性网卡到任意实例规格	是，但实例网络类型必须是专有网络 VPC	否，实例规格必须同时支持 IPv6 功能
能容纳的私网 IP 地址数量	2000	无限量

请注意，ECS 创建的实例和弹性网卡所属的安全组类型必须一致，同时 2019 年 5 月 30 日之前创建的 ECS 实例不可以加入企业安全组。

安全组具有状态检测能力，支持有状态服务，并且通过会话保持状态。如果数据包在出方向是被允许的，那么对应的此连接在入方向方向也是允许的。从 ECS 实例内发起请求时，默认放行同一会话中的响应（有默认保持最长时间限制）。

6.1.1.3. SSH 密钥对

SSH 密钥对是阿里云提供的远程登录 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

实例高可用性

单实例可用性高达 99.975%，跨 AZ 的多机可用性则达到了 99.995%。

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。具体请参见云产品安全-网络-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. 加密镜像

当用户的业务因为安全需求或法规合规要求等原因，需要对镜像中的数据进行加密保护时，

用户可以使用阿里云 ECS 镜像加密功能，无需构建、维护和保护自己的密钥管理基础设施，即可保护数据的隐私性和自主性。密钥管理服务（KMS）提供安全生成用户主密钥能力（Customer Master Key，CMK），也支持 BYOK 模式，即由用户上传密钥材料生成 CMK，并托管在 KMS 中。用户在加密镜像时，可以选择通过 KMS 生成的 CMK，可以选择自己上传的 CMK，也可以选择托管的服务密钥。

6.1.1.9. 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。

6.1.1.10.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 服务同时接入 STS，用户可以通过扮演 RAM 角色得到临时权限进行跨账号访问，该用户将拥有角色绑定策略内的访问权限，避免了 Access Key 在不同账号间的传播。

6.1.1.11.实例角色

ECS 同时支持通过接入 STS 来实现 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。

6.1.2. 弹性裸金属服务器（神龙）

弹性裸金属服务器（ECS Bare Metal Instance）是一种可弹性伸缩的高性能计算服务，计算性能与传统物理机无差别，且具有安全物理隔离的特点，提供给客户安全、可靠、稳定、独占的计算资源。

6.1.2.1. 用户独占计算资源

作为一款云端弹性计算类产品，弹性裸金属服务器具有与普通物理机无差别的高计算性能，使用户独占计算资源，无虚拟化性能开销和特性损失。在 CPU 规格选择上支持 8 核、32 核、96 核等多个规格，并支持超高主频实例。以 8 核产品为例，弹性裸金属服务器实例支持超高主频至 3.7 GHz ~ 4.1 GHz，与同类产品相比，它可以让游戏以及金融类业务获得更好的性能和更快的响应。同时，弹性裸金属服务器和阿里云其它产品完全互通兼容，使用户能够更好的构建完整的云端系统。

6.1.2.2. 加密计算

弹性裸金属服务器除了具备物理隔离特性外，为了更好地保障用户云上数据的安全性，弹性裸金属服务器支持 Intel ® SGX 芯片级可信执行环境，确保敏感数据可以在安全可信的环境中计算。这种芯片级的硬件安全保障相当于为用户云上的数据提供了一个保险箱功能，用户可以建立一个可信执行环境，并保护敏感数据（例如加解密密钥、账户凭证信息等）。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，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。

6.1.3. 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。

6.1.3.1. 身份认证

弹性伸缩会对每个 API 访问请求进行身份认证，因此用户需要在请求中包含签名（Signature）信息。弹性伸缩使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见阿里云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

6.1.3.2. RAM 和 STS 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。

弹性伸缩服务同时接入 STS，通过扮演 RAM 角色得到临时权限进行跨账号访问，该用户将拥有角色绑定策略内的访问权限，避免了 Access Key 在不同账号间的传播。

6.1.4. 资源编排

阿里云资源编排服务（Resource Orchestration Service，简称 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。

6.1.4.1. RAM 和 STS 支持

ROS 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。

ROS 服务同时接入 STS，用户可以通过扮演 RAM 角色得到临时权限进行跨账号访问，该用户将拥有角色绑定策略内的访问权限，避免了 Access Key 在不同账号间的传播。

6.1.5. 容器服务 Kubernetes 版

容器服务 Kubernetes 版提供高性能可伸缩的容器应用管理服务，支持用 Docker 和 Kubernetes 进行容器化应用的生命周期管理，提供多种应用发布方式和持续交付能力并支持微服务架构。

6.1.5.1. RAM 和 STS 支持

容器服务接入了 RAM 服务，用户可以通过 RAM 的访问控制能力限制子账号对容器服务集群的读写权限，同时支持通过 RAM 策略的定义限制请求 IP 源地址的黑白名单。

容器服务同时接入 STS，容器服务用户可以通过扮演 RAM 角色得到临时权限进行集群的跨账号访问，该用户将拥有角色绑定策略内的访问权限，避免了 Access Key 在不同账号间的传播。

6.1.5.2. 支持集群内资源的 RBAC 授权管理

主账号或集群管理员可以通过容器服务授权管理功能配置子账号在指定集群内调用 API server 访问 Kubernetes 集群内资源模型的访问权限。通过提供了管理员、运维人员、开发、受限等预置角色简化了集群内资源的授权管理，同时支持用户自定义的集群角色绑定，支持 namespace 的细粒度访问控制，同时支持所有集群维度和多个子账号的批量授权。

6.1.5.3. 审计支持

容器服务一方集成对接了阿里云日志服务（LogService），支持 apiserver 和 ingress 访问审计日志的自动采集和可视化过滤、检索。

6.1.5.4. 集群安全加固

容器服务依据国际第三方 Cyber Internet Security（CIS）组织的 CIS Kubernetes benchmark 进行了集群组件配置和集群运行环境的安全加固。

6.1.5.5. 容器 Runtime 安全监控

容器服务和云安全中心通过与云安全中心的集成监控容器应用运行时刻的行为安全，实时捕获并上报可疑攻击事件。当前云安全中心在容器服务产品支持容器内 Web-CMS 漏洞检测和修复、Webshell 检测和修复、云查杀、进程异常行为、异常网络连接、进程启动日志、网络连接日志的功能。

6.1.5.6. 安全沙箱容器支持

容器服务 ACK 提供基于阿里云神龙的安全容器版本，整套技术基于阿里云安全沙箱技术实

现，不同于传统的 Docker 共用内核架构，每个安全容器都有独享的内核，对内存、网络、IO 等实现了更强的隔离，用户可以基于这套框架，在单宿主机上更好地保障用户的多租户安全隔离。

6.2. 存储

6.2.1. 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。

6.2.1.1. 数据加密

当用户的业务因为安全需求或法规合规要求等原因，需要对存储在云盘上的数据进行加密保护时，用户可以使用阿里云 ECS 云盘加密功能。通过和阿里云密钥管理服务（KMS）的一方集成，用户无需构建、维护和保护自己的密钥管理基础设施和加密实现机制，即可通过云盘加密功能保护数据的隐私性和自主性。

ECS 云盘的加密功能默认使用服务密钥为用户的数据进行加密，同时也支持使用用户自选密钥为用户的数据进行加密。ECS 云盘的加密机制中，每一块云盘（Disk）会有相对应的用户主密钥（CMK）和数据密钥（DEK），并通过信封加密机制对用户数据进行加密。信封加密机制具体实现机制，请参见阿里云安全架构-用户数据安全-全链路加密-存储加密章节。

使用 ECS 云盘加密功能，系统会将从 ECS 实例传输到云盘的数据自动加密，并在读取数据时自动解密。加密解密在 ECS 实例所在的宿主机上进行，在加密解密的过程中，云盘的性能几乎没有衰减。

在创建加密云盘并将其挂载到 ECS 实例后，系统将对以下数据进行加密：

- 云盘中的静态数据
- 云盘和实例间传输的数据（实例操作系统内数据不加密）
- 从加密云盘创建的所有快照（即加密快照）

ECS 云盘加密支持所有在售云盘（普通云盘、高效云盘、SSD 云盘和 ESSD 云盘）和共享块存储（高效共享块存储和 SSD 共享块存储）。ECS 云盘加密支持所有在售的实例规格。所有地域都支持云盘的加密。

6.2.1.2. 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% 的数据持久性保证。

6.2.2. 文件存储

阿里云文件存储（Network Attached Storage，简称 NAS）是面向阿里云 ECS 实例、HPC 和 Docker 等计算节点的的文件存储服务，提供标准的文件访问协议。NAS 是一个可共享访问，弹性扩展，高可靠，高性能的分布式文件系统。它基于 POSIX 文件接口，天然适配原生操作系统，提供共享访问，同时保证数据一致性和锁互斥。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。

6.2.2.1. 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 同时提供了权限组功能，通过白名单添加权限组规则，允许指定的 IP 地址或网段访问文件系统，并可以给不同的 IP 地址或网段授予不同级别的细粒度访问权限。

6.2.2.2. RAM 支持

NAS 接入了 RAM 服务，支持通过 RAM 进行控制台访问权限的主子账号授权。

6.2.2.3. 高可用性

文件存储 NAS 中的数据自动地在可用区内以多副本冗余方式存储，避免数据的单点故障风险，提供高达 99.999999999%的数据持久性，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。

6.2.2.4. NFS 数据传输加密

NAS 支持通过 NFS 传输加密客户端以 TLS 方式挂载文件系统,并在挂载时使用阿里云 NAS 推荐的挂载选项。同时，该客户端还提供了日志功能，便于在挂载出错时定位错误原因。

NFS 传输加密客户端定义了一个新的网络文件类型：alinas。该文件类型能够与标准的 mount 命令无缝兼容。客户端还支持在系统启动时自动挂载文件系统，用户可以在/etc/fstab 文件中添加相关参数完成。使用 NFS 传输加密客户端进行 TLS 挂载时，工具会启动一个 stunnel 进程和一个监控进程 aliyun-alinas-mount-watchdog. stunnel 进程会对应用与 NAS 间的读写进行 TLS 加密并转发给 NAS 服务器。

6.2.2.5. 数据加密

当用户的业务因为安全需求或法规合规要求等原因，需要对存储在 NAS 上的数据进行加密保护时，用户可以使用 NAS 存储加密功能。通过和阿里云密钥管理服务（KMS）的一方集成，用户无需构建、维护和保护自己的密钥管理基础设施和加密实现机制，即可通过 NAS 加密功能保护数据的隐私性和自主性。

NAS 的加密功能默认使用服务密钥为用户的数据进行加密。NAS 的加密机制中，每一卷（Volume）会有相对应的用户主密钥（CMK，目前只支持 NAS 的服务密钥，后续会对自选密钥

进行支持）和数据密钥（DEK），并通过信封加密机制对用户数据进行加密。信封加密机制具体实现机制，请参见阿里云安全架构-用户数据安全-全链路加密-存储加密章节。

6.2.3. 对象存储

阿里云对象存储服务（Object Storage Service，简称 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。

6.2.3.1. 身份认证

OSS 会对每个非匿名的 API 访问请求进行身份认证。因此用户需要在请求中包含签名（Signature）信息。OSS 使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见阿里云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

6.2.3.2. 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。

针对存放在 Bucket 的 Object 的访问，OSS 提供了多种权限控制方式，包括 ACL、RAM Policy 和 Bucket Policy。

- ACL：OSS 为权限控制提供访问控制列表（ACL）。ACL 是基于资源的授权策略，可授予 Bucket 和 Object 访问权限。 用户可以在创建 Bucket 或上传 Object 时设置 ACL，也可以在创建 Bucket 或上传 Object 后的任意时间内修改 ACL。

- RAM Policy：Resource Access Management（RAM）是阿里云提供的资源访问控制服

务。RAM Policy 是基于用户的授权策略。通过设置 RAM Policy，可以集中管理用户（例如员工、系统或应用程序），以及控制用户可以访问哪些资源的权限。例如，能够限制用户只拥有对某一个 Bucket 的读权限。

- Bucket Policy：Bucket Policy 是基于资源的授权策略。相比于 RAM Policy，Bucket Policy 操作简单，支持在控制台直接进行图形化配置，并且 Bucket 拥有者直接可以进行访问授权，无需具备 RAM 操作权限。Bucket Policy 支持向其他账号的 RAM 用户授予访问权限，以及向匿名用户授予带特定 IP 条件限制的访问权限。

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。

请注意，用户上传 Object 时，如果不指定 Object 权限，OSS 会为 Object 设置为 default 权限和 Bucket 权限一致。如果没有设置 Object 的权限，那么 Object 的权限 Default 和 Bucket 权限一致。如果设置了 Object 的权限，则 Object 的权限大于 Bucket 权限。例如，设置了 Object 的权限是 public-read，则无论 Bucket 是什么权限设定，该 Object 都可以同时被身份验证访问和匿名访问。如果当一个 Object 被访问时，同时有 RAM Policy 和 Bucket Policy 生效，那么权限控制取并集，并做到 DENY 优先。

6.2.3.3. RAM 和 STS 支持

OSS 已支持 RAM 服务。使用阿里云的 RAM 服务，用户可以将云账号下 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。

6.2.3.4. 高可用性

OSS 采用多可用区（AZ）机制，将用户的数据分散存放在同一地域（Region）的 3 个可用区。当某个可用区不可用时，仍然能够保障数据的正常访问。OSS 同城冗余存储（多可用区）是基于 99.9999999999%（12 个 9）的数据可靠持久性设计，并且能够提供 99.95%的数据可用性 SLA 。

OSS 的同城冗余存储能够提供机房级容灾能力。当断网、断电或者发生灾难事件导致某个机房不可用时，仍然能够确保继续提供强一致性的服务能力，整个故障切换过程用户无感知，业务不中断、数据不丢失，可以满足关键业务系统对于“恢复时间目标（RTO）”以及“恢复点

目标（RPO）”等于 0 的强需求。

6.2.3.5. 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。

6.2.3.6. 访问日志

OSS 提供日志存储功能。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，可将 OSS 的访问日志，以小时为单位，按照固定的命名规则，自动生成一个 Object 写入用户指定的 Bucket（目标 Bucket，Target Bucket）。用户可以使用阿里云 DataLakeAnalytics 或搭建 Spark 集群等方式对这些日志文件进行分析。同时，用户可以配置目标 Bucket 的生命周期管理规则，将这些日志文件转成归档存储，长期归档保存。

实时日志查询功能将 OSS 与日志服务（LogService）相结合，允许用户在 OSS 控制台直接查询 OSS 访问日志，帮助用户完成 OSS 访问的操作审计、访问统计、异常事件回溯和问题定位等工作。

6.2.3.7. 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。

6.2.3.8. 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。例如，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。

6.2.3.9. 服务器端加密

OSS 支持在服务器端对上传的数据进行加密编码（Server-Side Encryption）：上传数据时，OSS 对收到的用户数据进行加密，然后再将得到的加密数据持久化保存下来；下载数据时，OSS 自动对保存的加密数据进行解密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。

OSS 有以下三种服务器端加密方式：

- 使用 OSS 托管的 CMK 进行加密（SSE-KMS）

  将 Bucket 默认的服务器端加密方式设置为 KMS 且不指定具体的 CMK ID，也可以在上传 Object 或修改 Object 的 meta 信息时，在请求中携带 X-OSS-server-side-encryption 并指定其值为 KMS 且不指定具体的 CMK ID。OSS 将使用 KMS 默认托管的服务密钥作为 CMK，并使用由 KMS 生成的数据加密密钥对数据对象进行信封加密，并且在下载时自动解密。

- 使用 BYOK 进行加密（SSE-KMS BYOK）

  服务器端加密支持使用 BYOK 进行加密，可以将 Bucket 默认的服务器端加密方式设置为 KMS 并指定具体的 CMK ID，也可以在上传 Object 或修改 Object 的 meta 信息时，在请求中携带 X-OSS-server-side-encryption，指定其值为 KMS，并指定 X-OSS-server-side-encryption-key-id 为具体的 CMK ID。OSS 将使用指定的 CMK，并使用由 KMS 生成的数据加密密钥对数据对象进行信封加密，并将加密 Object 的 CMK ID 记录到对象的元数据中，因此具有解密权限的用户下载对象时会自动解密。请注意本加密方式支持的是用户的自选密钥能力，即可指定使用用户在 KMS 中自行上传的 CMK，也可指定使用用户在 KMS 中自行生产的 CMK。

- 使用 OSS 完全托管加密（SSE-OSS）

  基于 OSS 完全托管的加密方式，是 Object 的一种属性。OSS 服务器端加密使用 AES256 加密每个对象，并为每个对象使用不同的密钥进行加密，作为额外的保护，它将使用定期轮转的主密钥对加密密钥本身进行加密。用户可以将 Bucket 默认的服务器端加密方式设置为 AES256，也可以在上传 Object 或修改 Object 的 meta 信息时，在请求中携带 X-OSS-server-side-encryption 并指定其值为 AES256，即可以实现该 Object 的服务器端加密存储。

6.2.3.10.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，即使数据泄露别人也无法解密得到原始数据。

- 使用 KMS 托管用户主密钥

  当使用 KMS 托管用户主密钥用于客户端数据加密时，无需向 OSS 加密客户端提供任何

加密密钥。只需要在上传对象时指定 KMS 用户主密钥 ID（也就是 CMK ID）。

- **使用用户自主管理密钥**

  使用用户自主管理密钥，需要用户自主生成并保管加密密钥。当用户本地客户端加密时，由用户自主上传加密密钥（对称加密密钥或者非对称加密密钥）至本地加密客户端。

6.2.3.11. 合规保留策略

OSS 现已全面支持 WORM（一次写入，多次读取）特性，允许用户以“不可删除、不可篡改”方式保存和使用数据，符合美国证券交易委员会（SEC）和金融业监管局（FINRA）的合规要求。OSS 提供强合规策略，用户可针对存储空间（Bucket）设置基于时间的合规保留策略。当策略锁定后，用户可以在 Bucket 中上传和读取文件（Object），但是在 Object 的保留时间到期之前，任何用户都无法删除 Object 和策略。Object 的保留时间到期后，才可以删除 Object。OSS 支持的 WORM 特性，适用于金融、保险、医疗、证券等行业。

6.2.3.12. 版本控制

OSS 支持版本控制功能。开启存储空间（Bucket）版本控制特性后，针对数据的覆盖和删除操作将会以历史版本的形式保存下来。通过文件（Object）的版本管理，用户在错误覆盖或者删除 Object 后，能够将 Bucket 中存储的 Object 恢复至任意时刻的历史版本。

版本控制应用于 Bucket 内的所有 Object。当第一次针对 Bucket 开启版本控制后，该 Bucket 中所有的 Object 将在之后一直受到版本控制，并且每个版本都具有唯一的版本 ID。Bucket 开启版本控制后，用户可以通过 lifecycle 自动删除过期版本。

6.3. 网络

6.3.1. 负载均衡 SLB

阿里云负载均衡（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。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。

6.3.1.1. 高可用性

SLB 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。

SLB 已在大部分地域部署了多可用区以实现同地域下的跨机房容灾。当主可用区出现故障或不可用时，负载均衡有能力在非常短的时间内（约 30 秒）切换到备可用区并恢复服务；当主可用区恢复时，负载均衡同样会自动切换到主可用区提供服务。

6.3.1.2. 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。

6.3.1.3. 抗 CC 攻击

SLB 支持 4 层和 7 层负载均衡。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 DDoS 高防产品可提供防御 DDoS 攻击能力。

采用 Tengine（淘宝网发起的 Web 服务器项目，在 Nginx 的基础上，针对有大访问量的网站需求进行了优化）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。

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

6.3.1.5. 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。

6.3.1.6. 日志功能

用户可以通过 ActionTrail 控制台查看负载均衡相关的操作日志。结合阿里云日志服务，用户可以通过分析负载均衡的访问日志了解客户端用户行为、客户端用户的地域分布，排查问题等。负载均衡也提供日志管理功能，用户可以查看健康检查日志。

6.3.1.7. RAM 和 STS 支持

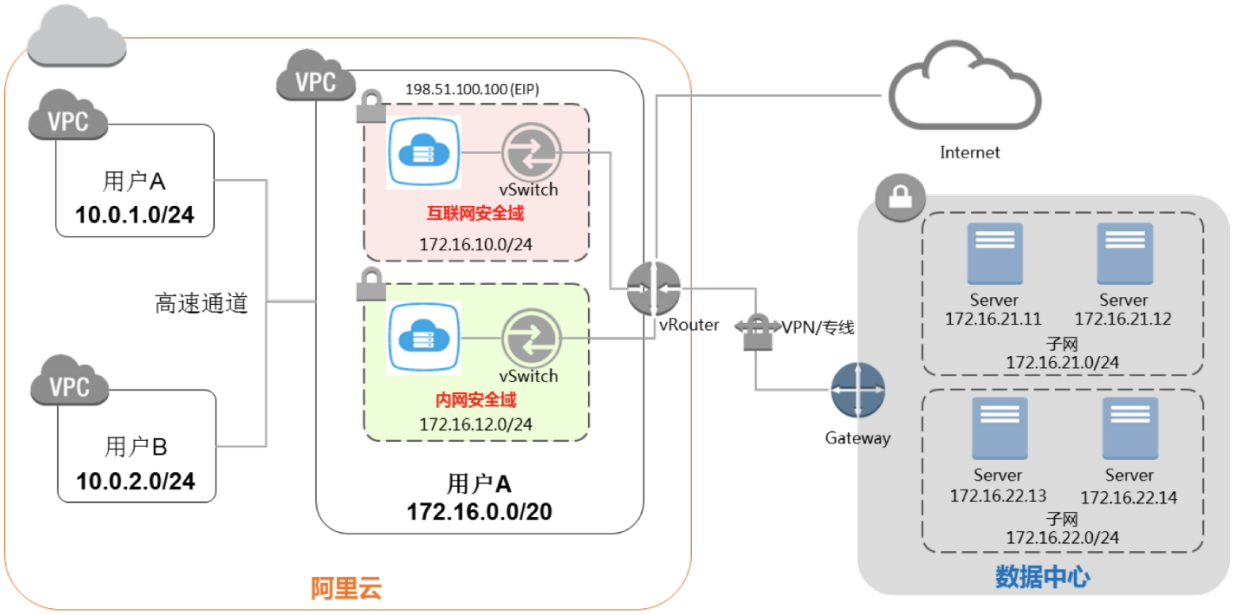
SLB 已支持 RAM 服务。用户可以将用户云账号下负载均衡资源的访问及管理权限授予 RAM 中子用户。

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。

6.3.2. 专有网络 VPC

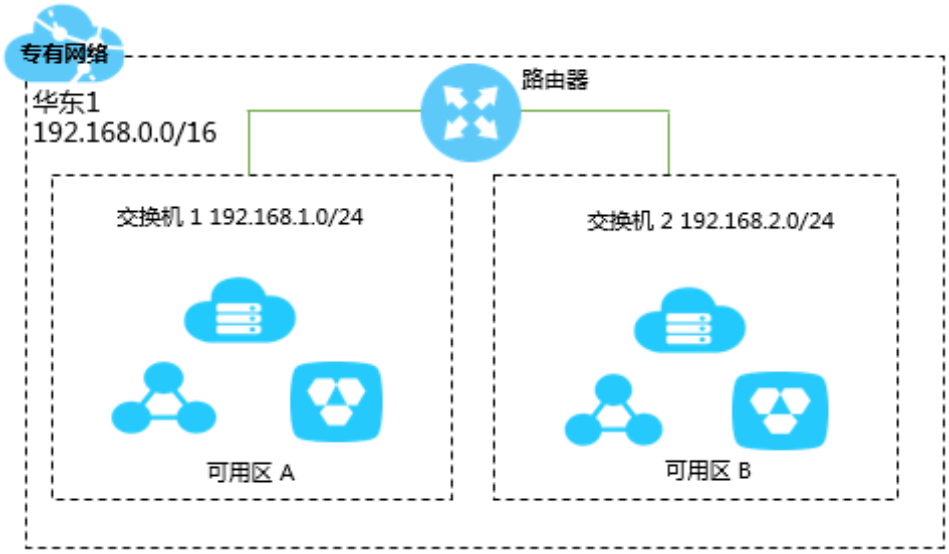
专有网络 VPC（Virtual Private Cloud，简称 VPC）是阿里云推荐使用的网络类型，专有网络之间逻辑上彻底隔离。VPC 能够为用户构建出一个隔离的网络环境（二层逻辑隔离），并可以自定义 IP 地址范围、网段、路由表和网关等；此外也可以通过 VPN 网关、高速通道物理专线、智能接入网关等服务将本地数据中心和云上 VPC 打通，也可以通过云企业网实现全球网络互通，在 VPC 间以及 VPC 与自有数据中心间搭建私网通信通道，从而形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

典型的 VPC 网络架构如下图所示：



6.3.2.1. 自定义网络

每个 VPC 都由一个私网网段（IPv4/IPv6）、一个路由器和至少一个交换机组成。路由器（VRouter）是专有网络的枢纽。作为专有网络中重要的功能组件，它可以连接 VPC 内的各个交换机，同时也是连接 VPC 和其他网络的网关设备。交换机（VSwitch）是组成专有网络的基础网络设备，用来连接不同的云资源。创建专有网络后，通过创建交换机为专有网络划分一个或多个子网。



自定义私网网段

IPv4 地址范围均处于 RFC 1918 中指定的私有（非公有可路由）IP 地址范围内，如下表所示。

开启 IPv6 功能的 VPC，阿里云自动为 VPC 分配一个掩码为/56 的 IPv6 网段，并免费创建一个 IPv6 网关，该网关默认只具备私网通信能力。

网段	可用私网 IP 数量（不包括系统保留地址）
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

自定义路由

VPC 中的路由表包括系统路由表和自定义路由表。系统路由表指的是在创建专有网络后，系统会默认创建一个路由表控制专有网络的路由，所有专有网络内的交换机默认使用该路由表。如果用户期望更灵活地进行网络管理，可在专有网络内创建自定义路由表，然后将其和交换机

绑定来控制子网路由。

系统路由表和自定义路由表都支持自定义路由 entry。在添加自定义路由 entry 时，用户可以指定以下下一跳类型，以支持不同的公私网访问场景：

- ECS 实例：将指向目标网段的流量转发到专有网络内的一台 ECS 实例。

  当需要通过该 ECS 实例部署的应用访问互联网或其他应用时，配置此类型的路由。

- VPN 网关：将指向目标网段的流量转发到一个 VPN 网关。

  当需要通过 VPN 网关连接本地网络或者其他专有网络时，配置此类型的路由。

- NAT 网关：将指向目标网段的流量转发到一个 NAT 网关。

  当需要通过 NAT 网关连接互联网时，配置此类型的路由。

- 路由器接口（专有网络方向）：将指向目标网段的流量转发到一个专有网络内。

  当需要使用高速通道连接两个专有网络时，配置此类型的路由。

- 路由器接口（边界路由器方向）：将指向目标网段的流量转发到一个边界路由器。

  当需要使用高速通道连接本地网络（物理专线接入）时，配置此类型的路由。

- 辅助弹性网卡：将指向目标网段的流量转发到指定的辅助弹性网卡。

- IPv6 网关：将指向目标网段的流量转发到一个 IPv6 网关。

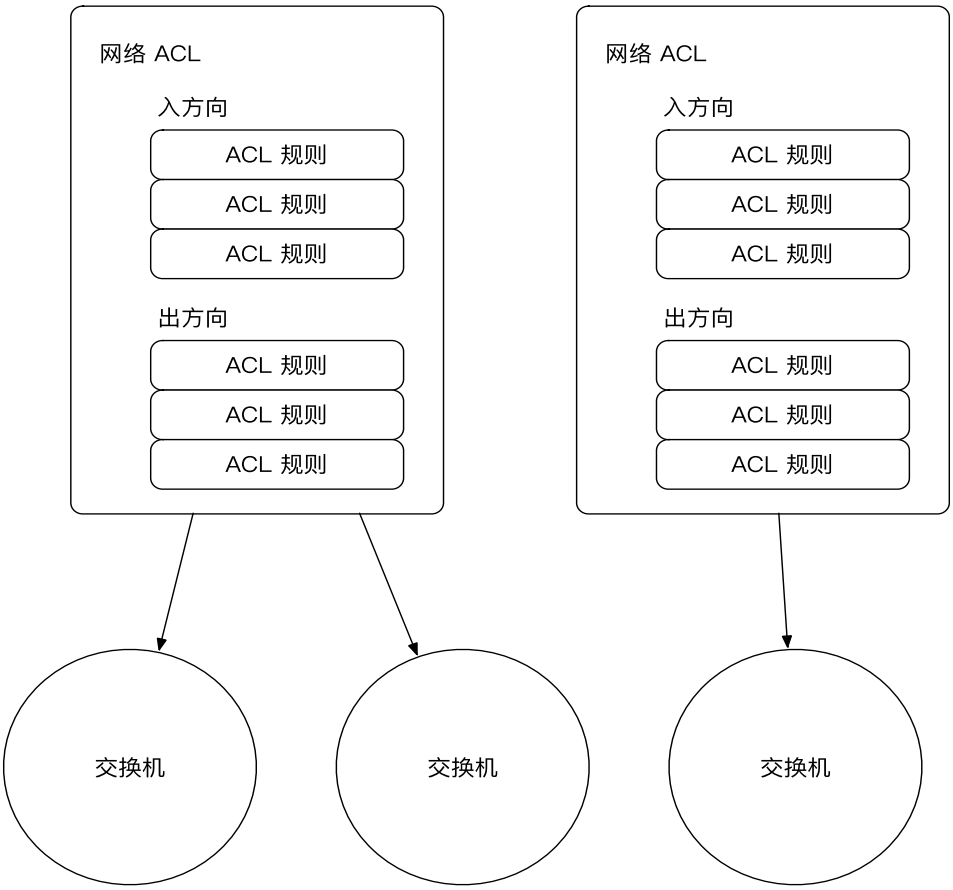
  当需要通过 IPv6 网关进行 IPv6 通信时，配置此类型的路由。

6.3.2.2. 访问控制

VPC 提供 2 种功能以提高 VPC 使用的安全性：

- 网络 ACL

网络访问控制列表是 VPC 中的网络访问控制功能，可以与交换机进行关联，实现在交换机级别同时控制入站和出站流量。规则包括入方向和出方向，用户可以对网络 ACL 的规则进行自主设置自定规则。网络 ACL 的规则是无状态的，设置入站规则允许某些请求后，需要同时设置相应的出站规则，否则可能会导致某些请求无法响应。



- ECS 安全组

安全组是一种用作关联 ECS 实例的虚拟防火墙，在实例级别同时控制入站和出站流量，具备状态检测和数据包过滤功能，用于在云端划分安全域。用户可以通过配置安全组规则，允许或禁止安全组内的 ECS 实例对公网或私网的访问。

6.3.2.3. 日志和监控

VPC 提供流日志功能，可以记录 VPC 网络中弹性网卡（ENI）的传入和传出流量信息，帮助用户检查访问控制规则、监控网络流量、进行网络故障排查。

用户可以捕获指定弹性网卡的流量，也可以捕获指定 VPC 或交换机的流量。如果选择为 VPC 或交换机创建流日志，则会捕获 VPC 和交换机中所有弹性网卡的流量，包括在开启流日志功能后新建的弹性网卡。

捕捉到的流量信息存储在阿里云日志服务中，可以在日志服务中查看和分析相关数据。

6.3.2.4. 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 之间互访建议使用云企业网。云企业网（CEN）支持将多个不同地域、不同账号的 VPC 连接起来，构建互联网络。

6.3.2.5. 网络边界控制

访问 Internet

专有网络是用户自定义的云上私有网络。专有网络中的云资源默认无法访问公网，也无法被公网访问。用户可以通过配置 ECS 实例固定公网 IP、弹性公网 IP、NAT 网关、负载均衡的方式连接公网。

产品	功能	优势
ECS 固定公网 IP	创建专有网络类型的 ECS 实例时，可以选择分配公网 IPv4 地址，系统会自动分配一个支持访问公网和被公网访问的 IP 地址。	支持使用共享流量包，将公网 IP 转换为 EIP 后也可以使用共享带宽。
弹性公网 IP（EIP）	能够动态和 VPC ECS 实例绑定和解绑，支持 VPC ECS 实例访问公网（SNAT）和被公网访问（DNAT）。	EIP 可以随时和 ECS 实例绑定和解绑。 可以使用共享带宽和共享流量包，降低公网成本。
NAT 网关	支持多台 VPC ECS 实例访问公网（SNAT）和被公网访问（DNAT）。	NAT 网关和 EIP 的核心区别是 NAT 网关可用于多台 VPC ECS 实例和公网通信，而 EIP 只能用于一台 VPC ECS 实例和公网通信。
负载均衡	基于端口提供四层和七层负载均衡功能，支持用户从公网通过负载均衡（SLB）访问 ECS。	在 DNAT 方面，负载均衡是基于端口的负载均衡，即一个负载均衡的一个端口可以对应多台 ECS。 负载均衡通过对多台 ECS 进行流量分发，可以扩展应用系统对外的服务能力，并通过消除单点故障提升应用系统的可用性。 绑定 EIP 后，可以使用共享带宽和共享流量包，降低公网成本。

VPC 互连

可以通过 VPN 网关、云企业网实现 VPC 见互连。

产品	功能	优势
VPN 网关	可以通过在两个 VPC 之间创建 IPsec 连接，建立加密通信通道。	• 安全：使用 IKE 和 IPsec 协议对传输数据进行加密，保证数据安全可靠。 • 高可用：采用双机热备架构，故障时秒级切换，保证会话不中断，业务无感知。 • 成本低：基于 Internet 建立加密通道，比建立专线的成本更低。 • 配置简单：开通即用，配置实时生效，快速完成部署。
云企业网	支持将多个不同地域、不同账号的 VPC 连接起来，构建互联网络。	• 一网通天下，实现阿里云全球网络资源互连。 • 低时延高速率。 • 就近接入与最短链路互通。 • 链路冗余及容灾。 • 系统化管理。

线下 IDC 接入

可以通过高速通道物理专线、VPN 网关、云企业网、智能接入网关将本地数据中心和云上 VPC 打通。

产品	功能	优势
高速通道	通过物理专线接入使 VPC 与本地 IDC 网络互通。	• 基于骨干网络，延迟低。 • 专线连接更加安全、可靠。
VPN 网关	可以通过建立 IPsec-VPN，将本地 IDC 网络和云上 VPC 连接起来。 可以通过建立 SSL-VPN，将本地客户端远程接入 VPC。	• 安全 • 高可用 • 低成本 • 配置简单
云企业网	**与本地 IDC 互通** 支持将要互通的本地 IDC 关联的边界路由器（VBR）加载到已创建的云企业网实例，构建互联网络。 **多 VPC 与 IDC 互通** 支持将要互通的多个网络实例（VPC 和 VBR）加载到已创建的云企业网实例，构建企业级互联网络。	• 一网通天下，实现阿里云全球网络资源互连。 • 低时延高速率。 • 就近接入与最短链路互通。 • 链路冗余及容灾。 • 系统化管理。
智能接入网关	可实现线下机构（IDC/分支机构/门店等）接入阿里云数据中心，轻松构建混合云。	配置高度自动化，即插即用，网络拓扑变化自适应快速收敛。

产品	功能	优势
	可实现线下机构之间互通。	城域内 Internet 就近接入，可通过设备及链路级主备方式实现线下多机构可靠上云。 混合云私网加密互连，Internet 传输过程中加密认证。

6.3.2.6. RAM 和 STS 支持

VPC 已支持 RAM 服务,用户可以将用户云账号下 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。

例如，在特定区域中只允许操作路由表以及路由表中的条目。

假设用户账号为 11111111，在阿里云上多个区域创建了 VPC，该权限只授予对杭州区域 VPC 的操作权限，且操作权限仅限于：允许删除/增加路由 entry，允许创建子网路由并关联 VSwitch，对于云产品只有查看权限。

6.4. 数据库

6.4.1. 云数据库 RDS 版

阿里云关系型数据库（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。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）、实例落盘加密、自动备份
- 容灾：同城容灾（多可用区实例）、异地容灾（容灾实例）
- 审计：SQL 洞察（SQL 审计）

6.4.1.1. 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。

6.4.1.2. 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，提高数据可回溯性。

6.4.1.3. 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，例如表/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。IP 白名单内还提供高安全白名单模式供用户在创建 IP 白名单分组时指定对于的网络类型（经典网络或专有网络）。

6.4.1.4. 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。

6.4.1.5. 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（Transparent Data Encryption，简称 TDE）功能。RDS for MySQL 的 TDE 功能由阿里云自研，RDS for SQL Server 的 TDE 功能基于 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时动态读取一次密钥。RDS for MySQL5.6/5.7/8.0, for SQL Server 2008 R2 支持 TDE 功能，并可通过服务密钥作为主密钥进行加密操作。同时 RDS for MySQL5.6/5.7/8.0 支持用户使用自选密钥作为主密钥进行加密操作。当 RDS 实例开启 TDE 功能后，用户可以指定参与加密的数据库或者表。这些数据库或者表中的数据在写入到任何设备（如磁盘、SSD、PCIe 卡）或者服务（如对象存储 OSS）前都会进行加密，因此实例对应的数据文件和备份都是以密文形式存在的。

云盘落盘加密

针对 RDS 云盘版实例，阿里云提供云盘加密功能，基于块存储对整个数据盘进行加密。

云盘加密使用的密钥由 KMS 服务加密保持，RDS 只在启动实例和迁移实例的时候动态读取一次密钥。RDS for MySQL 5.7/8.0, RDS for SQL Server 2012/2014/2016/2017，RDS for PostgreSQL 10/11 支持 RDS 云盘版实例落盘加密功能，并支持使用通过 KMS 保存管理的服务密钥和自选密钥作为主密钥进行加密操作。

6.4.1.6. SQL 洞察

RDS 提供 SQL 洞察功能。不仅能通过 SQL 审计日志记录对数据库执行的所有操作，从而对数据库进行故障分析、行为分析、安全审计等。同时提供增强搜索功能，可以按照数据库、用户、客户端 IP、线程 ID、执行时长、扫描行数等进行多维度检索，并支持导出和下载搜索结果。此外，新增 SQL 分析功能，可以对指定时间段的 SQL 日志进行可视化交互式分析，找出异常 SQL，定位性能问题。

6.4.1.7. 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。

6.4.1.8. 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（AZ）。

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（也称为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）。

6.4.1.9. 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。

6.4.1.10.RAM 和 STS 支持

RDS 已支持 RAM 服务。使用阿里云的 RAM 服务，用户可以将云账号下 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。

6.4.2. 表格存储

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 Serverless NoSQL 多模型数据库服务，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

表格存储会对每个 API 访问请求进行身份认证，因此用户需要在 请求中包含签名（Signature）信息。表格存储使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见阿里云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

6.4.2.2. 高可用性

通过自动的故障检测和数据迁移，表格存储对应用程序屏蔽了机器和网络的硬件故障，提供了高可用性。表格存储的服务可用性可以达到 99.9%。

表格存储将数据的多个备份存储在不同机架的不同机器上，并会在备份失效时进行快速恢复，提供 99.99999999%（10 个 9）的数据持久性。

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. 数据加密

当用户的业务因为安全需求或法规合规要求等原因，需要对存储在表格存储上的数据进行加密保护时，用户可以使用表格存储的加密功能。通过和阿里云密钥管理服务（KMS）的一方集成，用户无需构建、维护和保护自己的密钥管理基础设施和加密实现机制，即可通过表格存储的加密功能保护数据的隐私性和自主性。

表格存储的加密功能默认使用服务密钥为用户的数据进行加密，同时也支持使用用户自选密钥为用户的数据进行加密。表格存储的加密机制中，每一个表格（Table）会有相对应的用户主密钥（CMK）和数据密钥（DEK），并通过信封加密机制对用户数据进行加密。信封加密机制具体实现机制，请参见阿里云安全架构-用户数据安全-全链路加密-存储加密章节。

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，用户可以将云账号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。

6.5. CDN

6.5.1. 内容分发网络 CDN

阿里云内容分发网络（Content Delivery Network，简称 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。

6.5.1.1. 身份认证

阿里云 CDN 会对每个 API 访问请求进行身份认证，因此用户需要在 请求中包含签名（Signature）信息。阿里云 CDN 使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见阿里云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

6.5.1.2. 租户隔离

CDN 上用户的缓存数据，每片用户数据会打上用户标签，并且用户数据和数据索引会分离存储。用户认证采用 Access Key 对称密钥认证技术，对于用户请求会按域名颗粒度来区分。在用户验证通过后，根据用户域名来访问存储的数据，从而实现多用户间的数据存储隔离。

6.5.1.3. 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。

6.5.1.4. HTTPS 加速

HTTPS 是以安全为目标的 HTTP 通道，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。
- HTTPS 是主流趋势：未来主流浏览器会将 HTTP 协议标识为不安全，谷歌浏览器 Chrome 70 以上版本以及 Firefox 已经在 2018 年将 HTTP 网站标识为不安全，若坚持使用 HTTP 协议，除了安全会埋下隐患外，终端客户在访问网站时出现的不安全标识，也将影响访问。
- 百度与 Google 均对 HTTPS 网站进行搜索加权，主流浏览器均支持 HTTP/2，而支持 HTTP/2 必须支持 HTTPS。可以看出来，无论从安全，市场，还是用户体验来看，普及 HTTPS 是未来的一个方向，所以强烈建议用户将访问协议升级到 HTTPS。

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。

同时支持配置 HSTS 将实现客户端和阿里云 CDN 节点之间请求的 HTTPS 加密。CDN 节点返回从源站获取的资源给客户端时，按照源站的配置方式进行。支持 HTTP/2 建议源站配置并

开启 HTTPS，实现全链路的 HTTPS 加密。HTTP/2 基于 HTTPS，使用 HTTP/2 特性可以避免单纯使用 HTTPS 引起的性能下降问题。

6.5.1.5. 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。

6.5.1.6. 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。

6.5.1.7. RAM 和 STS 支持

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

CDN 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。

6.5.1.8. 图片鉴黄

图片鉴黄是 CDN 加速的一项增值服务，基于云计算平台，能对海量数据进行快速检测，可以帮助用户节省 90%以上的人力成本。开通图片鉴黄功能后，系统会自动检测通过 CDN 加速的图片是否涉黄，违规图片的 URL 将会被记录下来供用户导出和删除。

6.5.1.9. IP 黑白名单

阿里云 CDN 提供 IP 黑白名单功能，并支持 IPv6 地址和网段描述。

- IP 黑名单：黑名单内的 IP 均无法访问当前资源。如果一个 IP 被加入黑名单，该 IP 的请求仍可访问到 CDN 节点，但是会被 CDN 节点拒绝并返回 403，CDN 日志中仍会记录这些黑名单中的 IP 请求记录。
- IP 白名单:只有白名单内的 IP 能访问当前资源,白名单以外的 IP 均无法访问当前资源。

请注意，黑名单和白名单互斥，同一时间只支持其中一种方式生效。

6.5.1.10.UA 黑白名单

阿里云 CDN 提供配置 User-agent 黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问 CDN 资源的用户，提升 CDN 的安全性。

当用户需要根据请求的 User-Agent 字段进行访问控制时，可以配置 User-Agent 黑/白名单功能，实现对请求过滤。

- User-Agent 黑名单:黑名单内的 User-Agent 字段均无法访问当前资源。如果一个 User-Agent 字段被加入黑名单，该带有 User-Agent 字段的请求仍可访问到 CDN 节点，但是会被 CDN 节点拒绝并返回 403，CDN 日志中仍会记录这些黑名单中的 User-Agent

字段请求记录。

- User-Agent 白名单：只有白名单内的 User-Agent 字段才能访问当前资源，白名单以外的 User-Agent 字段均无法访问当前资源。

请注意，黑名单和白名单互斥，同一时间只支持其中一种方式生效。

6.6. 数据与智能

6.6.1. 大数据计算服务

阿里云大数据计算服务（MaxCompute）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。

6.6.1.1. 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。

RAM 是阿里云为客户提供的用户身份管理与资源访问控制服务。MaxCompute 与 RAM 的集成使用主要有两个场景：

- 通过 DataWorks 使用 MaxCompute 时，子账户的身份管理。具体表现为主帐号开通并创建项目后，若需要通过 DataWorks 使用 MaxCompute 且多个账户协同开发，必须由主帐号到 RAM 服务中创建子账户，将 RAM 子账户添加为项目成员从而进行协同开发。
- MaxCompute 处理非结构化数据时，通过 RAM 对非结构化数据进行授权。目前 MaxCompute 支持直接处理非结构化数据（包含 OSS 和 Table Store），前提条件之一就是需要在 RAM 中授予 MaxCompute 访问 OSS 或 Table Store 的权限。

MaxCompute 会对每个 API 访问请求进行身份认证，因此用户需要在 请求中包含签名（Signature）信息。MaxCompute 使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

6.6.1.2. 访问授权

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（例如，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，针对项目空间、表（View 也需要单独授权）、函数、资源、 任务实例等多种对象，授予不同权限。同时，MaxCompute 支持列级别的敏感数据打标（Label Security）以达到细粒度的访问控制。

授权机制

MaxCompute 支持通过 ACL 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。

当前 MaxCompute 权限模型支持真正意义上的字段（列）级别的 ACL 访问控制，字段也作为 ACL 支持的对象之一，和表一样是独立的授权主体，包含完整的授权信息(如权限有效期)。例如：

grant Alter on Table T1(c1,c2) to USER ALIYUN$bob@aliyun.com;

//收取修改 c1、c2 两个字段的权限

revoke Alter on Table T1(c1,c2) from USER ALIYUN$bob@aliyun.com;

//回收修改 c1、c2 两个字段的权限

基于标签的安全（Label Security）是项目空间级别的一种强制访问控制策略（Mandatory Access Control，简称 MAC），它的引入可以让项目空间管理员更加灵活地控制用户对列级别敏感数据的访问。Label Security 默认关闭，一旦开启，管理员可以对表的任何列设置敏感度标记（Label），一张表可以由不同敏感等级的数据列构成。默认时所有用户的访问许可等级为 0 级，数据安全级别默认为 0 级。在对数据和人分别设置安全等级标记之后，LabelSecurity 的默认安全策略如下：

- No-ReadUp：不允许用户读取敏感等级高于用户等级的数据，除非显式授权。
- Trusted-User：允许用户写任意等级的数据，新建数据默认为 0 级(不保密)。

管理类操作授权和项目所有权分离

MaxCompute 为管理类操作定义了权限。例如，拥有 CreatePackage 权限的项目空间内成员就可以创建 package；拥有 AddPackageResource 权限的项目空间内成员就可以向 package

中添加资源。用户可以用 MaxCompute 的 Policy 方式对管理类的操作进行授权。并且 MaxCompute 利用这个特性定义了一个新的系统角色，这个角色在访问控制的管理上和项目 Owner 有同等的权限，以此实现项目空间所有权和管理权的分离。后续 MaxCompute 还会支持用户创建自定义的管理类角色，实现分级管理。

RAM 用户组支持

RAM 新增了 RAM Group 用于管理一组用户，MaxCompute 也相应增加了对 RAM Group 的支持，对 RAM Group 的授权会作用到 group 里的所有成员。例如，只要把 RAM Group 加到项目空间，那么 group 下的所有用户都有访问空间的权限，而不需要单独加账号。

6.6.1.3. 数据保护机制

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”。

MaxCompute 增加了数据下载权限的管理，之前有 Select 权限即可通过 Tunnel 下载数据，现在 MaxCompute 定义了 Download 权限，与 Select 权限剥离。Download 权限后可以通过 ACL 授予，可以把数据下载的粒度控制的更细。

6.6.1.4. 跨项目空间的资源分享

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资源共享和用户授权问题。 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，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，并且可以对 package 内的资源进行单独授权。

6.6.1.5. 数据隔离

MaxCompute 支持多租户的使用场景，认证方式采用阿里云账号体系的 AccessKey 对称密钥认证技术，同时对于用户的每一个 HTTP 请求都会进行签名认证，针对不同的用户数据进行数据存储隔离，用户数据被离散存储在分布式文件系统中。可以同时满足多用户协同、数据共享、数据保密和安全的需要，做到真正的多租户资源隔离。

同时，MaxCompute 中所有计算是在受限的沙箱中运行，多层次的应用沙箱，从 KVM 级到 Kernel 级。系统沙箱配合鉴权管理机制，用来保证数据的安全，以避免出现内部人员恶意或粗心造成服务器故障。

6.6.1.6. 数据加密

传输加密

MaxCompute 提供 Restful 的传输接口，其传输安全性由 HTTPS 保证。

存储加密

当用户的业务因为安全需求或法规合规要求等原因，需要对存储在 MaxCompute 中的数据进行加密保护时，用户可以使用 MaxCompute 加密功能。通过和阿里云密钥管理服务（KMS）的一方集成，用户无需构建、维护和保护自己的密钥管理基础设施和加密实现机制，即可通过 MaxCompute 加密功能保护数据的隐私性和自主性。

MaxCompute 的加密功能默认使用服务密钥为用户的数据进行加密。MaxCompute 以项目为单位支持表的加密存储，目前仅支持全表加密。每一个项目（Project）会有相对应的用户主密钥（CMK）和多个数据密钥（DEK），并通过信封加密机制对用户数据进行加密。信封加密机制具体实现机制，请参见阿里云安全架构-用户数据安全-全链路加密-存储加密章节。

6.6.1.7. 敏感数据保护

数据分类分级

基于 Label Security，用户可以对字段进行类别标识并定义分级，以此实现敏感数据的分类分级。

数据脱敏

MaxCompute 提供了接入脱敏应用的能力，即 MaxCompute 可接入各类脱敏应用生态，脱敏算法由具备专业脱敏能力的应用提供。 例如数据保护伞提供脱敏算法，MaxCompute 在计算中调用脱敏算法，输出脱敏后内容。

6.6.1.8. 数据备份和删除

备份

阿里云提供一个扁平的线性存储空间，并在内部对线性地址进行切片，一个分片称为一个 Chunk。 对于每一个 Chunk，都会复制出三个副本，并将这些副本按照一定的策略存放在集群中的不同节点上，保证用户数据的可靠。

删除

在用户进行删除操作后，释放的存储空间由飞天分布式文件系统回收，禁止任何用户访问，同时进行内容擦除，最大限度保证用户的数据安全性。

6.6.1.9. 日志审计

MaxCompute 会针对不同用户不同日志数据进行日志审计，提供日志数据存储，包括静态数据、运行记录及安全信息等内容。

- Information_Schema

  参考业界规范，开放 MaxCompute 元数据及作业历史，客户可以低成本、自助地获取

元数据，满足用户安全管理、作业优化、成本分析的需求。

- 审计日志

  捕获用户的关键行为，并通过接入阿里云 Action Trail 服务将 MaxCompute 用户行为日志实时推送给客户，满足客户实时审计、问题回溯分析等需求。

6.6.1.10.IP 白名单

MaxCompute 安全上的访问控制有多个层次：如项目空间的多租户及安全认证机制，只有获取了正确的、经过授权的 AccessKey ID 及 Access Secret 才能通过鉴权，在已经赋予的权限范围内进行数据访问和计算。在以上访问认证基础上还有一种增强的、以 IP 白名单的方式，进行访问控制的配置方法和策略。配置之后，满足配置规则的 IP 地址及 IP 地址段才能访问该项目空间。在原有 AccessKey ID 及 AccessKey Secret 认证基础上叠加了 IP 规则的检查。

IP 白名单支持可以设置整个 VPC 或者 VPC 的内部 IP。

6.6.2. 分析型数据库 MySQL 版

分析型数据库 MySQL 版（AnalyticDB for MySQL），是阿里巴巴自主研发的海量数据实时高并发在线分析（Real-time 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 MySQL 版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。

分析型数据库目前已升级至 AnalyticDB for MySQL 3.0 版本，下文的安全特性以 3.0 版本为准。

6.6.2.1. 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，连接时以数据库的账号名为连接用户名，数据库库账号对应的密码为连接密码。如果是原 2.0 版客户，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。

分析型数据库支持 VPC，用户可以在创建集群时指定集群所属的 VPC。VPC 能够保证网络层面的安全隔离，进一步保护用户的安全。

6.6.2.2. 集群白名单

分析型数据库支持集群白名单功能，以进一步控制外部设备对集群的访问。集群默认的白名单只包含默认 IP 地址 127.0.0.1，表示任何设备均无法访问该集群，用户可以根据自身业务需求添加允许访问的 IP 地址或 IP 段。白名单可以让 AnalyticDB for MySQL 集群得到高级别的访问安全保护，设置白名单不会影响集群的正常运行。

6.6.2.3. 高可用性

基于分布式高可用存储提供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 SLB 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。

6.6.2.4. 用户与权限

分析型数据库支持两种类型的数据库账号：高权限账号和普通账号。高权限账号相当于MySQL 中的 root 账号，可以管理所有普通账号和数据库。

数据库支持层级权限管理模型，提供类似 MySQL 的 ACL 授权模式。分析型数据库支持四个粒度的权限控制：GLOBAL 集群级别、DB 数据库级别、TABLE 表级别、COLUMN 列（字段）级别。类似 MySQL，分析型数据库中的高权限账号可以使用 GRANT/REVOKE 语句进行授权和权限回收。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。

6.6.2.5. RAM 支持

阿里云分析型数据库支持通过阿里云 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在数据库实例中创建的数据库账号和密码作为连接用户名和连接密码。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。

6.6.3. 数加 DataWorks

DataWorks 是一站式大数据智能云研发平台，可提供数据集成、数据开发、监控运维、数据地图、数据质量、数据安全和数据服务等全方位的大数据服务，帮助企业专注于数据价值的挖掘和探索。

6.6.3.1. 访问控制

登录控制

主账号在阿里云访问控制的控制台中，可以新建多个 RAM 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 DataWorks。条件限制包括：IP 地址/地址段、MFA 多因素认证、HTTPS 访问协议等。

通过限制能够访问 DataWorks 的来源 IP 或 IP 地址段，可进一步防止非法访问，保障数据与业务安全。例如，当用户自身访问密钥不慎丢失或被盗时，用户在更换新密钥之前，能够防止来自非法 IP（如非公司内网来源 IP）的访问登录。

沙箱隔离

“工作空间”是 DataWorks 用户数据隔离的基本单位，工作空间内的所有任务均运行在沙箱内，以保证数据不被泄露，同时也防止开发人员擅自操作外部资源。默认情况下，仅可访问：

- 数据开发任务仅可访问指定的计算引擎
- 数据集成任务仅可访问已添加的数据源

如需在工作空间中访问除以上两种情形之外的外部资源，需要由工作空间管理员进行沙箱白名单设置。如需访问 VPC 网络中的资源，需使用独享资源组。

6.6.3.2. 开发/生产权限隔离

DataWorks 支持以“工作空间”为单位管理代码与配置。工作空间又分为标准模式及简单模式。

标准模式的工作空间具有隔离的开发/生产环境。以 MaxCompute 引擎为例，标准模式工作空间对应两个 MaxCompute 项目，分别为开发环境与生产环境。开发环境与生产环境的数据完全隔离。开发人员通过 DataWorks 数据开发界面，仅能操作开发环境数据；对于生产环境数

据的变更，需要由运维人员执行“发布”操作后，方可实现。标准模式工作空间可以严格控制表权限，禁止随意操作生产环境的表，保证生产表的数据安全。

简单模式的工作空间开发与生产环境合二为一，优势在于迭代快，代码提交后，无需发布即可生效，但无法保证开发/生产环境的权限隔离。

6.6.3.3. 权限管理

角色管理

DataWorks 自带的权限托管策略中包含所有者、管理员、开发、运维、部署、访客和安全管理员七种角色定义：

- 所有者是工作空间的最高权限者，具有所有权限。
- 管理员是所有者委托的管理者，具有除删除工作空间之外的所有权限。
- 开发是开发环境的操作者，具有开发节点、业务流程与操作开发环境数据的权限。
- 运维是生产环境的操作者，可对生产环境的任务节点进行中止、重跑等操作，同时具备部署权限。
- 部署是开发、生产环境的连接者，具有将开发环境的代码发布至生产环境的权限。
- 安全管理员是数据安全的管理者，具备操作数据保护伞配置的权限。
- 访客具备最小权限，仅能查看代码，无法进行任何操作。

权限管理

DataWorks 支持对工作空间中的数据权限进行管理。支持表级、字段级授权，并支持权限的查看与审计。

数据下载控制

DataWorks 支持配置数据下载控制，可以降低用户数据外泄的风险，保障用户数据安全。

6.6.3.4. 数据加密

DataWorks 所有敏感信息包括用户代码、业务流程配置、数据源连接等信息均加密存储。只有合法并具备权限的用户，方能查看、使用、修改这些数据。底层数据加密依靠 MaxCompute 存储的加密能力。

6.6.3.5. 敏感数据保护

DataWorks 提供数据识别、敏感数据发现、数据分类分级、脱敏、访问监控、风险发现预警与审计能力。

- 通过数据识别，可以按照预设的规则，自动识别工作空间中的敏感数据。
- 通过数据分级分类，可对数据的密级进行定义，并分别进行访问控制。
- 通过数据脱敏，可通过遮蔽、假名、哈希等方式对敏感数据进行脱敏。
- 通过访问监控，可以对敏感数据的导出、访问进行监控。
- 通过风险发现，可以对特定场景下的敏感数据访问行为进行监控。

6.6.4. 实时计算

阿里云实时计算（Alibaba Cloud Realtime Compute）是一套基于 Apache Flink 构建的一站式、高性能实时大数据处理平台，广泛适用于流式数据处理、离线数据处理等多种场景。

6.6.4.1. 租户隔离

阿里云实时计算支持共享模式和独享模式两种产品模式。相比于多用户共享集群物理资源的共享模式，独享模式是指在阿里云 ECS 上单独为用户创建独立计算集群，单个用户独享计算

集群的物理资源（网络、磁盘、CPU 或内存等），与其他用户的资源完全独立。用户在独享模式下能够使用专有网络 VPC 和独享计算资源，充分保障用户的安全隔离。由于独享模式在网络及计算资源层面与其他用户完全的隔离，能够支持自定义函数等更底层的 API，满足用户的业务需求。

6.6.4.2. RAM 支持

实时计算支持 RAM 账号体系，用户可以通过角色管理等方法进行自定义授权。对于调用其他服务与资源的情形，用户可以通过设置针对实时计算的 AliyunStreamDefaultRole 角色，方便的进行产品间授权。

此外，如用户长时间没有对作业进行操作，系统会自动发起 MFA 多因素认证，以提高账号安全性。

6.6.4.3. 数据存储账号保护

支持利用存储注册方式连接同账户下数据存储资源，不需要用户明文输入 AccessKey 引用上下游存储资源，防止用户秘密信息泄露。存储注册方式是将上下游存储资源预先注册至实时计算开发平台，然后通过实时计算控制台的数据存储管理功能，对上下游存储资源进行引用。使用存储注册方式后，实时计算控制台能够为用户提供数据预览、数据抽样、DDL 自动生成等功能，便于用户一站式管理云上存储资源。

6.6.4.4. 数据加密

在数据传输加密方面，传输链路使用上下游组件的 SDK，复用 SDK 中的加密能力。在数据静态加密方面，实时计算本身不负责存储用户的业务数据，具体数据静态加密由相关联的阿里云存储系统保证。

6.6.4.5. 监控审计

在日志审计方面，实时计算支持日志下载功能，用户可以通过编辑实时计算作业参数，自定义实时计算作业日志输出的级别和路径。

在监控报警方面，实时计算接入云监控服务，能够收集阿里云资源或用户自定义的监控指标、探测服务可用性以及针对指标设置警报，让用户全面了解阿里云上的资源使用情况、业务的运行状况和健康度，并及时接收异常报警，保证应用程序顺畅运行。

6.7. 应用服务

6.7.1. 开放搜索服务

阿里云开放搜索（OpenSearch）基于阿里巴巴自主研发的大规模分布式搜索引擎平台，为开发者提供简单、高效、稳定、低成本和可扩展的搜索解决方案。用户通过在控制台创建实例后，根据业务场景需求可定制数据表结构、字段的搜索属性以及对接数据源信息等，完成基础搜索服务的搭建；对于追求高质量搜索效果的用户，在基础搜索服务以外可通过配置查询分析、排序表达式、排序算法模型训练等功能实现搜索效果指标（比如 CTR）的提升，同时配套 abtest、效果指标报表等功能的使用，用户可在 OpenSearch 平台上实现持续迭代、持续优化搜索效果的全闭环流程。

6.7.1.1. 高可用性

开放搜索服务（Open Search）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。

6.7.1.2. 数据隔离与备份

开放搜索服务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。

6.7.1.3. 数据配额

开放搜索服务提供针对存储容量大小、计算资源（LCU）的配额机制。

6.7.1.4. 身份认证

开放搜索服务（Open Search）会对每个 API 访问请求进行身份认证，因此用户需要在 请求中包含签名（Signature）信息。开放搜索服务使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息,请参见云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

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。

6.7.1.5. 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。

6.7.1.6. RAM 支持

OpenSearch 已支持 RAM 服务。使用阿里云的 RAM 服务,用户可以将云账号下 OpenSearch 资源的访问及管理权限授予 RAM 中子用户。

6.7.2. 媒体处理

媒体处理（ApsaraVideo Media Processing，原 MTS）是一种多媒体数据处理服务。它以经济、弹性和高可扩展的转换方法，将多媒体数据转码成适合在全平台播放的格式。并基于海量数据深度学习，对媒体的内容、文字、语音、场景多模态分析，实现智能审核、内容理解、智能编辑。

6.7.2.1. RAM 和 STS 支持

媒体处理服务接入了 RAM 与 STS 服务，用户可通过 RAM 完成子账号的授权与管理，通过 STS 生成临时访问凭证以进行短期访问权限管理。

6.7.2.2. 身份认证

媒体处理服务接入 API 网关，会对每个 API 访问请求进行身份认证，因此用户需要在请求中包含签名（Signature）信息。媒体处理使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

媒体处理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。

6.7.2.3. 监控报警

媒体处理服务通过对接云监控服务提供包括系统性能和用量在内的监控数据指标，用户还可以使用自定义报警服务，监控服务稳定性、分析使用情况，及时发现以及诊断相关问题。

6.7.2.4. 视频加密

媒体处理服务支持视频加密功能。视频加密是对视频内容保护的一种手段，对视频中的内容进行加密，可有效防止视频泄露和盗链问题。媒体处理服务目前支持私有加密和 HLS 标准加密两种加密方式，用户可以通过媒体处理控制台或 API 方式进行配置与管理。

6.7.2.5. 智能审核

媒体处理服务的智能审核功能可以智能识别视频内语音、文字、画面的色情、暴恐涉政、不良画面等内容，大幅节省人工审核人力成本，降低违规风险。

6.7.2.6. 视频版权保护

媒体处理服务通过视频版权管理 DRM 和视频指纹功能帮助用户进行视频版权保护。媒体处理服务支持 ChinaDRM 和 Widevine 两种 DRM 视频加密方案。同时，正在研发基于 PlayReady 和 FairPlay 等国际通用 DRM 协议的视频加密方案，进一步加固 H5 端内容安全。视频指纹功能可以提取视频中的声音、图像及时序特征，生成视频指纹，能够适用于侵权视频过滤、原创视频保护等场景。

6.7.3. 消息队列 RocketMQ

消息队列 RocketMQ 是阿里云基于 Apache RocketMQ 构建的低延迟、高并发、高可用、高可靠的分布式消息中间件。该产品最初由阿里巴巴自研并捐赠给 Apache 基金会。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。消息队列 RocketMQ 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。

6.7.3.1. RAM 和 STS 支持

消息队列 RocketMQ 默认情况下，只支持队列创建者访问消息队列数据。同时，消息队列 RocketMQ 接入了阿里云的访问控制 RAM 服务，用户可以将用户云账号下的消息队列资源的访问及管理权限授予 RAM 中子用户。

消息队列 RocketMQ 服务同时接入 STS，用户可以通过扮演 RAM 角色得到临时权限进行跨账号访问，该用户将拥有角色绑定策略内的访问权限，避免了 Access Key 在不同账号间的传播。

6.7.3.2. 监控告警

用户可使用消息队列提供的监控报警功能，监控消息消费状态并接收报警短信，帮助用户

实时掌握消息消费状态，以便及时处理消费异常。

6.7.4. 性能测试服务

性能测试（Performance Testing Service，简称 PTS）是具备强大的分布式压测能力的 SaaS 压测平台，可模拟海量用户的真实业务场景，全方位验证业务站点的性能、容量和稳定性。

PTS 目标是将性能压测本身的工作持续简化，使用户可以将更多的精力回归到关注业务和性能问题本身。在 PTS 平台上，用户可以用最低的人力和资源成本，构造出最接近真实业务场景的复杂交互式流量，快速衡量系统的业务性能状况，为性能问题定位、容量最佳配比、全链路压测的流量构造提供最好的帮助。进而提升用户体验，促进业务发展，最大程度实现企业的商业价值。

6.7.4.1. 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。

6.7.4.2. 监控和审计

PTS 本身已经具备的强大的客户端监控指标，以及应用服务器、数据库、中间件、网络入口等方面的指标。

PTS 集成云监控与业务实时监控服务（Application Real-Time Monitoring Service，简称 ARMS），在监控硬件层面指标的同时，也能够从业务角度监控应用的指标。

当用户在测试时，PTS 会根据监控指标进行告警，保障性能测试服务的可用性，监控告警措

施包括旺旺、邮件和短信等。

6.7.4.3. RAM 和 STS 支持

PTS 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。

PTS 服务同时接入 STS，用户可以通过扮演 RAM 角色得到临时权限进行跨账号访问，该用户将拥有角色绑定策略内的访问权限，避免了 Access Key 在不同账号间的传播。

6.7.5. 企业邮箱

企业邮箱业务是以企业域名做后缀的邮箱，既能体现公司的品牌和形象，又能方便公司主管人员对员工信箱进行统一管理，还能使得公司商业信函来往获得更好更安全的管理，是现今互联网时代中不可缺少的现代化的通讯工具。

阿里企业邮箱是阿里云重要产品之一，基于阿里云专业云计算技术和平台打造，庞大的服务器集群构建在全球多个节点之上，保证邮件在全球收发无阻；产品方面围绕“高效、安全、智能”，深度结合钉钉高效的工作方式，致力于打造移动智能时代的高效办公邮箱。目前已经服务于 500 万家企事业单位，是中国最大的企业邮箱服务提供商之一。

6.7.5.1. 认证与权限管理

企业邮箱支持设置统一的企业登录密码策略，并支持初始密码未修改提醒，以降低弱密码引入的风险。同时支持多次不同密码认证失败的账号自动锁定，以防止暴力破解。企业邮箱具备双因素认证能力，支持对于客户办公网外的“密码+验证码”认证策略。

企业邮箱配备包括 Windows、MAC、Android、iOS 版在内的多种邮件客户端以便于用户进行安全登录。对于 Web 端登陆而言，支持水印二次验证码、App 扫码登录、钉钉扫码登录等多种安全验证方式。

企业邮箱支持分级管理，实现管理员权限的进一步分隔。就企业实际使用场景而言，不仅支持设置多个部门管理员对不同部门人员进行分隔管理，还支持对某些特定功能权限进行单独分隔管理。

6.7.5.2. 邮件控制

企业邮箱具备完善的邮件控制机制。不仅支持对各成员进行外域发信/收信的使能设置以限制邮件外发，还支持邮件审批，邮件撤回，发信数量和频率限制等一系列邮件控制措施。

企业邮箱配备自研的用于亿级用户量的反垃圾邮件系统，从攻击防护和异常检测、身份识别、用户行为和邮件内容检测等多个层面帮助用户自动识别垃圾邮件。用户也可以通过设置外域入信黑名单和白名单的方式对邮件实现进一步管控。

企业邮箱对接由阿里巴巴安全团队专业维护和更新的钓鱼库&病毒查杀引擎，针对钓鱼和病毒邮件进行深入分析，专项查杀。

6.7.5.3. 传输加密

企业邮箱支持使用 SSL/TLS 协议进行传输加密以保证用户数据的机密性。

6.7.5.4. 审计与告警

除用户可以查看自己的登录情况以及收发邮件情况外，管理员也可以通过域管理查询员工的登录使用情况，实时关注员工使用状态。在域管理页面中，同样可以查询管理员的操作日志。

企业邮箱支持对邮件日志进行提取，可以通过提交工单的方式进行申请。

企业邮箱提供对于异地登录（非此前常用 IP）等异常登录行为的提醒，方便用户及时采取修改密码等安全应对措施。

6.7.6. 云监控

云监控（Cloud Monitor）是一项针对阿里云资源和互联网应用进行监控的服务。

云监控为云上用户提供开箱即用的企业级开放型一站式监控解决方案。涵盖 IT 设施基础监控，外网网络质量拨测监控，基于事件、自定义指标、日志的业务监控。为用户全方位提供更高效、更全面、更省钱的监控服务。通过提供跨产品、跨地域的应用分组管理模型和报警模板，帮助用户快速构建支持几十种云产品、管理数万实例的高效监控报警管理体系。通过提供 Dashboard，帮助用户快速构建自定义业务监控大盘。使用云监控，不但可以帮助用户提升用户的系统服务可用时长，还可以降低企业 IT 运维监控成本。

云监控服务可用于收集获取阿里云资源的监控指标或用户自定义的监控指标，探测服务可用性，以及针对指标设置警报。使用户全面了解阿里云上的资源使用情况、业务的运行状况和健康度，并及时收到异常报警做出反应，保证应用程序顺畅运行。

6.7.6.1. 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。

云监控也支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

RAM 访问控制系统权限中的只读访问云监控（CloudMonitor）的权限包含查询监控数据、报警服务相关数据。

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. 阿里云安全产品

阿里云安全产品和服务（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，为用户提供基础安全，数据安全，应用安全，业务安全，账户安全，安全监控和运营等全面的安全产品。限于篇幅，本章只会覆盖较典型的安全产品，如需了解更多安全产品和服务请参照阿里云官网（www.aliyun.com）。

本章的以下所有产品都已支持接入 RAM 服务。

7.1. 云上基础安全

7.1.1. DDoS 防护

DDoS 防护（Anti-DDoS Service）是针对在互联网上提供服务的企业在遭受 DDoS 攻击后导致服务不可用的情况下，使用阿里云全球 DDoS 清洗网络，秒级检测系统，AI 大数据引擎，高效地缓解 DDoS 攻击，保障业务持续稳定运行。

7.1.1.1. 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有限时间的 DDoS 免费防护能力。

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。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,从而获得更高的有限时间免费 DDoS 防护能力，用于抵御偶然突发的 DDoS 攻击。

7.1.1.2. DDoS 防护包

DDoS 防护包是针对阿里云上大型企业客户，通过阿里云原生网络和透明防护引擎缓解

DDoS 攻击，支持 ECS、SLB、Web 应用防火墙、EIP 等云产品。

默认提供免费 DDoS 基础防护能力，付费升级后可直接提升云产品防护能力，无需更换 IP，无四层端口、七层域名数等接入规格限制，部署简单，只需要绑定需要防护的云产品的公网 IP 地址即可使用。

功能特点

- 阿里云上默认 DDoS 防护

  提供免费版本-DDoS 基础防护，提供最大 5G 防护能力，默认为阿里云用户提供基础能力。

- 即刻购买，即刻生效

  最短一分钟内即可完成 DDoS 防护包的部署，直接把防御能力加载到阿里云产品，免去部署和切换 IP 的烦恼。

- 阿里云原生防护网络，极速访问业务

  采用阿里云原生 BGP 带宽，覆盖电信、联通、移动、教育网、长城宽带等不同的运营商，只需要一个 IP，即可实现多个不同运营商的极速访问。

- 全力防护，无额外弹性后付费

  遭受大规模攻击时调用当前地域阿里云最大 DDoS 防护能力提供全力防护，最大程度防护每一次 DDoS 攻击。

- 共享防护，全量保护企业资产

  同一个企业的多个公网 IP 地址可共享防护能力，降低配置复杂度。

- 阶梯防护，整体解决方案防护能力可提升到 Tbps 级别

可配合 DDoS 高防产品实现自动切换，在超大型流量攻击发生时，引流到备份的 DDoS 高防产品处理。

使用场景

DDoS 防护包适用于部署在阿里云上业务规模大，网络质量要求高的客户，此类型客户虽然 DDoS 攻击风险较低，但是一旦遭受 DDoS 攻击导致业务中断或受损将会带来巨大的商业损失，阿里云原生网络 DDoS 防护产品-DDoS 防护包可在最小接入成本的情况下提升 DDoS 防护能力，降低 DDoS 攻击对业务带来的潜在风险。

DDoS 防护包适用于以下典型场景：

- 资源部署在阿里云上
- 需要保护的公网 IP 数量多
- 业务带宽或 QPS 较大
- 具有 IPv6 访问流量的防护需求

7.1.1.3. DDoS 高防

DDoS 高防（Anti-DDoS Pro/Premium）是针对阿里云上以及云下企业客户，使用阿里云在全球部署的大流量清洗中心资源，结合 AI 智能防护引擎，通过全流量代理的方式实现大流量攻击防护和精细化 Web 应用层资源耗尽型攻击防护。

功能特点

DDoS 高防具有以下特点和优势：

- **优质 BGP 高防网络，防护不降速**

国内首家提供 T 级优质 BGP 清洗资源，业务访问网络质量和大流量防护同时兼顾。国

内平均访问时延 20ms 左右，成功防护攻击峰值超过 1T 的大流量攻击，清洗中心 BGP 路由冗余备份，自动容灾，确保高防业务高可用性。

- 全类型 DDoS 攻击防护支持

  支持常见的流量型 DDoS 攻击防护，包括畸形报文攻击防护和各类流量型 Flood 攻击防护：不限于 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood 、SSDP Flood、DNS Flood、HTTP Flood 等攻击类型；同时支持常见的 Web 资源耗尽型 DDoS 攻击（CC 攻击）防护。如 HTTP Get Flood、HTTP Post flood 等攻击类型

- AI 智能防护，无忧对抗复杂攻击

  智能学习业务流量基线，精准识别攻击流量和攻击特征，自动化防护 TCP 连接耗尽型/应用层资源耗尽复杂型 CC 攻击,自动加载精准匹配防护规则：IP、URI、Cookie、Referer、User-Agent、X-Forwarded-for、Content-Type、Content-Length、Post-Body、Http-Method、Header、Params 等 HTTP 头部字段，区域封禁，黑白名单，智能组合多维度防护策略，高精度阻断复杂攻击，误杀率远低于万分之一。

- 丰富的安全报表，实时监控网络安全风险

  DDoS 防护安全报表，支持实时查询和分析各时间段的多维度数据，包括正常业务流量和攻击流量、端口连接数据、被攻击 IP、端口和域名信息、攻击源 IP 信息、攻击源的地域和运营商分布信息、网站访问响应状态码分布信息，网站访问的 URI 请求次数&响应时间、网站加速缓存命中率等，方便客户直观、快速地了解业务和攻击防护情况。

使用场景

DDoS 高防可保护部署在阿里云上或线下 IDC 机房的客户，适用于 DDoS 攻击频繁的行业。

DDoS 高防适用于以下典型场景：

- 遭受恶意攻击者的 DDoS 攻击勒索
- DDoS 攻击已经导致您的业务不可用，需要紧急防护恢复业务
- 频繁遭受 DDoS 攻击，需要持续防护 DDoS 攻击，保护业务的稳定性

7.1.1.4. 游戏盾

游戏盾（GameShield）是阿里云针对游戏行业面对的 DDoS 攻击推出的针对性的网络安全解决方案，相比 DDoS 高防，除了能针对大流量 DDoS 攻击（T 级别）进行有效防御外，还具备彻底解决游戏行业特有的 TCP 协议资源耗尽型攻击（L4-CC 攻击）问题能力，防护成本更低、效果更好。

游戏盾由两大模块组成：

- 分布式抗 D 节点：通过分布式的抗 D 节点，游戏盾可以做到 DDoS 的攻击的免疫。
- 游戏安全网关：通过针对私有协议的解码，支持防御游戏行业特有的 CC 攻击。

功能特点

- 大流量 DDoS 攻击防护特点

  与 DDoS 高防机房不同，游戏盾并不是通过海量的带宽硬抗攻击，而是通过分布式的抗 D 节点，将黑客的攻击进行有效的拆分和调度，使得攻击无法集中到某一个点上。同时基于 SDK 端数据、流量数据，可以通过动态的调度策略精准定位攻击者，并将攻击者隔离，来达到从源头主动遏制风险来抵御攻击的目的。

- 资源耗尽型 DDoS 攻击（CC 攻击）防御特性

  一般来说，游戏行业的 CC 攻击跟网站的 CC 攻击不同。网站类的 CC 攻击主要是基于

HTTP 或者 HTTPS 协议，协议比较规范，相对容易进行数据分析和协议分析。但是游戏行业的协议大部分是私有的或者不常见的协议，因此对于游戏类 CC 攻击的防御，阿里云推出了专业的云上防御游戏安全网关（原称 NetGuard、简称 NG）。

- 游戏安全网关通过在用户业务和攻击者之间建立起一道游戏业务的防火墙，根据攻击者的 TCP 连接行为、游戏连接后的动态信息、全流量数据，准确分辨出真正的玩家和黑客。
- 游戏安全网关支持大数据分析，根据真实用户业务的特点分析出正常的玩家行为，从而直接拦截异常的客户端（协议非法），且可以随时针对全国省份、海外的流量进行精确封禁，支持百万级的黑白名单。
- 游戏安全网关可以同 SDK 建立加密通信隧道，全面接管客户端和服务端的网络通信，仅放行经过 SDK 和游戏安全网关鉴权的流量，彻底解决 TCP 协议层的 CC 攻击（模拟协议型攻击）。

7.1.2. 云安全中心

云安全中心是一个实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地主机并满足监管合规要求。

7.1.2.1. 产品功能

主动防御

- 防病毒:在云安全中心纵深的威胁检测架构,采用阿里云自研的 AliHIPS 实时拦截组件，实现对主流勒索、挖矿、DDoS 木马等病毒的实时拦截能力。可以在系统内核层面实现云上文件和进程行为的全局监控和实时分析，有效绕过顽固木马和恶意程序的反查杀

能力；还可以基于程序行为分析，挖掘出黑名单未能辨识的恶意威胁，实现主动拦截；其云端病毒库实时更新，集成了国内外主流杀毒引擎、阿里云自研沙箱和机器学习引擎等前沿技术，可以避免因病毒库更新不及时而造成的损失。

- 网页防篡改能力：可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。
- 应用白名单能力：通过智能学习应用白名单的能力，识别可信和可疑/恶意程序形成应用白名单，防止未经白名单授权的程序悄然运行。可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。

安全预防

- 云平台配置检查：从身份认证、网络访问控制、数据安全、日志审计、基础安全防护五个维度，为用户提供最佳安全配置实践。同时由于云安全中心和云平台的深度集成，可以帮助用户看到在从云主机到云平台等各个维度的安全隐患，从而降低因云环境和云产品配置错误导致的风险隐患。
- 漏洞检测和修复：基于自主研发的跨平台漏洞扫描及修复引擎，帮助用户实现同时对多个系统和应用进行扫描和修复的运维工作，目前已支持 Windows 系统、阿里云提供的第三方 Linux 版本、主流的 CMS 系统，同时还能检测官方未能提供补丁的系统或是应用的应急漏洞。
- 基线检查：通过任务下发模式，对主机进行安全配置扫描，包括账号安全、系统配置、数据库风险、合规对标要求等方面，对未符合标准的项目进行提醒。除此之外，用户还可以自定义检测策略，设置检测项目、检测周期、应用的服务器组等。

威胁检测

云安全中心采用机器学习、深度学习、UEBA、威胁情报、AV 引擎等安全能力构建纵深立体的威胁检测架构，使威胁无处隐藏，让一切攻击都有迹可循，主要功能包括入侵检测、云产品异常调用、AccessKey 泄露监控、攻击分析等。

调查响应

- 根据资产资产指纹功能定期收集并记录服务器的运行进程、系统账号、开放端口、软件版本、和网站后台信息，帮助用户全面了解资产的运行状态并提供回溯分析能力。
- 利用自动化攻击溯源帮助用户自动定位攻击源头和原因，并提供安全建议，快速形成止损行动，降低对用户业务造成的损失

日志分析

提供主机和网络日志分析功能，将散落在云平台中各系统的日志集中管理，便于用户在出现主机和 Web 问题时一站式搜索定位问题根源。

可视化大屏

基大数据可视化技术，云安全中心将收集的网络、应用、主机信息后大数据威胁分析结果以直观的图形呈现于可视化大屏，从知己知彼知威胁三个维度为您展现当前资产的网络安全态势，作为用户云平台安全决策的重要支撑工具，支持自定义场景，可灵活用于实时安全监控和工作汇报，具体包括全球业务运营实时监控大屏、业务安全态势和评分、主机层安全态势大屏、业务访客概览、网络层安全态势、安全防御体系大图等。

7.1.2.2. 技术能力

纵深立体的威胁检测模型

- 云安全中心在服务器系统内核层面通过云安全中心 Agent 插件实现云上文件和进程行为的全局监控和实时分析，有效绕过顽固木马和恶意程序的反查杀能力；还可以基于程

序行为分析，挖掘出黑名单未能辨识的恶意威胁，实现主动拦截；其云端病毒库实时更新，集成了国内外主流杀毒引擎、阿里云自研沙箱和机器学习引擎等前沿技术，可以避免因病毒库更新不及时而造成的损失。

- 利用机器学习、深度学习技术，发布 200+大数据安全威胁检测模型，用于挖掘潜在的安全威胁。
- 具有 UEBA 的能力，基于用户行为进行威胁检测，识别内部、外部的安全威胁，例如针对云产品的威胁检测能力,其中 AK 就是一个典型的案例。此外云安全中心已与 GitHub 进行官方合作，如果 AK 不小心泄露在 GitHub 后，会进行泄露告警，确保 AK 安全。
- 在网络层，对流量进行威胁检测，感知黑客在网络中的行动，并通过攻击分析功能实时进行展示，预防可能的黑客入侵。
- 除了阿里云自身的威胁情报以外，同时也集成了互联网威胁情报，三方生态合作伙伴微步的威胁情报为您提供安全服务。

纵深防御的安全体系架构

云安全中心由涵盖网络安全、主机安全、应用安全等多层次安全防护模块组成，在云边界、云网络中、云服务器上形成一套纵深的防御体系，通过集中管控的管理中心协调调度，综合各模块提供的安全信息，做出最准确的判断，并且可以在最合适的位置检测和阻断恶意的攻击行为，有效地保护了云环境不受外界攻击者的侵扰，保障用户业务系统的安全。

跟云平台深度耦合的安全方案

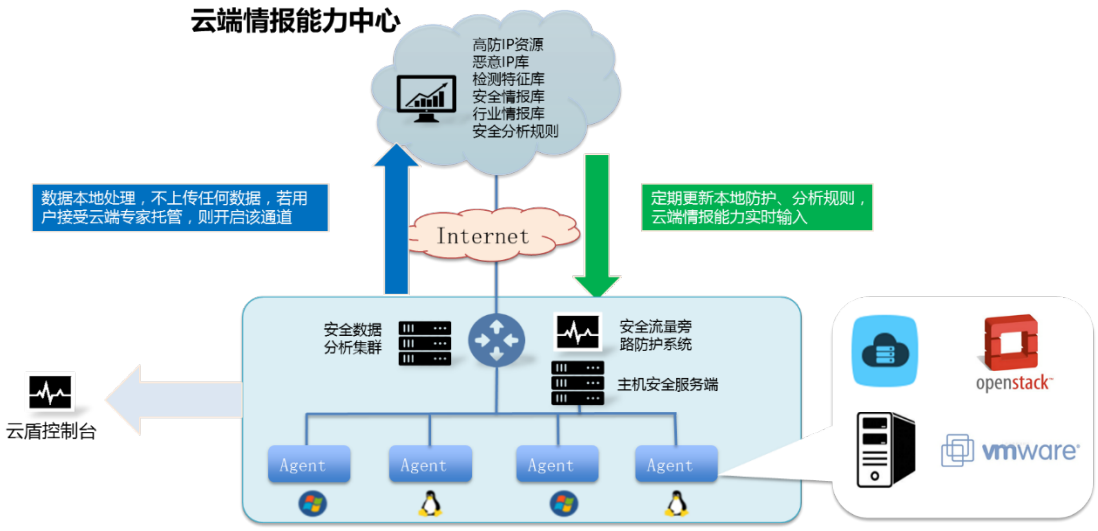
云安全中心是基于阿里云安全团队多年攻防经验开发出来的一套专门面向云平台的攻击防护产品，有效保护公共云和混合云用户的云网络环境和业务系统的安全。云安全中心的各组件是软件虚拟化，具有较为广泛的硬件兼容性，可以快速的部署扩容和投入使用，适应云计算弹

性的特点；云边界、云网络上防御模块采用的是旁路的架构，贴切云的业务，对云平台业务影响最小化；云服务器上的防御模块是虚拟化，适应虚拟机灵活的特点。

阿里云安全能力输出

云安全中心的防护策略和数据源自于多年的积累，阿里云上多达百万级的用户，每天面临多达几十万次的各种攻击。阿里云安全团队充分利用了这些安全攻防的数据积累，每天对公共云上 10 多 TB 的安全数据进行分析，形成恶意 IP 库、恶意行为库、恶意样本库、安全漏洞库等基础安全能力，并及时应用到云安全中心的各个防护模块中，提升防护能力，为用户带来更好的安全保障。

7.1.2.3. 应用场景



在上图的应用场景中，云安全中心在云平台网络出入口，通过流量安全监控模块在网络层对恶意的攻击行为进行识别，实时地阻断网络攻击行为。在主机层对 Web 木马和恶意文件进行实时查杀，避免服务器被攻击者利用。实时拦截暴力破解行为，并对异常的登录行为进行告警，避免攻击者利用弱口令登录系统窃取或者破坏用户业务数据。

7.1.3. 云防火墙

云防火墙是业界首款公共云环境下的 SaaS 化防火墙，可以统一管理互联网到业务的南北

向访问策略和业务与业务之间的东西向微隔离策略，针对云环境对互联网的资产暴露情况，进行全面梳理并集中管理公网 IP 的访问策略，并且一键接入，是业务上云的网络安全基础设施。该产品集成了入侵检测（IPS）功能，具有智能防御，同时支持失陷主机检测、主动外联行为的阻断、支持全网流量可视、业务间访问关系可视。该产品对满足等保 2.0 对虚拟边界、内到外管控、IPS 入侵检测、6 个月网络日志的相关要求，是等保 2.0 合规必选产品。

7.1.3.1. 产品功能

网络流量分析

- 互联网访问分析：通过流量可视化技术，分析云上的业务对外开放的公网 IP、端口、应用、风险等，并给出处置建议。
- 主动外联活动分析：对于主动外联行为，统计出外联的资产、外联的域名，判断该域名是否为风险域名。
- 基于安全组的流量可视化：无需任何配置，呈现安全组和安全组之间的流量访问关系。并通过红线呈现最近 3 天的访问，可以通过流量可实现监控帮助管理员发现内部可疑主机。例如，被入侵 ECS 对其它 ECS 的探测行为，或 ECS 被设置为代理服务器的上网行为等。

全网隔离管控

- 统一的公网 IP 地址管控：全面梳理云环境对互联网的资产暴露情况，集中管理公网 IP 的访问策略，一键接入云防火墙的防护。
- 基于域名的访问控制：由于主动外联行为，对服务器是非常危险的行为，因此建议只允许内部服务器访问授权的域名和 IP，其它未授权的缺省禁止。
- 基于 VPC 的隔离管控及阿里云与 IDC 专线的隔离管控：根据业务的风险程度，进行隔

离管控，不同风险级别的业务，划分到不同的 VPC，并通过云防火墙进行访问控制。

智能防御

集成 IPS 实时防御能力，并集成了威胁情报能力：无需在业务系统上安装软件补丁，即可智能阻断入侵行为。并支持入侵检测分析，清晰的列举出 IPS 检测到的入侵活动。支持 IPS 阻断分析，所有被 IPS 阻断的流量，可快速查询。

日志存储

支持网络流量及安全事件日志：默认保存 6 个月的安全事件日志和网络流量日志及防火墙操作日志，满足网安法和等保的相关要求。

7.1.3.2. 技术能力

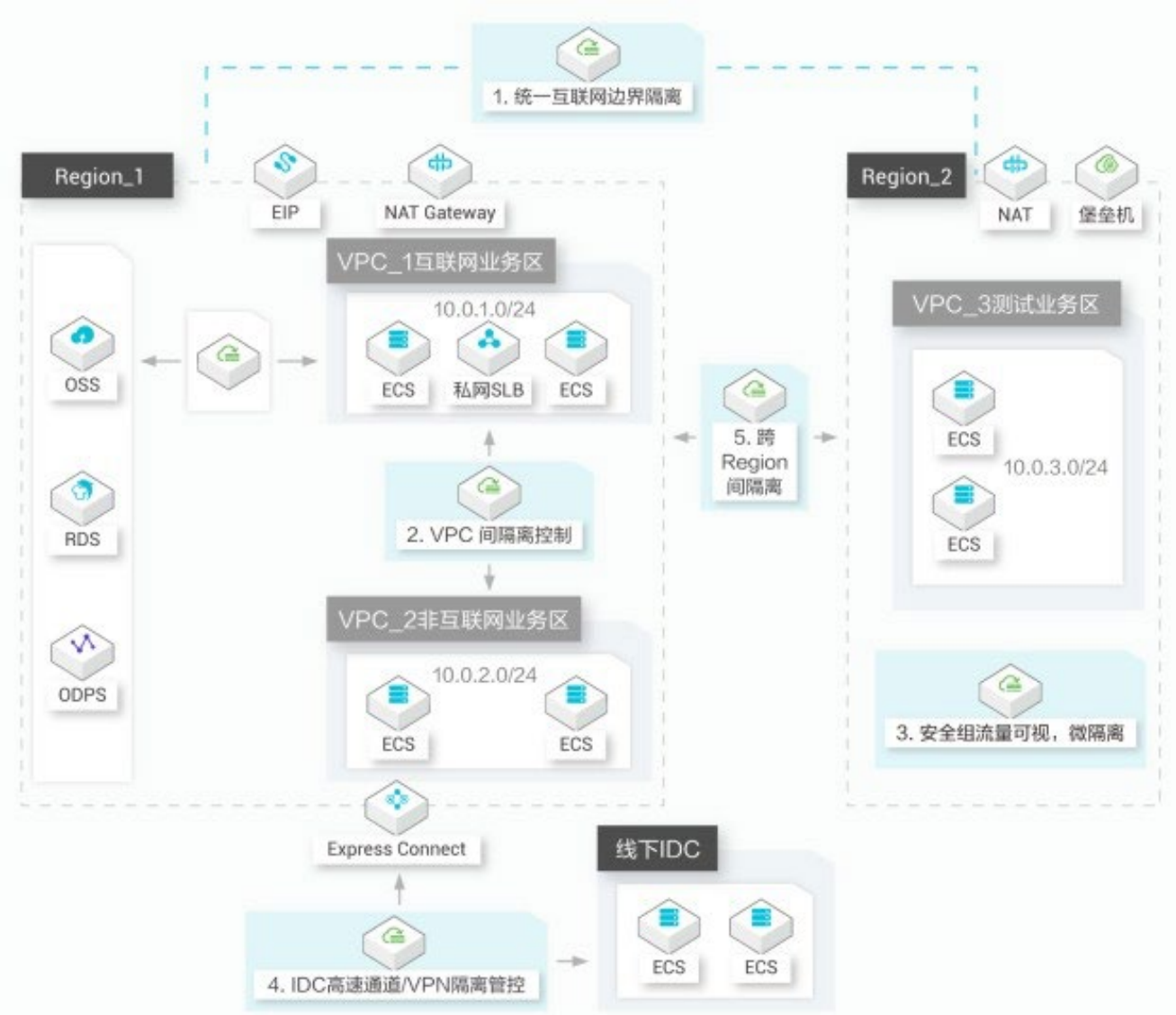
适应云环境的安全防护

云环境中，防护边界比传统 IDC 变得更加模糊，不仅需在互联网边界，还需在 VPC 边界即 SaaS 化的云产品边界，甚至是虚拟机的边界。云防火墙使用 SDN Service Chain、虚拟化技术首创在云环境下提供 Saas 化防火墙安全网络融合方案，通过流量可视化、威胁情报、微隔离等技术，云防火墙不仅可以统一管控来自互联网的访问， 还可以实现 VPC 间流量控制及主机间微隔离，为用户提供了完整的纵深防御体系。

全透明化部署方式

传统防火墙在公共云上的部署，通常需采用软件镜像方式。客户需要镜像安装、路由配置、系统 HA 部署等复杂的配置过程，操作繁琐，不符合云上用户对快速部署，性能弹性的需求。云防火墙做到全透明模式，云上用户一键开通即可使用，用户无需关注安装、容灾、扩容、接入等问题，让用户更聚焦于业务本身。

7.1.3.3. 应用场景



在上图的应用场景中，客户的业务分为：互联网业务、非互联网业务、测试业务和专线远程接入。为满足安全格力需求，其中互联网业务和非互联网业务部署在不同的 VPC。

- 互联网业务通过云防火墙统一管理暴露在互联网的资源，并对互联网访问通过云防火墙进行精细化的访问控制。
- 互联网业务和非互联网业务的 VPC ，通过云防火墙实现严格的访问控制。
- 同一 VPC 内的不同安全组，可通过云防火墙，实现安全组间的流量可视化、及时发现

异常流量。

- 通过云防火墙，隔离专线接入的 IDC 区域，和 VPN 远程接入，确保云上核心资产的安全。
- 如有跨 Region 的访问需求，也可以通过云防火墙进行隔离控制。

7.2. 云上数据安全

7.2.1. 敏感数据保护

敏感数据保护（Sensitive Data Detection and Protection，简称 SDDP）是一款基于业务需求实现数据分类分级，并在精准识别基础上实现数据权限监控、数据脱敏、全域流转监控与异常检测的阿里云安全服务。该服务从海量数据中发现、检测并分析敏感数据的使用情况，及时发现是否存在数据泄露的异常事件并对其进行风险预警，帮助用户防止数据泄露并满足个人信息保护、等保 2.0 以及 GDPR 等合规要求。

7.2.1.1. 产品功能

敏感数据分类分级识别

敏感数据分类分级识别功能，可根据租户授权情况，自动扫描自动发现授权范围内新增的实例/库/表/列、对象存储文件桶/文件对象等不同级别数据信息。通过关键字、规则、机器学习模型算法，精准识别云环境环境内的敏感数据，支持根据业务规则实现敏感自定义。针对敏感数据识别结果，结合业务属性，实现数据基于业务内容的分类以及基于敏感程度的分级，以供业务系统根据敏感分类分级结果系统实现联动。

敏感数据权限管控

敏感数据权限管控功能实现云环境场景下各类数据存储产品/数据传输产品权限的有效管控，支持“数据、人、权限”三要素即时查询，支持角色背后主账号权限映射解析，全局数据权

限统一查询。针对环境内不符合安全最佳实践的权限配置、权限使用异常进行告警。

数据流转与操作监控

数据流转与操作监控功能针对数据流转过程中的异常情况进行有效监控，实现数据流转链路动态展示，确保数据导出/数据传输合规有序。根据日志聚类分析，有效识别人工操作与应用接口调用。基于机器学习和大数据分析能力，针对环境内各类数据流转、数据操作中产生的异常行为进行监控告警。

数据脱敏

数据脱敏功能针对云环境中各类敏感数据，提供数据脱敏能力，为用户提供 Hash/加密/遮盖/替换/洗牌/变换等六大类近 30 种内置脱敏算法，同时支持客户自定义脱敏算法或者自定义脱敏参数。多种脱敏算法的组合使用，能够适应客户不同业务场景的脱敏需求，传递标记化、保留格式等脱敏能力，确保脱敏后的数据能够被测试业务、开发业务、分析业务有效使用。

异常事件处理

异常事件处理功能，实现异常事件的高效处理与应急响应，集中归集各类异常告警事件，支持各租户事件隔离处理，使用时序分析技术还原责任主体行为基线，动态展示历史基线轨迹，有效提升应急响应能力，处理结果自动回流机器学习样板库，让检测结果日趋准确。支持各款产品日志分析以及数据权限管控系统、数据流转与操作监控系统事件输出集中处理。

7.2.1.2. 技术能力

人工智能实现敏感数据识别

通过将阿里巴巴多年聚类分析、机器学习等人工智能技术沉淀产品化，基于自然语言处理模型和神经网络模型，能够从海量文档/图片/数据中精确识别出个人敏感信息、关键系统配置、机密文档等，并具备根据客户现有已识别数据，匹配新数据的学习能力，自动提高敏感数据识别能力。

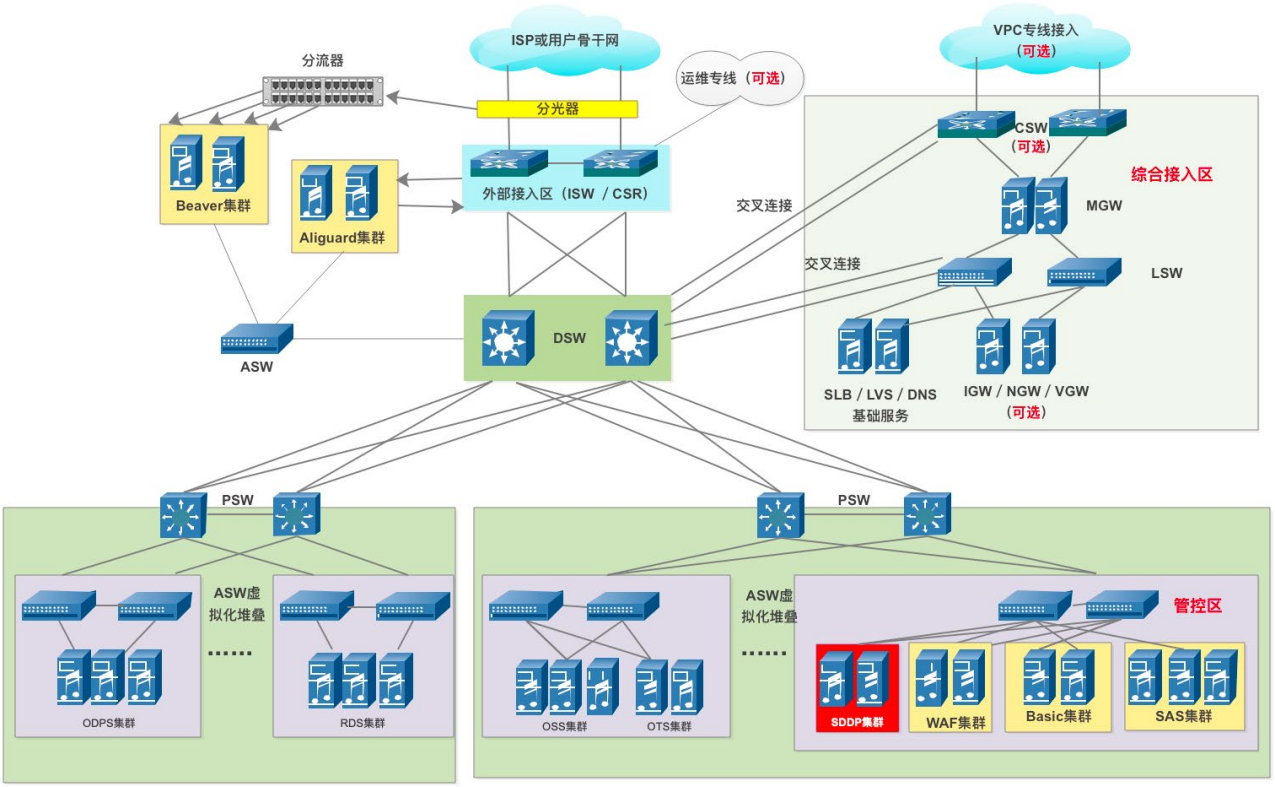
多元脱敏确保数据可用性

提供适用不同业务场景的数据脱敏算法能力，确保脱敏后的数据无需改变相应的业务系统逻辑，保留原有数据特征和分布，确保数据的有效性和可用性。脱敏后的数据能够安全地应用于测试、开发、分析及第三方使用场景中，与原始采购数据和生产模拟数据相比，客户可以低成本、高效率、安全地使用脱敏数据完成业务需求。

多层过滤提升异常检测准确性

根据账号、数据对象的行为学习基线结果，提供了针对数据对象基线分析、账号历史行为基线分析、多维异常检测模型分析、事件处理回流样本分析等多层过滤机制，有效实现事件数量的准确识别与有效收敛，确保检测结果可有效运营。

7.2.1.3. 应用场景



在上图的应用场景中，采用将敏感数据保护服务集群部署在管控区的方式，该非侵入、高灵活、分布式的部署方式，可实现基于部门（专有云）以及租户授权，进而完成针对 MaxCompute、

RDS、OSS、TableStore 等数据产品集群的有效管理。通过有效数据隔离，敏感数据保护确保不同部门的安全审计人员或者数据管理人员能够查看到本部门数据，实现数据安全管控过程本身安全可控。

7.2.2. 密钥管理服务

密钥管理服务（Key Management Service，简称 KMS）是一款安全易用的密码类服务（cryptographic service），提供密钥（cryptographic key）的安全托管、密码运算（cryptographic operation）等基本功能，内置密钥轮转等安全实践，同时支持其他云产品通过一方集成的方式对云产品管理的用户数据进行加密保护。

通过密钥管理服务，用户无需花费大量成本来建设专用的密码硬件基础设施以及设施之上的管理系统，而且还能获得云服务的高可用性和高可靠性，从而可以专注于开发用户真正需要关心的数据加解密、电子签名验签等业务功能场景。

7.2.2.1. 认证与访问控制

用户访问 KMS 来管理、使用密钥时，需要经过认证和授权。KMS 的认证和授权的权威（authentication and authorization authority）是阿里云的访问控制服务，作为仲裁者判定请求发起者是否是合法用户，并且具备访问特资源的权限；KMS 根据判定结果来执行，或者拒绝执行请求。

- 对用户的认证

  用户使用 Access Key（基于 HMAC 消息验证码）向 KMS 进行认证，保证请求的真实性（authenticity）和完整性（integrity）。HMAC 验证不通过的请求会被 KMS 拒绝。AK 身份认证详细信息，请参见云安全产品-云上账户安全和监控-身份和访问控制-AK 身份认证章节。

- 对 KMS 服务的认证

  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 KMS 的服务身份。针对服务端的认证可以防止攻击者伪装成 KMS。

- 访问控制

  如果一个请求通过认证环节，KMS 则认为请求发起者是合法用户，随后 KMS 通过访问控制服务（RAM）对当前用户以及当前请求所带的属性进行权限检查。当前用户所在组织的管理员需要提前在 RAM 服务中赋予当前用户访问 KMS 特定资源的权限以便权限检查可以通过；不通过权限检查的请求会被拒绝。

7.2.2.2. 传输安全

用户对 KMS 的访问，以及 KMS 内部系统之间的通信可能包含敏感数据。网络访问的传输安全通过安全信道，以及安全信道所附带的端到端认证来保证。

- KMS Endpoint

  所有针对 KMS 的用户请求都必须通过 HTTPS 的方式。阿里云 KMS 只会允许在 TLS 中使用业界通用具有强安全性的密码套件（cipher suite）。

- 内部通信安全

  KMS 内部由包含不同的服务模块，每一个服务模块都具备一个合法的身份证书，各服务模块之间的通信全部使用基于身份证书双向认证的 TLSv1.2 协议，保护内部节点的通信安全。

7.2.2.3. 密钥安全

密钥的安全性是 KMS 核心价值之一。通过将密钥限制在一定的安全边界之内，禁止跨边界

的密钥分发来保证了密钥的安全，同时通过特定的运算接口提供密码运算能力。

KMS 通过软件密码模块和硬件安全模块，提供两种不同级别的密钥安全规格。

私密性（Confidentiality）

KMS 保障用户托管在 KMS 的密钥的私密性：

- 用户可以将密钥托管在硬件安全模块（HSM）中，利用硬件机制来保护密钥的明文密钥材料不会离开 HSM 的安全边界。用户使用 HSM 密钥进行运算时，密码运算的过程也只会发生在 HSM 中，从而保证了用户密钥的私密性。HSM 托管密钥可以满足用户的高级别安全需求，同时通过 KMS 内建的管理能力，极大的减少用户的管理开销。
- KMS 也支持软件密钥托管，通过软件密码模块（Software Cryptographic Module）对密钥进行保护。KMS 通过加固软件密码模块，保护软件密钥的明文材料不会离开软件密码模块的边界，仅能在模块边界内被加载于内存中。软件密钥在一些场景中可以满足较为基础的安全诉求，例如云产品托管的“服务密钥”（也称为云产品托管密钥）。对于完全不想自己管理密钥的用户，阿里云赋能最基础的数据加密保护能力。

随机性（Randomness）

随机性是密钥强度的关键。

- 借助使用托管硬件安全模块（HSM），密钥的产生基于安全、许可、且以高系统熵值为种子的随机数生成算法，其强度远远高于软件库的伪随机算法所能达到的程度。并且由于密码运算不能离开 HSM 的硬件安全边界，您可以放心的使用密钥，而不用担心密钥被预判或者恶意恢复。
- KMS 支持的软件密钥，采用密码标准和行业协会所推荐的、符合密码规范的伪随机数（pseudo-random number）算法，基于通用计算 CPU 和硬件服务器所能提供的系统

熵值为种子生成密钥。

密钥版本和自动轮转

KMS 内建了密钥的版本管理能力，同时在多版本的基础上，支持通过配置的方式对用户主密钥进行自动轮转。自动轮转允许用户主密钥周期性地产生新的密钥版本作为加密密钥，而老的版本仅能用作解密历史数据，从而降低针对密钥和受保护数据的攻击面。

在某些场景下，用户亦可针对老数据进行重加密，从而将主密钥下老密钥版本产生的密文数据转换为新密钥版本加密的密文数据。

用户也可以在自动轮转周期之外，针对特定的需要，一次或者多次手动轮转密钥的版本。

7.2.2.4. 合规和安全等级

- 对中国大陆的地域
  - 硬件的国密认证：这些地域的 HSM，获得了国家密码管理局的商业密码认证资质。
  - 国密运行模式：这些地域的 HSM 运行在国密模式下。
- 对中国大陆之外的地域
  - 硬件的 FIPS 认证：这些地域的 HSM 的硬件和固件，获得了 FIPS 140-2 第三级认证。
  - FIPS 140-2 第三级合规：这些地域的 HSM 运行在 FIPS 许可的第三级模式下。

除了各市场分别符合市场认可的密码合规标准，阿里云的密钥管理服务的系统机制，包含其使用的 HSM，也符合 PCI-DSS 合规，可以帮助用户的应用和 IT 设施快速满足业务和行业的合规要求。

7.2.2.5. 运维安全

开发和运维流程

密钥管理服务的开发运维流程使用了阿里云最严格的标准，保证用户的密钥安全。

- 基于阿里云普遍适用的研发、运维流程，密钥管理服务的每一行代码的部署，都要经过DevOps、运维审核小组、安全审核团队的审核批准。
- 除此之外，密钥管理服务还引入了多人共同操作机制，通过来自不同角色和部门的人员的共同操作，完成对服务的部署和运维。

技术安全手段

- 可信执行环境：密钥管理服务的运行基于可信计算技术，在多人多角色共同操作初始化的基础上，建立了可信执行环境；基于受控可信根以及可信远程证明的执行环境才能正常运行，通过和多个服务模块的协作共同对外提供服务。
- HSM 的安全访问：密钥管理服务托管的 HSM 不受人工运维手段的支配 – 无论是 HSM 的初次部署、持续运维还是日常访问，都没有人工操作的机制；KMS 服务是 HSM 的唯一操作方，从而保证 HSM 的操作没有未定义和违法行为的发生。
- 访问控制加固：对 HSM 的操作还通过额外的手段进行加固 – 每一台进入到 KMS 安全边界内的 HSM，都被初始化为需要多方认证；其中的每一个 HSM 认证方都会独立生成随机访问凭证并注册到 HSM 中。

通过多种加固手段，密钥管理服务提供了一个安全的 HSM 执行环境，保证密钥安全性；以及保证对密钥的使用仅仅会来源于用户发起的访问。

严格的内部审计

KMS 内每一个系统调用的发生、KMS 运维系统的每一个运维事件、以及变更系统中的每一

个阶段性流程，均在阿里巴巴的内部审计系统中留下记录，接受审计团队的独立检查。

7.2.3. 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。

7.2.3.1. 产品功能

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。每个加密实例可支持 2048 个对称密钥和 64 对非对称密钥，支持 RSA 的 PKCS10 数据格式。

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

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。

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

7.2.3.2. 使用场景

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。

7.2.4. 证书服务

证书服务（Alibaba Cloud Certificates Service），可以在云上签发第三方知名 CA 证书颁发机构的 SSL 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，一键分发其它云产品。

证书服务提供以下功能：

- 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。

7.2.5. 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：

- 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。
- 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。

7.2.5.1. 产品功能

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。

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。

多维度告警机制

- 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：提供系统性的 SQL 注入库，以及基于正则表达式或语法抽象的 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。

精细化报表

针对各种异常行为的精细化报表：

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

7.2.5.2. 技术能力

安全事件追查

- 提供语句、会话、IP、数据库用户、业务用户、响应时间、影响行等多种维度的数据库操作记录和事后分析能力，成为安全事件后可靠的追查依据和来源。
- 通过 SQL 行为与业务用户的准确关联，使数据库访问行为有效定位到业务工作人员，可有效追责、定责。

数据库性能诊断

实时显示数据库的运行状况、数据库访问流量、并发吞吐量、SQL 语句的响应速度；提供低效语句、访问量最大语句的分析，帮助运维人员进行性能诊断。

发现程序后门

系统提供 SQL 学习和 SQL 白名单能力，实现对业务系统的 SQL 建模；通过合法系统行为的建模，使隐藏在软件系统中的后门程序在启动时，提供实时的告警能力，降低数据泄露损失。

数据库攻击响应

系统提供数据库风险告警能力，对于 SQL 注入、数据库漏洞攻击、过量数据下载、危险 SQL 语句（如 No where delete）等风险行为，提供策略制定和实时告警能力。

等保合规定制化

通过数据库审计可以监控每个用户的行为、各种可疑操作并进行告警通知，能对操作记录进行完整的分析，提供自身审计进程的监控，审计记录防止恶意删除，同时具备自动归档能力。

支持云数据库服务的审计产品

数据库审计通过两种方案解决云数据库服务的引流问题：

- 通过在应用服务器和运维客户端部署 agent，实现数据库流量的引流。
- 对于应用及运维节点较多、不固定等场景，提供代理部署方式，实现引流无漏点。

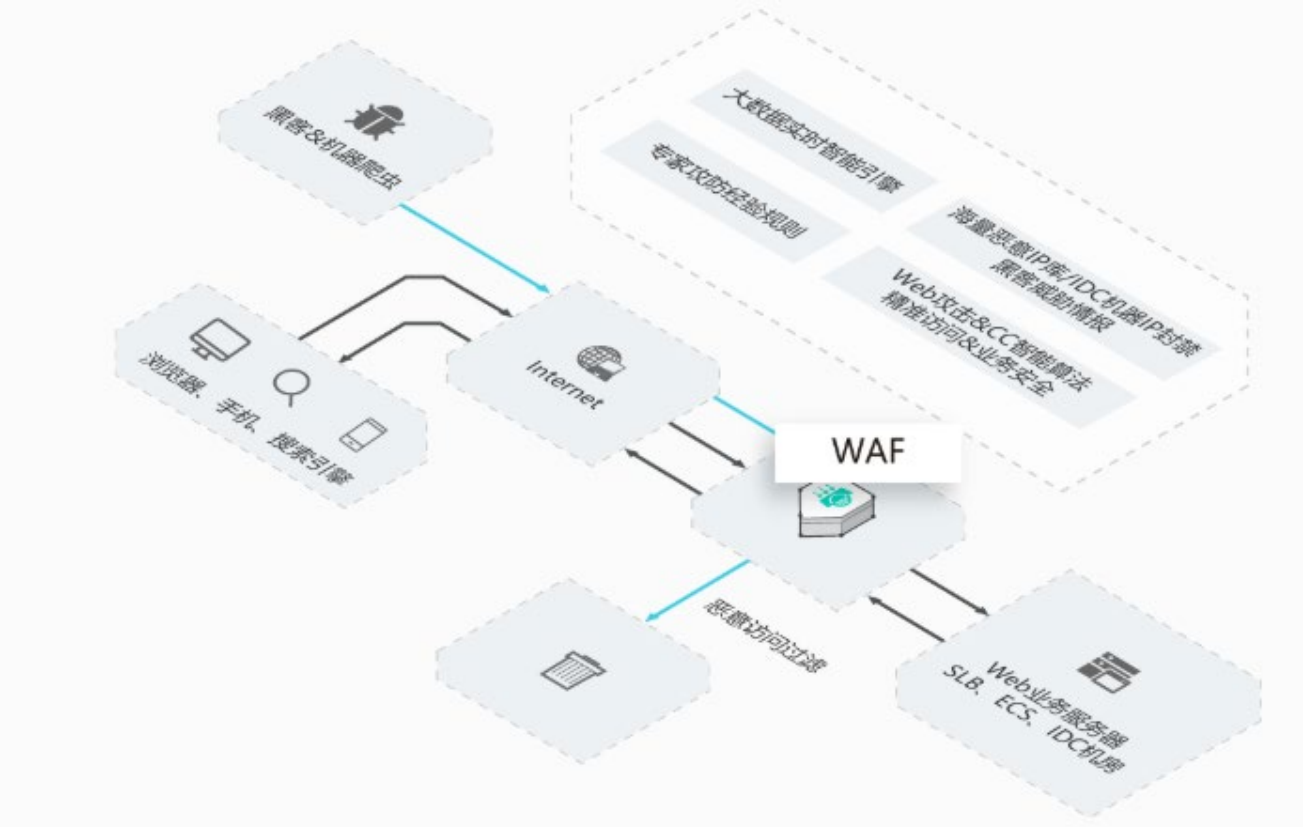
应用关联审计

数据库审计应用关联审计是通过部署 JDBC TAP 插件的方式实现的，该插件需要部署在 Web 服务器上，通过配置该插件来“代理”数据库原生的驱动和数据库的会话，连接时自动采集 Web 客户端的信息，这种方式的好处是不会对数据库有任何影响、不影响应用业务逻辑、能够准确匹配，并且能够满足任何并发压力。

7.3. 云上应用安全

7.3.1. Web 应用防火墙

Web 应用防火墙（Web Application Firewall，简称 WAF），基于云安全大数据和智能计算能力，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 Web 攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站应用的安全性与可用性。



在上图的应用场景中，Web 应用防火墙在网络出入口位置，通过智能防护引擎、专家防护规则、主动防御检测引擎并结合云端威胁情报能力，实时识别 Web 攻击以及恶意 Web 请求，根据预先配置的防护策略实时防御，从而保障网站应用的安全性与可用性。

7.3.1.1. 功能特点

Web 攻击防御能力

对 Web 流量进行检测，支持防御 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。

支持 0day 漏洞的快速响应，及时确认并更新最新漏洞防护能力，第一时间全球同步下发必要的针对性防护规则，确保网站安全性；同时，实时观察针对性攻击流量的变化趋势，持续观察攻击情况，确保防护能力的完整性。

CC 攻击防御能力

支持对单一源 IP 的访问频率进行控制、重定向跳转验证、人机识别等。

支持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、快速识别恶意请求攻击。

精准访问控制能力

提供友好的配置控制台界面，支持 IP、URL、Referer、User-Agent、Cookie 等 13 种 HTTP 常见字段的条件组合，配置强大的精准访问控制策略；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 防护等安全模块结合，搭建多层综合保护机制；依据防护需求，轻松识别可信与恶意流量。

全量日志记录和实时分析能力

WAF 日志实时分析可以近实时地自动采集并存储网站访问日志，并基于日志服务（LogService），输出查询分析、报表、报警、下游计算对接与投递等能力，帮助用户专注于分析，远离琐碎的查询和整理工作。

支持存储网站六个月以上的访问日志，助力网站满足网安法和等保合规相关要求。

安全防护可视化能力

- 安全事件识别和告警能力：基于安全大数据智能算法，从海量的攻击和访问日志中，聚合和识别特定的攻击事件，以及事件的攻击特征分析，并支持给与针对具体事件特征提供具体的专家处置建议，协助客户打造安全运维闭环能力。
- 安全报表和服务总览：提供方便的数据可视化和统计功能，方便您查看网站业务信息和安全统计数据；支持展示您已接入 WAF 的所有网站的总体威胁情况，包括攻击防护和威胁概述、以及业务、攻击、威胁的详细分析。
- 数据可视化大屏展示：依托接入 WAF 后的网站业务详细日志，WAF 提供数据大屏服务，通过将数据转化为直观的可视化大屏，对您网站的实时攻防态势进行监控和告警，为您提供可视化、透明化的数据分析和决策能力，让安全攻防一目了然。

云上网站资产识别能力

在获取用户授权访问其在阿里云平台上的 SSL 证书、云解析 DNS、Web 应用防火墙等云产品的配置信息和站点通信流量中的网站信息的基础上，主动发现用户云上的网站资产，同时提供一键接入 web 应用防火墙防护功能帮助您的企业实现全面的网络资产管理和安全防护。

7.3.1.2. 技术能力

纵深智能闭环防御体系

Web 应用防火墙依托阿里云强大的存储以及计算能力，通过分类以及异常探测等机器学习方法，建立用户的正常业务模型，输出业务画像，来避免统一的特征规则带来的误杀，最大程度上降低了 WAF 的误报率；同时，结合计算机视觉以及深度神经网络在文本分类上的应用，基于监督学习改进传统的卷积神经网络算法，打造可直接提取攻击 payload 的深度学习攻击检测引擎，并实时用于用户的业务保护中，有效的提高攻击检出率；此外，基于用户业务访问端上的模型收集和分析能力，可以对访问用户业务的每一条业务请求进行评分分级，同时结合风控的思想，以基础安全的全局视角进行威胁建模，准实时发现由于某些特殊原因绕过 WAF 的攻击以及 0day 攻击等高危请求，并可自动报警，结合安全专家分析后进行规则下发，并全网同步升级，完成从预警到防护的最短链路闭环，打造数据驱动安全的纵深智能闭环防御体系。

丰富接入方式

- DNS 配置方式：通过修改域名解析的方式，将被防护域名的访问流量指向 WAF；WAF 根据域名配置的源站服务器地址，将处理后的请求转发回源站服务器。实现网站服务器网络隐身功能，避免攻击者绕过 Web 应用防火墙直接攻击。
- 透明接入方式：Web 应用防火墙做到全透明模式，云上 ECS 用户网站支持一键开通即可使用，自动牵引 web 应用流量到 WAF 进行防护，用户无需调整 DNS 解析记录，更透明的方式避免对业务造成影响，让用户更聚焦于业务本身。

7.4. 云上业务安全

7.4.1. 爬虫风险管理

爬虫风险管理（Anti-Bot Service）专业检测高级爬虫，降低爬虫及自动化工具对网站的业务影响，提供对 Web 网页端、H5 页面、APP、API 全方位防护。主要防护场景包括航空占座、

电商黄牛、恶意撞库、核心接口被刷、刷票刷积分等。

7.4.1.1. 产品功能

精准访问控制

指对常见的 HTTP 字段（如 IP、URL、Referer、UA、参数等）进行条件组合，配置支持业务场景定制化的防护策略，由匹配条件与匹配动作构成。

频次限制

限制特定路径（URL）上单个 IP、Cookie、Header 的某个字段对服务器的访问频率，或者基于响应码的比例及数量达到一定阈值做封禁。

合法爬虫放行

提供合法搜索引擎白名单（例如 Google、Bing、百度、搜狗、360、Yandex 等）,可应用于全域名或指定路径下放行。

爬虫威胁情报

基于云平台强大的计算能力，提供拨号池 IP、IDC 机房 IP、恶意扫描工具 IP、以及云端实时模型生成的恶意爬虫库等多种纬度的威胁情报，可应用于全域名或指定路径下进行阻断。

智能算法防御

提供典型爬虫行为识别的通用算法实例，可配置基本业务参数和风险阈值进行机器学习，输出智能防护结果以对抗高级爬虫。

App 增强防护

专门针对原生 APP 端，提供可信通信，防机器脚本滥刷等安全防护，可以有效识别代理、模拟器、非法签名的请求。

人机验证

通过对用户的行为数据、设备特征与网络数据构建多维度数据分析，对风险设备使用、模拟行为、暴力重放等攻击进行综合实时风控判决。通过极简的验证交互逻辑，让真实用户无需思考即可通过人机识别的挑战，准确有效区分机器和真实用户的访问。

7.4.1.2. 技术能力

通过部署爬虫风险管理可以有效降低爬虫或者自动化工具对网站产生的业务影响。

多层次的智能组合防御

- 反向代理部署架构将第一层机器流量过滤拦截在源站之前，有效降低机器流量给源站带来的额外资源消耗。对可疑流量的处置可以提供滑块或者 javascript 校验等方式，作为做第二层的机器流量过滤
- 提供多维度的识别，包括精准策略、高频识别、爬虫情报、爬虫行为智能算法等模块可以应对从低级的脚本爬虫到高级的模拟真人爬虫的不同程度的对抗。
- 可支持独立接入人机验证模块，包括滑块验证、无痕验证、智能验证等多种人机验证方式。有效降低登录、注册、短信、领取红包等接口被刷的风险

App 端的增强防护方案

提供 App 端集成的 SDK，除流量层防御能力之外，叠加了请求加验签过程以及风险设备维度的识别，能更有效地对抗 App 端的机器流量风险。

7.4.2. 风险识别

风险识别（Anti-Fraud Detection）基于大数据、机器学习算法、流式计算等阿里巴巴的业务风控最佳实践，为客户提供从 API 服务、到决策引擎平台的一站式智能风控解决方案。解决企业客户在用户注册、运营活动、交易、信贷审核等关键业务中面临的欺诈问题。

7.4.2.1. 产品功能

风控 API 服务

通过轻量 API 的形式帮助客户快速接入和应用阿里云的业务风控能力。目前核心的 API 服务包括注册风险识别、营销风险识别、登录风险识别、中文地址评分、邮箱画像等，可分别应对不同互联网业务场景的欺诈风险。客户调用 API 传入识别所需信息，系统智能分析、并返回识别结果，可覆盖手机风险、IP 风险、恶意设备以及行为突变、团伙识别等主流攻击手段。

决策引擎平台

决策引擎在原阿里自用风控引擎基础上，提供个性化业务场景事件管理，可视化编排复杂决策，丰富的特征变量与场景识别服务等功能。相较于需要开发背景及算法背景才能使用的传统风控引擎，阿里云决策引擎无需开发背景甚至无需算法建模背景，也可以将大数据与人工智能算法应用到业务智能决策中，实现数字化业务运营转型。

7.4.2.2. 技术能力

实时计算，同步结果实时返回

通过线上实时请求，实时流量进行实时的指标计算，模型计算，策略规则计算，直接返回给客户结果。整体响应时间根据事件和场景不超过 200ms，最短可以在 20ms 内返回。

大数据计算和关系计算

依托阿里集团的大数据计算能力，可以做到 PB 级别的运算和模型建设能力。具有支持各种算法：GBDT，聚类，线性，贝叶斯，决策树，神经网络，图计算。深入挖掘和建设在垃圾注册，防薅羊毛，资金安全场景的业务模型和特征，为业务健康和资损防空提供算法、模型、特征等基础数据和计算能力支持。

动态规则实时生效

采用 server-client 模式，安全专家通过统一的控制台配置专家策略和模型，实时动态地推

送到执行引擎，实现一处配置全部执行、有效实现实时对抗，减少客户损失。

云生态深度联动

集成各种云产品，使客户在云上充分体会到云的能力。目前已经集成的云产品包括云市场、MaxComputor、LogService、OSS、RDS、Redis 等，实现零代码即插即用。

全球调用，就近部署，Region 联动

目前已经开放的 Region 包括上海、杭州、深圳、张家口、北京、成都；海外开放新加坡区域。控制台中心部署，执行引擎全球执行，就近执行，大大降低了客户对网络方面的感知和需求。

7.4.3. 内容安全

内容安全是一款多媒体内容智能识别服务，支持对图片、视频、文本、语音等对象进行多样化场景检测，有效帮助用户降低内容违规风险。常用的检测场景包括：智能鉴黄、暴恐涉政识别、图文广告识别、logo 识别、敏感人脸识别、二维码识别、OCR 图文识别、文本反垃圾、语音反垃圾、文件内容反垃圾等。内容安全提供站点检测功能，可以定期自动检测您的网站上的风险和违规内容；OSS 违规检测功能，对用户指定的 OSS 空间中的图片和视频进行涉黄、涉政等敏感信息检测；用户也可以直接调用内容检测 API，提交指定场景的机器识别任务。

内容安全服务提供以下功能：

- 站点检测服务

  站点检测服务定期检查用户的网站首页和全站内容，及时发现用户网站在内容安全方面可能存在的风险（例如首页篡改、挂马暗链、色情低俗、涉政暴恐等），并向用户展示违规内容的具体地址，帮助用户查看和修复。支持用于以设置消息通知，选择邮件、短信、站内信的方式，获取实时的站点首页风险提醒。

- OSS 违规检测

OSS 违规检测使用人工智能技术帮助您智能检测存储在阿里云对象存储服务 OSS 中的图片、视频是否包含有色情、涉政等风险内容，并支持自动冻结检测出的违规内容。

- 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检测。具体应用场景如下表所示：

应用场景	描述
图片违规内容检测	检测图片违规或识别图片中的不良信息。具体支持以下场景： • 智能鉴黄 • 暴恐涉政检测 • 图文违规检测 • 二维码检测 • 不良场景检测 • logo 检测
视频违规内容检测	检测视频中的违规内容或不良信息。具体支持以下场景： • 智能鉴黄 • 涉政暴恐检测

应用场景	描述
	• 图文违规检测 • 不良场景检测 • logo 检测
文本垃圾内容检测	检测文本中的违规或不良内容，具体包括以下场景： • 广告内容检测 • 涉政暴恐检测 • 辱骂检测检测 • 色情内容检测 • 灌水内容检测 • 无意义内容检测 • 违禁品内容检测 • 自定义关键词检测
语音垃圾内容检测	检测语音中的违规或不良内容，具体包括以下场景： • 广告内容检测 • 涉政暴恐检测 • 辱骂检测检测 • 色情内容检测

应用场景	描述
	• 灌水内容检测 • 无意义内容检测 • 违禁品内容检测 • 自定义关键词检测
图文 OCR 识别	识别图片中的各种文字信息（结构化或非结构化信息），支持识别的结构化卡证对象包括： • 身份证 • 护照 • 银行卡 • 营业执照 • 增值税发票 • 行驶证 • 驾驶证 • 车牌 • 车辆 Vin 码 **说明** 图文 OCR 支持自定义模板进行识别。
人脸识别	人脸识别包括以下能力：

应用场景	描述
	• 人脸属性检测 • 人脸比对 • 人脸检索 • 翻拍检测 • 端上活体检测 **说明** 端上活体检测提供离线安卓 SDK，翻拍检测指服务端 API。
相似图检索	根据给定的图片到用户自定义图库检索相似的 topN 张图片。
图片标签	识别图片中的主体，并输出对应的标签。
视频指纹	根据给定的视频，从视频库中检索同源视频。
视频标签	识别视频中的主体、场景、行为等内容，并输出标签以及出现的时间点。

7.4.4. 实人认证

实人认证服务是指依托活体检测、人脸比对等生物识别技术、证件 OCR 识别技术等进行的自然人真实身份的校验服务。目前实人认证服务只对企业用户开发，并只支持对拥有中华人民共和国第二代居民身份证的居民进行认证。

实人认证服务包括以下功能：

实名校验

用于验证用户证件信息，核实用户的姓名和身份证号码是否真实存在、匹配，防止身份造

假，确保用户身份真实。

使用时，用户按要求拍摄并上传身份证正反面照片，实名校验采用业界领先的证件 OCR 识别技术，自动识别并读取姓名、身份证号、有效期等信息，并呈现给用户进行确认。该技术综合识别率达到 99% 以上，且避免户手工输入的麻烦，提升使用体验。

生物识别

通过交互式动作活体、视频活体等方式进行活体验证。获取照片后，生物识别使用业界领先的人脸识别系统进行人脸检测，检测照片图像中的人脸特征，自动审核、验证该照片是否为本人照片。

使用活体验证时，用户需要在摄像头前根据提示执行互动操作（例如，凝视屏幕、张嘴、摇头、眨眼睛、点头等动作），从而达到鉴别真人的目的。

权威数据源核身

实人认证操作过程中采集到的活体照片，以及姓名和身份证号，会与权威数据源进行核身比对，核身是同人和本人。

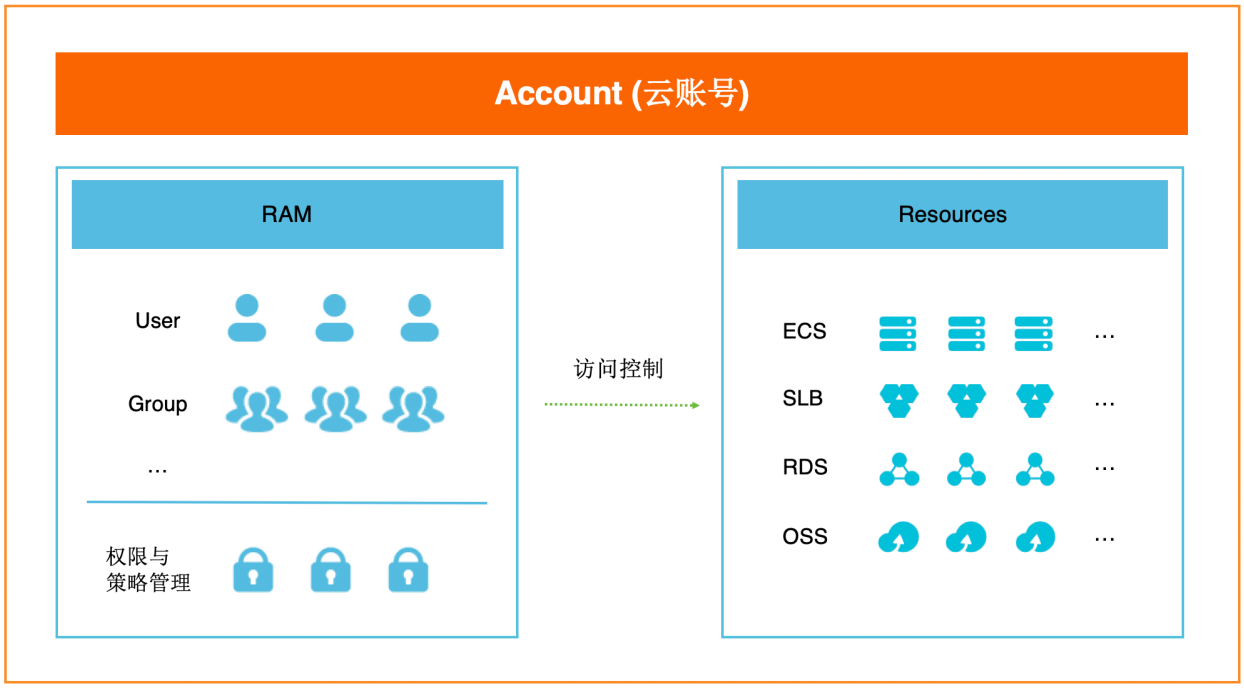
7.5. 云上账户安全和监控

7.5.1. 身份和访问控制 RAM

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 Resource Access Management（RAM）资源访问控制服务，用于用户身份管理与资源访问控制。RAM 使得一个阿里云账号（可理解为主账号）可拥有多个独立的子用户，并支持多因素认证、强密码策略、控制台用户与 API 用户分离、自定义细粒度权限策略，用户分组授权、临时授权令牌等功能。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、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，下图展示了 RAM 与其它云服务之间的关系：



RAM 是阿里云账号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），消除了云账号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，大大降低了因用户权限过大带来的风险。

7.5.1.1. 用户管理

一个云账号可以通过 RAM 服务来创建一个或多个独立的子用户。云账号与 RAM 子用户的关系如下：

- 从资源归属关系上来看，云账号是阿里云资源归属、资源使用计量计费的基本主体，而 RAM 子用户只能存在于某个云账号中。RAM 子用户不拥有资源，在被授权操作时所创建的资源归属于云账号；RAM 子用户不拥有账单，被授权操作时所发生的费用也计入云账号账单。

- 从权限关系上来看，云账号与 RAM 子用户是一种类似 Linux 下 Root 与 User 的关系，云账号对资源拥有一切操作控制权限，而 RAM 子用户只能拥有被云账号所授予的某些权限，而且云账号在任何时刻都可以撤销 RAM 子用户身上的权限。同时，云账号也可以授权 RAM 子用户使其拥有 RAM 资源本身的操作权限。

每一个 RAM 子用户应当对应到某一个身份实体，如操作员或应用程序。如果有新的操作员或应用程序需要访问云账号下的云资源，则需要创建 RAM 子用户并授权其访问相关资源。对云账号下有多个 RAM 子用户的情况，为更好的管理用户及其权限，建议使用用户组（Group）来为职责相同的 RAM 子用户进行归类，并在授权时选择给用户组授权。

管理员通过 RAM 还可以创建一种称为“RAM 角色”的身份。RAM 角色与普通 RAM 子用户类似，都是 RAM 中管理的身份实体。与 RAM 子用户相比，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。

7.5.1.2. 身份凭证

身份凭证是用于证明用户真实身份的凭据，它通常是指账号登录密码或访问密钥（Access Key，简称 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 子用户支持如下的身份凭证：

- 账号密码（Password）

  用户可以使用其云账号（即主账号）或其云账号下 RAM 用户的密码登录阿里云控制台并对其云上资源进行操作。阿里云的账号密码规范、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。例如，用户可以通过 RAM 控制台为 RAM 用户创建密码策略，以保证各个子用户都使用定期轮转的强密码从而提高整体账户的

安全性。

- API 访问密钥（Access Key）

  阿里云的 Access Key（AK）是用户调用云服务 API 的身份凭证，用于在用户通过 API 访问阿里云资源时对用户身份进行认证。API 凭证相当于登录密码，只是使用场景不同。前者用于程序方式调用云服务 API，而后者用于登录控制台。Access Key 包括访问密钥 ID（AK ID）和秘密访问密钥（AK Secret）。

  请注意，出于有效权限分割和降低风险的考虑，云上最佳安全实践中不建议用户为其云账号（即主账号）创建 AK 凭证，而建议为其下属的 RAM 用户各自创建 AK 凭证。这是因为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 子用户进行资源操作并遵循最小授权原则。

- 多因素认证（Multi-Factor Authentication，简称 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。

7.5.1.3. AK 身份认证机制

阿里云服务可以通过 Access Key（AK）来进行 API 的调用，并进行相应的身份认证。Access

Key 包括访问密钥 ID（AK ID）和秘密访问密钥（AK Secret）。AK ID 和 AK 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 AK ID 用于标识访问者的身份；而 AK 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，保证只有阿里云和用户知道。当用户在调用云服务时会传入 AK ID，并使用 AK Secret 对请求进行加密签名（HMAC 算法）。加密签名自带时间戳，可以放在重复攻击。服务在收到用户请求时，会通过请求中的 AK ID 找到对应的 AK Secret，以同样的方法计算出加密签名并进行请求的身份验证校验。

用户可以登录阿里云用户中心或 RAM 控制台来管理 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。

7.5.1.4. 用户组管理

对云账号下有多个 RAM 子用户的情况，为更好的管理用户及其权限，建议使用用户组（Group）。为职责相同的 RAM 用户（如 Admins、Developers、Accounting 等）创建用户组进行归类，并在授权时选择给用户组授权。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用户组下，不会对其他用户产生影响；当用户组的权限发生变化时，只用修改用户组的权限策略，可以直接应用到与该用户组关联的所有 RAM 子用户身上。

7.5.1.5. 权限和权限策略管理

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。

- 云账号（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）。该属主必须是云账号，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。例如，一个 RAM 子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号，该用户是资源创建者但不是资源属主。

- 一个新创建的 RAM 子用户默认无任何权限
  - RAM 子用户代表的是操作员，其所有操作都需被显式授权。
  - 新建 RAM 子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 子用户不会自动拥有对其所创建资源的任何权限
  - 如果 RAM 子用户被授予创建资源的权限，用户将可以创建资源。
  - 但是 RAM 子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。

权限策略（Policy）

权限的载体是权限策略。权限策略是一组权限的集合，它以一种策略语言来描述。通过给用户或用户组附加权限策略，用户或用户组中的所有用户就能获得权限策略中指定的访问权限（默认拒绝优先）。

RAM 支持两种类型的权限策略：系统权限策略和自定义权限策略。

- 系统权限策略

  系统权限策略是阿里云提供的一组通用权限策略，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权限

策略，用户只能用于授权，而不能编辑和修改。对于这些系统权限策略，阿里云会自动进行更新或修改。

- **自定义权限策略**

  RAM 支持用户创建自定义权限策略，使用权限策略（Policy）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，RAM 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 2019 年 9 月 30 日 9 点前，否则拒绝访问。

7.5.1.6. RAM 角色管理

RAM 角色可以被看成一种虚拟 RAM 子用户，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、进行角色 SSO 登录等场景。

RAM 角色主要有三种：

- **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号下的子用户，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。

- **实例角色**

  实例 RAM 角色允许用户将一个 RAM 角色关联到 ECS 或 ECI 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。

- **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。

- **身份提供商**

  允许受信身份提供商下的用户所扮演的角色。此类角色主要用于实现与阿里云的角色 SSO。

相比于 RAM 子用户，在使用方法上 RAM 角色需要被一个授信的实体 RAM 子用户扮演，扮演成功后实体 RAM 子用户将获得 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 子用户切换到 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取代。当 RAM 子用户切回登录身份时，将拥有 RAM 子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。

7.5.1.7. SSO 管理

阿里云支持基于 SAML 2.0 的单点登录（Single Sign On，简称 SSO），可以支持企业客户使用企业自有身份系统（作为 Identity Provider）的登录服务登录访问阿里云（作为 Service Provider）。

为了满足不同企业客户的登录场景需求，阿里云提供了以下两种基于 SAML 2.0 协议的 SSO 机制：

- 用户 SSO：阿里云通过 IdP 颁发的 SAML 断言确定企业用户与阿里云 RAM 用户的对应关系。企业用户登录后，使用该 RAM 用户访问阿里云资源，对应的访问权限由 RAM 用

户的授权策略所限制。

- 角色 SSO：阿里云通过 IdP 颁发的 SAML 断言确定企业用户在阿里云上可以使用的 RAM 角色。企业用户登录后，使用 SAML 断言中指定的 RAM 角色访问阿里云资源，对应的访问权限由 RAM 角色的授权策略所限制。

7.5.1.8. 资源分组管理

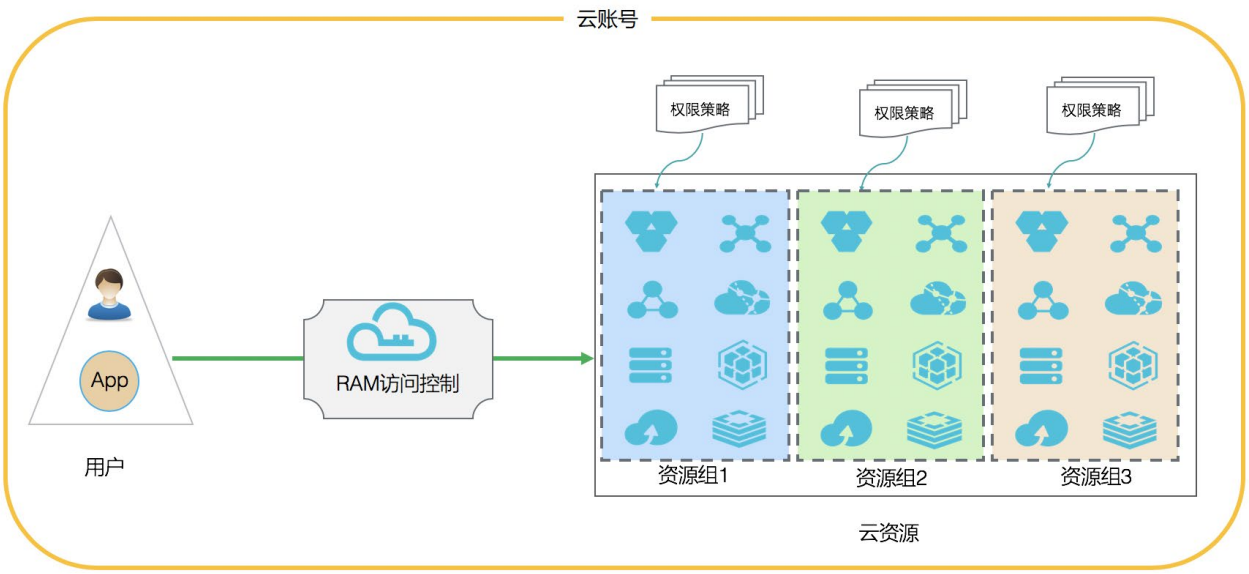
资源分组管理是企业客户管理海量云资源的基础能力。阿里云提供了两种机制来帮助客户进行资源分组：基于资源标签（ResourceTag）的资源分组和资源组（ResourceGroup）管理。

- 资源标签（ResourceTag）

  客户可以对海量资源进行标签设计和管理，利用云产品提供的打标、按标签过滤资源、按标准编写 RAM 授权策略、按标签进行账单分类等，通过标签管理可以完成一些基本的资源分组管理需求。

- 资源组（ResourceGroup）

  资源组是在单个云账号内进行资源分组管理的一种增强技术，可以帮助解决单个云账号内的资源分组和授权管理的复杂性问题。与标签相比，资源组功能不仅简单易用，而且还可以按资源组维度提供分级授权的能力（即允许设置资源组管理员，而标签分组则无法提供类似能力）。



7.5.1.9. 多账号管理

云账号是阿里云资源隔离和计量计费的最小管理单元。为了资源隔离或成本管理的需要，企业往往需要使用和管理多个云账号。为此，阿里云面向企业客户提供的一套基于多账号的分级管理服务 —— 资源目录（Resource Directory）。

资源目录支持按照基于企业的业务或生态环境，让管理员方便的创建出体现业务关系的资源目录结构，并将企业多个账号分布到这个目录结构中的相应位置，从而形成资源间的多层级关系。企业可依赖设定的组织关系进行资源的集中管理，满足企业资源在财资、安全、审计及合规方面的管控需要。

7.5.1.10.STS 安全令牌服务

阿里云 Security Token Service（STS）是为 RAM 子用户、阿里云服务、身份提供商等受信实体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号下的云资源，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 子用户账号及密钥。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。

7.5.2. 应用身份服务

阿里云应用身份服务 IDaaS（Alibaba Cloud Identity as a Service，简称 IDaaS）是阿里云为企业用户提供的一套集中式身份、权限、应用管理服务，帮助用户整合部署在本地或云端的内部办公系统、业务系统及三方 SaaS 系统的所有身份，实现一个账号打通所有应用服务。

7.5.2.1. 适用场景

使用 IDaaS 统一管理三方应用系统

IDaaS 本质上是一种“云连接器”，帮助用户将公司及员工使用的大量软件应用整合在一起，以便让员工很方便地使用单一、安全的账号，登录他们工作中需要使用的各种网络服务，或者供应商、承包商、合作伙伴和客户所使用的网络服务。

使用 IDaaS 整合及新开发公司内部的办公系统（简称 OA 系统）

IDaaS 提供一个完整的账号、认证、授权系统，用户可以使用 IDaaS 完成以下任务：

- 为新入职员工开通账号，分配应用访问权限；在员工转岗离职时管理权限变更。
- 通过单点登录打通多个内部应用系统（这些系统有不同账号体系），以便员工登录一个

系统后，可以免登进入另一个系统。

- 开发新的应用系统。

使用 IDaaS 开发一个面向其他客户的业务系统

IDaaS 可以为用户提供用户池的功能。IDaaS 用户可以新创建一个用户池，然后在应用程序中通过 IDaaS 的 API 接口来调用新用户的注册、登录、注销等流程，以此用户可以专注在业务系统流程本身，减少账户管理方面的工作。

7.5.2.2. 产品功能

统一账户

- 一个账号对接多个子系统，同一用户在各种不同类型应用系统之间的账号相互打通。
- 各子系统的账户关联到主账户中，实现账号体系的统一，方便员工的生命周期管理。

统一认证

- 采集多种认证因子，通过发行加密身份凭证到不同应用的服务端进行认证，实现统一认证和单点登录。
- 支持多种账户数据源，如 AD、LDAP、以及任何提供 SCIM 标准 API 的应用，可快速导入企业既有账户体系。支持 SAML、OIDC、OAuth、CAS 等所有主流标准单点登录协议，对于未支持标准协议的应用，也支持采用 API、SDK、密码代填等方式进行快速集成。
- 提供多因素认证，支持主流的认证方式，例如，账号/密码、 账号/SM2 加密密码、短信验证码、OTP 码、声纹、指纹、面部人脸识别、证书认证等。

集中授权

- 对角色、组及账户进行不同维度的授权，从不同颗粒度集中分配权限，防止越权操作。
- 支持二级授权，支持定义应用内的组织和角色，可以按照组织、角色等为单位进行授权，

进一步定义该应用的二级权限资源，如菜单、按钮、后台使用资源等。

应用管控

- 集中管理企业私有云和公共云应用、移动应用、IoT 设备的访问权限和账户。
- 预集成了市面上常见的公有云服务，并可对接阿里云 RAM。

透明审计

通过审计报告追溯用户的访问行为，了解公司数字资产的使用效率。

7.5.3. 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。

请注意，虽然日志服务不是一款安全产品，但其日志的采集、消费查询和投递相关功能与云上安全监控和运营关联度非常高，因此在此一并介绍。

7.5.3.1. 高可用性

日志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。

7.5.3.2. 只读日志系统

日志服务有一个重要特性就是防篡改。日志服务提供的是一个 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。

7.5.3.3. 离线归档

日志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。

7.5.3.4. 身份认证

日志服务会对每个 API 访问请求进行身份认证，因此用户需要在请求中包含签名（Signature）信息。日志服务使用 Access Key 作为身份认证的凭证。AK 身份认证详细信息，请参见云安全产品-云上账户安全和监控-身份与访问控制-AK 身份认证章节。

7.5.3.5. 功能特性

实时采集与消费

- 通过 ECS、容器、移动端，开源软件，JS 等接入实时日志数据（例如 Metric、Event、BinLog、TextLog、Click 等）。
- 提供实时消费接口，与实时计算及服务对接。

用途：数据清洗（ETL）、流计算（Stream Compute）、监控与报警、机器学习与迭代计算。

查询与实时分析

- 查询：关键词、模糊、上下文、范围。
- 统计：SQL 聚合等丰富查询手段。
- 可视化：Dashboard + 报表功能。
- 对接：Grafana，JDBC/SQL92。

用途：DevOps/线上运维，日志实时数据分析，安全诊断与分析，运营与客服系统。

权威数据源核身

稳定可靠的日志投递。将日志中枢数据投递至存储类服务进行存储。支持压缩、自定义

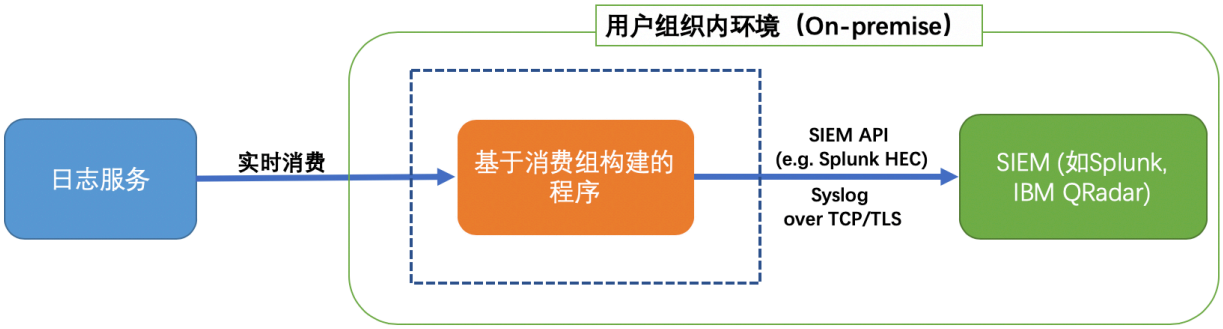
Partition、以及行列等各种存储方式。

用途：数据仓库 + 数据分析、审计、推荐系统与用户画像。

7.5.3.6. 日志投递到 SIEM

日志服务支持将日志投递到 Security Information and Event Management（SIEM），以确保阿里云上的所有法规、审计、与其他相关日志能够导入到用户的安全运维中心（SOC）中（如 Splunk，IBM QRadar 等）。

日志服务支持通过 HTTPS 投递日志到 SIEM（以 Splunk 为例）。一般而言，SIEM 应该是在用户组织内部。这种情况推荐使用日志服务消费组构建程序进行实时消费，然后通过 Splunk API（HEC）来发送日志给 Splunk。日志服务也支持通过 Syslog 投递日志到 SIEM。Syslog 是一个常见的日志通道，几乎所有的 SIEM（如 IBM Qradar、HP Arcsight 等）都支持通过 Syslog 渠道接受日志。如下图所示，通过使用日志服务消费组构建程序来进行实时消费，并通过 Splunk HEC 或 Syslog over TCP/TLS 来发送日志给 SIEM。如果 SIEM 支持 TCP 通道及 TLS，建议优先使用。



7.5.3.7. RAM 和 STS 支持

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

日志服务同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

7.5.4. 操作审计

操作审计（ActionTrail）会记录用户的云账号资源操作，提供操作记录查询，并可以将审计事件保存到用户指定的日志服务或 OSS 存储空间。利用操作审计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。

操作审计收集云服务的 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日志形式投递到日志服务，或以文件形式保存到指定的 OSS 存储空间。操作审计可以利用日志服务的检索能力、分析功能或进一步转存到大数据产品来管理这些数据，例如授权、开启生命周期管理、归档管理、检索、分析和报警等。操作审计支持从操作时段、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，当操作审计收集到用户使用阿里云服务的操作记录（包括用户通过控制台触发的操作、调用阿里云 API 进行的操作以及云服务通过服务角色进行的操作等），操作记录会在 10 分钟内保存到操作审计。用户可以通过操作审计控制台查看最近 30 天的操作记录。

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。例如，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。例如，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。

7.5.4.1. 云平台操作事件（Inner-ActionTrail）

传统上，云平台侧的内部运维操作，对用户是不可见的黑盒子，即用户不可感知也不可监控或审计。虽然阿里云已经获得了业界领先的三方合规认证资质，但用户在其数据上云后，对数据在云平台内部是否得到了妥善的保护和管理仍然应当能让用户直观的感受到。因此，阿里云对用户提供了平台侧的内部操作透明化能力，让阿里云的相关内部操作事件对用户可见透明，使得用户可以对云平台内部操作事件也可以进行审计监控等操作，让用户使用阿里云的时候更加安心。

Inner-ActionTrail 可以近实时地自动采集并存储阿里云平台侧操作事件，并基于日志服务输出查询分析、报表、报警、下游计算对接与投递等能力，满足用户对云平台操作事件相关的分析与审计需求。

Inner-ActionTrail 支持透出以下三种操作类型：

- CUSTOMER_INITIATED_SUPPORT

  阿里云运维人员针对用户授权的技术支持操作，如基于用户工单发起的问题处理等操作日志。

- ALIYUN_INITIATED_SERVICE

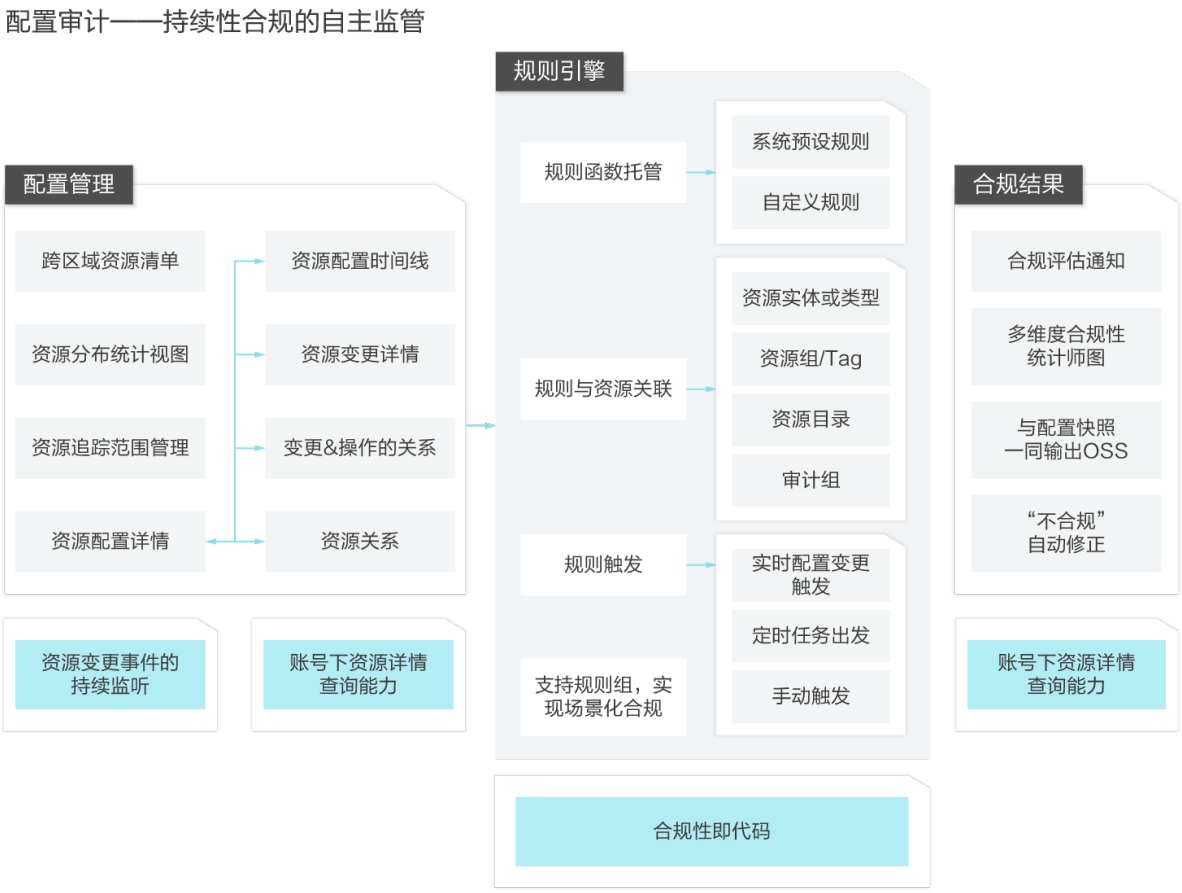
阿里云内部人员或系统基于运维需求所发起的操作，如因集群硬件过保发起的跨集群 Bucket 迁移。

- ALIYUN_INITIATED_PENALTY

  阿里云内部人员或系统基于法律法规要求对用户公开（Public）数据进行处罚的操作日志。

7.5.5. 配置审计

配置审计（Cloud Config）是面向资源的审计服务。为用户提供跨区域的资源清单和检索能力，记录资源的历史配置快照，形成配置时间线。当资源发生配置变更时，自动触发合规评估，并针对“不合规”配置发出告警。使用户能够轻松实现海量资源合规性的自主监控，应对企业内部和外部合规的需要。



在开通配置审计服务时，将扫描用户账号下各区域的保有资源，整理成跨区域的资源清单，并支持简单的检索。用户可以设置将所有/部分资源类型纳入监控范围，配置审计将持续监控并记录资源的配置变更详情，详细对比变更的具体内容，整理成资源的配置时间线，用户能清晰的看到资源配置随时间的演变过程。

配置审计可以将资源的配置快照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，例如授权、开启生命周期管理、归档管理等。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。将资源的历史配置快照与 ActionTrail 的操作日志相结合，可以快速定位问题出现的时间、受影响的资源、配置的前后变化、相关人员等重要信息。

由于配置审计是直接面向资源变更的既定结果做分析，若资源在窗口期（10 分钟）内发生了配置的变更和复原，配置审计无法感知，所以无法生成相应的配置变更快照。若资源在窗口期（10 分钟）内发生了多次变更，配置审计会将多次变更的结果汇总成一个配置变更记录呈现在配置时间线上，并将快照保存到用户的 OSS 存储空间。

配置审计依赖函数计算的函数作为合规规则的编辑器和执行器。用户将合规需求实现为规则代码放在规则函数中。规则需在配置审计服务中与指定的资源关联，当资源出现配置变更记录时，将自动执行规则函数对资源配置进行合规评估，并根据用户的订阅向相应人员发送通知和告警。除了配置变更触发规则执行，还支持规则的定时执行和手动执行。配置审计结合实际合规需求，为用户预设了数十种规则函数供选用，也支持用户自定义规则函数。

配置审计的服务场景主要包括：

- **集中的资源配置管理**

跨区域的资源部署在资源管理时有诸多不便。开通配置审计服务后，为用户提供跨区域

的资源清单和检索能力。用户可以把清单作为资源管理的集中入口，可以直接在线看到资源的配置时间线，也可以通过快捷的链接去往云产品控制台进行管理。

- 持续的合规审计

  用户面对海量云上资源，每日进行频繁的资源变更。用户要确保购买的资源规格符合预期、存储空间禁止了公网访问、磁盘均已加密等合规条例都被遵守和执行，就需要持续性的自主监管方案。当“不合规”出现时能尽早被通知，快速定位相关资源进而快速修正。

- 问题定位与复盘

  问题出现时最重要的是快速定位和解决，而问题解决后的复盘、追责、归档同样重要。用户可将配置审计输出的资源历史配置快照与 ActionTrail 的操作记录相结合，梳理清楚整个事件的脉络，找到问题的初始位置、相关人员、影响的资源列表、触犯的合规规则列表、相关的操作日志等信息，快速整理成问题报告。

7.5.6. 堡垒机

堡垒机是阿里云提供的一个核心系统运维和安全审计管控平台。

堡垒机集中了运维身份鉴别、账号管控、系统操作审计等多种功能。基于协议正向代理实现，通过正向代理的方式实现对 SSH、Windows 远程桌面及 SFTP 等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的。

堡垒机为用户实现以下价值：

- 技术层三个统一：统一运维入口，统一自然人与主机帐号间的权限关系，统一运维操作审计管控点。

- 满足法规要求
  - 政府：满足《等级保护》系列文件中的技术审计要求。
  - 金融：满足金融监管部门系列文件中的技术审计要求。
  - 企业：满足《ISO27000》系列文件中的技术审计要求。

7.5.6.1. 产品功能

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。

- 统一审计

  堡垒机对所有的操作进行详细记录，并提供综合查询功能；审计日志可以在线播放也可以离线播放，所有的审计日志支持自动备份和自动归档。

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。支持多种用户角色：超级管理员、审计管理员、运维员、审计员、系统管理员，每种用户角色的权限都不同，为用设立不同的角色提供了选择，并且满足合规对三权分立的要求。

- 集中授权

  通过集中授权，帮助客户梳理用户与主机直接的关系，并且提供一对一、一对多、多对一、多对多的灵活授权模式。

- 命令控制

  堡垒机提供了集中的命令控制策略功能，实现基于不同的主机、不同的用户设置不同的命令控制策略，策略提供命令阻断、命令黑名单、命令白名单、命令审核四种动作条件。

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。

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、VNC Viewer、flashFXP、SecureFX、OpenSSH 等。

- ECS 高效接入

  一键同步并导入云服务器 ECS。堡垒机支持托管主机的账户和密码，运维人员直接登录即可成功自动登录到目标主机中进行运维操作，无需输入主机的账户和密码。

- 自动运维

  对运维人员来说，需要定期手工执行命令；对网管人员来说，需要定期手工备份网络设备的配置信息。通过堡垒机的自动化运维功能，实现自动化的运维任务并将执行结果通知相关人员。

7.5.6.2. 技术能力

支持手机 APP、短信验证码等多种双因子认证

为了提高来源身份的可靠性，防止身份冒用；堡垒机可以利用以下认证机制实现：

- 内置了手机 APP 认证（TOTP 口令验证）引擎。
- 提供了短信认证、AD、LDAP、RADIUS 认证的接口。
- 支持多种认证方式同时使用、多种认证方式组合使用。

覆盖最全的运维场景

支持管理 Linux/Unix 服务器、Windows 服务器、网络设备（如思科/H3C/华为等）、文件

服务器、Web 系统、数据库服务器、虚拟服务器、远程管理服务器等等。

自动学习、自动授权，大大减轻管理员的配置工作

- 堡垒机采用自动学习技术：自动收集主机的 IP、协议、端口号、账户、密码等信息，并且可以学习到运维人员的权限关系，进一步实自动授权。特别适用与前期对授权关系不清晰、资产信息不完整的场景。
- 运维人员只需通过堡垒机成功登录一次目标主机即可自动录入主机信息，这大大减轻了管理员配置主机信息、用户与主机关系的工作量。

文件传输审计，让数据窃取行为无藏身之地

- 作为运维审计系统，审计是最终目标；审计内容的完整体现了产品的审计能力。
- 不仅实现了对所有操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）等行为记录。

8. 云上数据安全体系

用户的云上数据安全，是用户的生命线，也是云上安全整体能力的一个最重要具象表现。早在 2015 年 7 月，阿里云就发起了中国云计算服务商首个“数据保护倡议”，并在公开倡议书明确：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机密性、完整性和可用性。

在本白皮书中，对云上数据安全的保护，已经在不同维度都对阿里云的相关能力和产品做了详细介绍。本章会从整体的云上数据安全周期梳理并介绍如何在云上使用相关能力和产品构建全链路的数据安全体系。

阿里云的云上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（数据采集、数据传输、数据处理、数据交换、数据存储、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需求以及安全技术保障。

8.1. 数据采集安全

数据采集安全指的是在数据创建的源头就保障数据的识别和分类分级在第一时间能够完成，这样才能保证后续对云上数据的保护做到有的放矢。良好的数据分类分级能够保障后续的安全保护准确性和效率。其中，第一步是对数据中的敏感信息，如个人验证信息（Personal Identifiable Information，PII），进行发现和检测。第二步是针对数据中的敏感信息，根据用户的使用场景，合规需求，和安全要求，对数据进行分类分级，从而达到自知数据资产，并后续进行针对性保护的作用。

阿里云的敏感数据保护（Sensitive Data Discovery and Protection，简称 SDDP）产品支持对 MaxCompute、RDS 和 OSS 中的数据进行识别和分类。SDDP 可在得到云上用户授权后，自动扫描和发现授权范围内的新增实例/库/表/列、对象存储文件桶/文件对象等不同级别数据信息。通过关键字、规则、机器学习模型算法，精准识别云环境内的敏感数据，并支持根据用户自身业务规则进行敏感数据自定义。SDDP 根据敏感数据识别结果，可实现云上数据基于业务内容的分类以及基于敏感程度的分级，以供后续根据敏感分类分级结果在云上系统中对用户数据实现相关的保护机制。

阿里云的 Dataworks 服务也提供数据自动识别和分类分级规则定义，可以对数据进行自动发现和分类分级。同时，阿里云用户也可以利用 MaxCompute 中对字段打标（Label Security）的功能对相关数据进行分类分级。

8.2. 数据传输安全

8.2.1. HTTPS 传输加密

数据传输安全是通过数据传输链路加密来保障的。传输加密是指云产品为用户访问（包括读取和上传）数据提供了 SSL/TLS 协议来保证数据传输的安全。例如，用户如果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。所有的阿里云产品都为客户提供了支持

HTTPS 的 API 访问点，并提供高达 256 位密钥的传输加密强度，满足敏感数据加密传输需求。

8.2.2. VPN/SAG 网关

阿里云的网关产品也提供传输链路的加密功能。VPN 网关（VPN Gateway）服务，可通过传输链路加密通道将企业本地 IDC 和阿里云 VPC 安全可靠的连接起来。VPN 网关可建立 IPsec-VPN，将本地 IDC 网络和云上 VPC 连接起来，也可建立 SSL-VPN，将本地客户端远程接入 VPC。阿里云也提供智能接入网关（Smart Access Gateway，简称 SAG）服务，企业用户可通过智能接入网关实现就近加密接入，并在传输过程中通过使用 IKE 和 IPsec 协议对传输数据进行加密，保证数据安全。阿里云 VPN 网关和智能接入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。

8.2.3. SSL 证书服务

阿里云的证书服务（Alibaba Cloud Certificates Service），可以在云上签发第三方知名 CA 证书颁发机构的 SSL 证书，帮助用户实现其网站 HTTPS 化，使网站可信，防劫持、防篡改、防监听。证书服务对云上证书进行统一生命周期管理，简化证书部署，支持一键分发到各云产品（如 CDN、SLB、高防和 WAF 等），保障用户在传输加密过程中的证书管理需求。

8.3. 数据处理安全

数据处理安全主要体现在数据在使用中需要进行有效的隔离保护。隔离手段可以是用户侧通过使用 Intel® SGX 运行时态的加密计算环境实现隔离，可以通过各个产品中的权限管控等隔离手段实现，也可以通过在数据分类分级基础上的对数据脱敏使得未授权用户不得获取相关敏感信息来实现数据的隔离保护需求。在真实场景中，往往需要通过多维度的产品功能配合来达到用户需要的数据隔离保护需求。

8.3.1. 加密计算

阿里云平台提供了以 Intel® Software Guard Extensions （Intel® SGX）可信执行环境作为基础的硬件可信执行环。用户可以通过软件建立一个可信执行环境，并保护敏感数据（例如，加解密密钥、账户凭证信息等）。通过支持加密计算能力的 ECS 主机（神龙机型），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，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，阿里云为用户数据在执行态环境中提供了更强大的数据加密保护能力。

8.3.2. 云产品权限管控

阿里云的各个云产品基于 RAM 的资源访问控制服务和云产品自身的管控能力，可以提供相应的数据隔离保护能力。本章节只会对较为典型的产品权限管控机制做出介绍，具体细节请参照对应的产品章节。

8.3.2.1. 计算和网络环境隔离

用户的云上环境可以通过 ECS 安全组、VPC、云防火墙等手段对用户云上数据处理环境的隔离。

ECS 安全组是一种用作关联 ECS 实例的虚拟防火墙，在实例级别同时控制入站和出站流量，具备状态检测和数据包过滤功能，用于在云端划分安全域。用户可以通过配置安全组规则，允许或禁止安全组内的 ECS 实例对公网或私网的访问。

VPC 可以帮助用户基于隧道技术，实现数据链路层的隔离，为每个用户提供一张独立隔离的安全网络环境。

云防火墙作为 SaaS 化防火墙，可以统一管理互联网到业务的南北向访问策略和业务与业务之间的东西向微隔离策略。云防火墙满足等保 2.0 对虚拟边界、内到外管控、IPS 入侵检测、

6 个月网络日志的相关要求，是等保 2.0 合规必选产品。

8.3.2.2. RAM 访问控制

阿里云提供资源访问控制（Resource Access Management，简称 RAM）服务，用于用户身份管理与资源访问控制。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、多因素认证等等）。

通过使用 RAM 和其提供的 RAM 用户、用户角色、用户组、资源组、资源 tag 等功能，可以通过权限策略（RAM Policy）控制一个操作主体（如用户、用户组、RAM 角色等）对一个具体资源的访问能力。权限策略中可以指定在某种条件下允许（Allow）或拒绝（Deny）对某些资源执行某些操作，从而可以控制数据所在的相关资源隔离需求。

8.3.2.3. OSS 访问控制

针对存放在 Bucket 的 Object 的访问，OSS 提供了多种权限控制方式，其中包括 ACL、RAM Policy 和 Bucket Policy。

- ACL：OSS 为权限控制提供访问控制列表（ACL）。ACL 是基于资源的授权策略，可授予 Bucket 和 Object 访问权限。 用户可以在创建 Bucket 或上传 Object 时设置 ACL，也可以在创建 Bucket 或上传 Object 后的任意时间内修改 ACL。
- RAM Policy：Resource Access Management（RAM）是阿里云提供的资源访问控制服务。RAM Policy 是基于用户的授权策略。通过设置 RAM Policy，可以集中管理用户（比如员工、系统或应用程序），以及控制用户可以访问哪些资源的权限。比如能够限制用户只拥有对某一个 Bucket 的读权限。
- Bucket Policy：Bucket Policy 是基于资源的授权策略。相比于 RAM Policy，Bucket Policy

操作简单，支持在控制台直接进行图形化配置，并且 Bucket 拥有者直接可以进行访问授权，无需具备 RAM 操作权限。Bucket Policy 支持向其他账号的 RAM 用户授予访问权限，以及向匿名用户授予带特定 IP 条件限制的访问权限。

8.3.2.4. RDS 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。IP 白名单内还提供高安全白名单模式供用户选择。

8.3.2.5. MaxCompute 访问控制

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。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（例如，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，针对项目空间、表（View 也需要单独授权）、函数、资源、 任务实例等多种对象，授予不同权限。同时，MaxCompute 支持列级别的敏感数据打标（Label Security）以达到细粒度的访问控制。

授权机制

- MaxCompute 支持通过 ACL 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。
- MaxCompute 权限模型支持真正意义上的字段(列)级别的 ACL 访问控制，字段也作为 ACL 支持的对象之一，和表一样是独立的授权主体，包含完整的授权信息(如权限有效期)。
- MaxCompute 支持基于标签的安全访问控制策略。在对数据和人分别设置安全等级标记之后，LabelSecurity 的默认安全策略如下：
  - No-ReadUp：不允许用户读取敏感等级高于用户等级的数据，除非显式授权。
  - Trusted-User：允许用户写任意等级的数据，新建数据默认为 0 级（不保密）。
- MaxCompute 为管理类操作也定义了权限控制机制。例如，拥有 CreatePackage 权限的项目空间内成员就可以创建 package；拥有 AddPackageResource 权限的项目空间

内成员就可以向 package 中添加资源。用户可以用 MaxCompute 的 Policy 方式对管理类的操作进行授权。

沙箱隔离

MaxCompute 中所有计算是在受限的沙箱中运行，多层次的应用沙箱，从 KVM 级到 Kernel 级。系统沙箱配合鉴权管理机制，用来保证数据的安全，以避免出现内部人员恶意或粗心造成服务器故障。

8.3.3. 数据脱敏

阿里云的敏感数据保护（Sensitive Data Discovery and Protection，简称 SDDP）产品，提供 Hash、加密、遮盖、替换、洗牌、变换等六大类近 30 种内置脱敏算法并同时支持客户自定义脱敏算法或者自定义脱敏参数，确保脱敏后的数据无需改变相应的业务系统逻辑，保留原有数据特征和分布，确保数据的有效性和可用性。用户可以低成本、高效率、安全地使用脱敏数据完成业务上的数据保护需求。

阿里云的 Dataworks 服务提供数据保护伞功能，可以被 MaxCompute 接入并提供数据脱敏的能力。同时，MaxCompute 可以接入各类脱敏应用生态，脱敏算法由具备专业脱敏能力的应用提供。MaxCompute 能在计算中调用接入的脱敏算法，并输出脱敏后内容。

8.4. 数据交换安全

数据的价值是通过交换和共享来实现的。数据交换中的安全需求可以部分通过在上文的云上数据安全体系-数据处理安全章中介绍的云产品权限管控能力和敏感数据保护产品提供的数据脱敏能力来实现，在此不再赘述。同时，数据交换安全也需要依靠数据泄露的检测能力。

8.4.1. 数据泄露检测

用户数据的泄露检测，主要体现在对数据的权限控制的完整度和数据使用中的监控和检测

能力。如果想要防止数据泄露，首先需要实现对云上存储产品和传输产品权限的有效管控。阿里云的敏感数据保护（Sensitive Data Discovery and Protection，简称 SDDP）产品支持“数据、人、权限”三要素的即时查询，支持角色背后主账号权限映射解析，和全局数据权限统一查询。SDDP 服务可以针对云上环境内不符合安全最佳实践的数据权限配置、权限使用异常进行告警。

其次，需要对用户数据的流转和操作过程有全面的监控和检测能力，及时发现数据使用中可能的异常行为。SDDP 服务能针对数据流转过程中的异常情况进行有效监控，实现数据流转链路动态展示，确保数据导出/数据传输合规有序。根据日志聚类分析，有效识别人工操作与应用接口调用。基于机器学习和大数据分析能力，针对环境内各类数据流转、数据操作中产生的异常行为进行监控告警。

最后，在发现数据泄露告警后，SDDP 服务支持对异常事件进行分析以供后续的处理响应。其中，事件分析支持集中归集各类告警事件，并通过使用时序分析技术还原责任主体行为基线，动态展示历史基线轨迹，从而有效的提升分析效率。同时，SDDP 服务支持各租户事件隔离处理，并支持处理结果自动回流机器学习样板库，从而使得异常检测能力日趋准确。

敏感数据的泄露也可通过各个产品本身的防泄露功能实现。如在 Dataworks 中，可以通过数据的风险识别管理能力配置风险数据规则，从而识别日常访问中的风险以及启动 AI 自动识别数据风险能力，并对识别后的风险数据统一在数据风险页面进行展示和审计操作。相似功能也可以通过日志服务，数据库审计服务等云产品中对相关数据的使用情况进行规制定义的审计。

8.5. 数据存储安全

8.5.1. 落盘加密

数据存储安全主要是通过数据落盘加密来保障的。阿里云提供云产品落盘存储加密能力给用户，并统一使用阿里云密钥管理服务（Key Management Service，简称 KMS）进行密钥管理。

阿里云的存储加密提供 256 位密钥的存储加密强度（AES256），满足敏感数据的加密存储需求。

阿里云已拥有不同的云产品支持数据存储加密功能（具体产品请参见产品对应章节）：

- 块存储 EBS：支持虚拟机内部使用的块存储设备（即云盘）的数据落盘加密，确保块存储的数据在分布式系统中加密存放，并支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。
- 对象存储 OSS：支持服务端和客户端的存储加密能力。在服务端的加密中，支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。在客户端的加密中，支持使用用户自管理密钥进行加密，也支持使用用户 KMS 内的主密钥进行客户端的加密。
- RDS 数据库的数据加密：RDS 数据库的多个版本通过透明加密（Transparent Data Encryption，简称 TDE）或云盘实例加密机制，支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。
- 表格存储 TableStore：支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。
- 文件存储 NAS：支持使用服务密钥作为主密钥进行数据加密。
- MaxCompute 大数据计算：支持使用服务密钥作为主密钥进行数据加密。

还有更多产品也均支持了存储加密功能，包括支持使用服务密钥和用户自选密钥作为主密钥进行数据加密，具体情况请咨询各个产品官网信息（www.aliyun.com）

8.5.2. 自选密钥

云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。具体而言，当用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥管理服务（KMS）中的使用地域自动创建一个专为 该服务使用的用户主密钥（Customer Master

Key，简称 CMK）。本密钥会作为服务密钥且其生命周期是托管给云产品的。具体表现为用户可以在密钥管理服务控制台上查询到该用户主密钥，但不能删除。

但是，虽然云产品托管的服务密钥可以帮助用户获得最基本的数据保护能力，但是对于有明确诉求的用户，还可能存在一些密钥管理的短板，例如不能自主管理密钥的生命周期，不能设定自动轮转，保护级别仅仅为软件密钥等。

因此,用户可以通过在支持的云产品中选择自己创建或上传用户主密钥(CMK）到 KMS 中，并直接管理自选密钥的生命周期。通过 RAM 的授权后，自选密钥也可用于云产品的数据加密功能，并赋能用户更多的安全能力：

- 用户可以禁用或者启用密钥，控制云产品加解密数据的能力。
- 用户可以配置授权策略，控制云产品加解密数据的能力。
- 用户可以通过在 KMS 中导入自带密钥（Customer Supplied Key，即 BYOK），进一步增强密钥的生命周期管理能力和控制云产品的数据加解密能力。

用户自选的 CMK 是用户的资产，云产品必须得到用户的授权（通过 RAM）才可以使用其对数据进行加解密操作。用户也可以随时取消相对应的 CMK 授权,达到对数据加解密操作的可控。请注意，当使用自选密钥和上述安全能力时，也意味着，用户需要更多的考虑己方的责任，管理好对密钥的授权和生命周期。

8.5.3. 密钥托管 HSM

阿里云的 KMS 服务支持用户将密钥托管在硬件安全模块（Hardware Security Module，HSM）之中，并可利用 HSM 进行密码运算和安全托管等功能，为用户的主密钥提供更高层次的保护。用户可以将密钥托管在硬件安全模块（HSM）中，利用硬件机制来保护密钥的明文密钥材料不会离开 HSM 的安全边界。用户使用 HSM 密钥进行运算时，密码运算的过程也只会发生在

HSM 中，从而保证了用户密钥的私密性。HSM 托管密钥可以满足用户的高级别安全和合规需求。

8.6. 数据销毁安全

8.6.1. 物理销毁

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。阿里云建立废弃介质上数据安全擦除流程，处置数据资产前，检查含有敏感数据和正版授权软件的媒介是否已被覆写、消磁或折弯等数据清除处理，且不能被取证工具恢复。当因业务或法律原因，不再需要某些硬拷贝材料时，将其物理破坏，或取得数据处理第三方的损坏证明，以确保数据无法重建。

8.6.2. 数据清零

作为存储虚拟化的延伸，云用户实例服务器释放后，其原有的磁盘和内存空间将会被可靠的进行数字清零以保障用户数据安全。

8.6.3. 终止服务后清除

阿里云在终止为云服务客户提供服务时，会及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。阿里云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。

9. 阿里云安全最佳实践

各云产品使用中的安全最佳实践建议参考《阿里云企业上云安全指引 Guidebook》。Guidebook 从云上安全问题、云安全防护架构出发，帮助客户设计构建云上安全体系、全面保护云上资产，包含定义自身的安全体系，识别、分类并保护云上账户、应用、服务和基础设施安全，指导客户基于阿里云产品和生态建立起自身的云上安全防护体系。

同时，建议客户参考阿里云解决方案最佳实践中《安全和合规条目》下对应的最佳实践内容。阿里云解决方案最佳实践，是基于众多客户上云的成功案例萃取而成的最优化企业上云指导。每个最佳实践包括使用场景、多产品部署架构及部署手册。具体请参见**企业上云最佳实践**（https://cn.aliyun.com/acts/best-practice/index）。

10. 版本历史

2020 年 1 月：发布 4.1 版本：少量内容勘误，并同时发布英文版本。

2019 年 9 月：发布 4.0 版本：阿里云安全架构全面升级；增加云上数据安全体系；产品相关描述全面更新。

2017 年 9 月：发布 3.0 版本：阿里云安全架构和产品相关描述全面更新。

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

2015 年 12 月：发布 2.0 版本。

2014 年 1 月：发布 1.2 版本。