阿里云

阿里公共云
网络安全等级保护 2.0
合规能力技术白皮书

仅供阿里云用户参考使用，请勿私自传播和宣传

编号：20191201

版本：V1.0

总　述

《阿里公共云网络安全等级保护 2.0 合规能力技术白皮书》从网络安全合规责任划分、云安全合规能力评估、阿里公共云典型场景(IaaS)的合规实施分析及白皮书使用建议等方面做了详细阐述。借助该技术白皮书，云服务客户能够快速：

- 确定不同云计算服务模式下的网络安全合规要求和安全建设责任边界；
- 了解阿里公共云的安全能力，包括云平台原生安全能力，以及云产品和阿里云安全产品提供的安全能力；
- 依托并合理配置阿里公共云提供的安全能力，同时结合云服务客户业务应用系统的安全防护能力建设，构筑满足网络安全等级保护的安全合规体系。

本技术白皮书正文共分为五个部分，各部分内容具体安排如下：

第一部分为概述，对本技术白皮书的目的及主要内容进行简要介绍。

第二部分描述了在不同云计算服务模式下，阿里云分服务模式的产品划分、网络安全等级保护定级情况以及基于云安全责任模型对云服务商和云服务客户在网络安全等级保护基本要求条款适用性选择。

第三部分介绍了阿里云安全合规能力评估模型，并对阿里公共云平台、云产品以及云安全产品的安全能力进行阐述。

第四部分以 IaaS 模式下云服务客户典型场景为例，分析了云服务客户落实网络安全等级保护制度时，如何确定等级保护对象，如何引用云平台等级测评结论，以及识别云服务客户业务系统安全防护能力与网络安全等级保护基本要求间的符合程度。

第五部分从行业应用角度对技术白皮书的应用方法进行了解读，阐述了如何利用技术白皮书快速识别网络安全等级保护基本要求适用条款，以及分析符合基本要求需建设的安全能力。

附录部分，附录 A 介绍了不同云计算服务模式下的典型阿里云产品；附录 B 提供了在不同云计算服务模式下，云服务客户定级对象应满足的网络安全等级保护基本要求条款；附录 C 描述了云产品和云安全产品及其安全能力(措施)与网络等级保护基本要求间的对应关系。

仅供阿里云用户参考使用，请勿私自传播和宣传

声　明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解下列各条款的内容：

- 通过阿里云提供的授权通道下载、获取本文档，且仅能用于自身合法合规的业务活动，未经阿里云同意，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容，不得以任何方式或途径进行传播和宣传。
- 由于产品/服务升级、调整或其他原因，本文档内容有可能变更，您应当实时通过授权渠道下载、获取最新版的用户文档。
- 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。
- 本文档第二、三部分（含附录B）由公安部信息安全等级保护评估中心拥有其知识产权，其余部分归阿里云计算有限公司依法拥有。未经双方事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制公安部信息安全等级保护评估中心和阿里云的名称。
- 期望能够给本文档的阅读者提供有用的参考，限于编制时间仓促，内容难免疏漏和不足，诚望不吝赐教、斧正，以便后续改进和完善。
- 任何意见或建议敬请联系：aliyun_compliance@service.aliyun.com。

仅供阿里云用户参考使用，请勿私自传播和宣传

主要编制人

张振峰　　张志文　　黄少青　　姜友贵　　陈吴栋
李　阳　　崔旭东　　张　鹏　　蒋　晓　　张　瑜

特别感谢

张宇翔　　李　明　　肖　力　　董　侃　　郑原斌

目 录

总 述 I

声 明 II

1 概述 ..... - 1 -

2 安全合规责任 ..... - 2 -

2.1 阿里云服务模式划分 ..... - 2 -
2.2 安全合规责任划分 ..... - 3 -
2.3 云服务客户基本要求适用性条款 ..... - 5 -

3 安全合规能力模型 ..... - 7 -

3.1 保护对象 ..... - 7 -
3.2 安全措施 ..... - 7 -
3.3 安全能力 ..... - 11 -
3.3.1 云平台原生安全能力 ..... - 11 -
3.3.2 云产品安全能力 ..... - 12 -
3.3.3 云安全产品安全能力 ..... - 12 -
3.3.4 云客户自建能力 ..... - 12 -
3.4 安全合规评估 ..... - 12 -

4 安全合规实践指引 ..... - 13 -

4.1 云服务客户典型场景概述 ..... - 13 -
4.2 等级保护对象概述 ..... - 13 -
4.3 引用云平台等级保护结论 ..... - 14 -
4.4 基本要求合规分析（通用要求） ..... - 15 -
4.4.1 安全通信网络 ..... - 15 -
4.4.2 安全区域边界 ..... - 19 -
4.4.3 安全计算环境 ..... - 29 -
4.4.4 安全管理中心 ..... - 46 -
4.5 基本要求合规分析（云计算扩展要求） ..... - 52 -
4.5.1 安全通信网络 ..... - 52 -
4.5.2 安全区域边界 ..... - 53 -
4.5.3 安全计算环境 ..... - 54 -
4.5.4 安全管理中心 ..... - 56 -
4.5.5 安全建设管理 ..... - 57 -

5 合规白皮书应用指引 ..... - 60 -

5.1 快速识别基本要求适用条款 ..... - 60 -
5.2 快速分析基本要求安全合规能力 ..... - 60 -

附录 A：阿里云不同服务模式下的典型产品 ..... - 61 -

附录 B：不同模式下云服务客户等级保护适用条款 ..... - 65 -

仅供阿里云用户参考使用，请勿私自传播和宣传

B.1 网络安全等级保护基本要求（通用要求）..... - 65 -
B.2 网络安全等级保护基本要求（云扩展要求）..... - 76 -
附录 C：阿里云等级保护基本要求安全能力对照表..... - 77 -
C.1 网络安全等级保护基本要求（通用要求）..... - 77 -
C.2 网络安全等级保护基本要求（云扩展要求）..... - 94 -
C.3 网络安全等级保护基本要求（物联网扩展要求）..... - 96 -

仅供阿里云用户参考使用，请勿私自传播和宣传

1 概述

《网络安全法》2017 年 6 月 1 日实施标志着网络安全保护进入有法可依的 2.0 时代，“网络安全等级保护制度”首次从法律层面提及。网络安全等级保护对象由信息系统调整为基础信息网络、信息系统（含采用移动互联技术的系统）、云计算平台/系统、物联网、大数据应用/平台/资源、物联网和工业控制系统等。2019 年 12 月 1 日起，《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》(以下简称“基本要求”)等系列标准正式实施，落实网络安全等级保护制度是每个企业和单位的基本义务和责任。

阿里云作为网络安全等级保护的先行者和践行者，在确保云平台自身满足基本要求的基础之上，利用云平台原生安全和云安全产品技术优势，希望能够帮助云服务客户更快速、高效和持续的落实网络安全等级保护制度，提升“云上”业务系统的安全防护能力。

本白皮书介绍了阿里云如何助力云服务客户构建基于网络安全等级保护的安全合规体系，内容包括：

- 安全合规责任
- 安全合规能力建设
- 安全合规实践指引
- 合规白皮书应用指引

仅供阿里云用户参考使用，请勿私自传播和修改

2 安全合规责任

在云计算环境中，任何云服务客户业务应用系统安全性由云服务商和云服务客户共同保障，云服务客户业务系统所部署的云计算服务模式不同，双方安全责任边界也相应产生差异，详见《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》附录 D。

云计算的三种基本服务模式：IaaS（Infrastructure as a Service，基础设施即服务）、PaaS（Platform as a Service，平台即服务）和 SaaS（Software as a Service，软件即服务）。

2.1 阿里云服务模式划分

阿里云依托自主研发、服务全球的超大规模飞天云操作系统，在全球 200 多个国家和地区为云服务客户提供计算、存储、网络、数据处理和安全防护等多种服务。阿里云为云服务客户提供的云产品（服务）基于 IaaS、PaaS 和 SaaS 三种服务模式划分如图 2.1。

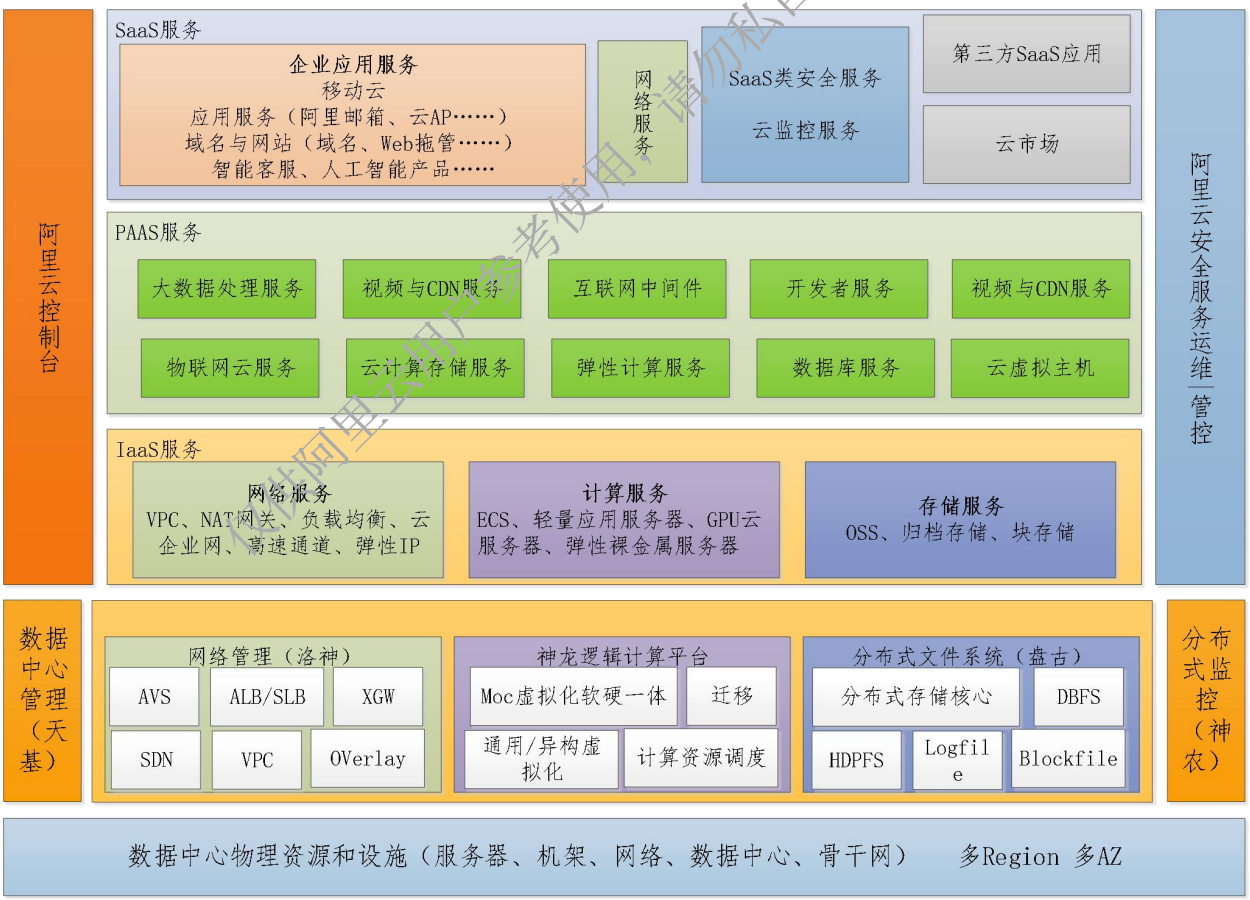

图 2.1 阿里公共云云上服务逻辑架构图

为确保不同云服务模式下网络安全等级保护测评工作的完备性，云服务商对提供的不同服务模式的云计算平台分别进行等级保护定级和开展等级保护测评工作。因此，阿里云

仅供阿里云用户参考使用，请勿私自传播和宣传

依据提供的云服务模式实行单独定级，确定公共云基础服务平台、公共云数据及开发服务平台、公共云应用服务平台三个等级保护定级对象，具体为：

1）公共云基础服务平台：通过 IaaS 模式提供网络、计算和存储等基础云服务；

2）公共云数据及开发服务平台：通过 PaaS 模式提供大数据、中间件、开发者以及物联网云服务；

3）公共云应用服务平台：通过 SaaS 模式提供云邮箱、域名、人工智能、安全以及第三方应用服务。

为便于云服务客户能够快速判断采购的云产品所属云计算服务模式类型，云服务客户可参考：**附录 A 阿里云不同服务模式下的典型产品。**

2.2 安全合规责任划分

在不同云计算服务模式下，云服务商和云服务客户安全责任存在一定差异，如图 2.2，云服务客户安全责任范围从 IaaS 到 SaaS 逐步缩小。在 IaaS 模式下，云服务商要确保云平台基础设施安全，云服务客户负责虚拟环境以及自身业务应用安全，而在 SaaS 模式下，云服务商需对整个云计算环境提供安全防护责任，云服务客户仅需对其选用的应用进行安全配置，并对自身重要数据做好安全防护工作。

仅供阿里云用户参考使用，请勿私自传播和宣传

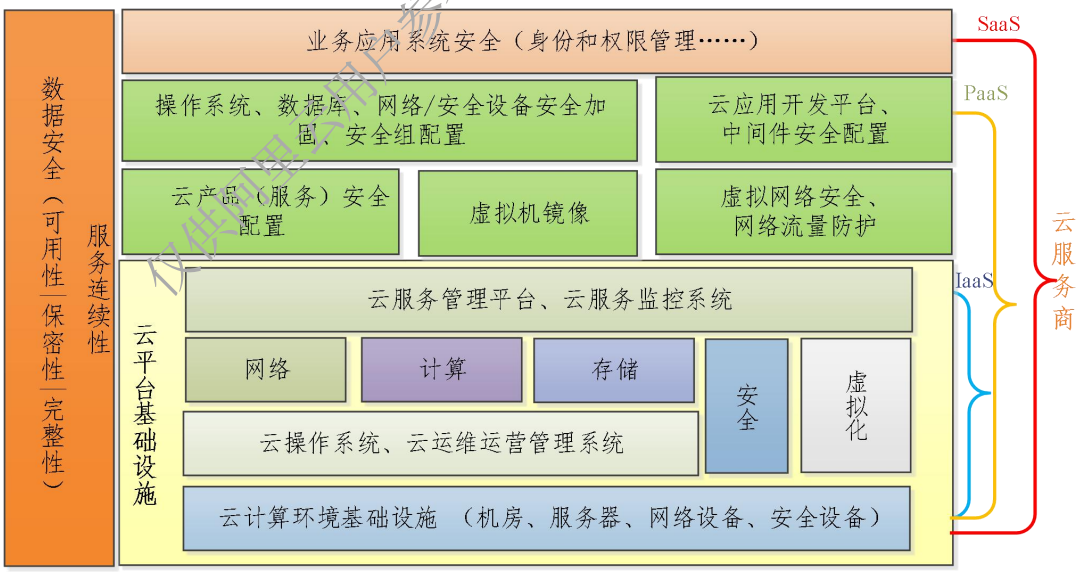

图 2.2 安全合规责任模型

根据图 2.2 中不同服务模式下云安全合规责任模型，结合等级保护标准框架和安全保护对象，云服务商和云服务客户等级保护对象划分如图 2.3 所示。

在 IaaS 服务模式中，云服务商的责任对象主要包括基础架构层硬件、虚拟化以及云服

务层的防护；云服务客户的责任对象包括虚拟机、数据库、中间件、业务应用和数据的安全防护。

在 PaaS 服务模式中，云服务商的责任对象主要包括基础架构层硬件、虚拟化以及云服务层、和虚拟机、数据库的安全防护，云服务客户责任主要为软件开发平台中间件以及应用和数据的安全防护。

在 SaaS 服务模式中，云服务客户仅需关心业务应用相关的安全配置、用户访问、用户账户以及数据安全的防护，云服务商的责任对象则包括基础架构层硬件、虚拟化以及云服务层和虚拟机、数据库、中间件、业务应用的安全防护。

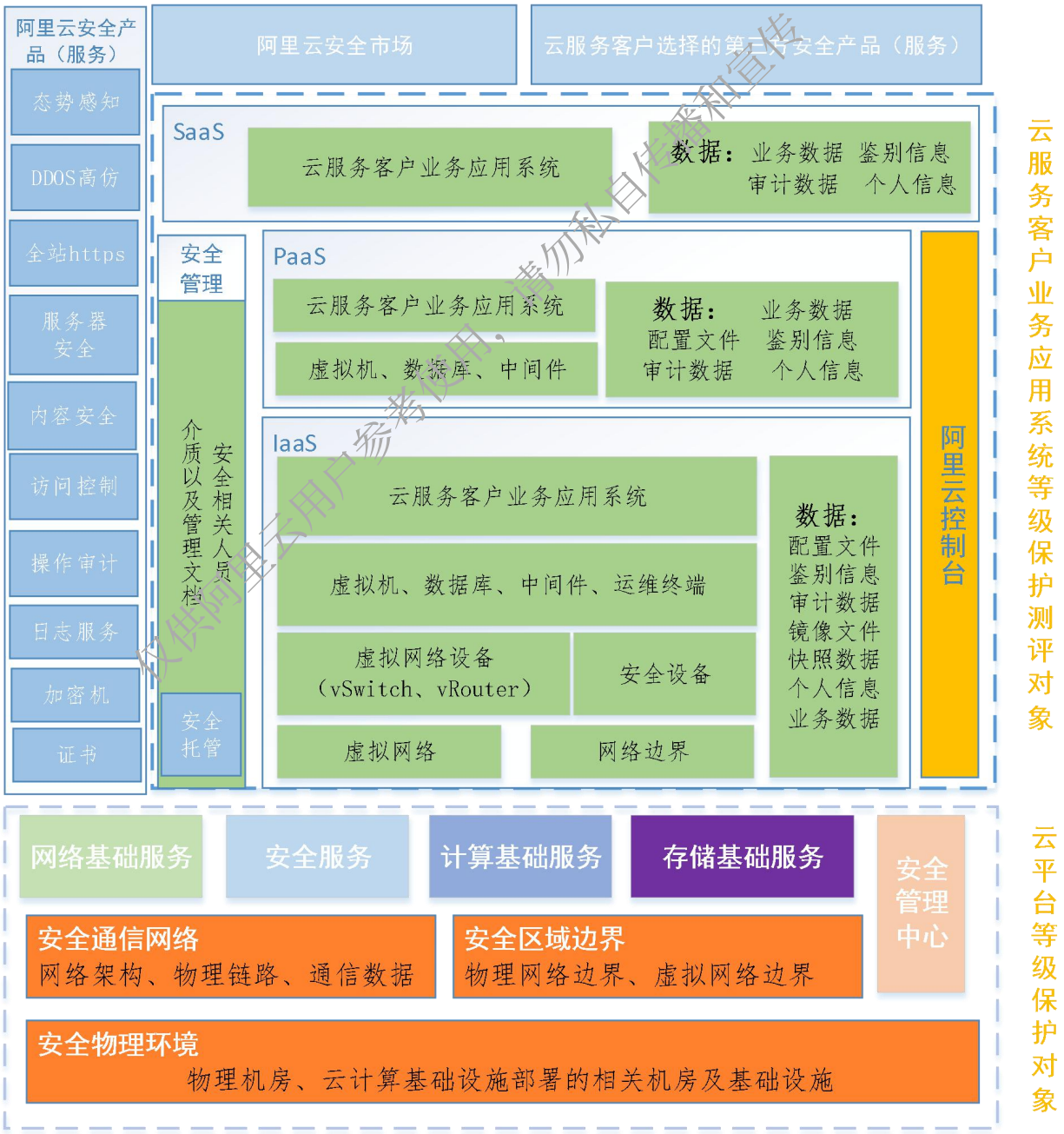

图 2.3 云计算环境等级保护对象划分

2.3 云服务客户基本要求适用性条款

在云计算等级保护形态下，依据基本要求及相关标准，**云服务客户业务系统和云服务商云计算平台分别作为单独的定级对象，即云计算平台和云服务客户业务系统，两种形态需分别满足网络安全等级保护相关标准、要求。**

考虑到云平台和云服务客户业务系统的关联性，需按照下列原则筛选分别适用于云平台和云服务客户业务系统的基本要求条款。

- 用于保障云平台自身安全能力，或云平台提供云服务客户使用但无需云服务客户进行自主配置的安全能力的基本要求条款，只适用于云平台；
- 云平台为云客户提供的云计算服务，为保障云计算服务能够提供其相应的安全能力，且需云服务客户自主进行配置的基本要求条款，同时适用于云平台和云服务客户业务系统；
- 用于保障云平台和云服务客户业务系统对各自保护对象进行安全防护的基本要求条款，适用于云平台和云服务客户业务系统；
- 针对云服务商选择的基本要求条款，只适用于云服务客户业务系统。

基于图 2.3 云计算环境等级保护对象划分，不同云计算服务模式下，云服务商和云服务客户安全责任和保护对象不同，基本要求对云服务商和云服务客户的适用性也存在一定差异。

基本要求（第三级）在不同的云计算服务模式下对云服务客户的适用条款数量统计如图 2.4 所示。

仅供阿里云用户参考使用，请勿私自传播和转售

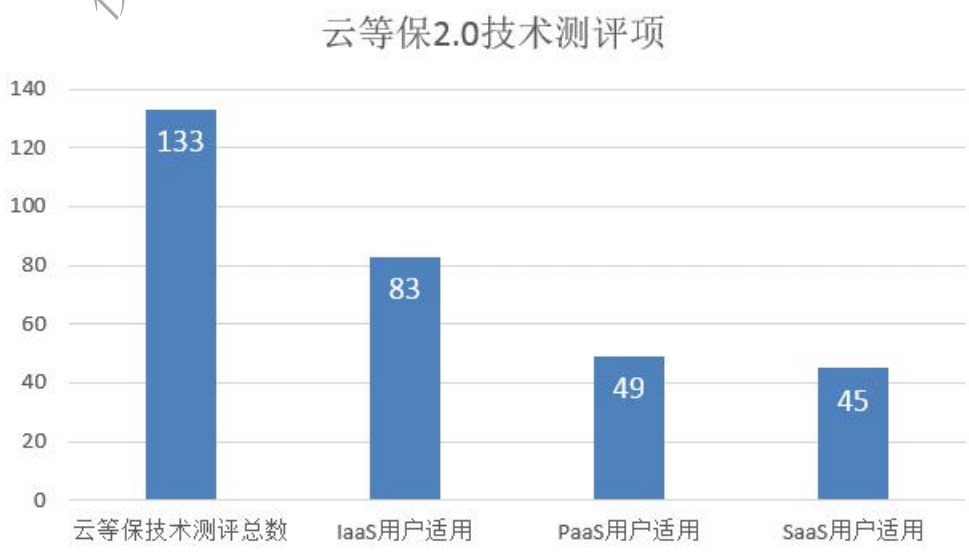

图 2.4 不同服务模式下的云服务客户等保 2.0 技术测评项数量

在不同云计算服务模式下对云服务客户的适用条款数量如下表 2.1。

表 2.1 不同服务模式下云服务客户等级保护标准适用条款数量

技术/管理	通用/扩展	安全类	公有云云服务客户适用条款数			
			三级条款数	IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
网络安全等级保护技术要求	通用	安全物理环境	22	0	0	0
		安全通信网络	8	8	0	0
		安全区域边界	20	20	0	0
		安全计算环境	34	34	34	34
		安全管理中心	12	12	9	7
	扩展	安全物理环境	1	0	0	0
		安全通信网络	5	0	0	0
		安全区域边界	8	4	2	0
		安全计算环境	19	5	4	4
		安全管理中心	4	0	0	0
技术部分总计			**133**	**83**	**49**	**45**
网络安全等级保护管理要求	通用	安全管理制度	7	7	7	7
		安全管理机构	14	14	14	14
		安全管理人员	12	12	12	12
		安全建设管理	34	34	34	19
		安全运维管理	48	48	45	44
	扩展	安全建设管理	8	7	7	7
		安全运维管理	1	0	0	0
技术+管理部分总计			**257**	**205**	**168**	**148**

具体适用项详见**附录 B 阿里云不同模式下云服务客户等级保护适用条款。**

仅供阿里云用户参考使用，请勿私自传播和宣传

3 安全合规能力模型

阿里公共云等级保护合规能力模型（图 3.1）是基于云计算环境保护对象、安全措施以及安全防护能力，构建的云计算环境安全合规状况分析、评估的安全合规模型。对于云服务客户业务系统的安全合规能力分析过程，包括确定保护对象、确定安全措施、确定安全能力及安全合规评估四个环节。

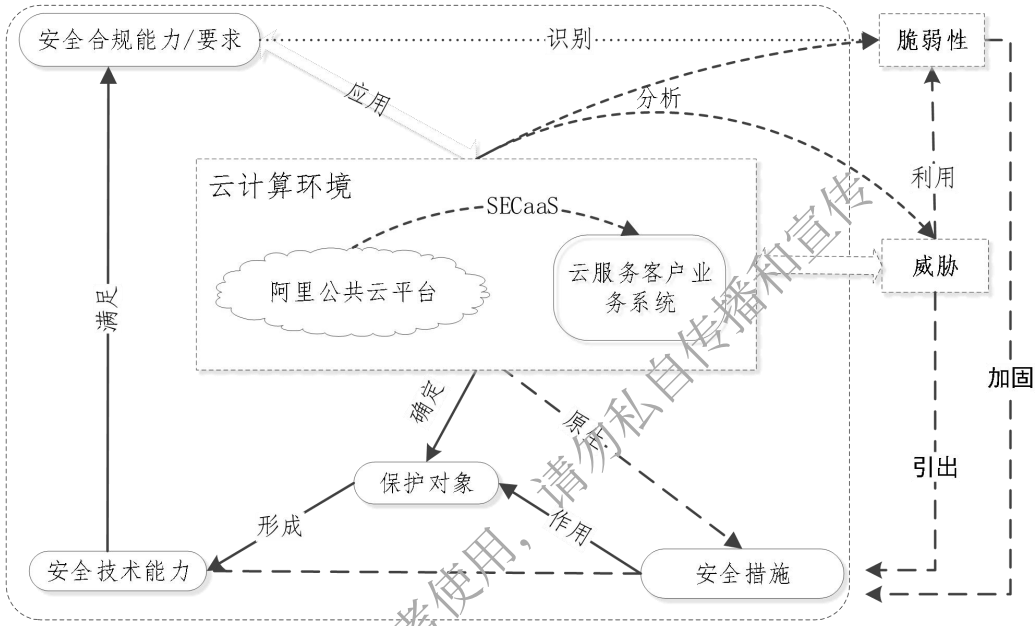

图 3.1 阿里公共云等级保护合规能力模型

仅供阿里云用户参考使用，请勿私自传播和宣传

3.1 保护对象

基于图 2.3 云计算环境等级保护对象划分，云服务客户可基于部署的云计算服务模式确定云服务客户业务系统的等级保护对象。

3.2 安全措施

安全措施是根据广泛的经验和学识为对抗云计算系统面临的威胁而采取的防护措施，有的安全措施是由云平台/云产品原生，有些则是云服务商为应对威胁而自研或由云生态合作伙伴提供。按照等级保护“一个中心，三重防护”纵深防护思想，即从通信网络到区域边界再到计算环境进行重重防护，通过安全管理中心进行集中监控、调度和管理，阿里公共云平台构建了动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控的防护架构，同时为阿里公共云云服务客户构建了完善的云上安全防护体系。

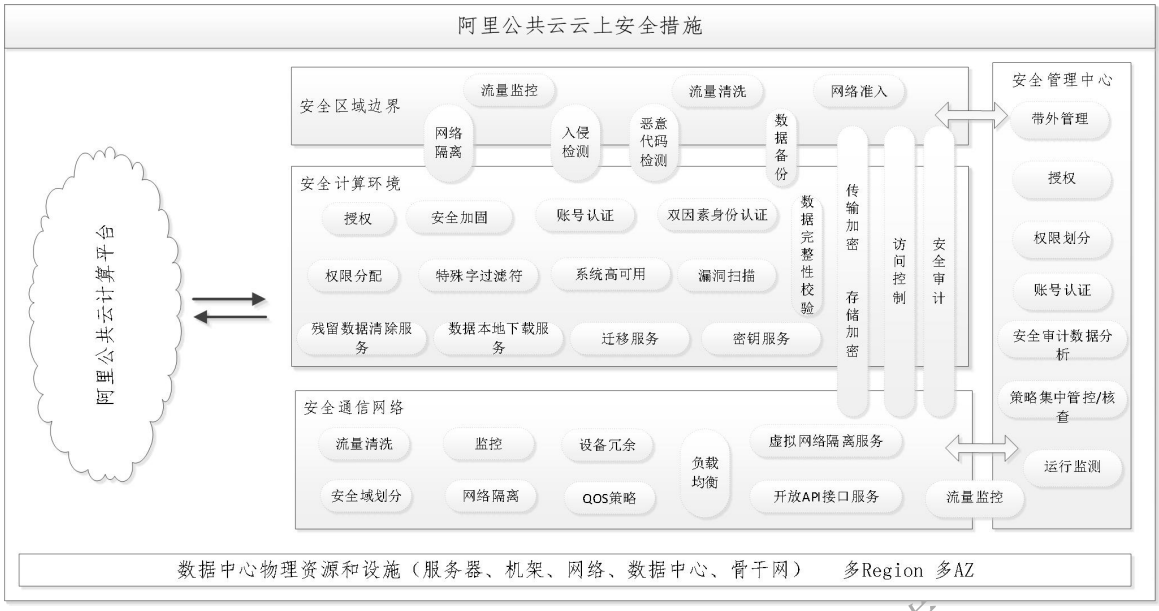

图 3.2 阿里公共云云服务客户安全措施

阿里云云平台/云产品为云服务客户提供多种安全防护措施，如虚拟网络隔离、双因素身份鉴别、访问控制、日志审计、负载均衡和数据备份等。

■ 虚拟网络隔离服务

阿里云产品提供了广泛的安全隔离措施，专有网络（Virtual Private Cloud）不仅支持用户自定义 IP 地址范围、配置路由表和网关等，还通过网络隔离提高了用户云上服务与数据的安全性。在网络隔离方面，专有网络（VPC）能够在三个层面实现隔离：

1) 专有网络之间通过隧道 ID 进行隔离，VPC 只能通过对外映射的 IP（弹性公网 IP 和 NAT IP）进行互连。
2) 专有网络同一子网内使用交换机互通互连，不同子网间使用路由器进行控制。
3) ECS 安全组与 RDS、ADB、ECS、SLB、Maxcompute 的 IP 黑白名单可以实现进一步的隔离与访问控制。

阿里云安全组，具备状态检测和数据包过滤功能，可用于在云端划分各个云服务器实例间的安全域。安全组是一个逻辑上的分组，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，是重要的网络安全隔离手段，适用于在云端划分网络安全域。

■ MFA

MFA（Multi-Factor Authentication）在用户名和口令之外再额外增加一层安全保护，在用户名和密码之外再额外增加一层安全保护。启用 MFA 后，用户登录阿里云控制台（云产品）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

仅供阿里云用户参考使用，请勿私自传播和宣传

备的动态验证码（第二安全要素），双因素的安全认证为账户认证提供更高的安全保护。目前阿里云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，遵循基于时间的一次性密码（TOTP）标准（RFC 6238），并支持在移动硬件设备上运行。

■ RAM

RAM（Resource Access Management，访问控制）为云服务客户提供用户身份管理与资源访问控制服务。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。

■ 日志审计服务

阿里云为云服务客户提供的日志审计服务包括操作审计（Action Trail）和日志服务（Log Service）。操作审计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 Action Trail 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。Action Trail 所记录的操作事件可以满足此类合规性审计需求。

日志服务为用户提供针对日志类数据的一站式服务，帮助用户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，建立海量日志处理能力。所有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。

■ 负载均衡

阿里云 SLB（Server Load Balancer，负载均衡）是对多台云服务器进行流量分发的负载均衡服务。SLB 可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提

仅供阿里云用户参考使用，请勿以自传播和宣传

升应用系统的可用性。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。

■ 数据备份服务

阿里云云服务器镜像文件、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%。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。

阿里云云数据库通过数据备份和日志备份的备份方式，保证数据完整可靠。同时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。

阿里云对象存储采用多可用区机制，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。对象存储的同城冗余存储（多可用区）是基于 99.9999999999%的数据可靠性设计，并且能够为用户提供 99.95%的数据可用性 SLA。

阿里云基于自研或第三方安全产品（服务）为云服务客户提供安全策略集中管理、入侵检测、恶意代码检测、流量检测、主机安全加固、数据加密和密钥管理等安全措施。

■ 云安全中心

阿里云通过云安全中心实现云服务客户安全威胁识别、分析、预警的集中安全管理，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，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。

■ 云防火墙

云防火墙实现云上虚拟环境下的统一管理互联网到业务的访问控制策略（南北向）和业务与业务之间的微隔离策略（东西向），内置的威胁入侵检测模块（IPS）支持全网流量可视和业务间访问关系可视，是用户业务上云的第一个网络安全基础设施。

■ Web 应用防火墙

仅供阿里云用户参考使用，请勿私自传播和宣传

Web 应用防火墙（Web Application Firewall）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。

- DDoS 高防

DDoS 高防支持防护全类型 DDoS 攻击，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。DDoS 高防支持通过安全报表，实时监控风险和防护情况，同时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，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。

- 加密服务

加密服务帮助云服务客户可以进行多种加密算法来进行加密运算和密钥安全管理。阿里云提供的加密服务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。

- 密钥管理服务

KMS（Key Management Service，密钥管理服务）为云服务客户提供密钥的安全托管、密码运算等基本功能，以及内置密钥轮转等安全实践。通过密钥管理服务，云服务客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云服务客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。

仅供阿里云用户参考使用，请勿私自传播和宣传

3.3 安全能力

安全能力是安全措施作用于保护对象上形成的抵抗外部攻击的一种防护能力，云服务客户安全能力主要包括云平台原生安全能力、云产品安全能力、云安全产品安全能力和云服务客户自建安全能力。

3.3.1 云平台原生安全能力

云平台原生安全能力主要针对云基础设施提供的安全保护能力，主要涉及物理环境安全、硬件安全、虚拟化安全和云平台安全管理和运营。

阿里公共云平台在物理安全、硬件安全、虚拟化安全、云平台内部身份和访问控制、云平台安全监控和运营等方面进行了全方位安全设计和建设，为云服务客户安全奠定了良好基础，详见《2019 年阿里云安全白皮书》5.1 云平台安全。

3.3.2 云产品安全能力

云产品安全能力指云平台提供的云产品（服务）为云服务客户提供的安全措施作用于保护对象后形成的安全能力，其中部分安全能力（如租户隔离）是云产品原生的，部分能力（如数据加密）是需要客户的开启和正确设置。

阿里云产品（服务）为云服务客户提供的云产品安全能力，详见附录 C。

3.3.3 云安全产品安全能力

云安全产品安全能力主要指云服务商通过自研或结合第三方安全服务商为云服务客户提供的安全措施作用于保护对象后形成的安全防护能力。

阿里云基于自研或第三方安全产品（服务）为云服务客户提供的云安全产品安全能力，详见附录 C。

3.3.4 云客户自建能力

云服务客户自建能力指云服务客户基于业务需求对云产品能力的开启和正确配置，以及云服务客户根据自身业务需求自行建设的安全能力，如业务数据保护、客户内部安全管理等。

阿里云为云服务客户提供的安全服务可帮助云服务客户完善自建能力，如业务应用系统和数据保护的安全防护能力、云产品安全合规配置、内部安全管理机制建立以及事件响应等。

仅供阿里云用户参考使用，请勿私自传播和宣传

3.4 安全合规评估

基于云服务客户构建的安全能力，结合《GB/T 22239-2019 网络安全等级保护基本要求》，分析和评估云服务客户业务系统的安全合规情况。

通过安全合规能力模型的评估，可识别当前云平台及云服务客户面临的威胁及脆弱性，同时对云平台及云服务客户系统面临的脆弱性和威胁进行分析，便于对其进行安全加固，强化安全防护措施，以提升云平台及云服务客户业务系统的安全防护能力。

4 安全合规实践指引

综合 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》及第三节安全合规能力模型，对阿里云 IaaS 模式云服务客户典型场景的业务应用系统等保 2.0 安全合规性评估，分析云服务客户业务应用系统等级保护对象、安全措施以及安全能力。

4.1 云服务客户典型场景概述

在基础设施即服务（IaaS）服务模式下，云服务客户基于云计算基础服务（网络、计算、存储、安全）搭建面向互联网应用是云服务客户最典型的场景。该场景中，云服务客户利用 VPC 实现不同云服务客户和系统间的虚拟网络隔离，基于云服务器、云数据库和云存储等基础资源进行应用建设和数据存储，通过公共云公网 IP 实现与互联网的互通，同时依靠系列安全产品和服务实现应用系统的安全防护和合规能力。

仅供阿里云用户参考使用，请勿私自传播和宣传

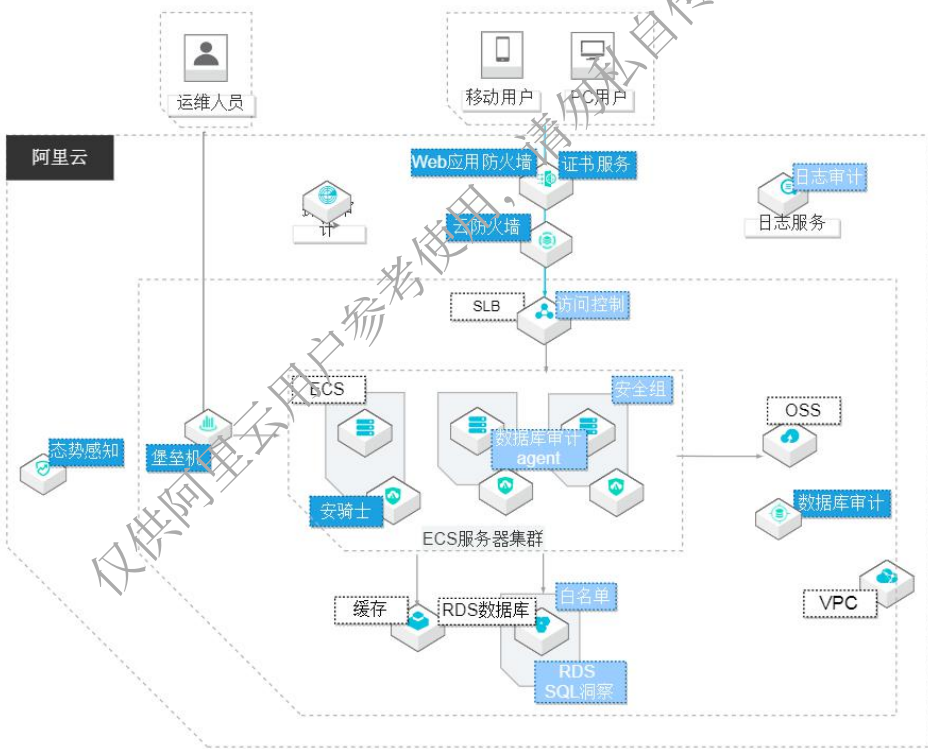

图 4.1 IaaS 模式云服务客户典型场景

4.2 等级保护对象概述

基于安全责任模型及云计算环境网络安全等级保护对象的差异，在 IaaS 服务模式下，云服务客户的安全责任主要有虚拟网络（架构、边界）安全防护、云产品安全配置、虚拟机镜像安全防护，虚拟机（操作系统、数据库、中间件）、运维终端安全防护以及云服务

客户业务应用系统和数据安全性。

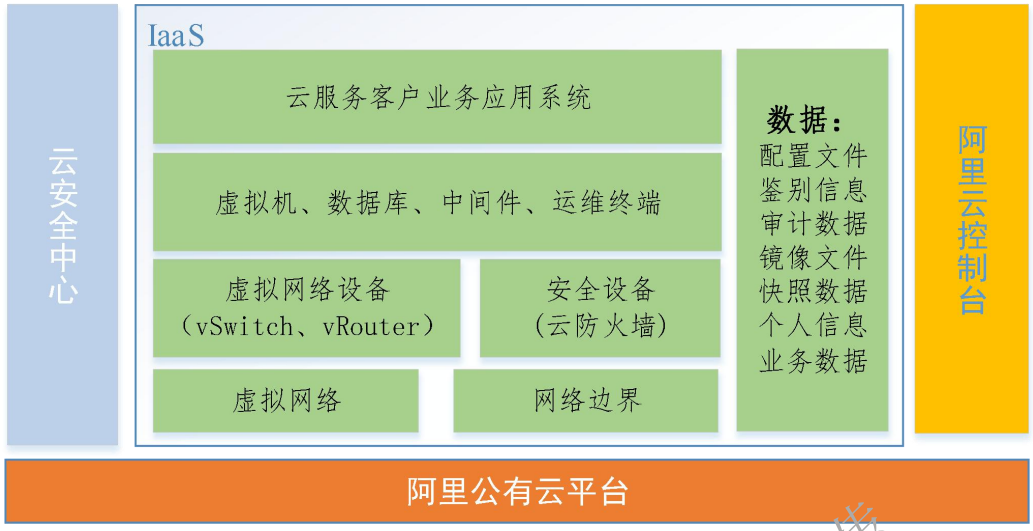

图 4.2 IaaS 模式下云服务客户等级保护对象

基于图 4.1 IaaS 模式云服务客户典型合规场景下，阿里公共云云服务客户在开展等级保护安全能力建设过程中安全保护对象涉及：

- 网络部分：虚拟网络 VPC、虚拟网络边界、网络设备（vSwitch、vRouter）
- 安全设备：云安全中心、云防火墙、Web 应用防火墙、DDoS 高防、堡垒机、数据库审计等
- 服务器/存储：虚拟机（操作系统、数据库/数据库实例）
- 终端：云服务客户运维终端
- 应用系统：云服务客户业务应用系统、阿里云控制台、云产品安全配置
- 重要数据：业务数据、鉴别数据、配置信息、审计数据、个人信息等
- 安全管理：包含运营单位主体的安全管理机制情况
- 物理机房：由云服务商统一负责，云服务客户无需对物理机房进行安全保护

4.3 引用云平台等级保护结论

按照网络安全等级保护相关要求，云服务客户在开展等级保护测评工作时，涉及阿里公共云平台等级测评报告部分内容，请访问阿里云工单系统申请阿里云最新云平台等级测评报告涉及到的以下内容：

（1） 网络安全等级测评基本信息表（云平台等级测评报告）

仅供阿里云用户参考使用，请勿私自传播和宣传

（2） 云平台等级测评结论扩展表（云计算安全）；

（3） 云平台总体评价；

（4） 云平台主要安全问题及整改建议；

（5） 云服务商针对这些主要安全问题的整改情况的详细说明。

云服务客户业务应用系统的安全保护能力依赖于云计算平台提供的安全服务。因此，**云服务客户应优先选择对应服务模式下的等级测评结论为“优”的云计算平台，为云服务客户业务应用系统等级测评结论为优奠定坚实技术基础。**

4.4 基本要求合规分析（通用要求）

基于附录 B 给出的不同模式下云服务客户等级保护适用条款内容以及 3.4 安全合规能力模型，本白皮书针对基本要求逐条进行安全合规性分析。

4.4.1 安全通信网络

（1） 网络架构

a）应保证网络设备的业务处理能力满足业务高峰期需要；

安全措施：负载均衡、性能监控

保护对象：虚拟网络设备、网络全局

安全能力：

■ 云产品安全能力

VPC 支持云服务客户构建虚拟网络，每个 VPC 由一个私网网段、一个路由器和至少一个交换机组成，VPC 控制台支持查询当前资源配额使用情况，若某个资源的剩余配额不满足业务需求，可以直接申请增加配额。

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。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户通过 VPC 控制台，定期查看当前资源配额使用情况。

合规性情况：符合

b）应保证网络各个部分的带宽满足业务高峰期需要；

仅供阿里云用户参考使用，请勿私自传播和宣传

安全措施：带宽监控

保护对象：网络全局

安全能力：

■ 云产品安全能力

云服务客户根据业务实际情况在创建实例是申请**带宽**，**云监控**支持监控弹性公网 IP 的流出流量、流入流量、流出数据包数、流入数据包数等监控项，帮助用户了解带宽使用情况。

■ 云安全产品能力

DDoS 原生防护采用 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，通过一个 IP 实现不同运营商访问，各线路按最优策略调度，高可用性有保障。

■ 云客户安全能力

——

合规性情况：符合

c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

安全措施：网络隔离、安全域划分

保护对象：网络全局

安全能力：

■ 云产品安全能力

VPC 支持云服务客户构建虚拟网络，支持自定义 IP 地址范围、网段、路由表和网关等，并根据业务需求自定义不同的安全域。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于业务需求划分不同的安全域，配置 IP 地址范围、配置路由表和网关等。

合规性情况：符合

d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

安全措施：网络隔离、访问控制

保护对象：网络全局

仅供阿里云用户参考使用，请勿私自传播和宣传

安全能力：

■ 云产品安全能力

不同 **VPC** 虚拟网络间完全隔离，云服务客户根据业务需求通过对外映射弹性公网 IP 和 NAT IP 进行互连。

同一 **VPC** 内基于网络 ACL 和安全组进行区域间的访问控制。

■ 云安全产品能力

云防火墙实现 VPC 间流量控制及主机间微隔离。

■ 云客户安全能力

云服务客户配置 ACL 访问控制策略。

合规性情况：符合

e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。

安全措施：网络设备冗余、链路冗余

保护对象：网络全局

安全能力：

■ 云产品安全能力

VPC 组件交换机是分布式的结点，网关和控制器都集群部署并且多机房互备，所有链路上冗余容灾。

负载均衡采用全冗余设计，无单点，支持同城容灾和跨地域容灾，可用性高达 99.95%，支持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。

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：符合

（2） 通信传输

a）应采用密码技术保证通信过程中数据的完整性；

安全措施：传输加密

保护对象：业务应用数据

安全能力：

仅供阿里云用户参考使用，请勿私自传播和宣传

■ 云产品安全能力

云服务客户通过 IPSEC VPN 远程访问，使业务数据可以在公网上通过 IP 加密信道进行传输，云服务客户访问使用 SSL VPN，保障通信链路中数据的保密性。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户设置 TLS，保障互联网通信的安全性和数据完整性。

合规性情况：符合

b）应采用密码技术保证通信过程中数据的保密性。

安全措施：传输加密

保护对象：业务应用数据

安全能力：

■ 云产品安全能力

云服务客户通过 IPSEC VPN 远程访问，使业务数据可以在公网上通过 IP 加密信道进行传输，云服务客户访问使用 SSL VPN，保障通信链路中数据的保密性。

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

（3） 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

安全措施：TPM 可信根

保护对象：网络设备

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：因该指标只要求“可”，不是强制要求项。

4.4.2 安全区域边界

（1） 边界防护

a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

不同 **VPC** 之间内部网络完全隔离，只能通过对外映射的 IP（弹性公网 IP 和 NAT IP）互连。

安全组用于在云端划分网络安全域，支持通过安全组规则授权两个安全组间的互访。

■ 云安全产品能力

云防火墙对 VPC 间的访问流量进行检测和控制。

■ 云客户安全能力

云服务客户配置 ACL 访问控制策略，访问控制粒度为端口级。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

b）应能够对非授权设备私自联到内部网络的行为进行限制或检查；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

安全组通过入口方向访问控制策略配置，限制云服务器非法内联。

■ 云安全产品能力

云防火墙支持云服务器从内对外访问控制策略配置。

■ 云客户安全能力

云服务客户部署第三方网络接入控制系统，限制运维终端等设备非法接入到内部网

络。

合规性情况：符合

c）应能够对内部用户非授权联到外部网络的行为进行限制或检查；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

安全组通过出口方向访问控制策略配置，限制云服务器非法外联，允许或禁止云服务器实例对公网或私网的访问。

■ 云安全产品能力

云防火墙支持云服务客户根据业务需求配置外对内访问控制策略。

云防火墙支持对云服务客户南北向和东西向访问的网络流量分析，支持全网流量可视化，支持对主动外联行为的分析和阻断，配置开通、变更白名单策略。

云安全中心支持对云服务客户非授权联到外部恶意域名、IP 地址的行为进行检查和拦截。

■ 云客户安全能力

云服务客户根据云下资产对象，独立部署第三方网络接入控制系统。

合规性情况：符合

d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络；

安全措施：安全准入

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户根据云下无线网络环境，部署第三方网络接入控制系统，配置禁用无线网卡的策略，无线网络的使用按照客户需求和具体应用场景而定。

合规性情况：——（视云服务客户云下环境而定）

仅供阿里云用户参考使用，请勿私自传播和宣传

（2） 访问控制

a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

安全组支持云服务客户通过安全组规则授权不同安全组间通信。

■ 云安全产品能力

云防火墙支持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，访问控制粒度可达端口级。

■ 云客户安全能力

云服务客户配置 ACL 访问控制策略，访问控制粒度为端口级。

合规性情况：符合

b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

安全组访问控制规则支持优先级设置，以及修改、克隆、删除，可实现云服务客户访问控制规则数最优。

■ 云安全产品能力

云防火墙支持策略命中计数功能，确保没有无效的冗余策略，**云防火墙**访问控制策略可配置优先级，优化访问控制列表。

■ 云客户安全能力

云服务客户根据业务需求优化访问控制列表。

合规性情况：符合

c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进

仅供阿里云用户参考使用，请勿私自传播和宣传

出；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

安全组规则属性包括网络类型、网卡类型、规则方向、授权策略、协议类型、端口范围、优先级、授权类型、授权对象。

■ 云安全产品能力

云防火墙支持对进出访问控制策略进行严格设置，访问控制策略包括源类型、访问源、目的类型、目的、协议类型、目的端口、应用协议、动作、描述和优先级。

■ 云客户安全能力

云服务客户根据业务需求配置恰当的访问控制策略表。

合规性情况：符合

d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云防火墙支持根据会话状态信息为数据流提供的访问控制能力。

■ 云客户安全能力

——

合规性情况：符合

e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

——

仅供阿里云用户参考使用，请勿私自传播和宣传

■ 云安全产品能力

云防火墙支持跨 VPC 数据流的应用协议、内容的访问控制。

WEB 应用防火墙支持应用级协议和内容访问控制。

DDoS 高防通过引流的方式对所有业务流量进行清洗，支持网络四层和七层防护。

■ 云客户安全能力

——

合规性情况：符合

（3） 入侵防范

a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

安全措施：入侵检测

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

阿里云基础防护支持实时地检测出各种攻击和异常行为，发现内部被控制的云服务器，对常见的 Web 应用攻击进行网络层拦截旁路阻断，并与其他安全防护模块联动防护。

■ 云安全产品能力

云安全中心通过大数据威胁检测、人工智能和病毒查杀引擎对网络流量和主机中的入侵行为和文件样本进行实时检测和防御。

云防火墙通过威胁检测引擎，对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截。

Web 应用防火墙支持将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器。

DDoS 高防支持抵御各类基于网络层、传输层及应用层的 DDoS 攻击，秒级启动流量清洗，过滤掉攻击流量支持全自动检测和攻击策略匹配，实时防护，清洗服务可用性 99.95%，可定制 99.99%。

■ 云客户安全能力

——

合规性情况：符合

b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

安全措施：入侵检测

仅供阿里云用户参考使用，请勿私自传播和宣传

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

阿里云基础防护对云内部的恶意主机对外发起的攻击行为进行检测，及时发现内部已经被控制的云服务器。

■ 云安全产品能力

云安全中心支持检测针对主机系统层和应用层的主动外联和恶意攻击行为，对进程、网络异常行为进行预警。

云防火墙能够检测东西向流量，配置相应的安全策略，阻断防止从内部发起的网络攻击行为。

■ 云客户安全能力

——

合规性情况：符合

c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

安全措施：入侵检测

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云安全中心基于主机、网络、云平台的安全数据进行分析，实现挖矿、勒索、蠕虫、DDoS 木马等基于新型网络攻击的攻击预警。

云防火墙对云上进出网络的恶意流量进行实时检测与阻断，支持防御挖矿蠕虫等新型网络攻击，并通过积累大量恶意攻击样本，形成精准防御规则；云防火墙入侵检测功能支持发现挖矿蠕虫感染事件。

■ 云客户安全能力

——

合规性情况：符合

d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重

仅供阿里云用户参考使用，请勿私自传播和宣传

入侵事件时应提供报警。

安全措施：入侵检测

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云安全中心支持检测到威胁时，记录事件账号/源地址、攻击类型、攻击时间、事件级别以及处置建议，同时支持自动化攻击溯源，展示攻击过程。

云防火墙支持检测到攻击行为时，提供网络阻断功能，记录风险级别、事件名称、防御状态、源 IP、目的 IP、方向、判断来源、发生时间和动作。

Web 应用防火墙支持 HTTP 和 HTTPS 流量攻击，记录攻击事件类型、攻击 URL、来源 IP、目的 Host、时间、Get 请求内容和拦截动作。

DDoS 高防检测到 DDoS 攻击时，记录攻击类型、攻击目标、攻击时间、攻击流量峰值和清洗防护结果。

■ 云客户安全能力

——

合规性情况：符合

（4） 恶意代码和垃圾邮件防范

a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

安全措施：入侵检测、恶意代码检测

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

阿里云基础防护支持对互联网出口的恶意代码检测和清除，恶意代码规则库定期更新。

■ 云安全产品能力

云安全中心支持蠕虫病毒、勒索病毒、木马、网站后门等恶意代码的检测和隔离清除，定期升级相关恶意代码规则库。

云防火墙支持通过入侵防护和集成威胁情报支持防恶意代码，若传输样本的 MD5 的

仅供阿里云用户参考使用，请勿私自传播和宣传

特征值匹配到威胁情报，则阻断该报文。

Web 应用防火墙流量恶意代码检测提供恶意代码检测功能，恶意代码规则库定期更新。

■ 云客户安全能力

——

合规性情况：符合

b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

安全措施：入侵检测、恶意代码检测

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

阿里云邮箱支持垃圾邮件检测功能。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户其他邮件服务器自身要求具备发垃圾邮件功能或部署第三方邮件防护系统。

合规性情况：——

（5） 安全审计

a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

安全措施：安全审计

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

操作审计（Action Trail）支持记录云账号对资源的操作日志，提供操作日志的查询和下载。

■ 云安全产品能力

云安全中心通过支持主机登录日志、进程启动、网络连接、端口快照、账户快照、暴

仅供阿里云用户参考使用，请勿私自传播和宣传

力破解、网络会话、DNS 解析、WEB 会话、安全告警、漏洞和基线日志进行审计。

云防火墙支持通过日志审计模块记录所有流量日志、事件日志和操作日志。

Web 应用防火墙对攻击日志支持日志实时查询分析。

堡垒机支持对云端虚拟主机 ECS 资产进行运维权限管控及运维审计。

数据库审计支持对云上数据库访问行为进行监控，分析危险操作及可疑行为。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

安全措施：安全审计

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

操作审计（Action Trail）记录云账号用户云上操作日志，包括事件、用户名、事件名称、资源类型、资源名称和错误码。

■ 云安全产品能力

云安全中心检测到威胁时，记录事件账号/源地址、攻击类型、攻击时间、事件级别以及处置建议。

云防火墙支持日志记录事件被扫描到的时间、威胁类型、出/入方向、源 IP 和目的 IP、应用类型、严重性等级以及动作状态信息；流量日志记录访问流量开始和结束的时间、出/入方向、源 IP 和目的 IP、应用类型、源端口、应用、支持的协议、动作状态、字节数以及报文数等信息；操作日志记录云防火墙中的所有操作执行的时间、操作类型、严重性以及具体操作信息。

Web 应用防火墙记录攻击事件类型、攻击 URL、来源 IP、目的 Host、时间、Get 请求内容和拦截动作。

DDoS 高防检测到 DDoS 攻击时，记录攻击类型、攻击目标、攻击时间、攻击流量峰值和清洗防护结果。

堡垒机日志记录包括重要性、时间、日志类型、日志内容、用户、源 IP 地址和结果。

■ 云客户安全能力

——

仅供阿里云用户参考使用，请勿私自传播和宣传

合规性情况：符合

c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

安全措施：安全审计

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

操作审计（Action Trail）默认支持在线查询 90 天的操作日志，支持将操作日志保存在云服务客户指定的对象存储空间或日志服务中，自定义更长久的保存。保存的操作记录可以用作追踪资源变更行为和行为风险分析。

■ 云安全产品能力

云安全中心、云防火墙、Web 应用防火墙、DDoS 高防、堡垒机和数据库审计等安全产品支持日志分析功能，依托日志服务产品，可存储 6 个月内的日志数据提供实时日志分析能力。

■ 云客户安全能力

——

合规性情况：符合

d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

安全措施：安全审计

保护对象：虚拟网络边界

安全能力：

■ 云产品安全能力

日志服务支持云服务客户操作审计进行单独审计，且提供审计数据分析能力。

■ 云安全产品能力

云安全中心支持云服务客户所有资产安全事件的综合分析。

■ 云客户安全能力

云服务客户根据云下环境配置行为审计安全配置。

合规性情况：符合

（6） 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用

仅供阿里云用户参考使用，请勿私自传播和宣传

程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

安全措施：TPM 可信根

保护对象：边界设备

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：因该指标只要求“可”，不是强制要求项。

4.4.3 安全计算环境

（1） 身份鉴别

a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

安全措施：安全加固、账号认证

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

阿里云控制台支持云服务客户设定口令 8-32 位，数字、大小写字母、特殊符号组成，允许自行配置 MFA、口令有效期。

云服务客户创建**云服务器**实例时，支持云服务客户选择不同登录凭证认证方式，支持 SSH 密钥对、自定义密码，创建后设置自定义口令，需 8-30 位必须包含大写字母、小写字母、数字及特殊符号中的三种。

云服务客户选择的**安全加固镜像**支持云服务客户在创建实例时，镜像云服务客户口令基于安全基线前口令策略进行配置，口令 8 位以上，限制最长使用期限。

云服务客户创建**云数据库**实例时，支持云服务客户分配账号和口令，账号由大小写字

仅供阿里云用户参考使用，请勿私自传播和宣传

母、数字、下划线组成，且字母开头，字母或数字结尾，最低 16 个字符，口令大小写字母、特殊符号中的三种，长度 8-32 位。

■ 云安全产品能力

堡垒机口令策略支持 8 个字符以上，必须包含大写字母、小写字母、数字及特殊符号，用户身份有唯一标识，口令 90 天定期跟换，新用户强制更改口令。

云安全中心支持对云服务客户登录的配置和密码复杂度进行定期安全检查，并提供安全建议并进行预警。

■ 云客户安全能力

云服务客户业务应用系统安全配置。

合规性情况：符合

b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

安全措施：安全加固

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

阿里云控制台支持设置登录失败处理策略，可设置最大登录失败 5 次，失败后锁定 15 分钟，会话超时会自动中断。

云服务客户选择的**安全加固镜**像对云服务客户进行安全策略配置，配置登录失败处理功能，并支持连接超时自动退出。

数据库实例支持设置连接超时和连接失败次数配置。

■ 云安全产品能力

堡垒机支持登录失败处理功能配置，建议配置云服务客户最大登录失败 5 次，临时锁定 30 分钟，登录连接超时时间为 30 分钟。

云安全中心支持登录失败防御配置，支持云服务客户配置最大登录失败 10 次数，临时阻断连接 1 天、3 天和 7 天。

■ 云客户安全能力

云服务客户业务应用系统安全配置。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

c）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

安全措施：传输加密

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

云服务客户控制台访问均通过 Https 加密协议来保证数据传输的安全。

云产品支持对外提供加密 Https 的 Endpoint API 调用，云产品访问采用加密协议。

■ 云安全产品能力

堡垒机远程连接至云服务器时，采用安全的 SSH 方式进行远程登录。

云安全中心支持对远程管理的配置进行检查，防止不安全的配置导致传输被窃听。

■ 云客户安全能力

云服务客户侧业务应用系统安全配置；

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

安全措施：双因素认证

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

阿里云控制台账户支持**虚拟 MFA**，支持主账号开启 MFA 安全检查，在登录云服务客户控制台时需通过用户名、口令可由虚拟 MFA 应用程序生成的动态安全码进行双因素认证，如使用用户名、口令和 Google Authenticator 等双因素认证登录到 RAM 控制台。

■ 云安全产品能力

堡垒机支持作为唯一入口管理服务器，支持包括虚拟 MFA、短信验证码在内的多因子认证。

云安全中心支持对云平台配置提供基线核查，能够实时发现主账号双因素认证风险。

■ 云客户安全能力

云服务客户业务应用系统安全配置。

仅供阿里云用户参考使用，请勿私自传播和售卖

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

（2） 访问控制

a）应对登录的用户分配账户和权限；

安全措施：授权

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

RAM 支持云产品接入，支持云服务客户通过开启 RAM 功能来完成授予 RAM 子云服务客户访问权限，权限的控制粒度可以细化到 API 级别。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户侧业务应用系统安全配置。

云服务客户需基于 RAM 对云服务客户进行合理授权。

合规性情况：符合

b）应重命名或删除默认账户，修改默认账户的默认口令；

安全措施：安全加固

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

默认账户限制远程登录，Root 用户未删除，但具有强口令。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户侧根据自身安全基线重命名或删除多余过期账户，或增强其口令。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和查阅

c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；

安全措施：安全加固

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

RAM 支持云服务客户对账户进行账户创建、删除和修改自行管理。

■ 云安全产品能力

堡垒机支持云服务客户对无用、多余账户会锁定或删除管理。

云安全中心支持对平台账户进行安全配置检查。

■ 云客户安全能力

云服务客户侧定期梳理账户状态，及时清除多余、过期的账户。

合规性情况：符合

d）应授予管理用户所需的最小权限，实现管理用户的权限分离；

安全措施：授权

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

RAM 支持子账号对云产品使用最小权限设置。

■ 云安全产品能力

堡垒机支持基于用户角色分配权限，实现三权分立，角色分为超级管理员、审计员和运维员。

云安全中心支持对账户权限配置的安全检查，实现针对云服务客户权限分离的检查。

■ 云客户安全能力

云服务客户基于 RAM 授予管理云服务客户所需的最小权限，针对虚拟机基于三权分立的原则对管理云服务客户进行授权。

合规性情况：符合

e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

安全措施：授权

仅供阿里云用户参考使用，请勿私自传播和宣传

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

RAM 支持创建 RAM 子云服务客户并授予特定权限策略从账户权限上实现对云产品资源细粒度访问，如网络层面访问控制策略、安全组规则、开发与用户权限分离策略。

■ 云安全产品能力

云安全中心支持对 RAM 用户提供高危风险配置的安全检查。

■ 云客户安全能力

云服务客户基于云产品配置指南和业务应用系统需求合理配置。

合规性情况：符合

f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

安全措施：授权

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

RAM 支持基于用户角色权限分配，授权主体为用户级，客体为云服务级别、操作级别和资源级别，云资源细粒度分配由云服务客户自行配置。

阿里云控制台支持主账号对子账号授权，可以控制到资源、接口和操作权限。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于云产品配置指南和业务应用系统需求合理配置。

合规性情况：符合

g）应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。

安全措施：安全标记

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

仅供阿里云用户参考使用，请勿私自传播和宣传

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：因现使用的操作系统安全级别无法达到 B 类强制保护级，操作系统侧自身暂无法实现强制访问控制。

（3） 安全审计

a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

安全措施：安全审计

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

操作审计（Action Trail）支持记录云账号对资源的操作日志，提供操作日志的查询和下载。

云服务客户使用**安全加固公共镜像**，Linux 类操作系统开启 auditd 审计进程和 rsyslog 日志进程，Windows 系统开启本地审核策略。

■ 云安全产品能力

堡垒机支持对所有云服务客户的虚拟主机操作进行审计，系统自身日志本地保存。

数据库审计支持对数据库风险操作行为进行记录，提供细粒度审计数据库访问行为。

云安全中心支持对账户 9 登录进行记录，提供细粒度审计登录时间、登录账户、登录结果的记录，并通过报表进行实时监控预警。

■ 云客户安全能力

云服务客户基于云产品配置指南和业务应用系统需求合理配置。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

b）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

安全措施：安全审计

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

操作审计（Action Trail）记录云账号用户云上操作日志，包括事件、用户名、事件名称、资源类型、资源名称和错误码。

■ 云安全产品能力

堡垒机日志记录包括重要性、时间、日志类型、日志内容、用户、源 IP 地址和结果。

数据库审计提供多维度线索分析，包括会话行为、SQL 行为、风险行为和政策性报表。

云安全中心日志记录包括主机登录日志、进程启动、网络连接、账户快照、端口快照、DNS、Web 访问、网站会话、云平台操作等日志结果。

■ 云客户安全能力

云服务客户基于云产品配置指南和业务应用系统需求合理配置。

合规性情况：符合

c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

安全措施：安全审计、数据备份、访问控制

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

操作审计（Action Trail）默认支持在线查询 90 天的操作日志，支持将操作日志保存在云服务客户指定的对象存储空间或日志服务中，自定义更长久的保存。保存的操作记录可以用作追踪资源变更行为和行为风险分析。

■ 云安全产品能力

堡垒机、数据库审计日志实时推送至日志服务，审计记录可按需调整存储空间，支持 6 个月以上保存期。

云安全中心支持日志记录保存期为 6 个月，同时支持对操作审计日志配置进行基线核查。

■ 云客户安全能力

仅供阿里云用户参考使用，请勿私自传播和售卖

云服务客户需在审计产品中进行安全配置。

合规性情况：符合

d）应对审计进程进行保护，防止未经授权的中断。

安全措施：安全审计、授权

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

阿里云控制台通过**操作审计（Action Trail）**记录云账号用户操作日志并基于日志审计，通过配置审计（Cloud Config）监控操作审计的有效运行状态，防止操作审计被误关闭。

■ 云安全产品能力

堡垒机、数据库审计支持日志实时推送至日志服务。

云安全中心对操作审计日志配置进行基线核查。

■ 云客户安全能力

云服务客户根据业务需求进行审计策略配置和审计监控告警设置。

合规性情况：符合

（4） 入侵防范

a）应遵循最小安装的原则，仅安装需要的组件和应用程序；

安全措施：安全加固

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统

安全能力：

■ 云产品安全能力

阿里云镜像上线前均经过内部安全审核，并提供安全加固公共镜像，遵循最小化安装原则。

■ 云安全产品能力

云安全中心客户端在上线前，均经过内部的安全审核，并进行安全加固，遵循最小化安装原则。

■ 云客户安全能力

仅供阿里云用户参考使用，请勿私自传播和宣传

云服务客户在使用过程中，仅安装需要的组件和应用程序。

合规性情况：符合

b）应关闭不需要的系统服务、默认共享和高危端口；

安全措施：安全加固

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

阿里云镜像上线前均经过内部安全审核，并提供安全加固公共镜像，删减不需要第三方组件和服务，关闭默认共享和高危端口。

云服务器实例通过安全组配置仅开启必要的端口。

■ 云安全产品能力

云安全中心支持对主机、SLB、RDS、OSS 等云产品进行高危配置、端口的基线检查。

■ 云客户安全能力

云服务客户基于自身业务需求，关闭不必要的服务、默认共享及高危端口。

合规性情况：符合

c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

安全措施：访问控制

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）

安全能力：

■ 云产品安全能力

VPC 虚拟网络隔离技术和 **RAM** 账户策略可以对访问终端方式进行限制。

安全组支持云服务客户配置安全组规则，限制虚拟机的访问策略，包括端口、协议和 IP 地址等。

■ 云安全产品能力

云安全中心支持联动云平台 IP 白名单、安全组的能力，对网络 IP、端口、协议进行管理和限制。

■ 云客户安全能力

云服务客户根据业务需求配置相应的安全组规则。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

安全措施：安全审计

保护对象：业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

阿里云控制台和产品在上线前均已经过内部开发流程，支持对输入数据的有效性进行验证，过滤特殊字符。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户需对业务系统对输入数据的有效性进行验证，过滤特殊字符。

合规性情况：符合

e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

安全措施：漏洞扫描

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云安全中心漏洞修复组件支持 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞和应急漏洞的一键修复功能，支持安全基线检测策略，支持平台安全配置等检查，能够实时检测已知漏洞。

漏洞扫描支持资产威胁检测，发现云服务客户业务系统关联资产，实现自动化漏洞渗透测试和敏感内容监测。

渗透测试服务支持通过模拟黑客对云服务客户业务系统进行安全测试，发现安全缺陷和漏洞，并提出修复建议。

■ 云客户安全能力

云服务客户侧根据业务需求制定恰当的漏洞扫描策略，及时发现漏洞并进行修复。

仅供阿里云用户参考使用，请勿私自传播和宣传

合规性情况：符合

f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

安全措施：入侵检测

保护对象：虚拟网络设备、安全设备、虚拟机（操作系统、数据库、中间件）、业务应用系统、阿里云控制台

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云安全中心能够检测到对重要节点入侵行为并进行告警，主要包括异常登录检测、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。

Web 应用防火墙支持将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器。

■ 云客户安全能力

——

合规性情况：符合

（5） 恶意代码防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

安全措施：恶意代码检测

保护对象：虚拟机

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云安全中心通过安全加固镜像部署代理，支持对恶意的代码实时拦截功能，在系统内核层面，识别恶意代码，并进行主动拦截。

■ 云客户安全能力

云服务客户对于自定义镜像或云下服务器部署第三方防恶意代码产品，对恶意代码进

仅供阿里云用户参考使用，请勿私自传播和售卖

行检测和查杀。

合规性情况：符合

（6） 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

安全措施：TPM 可信根

保护对象：虚拟机

安全能力：

■ 云产品安全能力

基于可信技术的云服务器正在部分区域试点，即将全面推出。

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：因该指标只要求“可”，不是强制要求项。

（7） 数据完整性

a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

安全措施：传输加密

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

阿里云支持云服务客户基于 Https 的 API 访问点，允许云服务客户使用 Access Key 以程序形式来调用 API。

阿里云支持标准 TLS 协议，支持提供 256 位密钥加密强度。

■ 云安全产品能力

——

■ 云客户安全能力

仅供阿里云用户参考使用，请勿私自传播和宣传

云服务客户在使用云产品支持常用产品开启加密链路功能。

合规性情况：符合

b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

安全措施：数据完整性校验

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

云存储产品支持自带完整性校验功能，OSS 通过上传 object 返回 CRC64 值，支持云服务客户在客户端与本地计算的 CRC64 值做对比，从而完成数据完整性验证，并支持在数据存储时进行校验码验证，实现数据进行细粒度的完整性校验保护。

■ 云安全产品能力

密钥管理服务 KMS 支持云服务客户自主密钥管理，支持云产品接入 KMS 实现密钥管理，并对敏感资源和信息进行加密存储，实现云服务客户管理自己密钥并实现数据加解密过程。

■ 云客户安全能力

云服务客户在使用阿里云产品时，启用各云产品自带的完整性校验功能。

合规性情况：符合

（8） 数据保密性

a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

安全措施：传输加密

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

阿里云支持云服务客户基于 Https 的 API 访问点，允许云服务客户使用 Access Key 以程序形式来调用 API。

■ 云安全产品能力

密钥管理服务 KMS 支持云服务客户自主密钥管理，支持云产品接入 KMS 实现密钥

仅供阿里云用户参考使用，请勿转自传播和复制

管理，并对敏感资源和信息进行加密存储，实现云服务客户管理自己密钥并实现数据加解密过程。

证书服务支持云上签发第三方 CA 证书颁发机构的 SSL 证书，实现 Https。

■ 云客户安全能力

云服务客户在使用阿里云产品时，如 SLB、CDN、OSS、RDS 等常用产品时开启加密链路功能。

合规性情况：符合

b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

安全措施：存储加密

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

阿里云计算、数据库、存储等产品支持存储加密。

■ 云安全产品能力

密钥管理服务 KMS 支持密钥管理，支持提供 256 位密钥加密存储，满足加密存储需求。

■ 云客户安全能力

云服务客户需选择、配置恰当的存储加密方式。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

（9） 数据备份恢复

a）应提供重要数据的本地数据备份与恢复功能；

安全措施：数据备份

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

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%。

云数据库通过数据备份和日志备份的备份方式，保证数据完整可靠。同时云服务客户

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。

对象存储采用多可用区机制，将云服务客户的数据分散存放在同一地域（Region）的 3 个可用区。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户需对重要的数据进行本地备份。

合规性情况：符合

b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

安全措施：数据备份

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

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%。

云数据库通过数据备份和日志备份的备份方式，支持设置指定数据备份云数据库。

对象存储采用多可用区机制，将云服务客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。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户根据自身重要数据和业务数据配置恰当备份策略，实现实时备份。

合规性情况：符合

c）应提供重要数据处理系统的热冗余，保证系统的高可用性；

安全措施：数据备份

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

云产品基于飞天分布式操作系统高可用架构，存储产品支持高可用性，支持用于基于

仅供阿里云用户参考使用，请勿私自传播和售卖

业务处理能力，按照需求动态调整资源，保证系统高可用。

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：符合

（10） 剩余信息保护

a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

安全措施：残留数据清除

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

阿里云对存储过云服务客户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖，对于重用或报废的物理设备，对存储介质进行覆写、消磁或折弯等数据清除处理。

■ 云安全产品能力

——

■ 云客户安全能力

——

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

安全措施：残留数据清除

保护对象：业务数据、配置数据、鉴别信息、存储数据、审计数据、个人信息等

安全能力：

■ 云产品安全能力

阿里云支持不同云服务客户内存和持久化存储空间相对独立，当资源释放时，云服务客户空间会被释放和清除。

■ 云安全产品能力

物理硬盘报废时使用随机数据多次写入进行数据写入和清除。

■ 云客户安全能力

——

合规性情况：符合

（11） 个人信息保护

a）应仅采集和保存业务必需的用户个人信息；

安全措施：隐私声明

保护对象：个人信息

安全能力：

■ 云产品安全能力

阿里云发布用户隐私政策声明，按照最小化原则采集和保存用户个人信息。

■ 云安全产品能力

敏感数据保护支持对个人信息进行发现、分类和保护。

■ 云客户安全能力

云服务客户根据部署的应用系统功能建设相应的个人信息清除机制。

合规性情况：——

b）应禁止未授权访问和非法使用用户个人信息。

安全措施：隐私声明

保护对象：个人信息

安全能力：

■ 云产品安全能力

阿里云发布用户隐私政策声明，按照最小化原则采集和保存用户个人信息，禁止未授权访问和非法、使用用户个人信息。

■ 云安全产品能力

——

■ 云客户安全能力

由云服务客户根据部署的应用系统功能建设相应的个人信息保护机制。

合规性情况：——

4.4.4 安全管理中心

仅供阿里云用户参考使用，请勿私自传播和售卖

（1） 系统管理

a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

安全措施：账号认证、授权、安全审计

保护对象：全局

安全能力：

■ 云产品安全能力

阿里云支持账号管理，支持基于 **RAM** 授权系统管理员通过阿里云控制台进行系统管理，通过**操作审计（Action Trail）**记录管理员的操作日志。

■ 云安全产品能力

堡垒机依赖云账号管理，支持对系统管理员身份鉴别并对其操作进行审计。

■ 云客户安全能力

云服务客户基于用户角色进行配置，实现用户三权分立。

合规性情况：符合

b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

安全措施：授权

保护对象：全局

安全能力：

■ 云产品安全能力

基于 **RAM** 授权系统管理员通过阿里云控制台对系统资源和运行进行配置，通过**配置审计（Cloud Config）**记录资源配置历史，并可基于资源配置数据完成合规性检测。

■ 云安全产品能力

——。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置系统资源。

合规性情况：符合

（2） 审计管理

a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

仅供阿里云用户参考使用，请勿私自传播和宣传

安全措施：账号认证、授权、安全审计

保护对象：全局

安全能力：

■ 云产品安全能力

阿里云支持账号管理，支持基于 **RAM** 授权审计管理员进行安全审计，使用**操作审计（Action Trail）**记录管理的操作日志。

■ 云安全产品能力

堡垒机依赖云账号管理，支持对审计管理员身份鉴别并对其操作进行审计。

■ 云客户安全能力

云服务客户基于用户角色进行配置，实现用户三权分立。

合规性情况：符合

b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

安全措施：审计分析

保护对象：全局

安全能力：

■ 云产品安全能力

操作审计（Action Trail）支持短期审计记录和依托日志服务长期进行存储，支持操作时段、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，对审计记录进行分析和管理。

■ 云安全产品能力

堡垒机依赖云账号管理，支持对审计记录进行查询、分析和管理，审计记录支持转存到日志服务中。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

（3） 安全管理

a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

仅供阿里云用户参考使用，请勿私自传播和宣传

安全措施：账号认证、授权、安全审计

保护对象：全局

安全能力：

■ 云产品安全能力

阿里云支持账号管理，支持基于 **RAM** 授权安全管理员进行安全管理，通过**操作审计（Action Trail**）记录安全管理的操作日志。

■ 云安全产品能力

安全管理员基于安全控制台通过安全产品对云资源进行安全管理操作。

■ 云客户安全能力

云服务客户侧基于用户角色，实现用户三权分立。

合规性情况：符合

b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

安全措施：授权

保护对象：全局

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

安全管理员基于业务需求可对云产品和云安全产品的资源主体、客体进行统一安全配置。

安全管理员可通过**云安全中心**进行基线核查、安全策略、访问控制策略统一配置。

■ 云客户安全能力

云服务客户侧基于用户角色，实现用户三权分立。

合规性情况：符合

（4） 集中管控

a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

安全措施：安全域划分

保护对象：全局

安全能力：

■ 云产品安全能力

仅供阿里云用户参考使用，请勿私自传播和宣传

通过云服务客户独立 **VPC**，建立独立安全管理区，基于 **RAM** 授权安全管理员对安全设备或安全组件进行管理和控制。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户制定安全策略，划分特定的管理区域。

合规性情况：符合

b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

安全措施：带外管理，加密传输

保护对象：全局

安全能力：

■ 云产品安全能力

阿里云支持全链路通信进行 SSL/TLS 安全加密处理，通过 Https 进行管理。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

安全措施：安全监测

保护对象：全局

安全能力：

■ 云产品安全能力

云监控支持针对负载均衡、弹性 IP 地址、DDoS 高防、云服务器等运行状态创建监测规则，并进行集中监测和报警。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和宣传

d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

安全措施：安全审计

保护对象：全局

安全能力：

■ 云产品安全能力

操作审计（Action Trail）支持记录云服务客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云服务客户指定的日志服务中，可自定义留存时间。

■ 云安全产品能力

云安全产品支持将自身采集安全审计记录在安全控制台上展示，并支持将审计记录统一保存到云服务客户指定的日志服务或存储空间，日志留存时间满足 6 个月。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

安全措施：策略集中管控/核查

保护对象：全局

安全能力：

■ 云产品安全能力

配置审计（Cloud Config）支持计算、存储、数据库、虚拟专用网络 VPC 等多类云产品的配置监控，持续记录资源的配置变更和配置历史，形成配置时间线。对资源的安全配置实现持续监控。

■ 云安全产品能力

云安全中心支持云平台配置核查、漏洞检测和修复、基线核查、云安全补丁修复，并对安全相关事件进行集中管理。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

f）应能对网络中发生的各类安全事件进行识别、报警和分析；

安全措施：流量监控、入侵检测

仅供阿里云用户参考使用，请勿私自传播和宣传

保护对象：全局

安全能力：

■ 云产品安全能力

——

■ 云安全产品能力

云安全中心支持自动采集计算、数据库、负载均衡等等多种资产，收集多种日志数据，对重点安全威胁时管控，对各类安全事件进行识别、分析和告警，告警方式包括短信、邮件、钉钉等。

云防火墙通过威胁检测引擎，对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截。

Web 应用防火墙支持将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器。

DDoS 高防通过引流的方式对所有业务流量进行清洗，支持网络四层和七层防护。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

4.5 基本要求合规分析（云计算扩展要求）

4.5.1 安全通信网络

a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

安全措施：云平台安全保护定级

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里公共云安全保护等级为第三级，阿里公共云平台上承载的系统均不高于三级。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户选择高于其业务系统安全保护等级的云平台。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和查阅

4.5.2 安全区域边界

（1） 访问控制

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

安全措施：访问控制

保护对象：云计算环境

安全能力：

■ 云产品安全能力

不同 **VPC** 间默认隔离，同一子网内默认互通，不同子网间可使用网络 ACL 进行安全控制，ECS **安全组**与 RDS/ECS/SLB 的 IP 黑白名单支持虚拟网的隔离与访问控制。

■ 云安全产品能力

云防火墙互联网边界防火墙支持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，访问控制粒度可达端口级。

■ 云客户安全能力

云服务客户配置恰当访问控制策略。

合规性情况：符合

b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

安全措施：访问控制

保护对象：云计算环境

安全能力：

■ 云产品安全能力

不同 **VPC** 间默认隔离，同一 VPC 内通过 ECS 安全组与 RDS/ECS/SLB 的 IP 黑白名单进行访问控制。

■ 云安全产品能力

云防火墙支持对 VPC 边界防火墙、互联网边界防火墙以及主机边界防火墙的访问控制，用于检测和控制两个 VPC 间的通信流量、限制主机对内、外双向的未授权访问和 ECS 实例间的未授权访问。

■ 云客户安全能力

云服务客户配置恰当访问控制策略。

合规性情况：符合

仅供阿里云用户参考使用，请勿私自传播和售传

（2） 安全审计

a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

安全措施：安全审计

保护对象：云计算环境

安全能力：

■ 云产品安全能力

操作审计（Action Trail）支持对云服务客户的云服务远程及本地管理进行审计，并基于日志服务保留审计记录。

■ 云安全产品能力

堡垒机支持操作审计、职权管控、安全认证功能，记录所有运维操作记录、Linux 命令审计、Windows 操作录像。

云安全中心支持云服务客户所有资产安全事件的综合分析。

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

安全措施：安全审计

保护对象：云计算环境

安全能力：

■ 云产品安全能力

云服务商对云服务客户系统的操作需提交工单，通过云服务客户授权后进行操作，相关操作行为通过云服务客户的管理平台进行审计。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

4.5.3 安全计算环境

仅供阿里云用户参考使用，请勿私自传播和查阅

（1） 身份鉴别

当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

安全措施：账号认证

保护对象：云计算环境

安全能力：

■ 云产品安全能力

云服务客户基于阿里云 **RAM** 授权和 **AccessKey**，支持通过密钥访问阿里云 API，如果双方均为合法证书则建立双向加密通道。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

（2） 数据完整性和保密性

a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

安全措施：——

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里云国内基础设施和存储空间均位于中国境内，云上数据均存储于中国境内，云服务客户数据是否存在出境的情况由云服务客户确定。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户业务数据不出境，若出境遵循国家相关规定。

合规性情况：符合

（3） 数据备份恢复

a）云服务客户应在本地保存其业务数据的备份；

仅供阿里云用户参考使用，请勿私自传播和宣传

安全措施：数据备份

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里云**数据库**支持数据迁移和保存至云服务客户指定的数据库对象，提供数据本地下载服务，云服务客户可根据需求自行选择恰当的备份方式。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户本地备份业务数据。

合规性情况：符合

4.5.4 安全管理中心

（1） 集中管控

c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

安全措施：账号授权、安全审计

保护对象：云计算环境

安全能力：

■ 云产品安全能力

操作审计（Action Trail）支持记录云账号对资源的操作日志，提供操作日志的查询和下载。

■ 云安全产品能力

堡垒机支持对所有云服务客户的操作进行审计，操作系统自身日志本地保存。

数据库审计支持对数据库风险操作行为进行记录，提供细粒度审计数据库访问行为。

云客户安全能力

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚

仅供阿里云用户参考使用，请勿私自传播和宣传

拟机、虚拟化安全设备等的运行状况的集中监测。

安全措施：安全监测

保护对象：云计算环境

安全能力：

■ 云产品安全能力

云监控支持针对负载均衡、弹性 IP 地址、DDoS 高防、云服务器等运行状态创建监测规则，并进行集中监测和报警。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户基于云产品配置指南根据业务需求合理配置。

合规性情况：符合

4.5.5 安全建设管理

（1） 云服务商选择

a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

安全措施：安全合规认证

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里云提供的公共云平台安全保护等级为第三级，并通过公安部指定测评机构等保测评。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户根据业务需求选择合规的云服务商。

合规性情况：——

b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授

仅供阿里云用户参考使用 请勿私自传播和宣传

权、隐私保护、行为准则、违约责任等；

d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；

e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

安全措施：SLA 文本协议

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里云各类云产品均为云服务客户提供服务等级协议。

■ 云安全产品能力

阿里云各安全产品均提供服务等级协议。

■ 云客户安全能力

云服务客户在选定云服务商后，需签订相关服务等级协议。

合规性情况：——

（2） 供应链管理

a) 应确保供应商的选择符合国家有关规定；

安全措施：——

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里公共云平台基础设施供应商选择均按照国家相关规定，对供应商资质、诚信以及产品情况进行审核筛选，阿里云提供云服务均按照国家相关规定对外售卖。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户在选择第三方安全产品接入时，应明确供应商是否满足国家相关规定。

合规性情况：——

c)应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

仅供阿里云用户参考使用，请勿私自传播和宣传

安全措施：——

保护对象：云计算环境

安全能力：

■ 云产品安全能力

阿里公共云平台推送通知和公告，云服务客户通过登录自己的控制台能够查看相关风险和控制变更的信息。

■ 云安全产品能力

——

■ 云客户安全能力

云服务客户通过登录自己的控制台能够查看相关风险和控制变更的信息。

合规性情况：——

仅供阿里云用户参考使用，请勿私自传播和宣传

5 合规白皮书应用指引

5.1 快速识别基本要求适用条款

云计算作为网络安全等级保护 2.0 时代新型技术领域，部分云服务客户不清楚基本要求哪些条款适用于云上虚拟环境，如何开展基于等级保护的安全防护体系建设。本白皮书基于阿里云自身云平台等级保护测评的经验，在公安部信息安全等级保护评估中心指导下，识别出部署在阿里云 IaaS、PaaS 和 SaaS 不同服务模式下的云服务客户系统的保护对象，给出了基本要求中云服务客户等级保护适用条款建议。

同时，本白皮书也为等保测评机构开展云服务客户业务系统等保测评提供了参考，明确基本要求哪些指标的测评对象为云服务客户业务应用系统（附录 B）。

5.2 快速分析基本要求安全合规能力

本白皮书可有效帮助云服务客户梳理业务应用系统部署的云计算服务模式（附录 A）和基本要求适用条款（附录 B）。同时，本白皮书从云平台、云产品、云安全产品和云客户需自行建立的安全能力四个维度，以云服务客户需要承担安全责任最多的 IaaS 服务模式下的典型场景为例，结合《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》，为云服务客户构建等级保护合规能力提供了符合性分析，让云服务客户快速识别自身虚拟环境下等级保护的安全合规性。

本白皮书可有效帮助云服务客户在不同阶段分析自身业务应用系统安全合规能力，在业务系统安全体系建设初期，云服务客户可结合附录 A，附录 B、附录 C 以及第四章基本要求合规性分析，设计云服务客户业务系统安全防护体系；在云服务客户业务应用系统运营（使用）阶段，可参考白皮书附录 B 及第四章基本要求合规性分析，明确自身需满足的等级保护基本要求条款，自评估业务系统安全合规能力。基于本白皮书，等级保护测评机构可快速了解在开展云服务客户业务系统等级保护工作中，如何合理选取测评对象、测评指标以及合理准确的评测业务系统安全能力。

仅供阿里云用户参考使用，请勿私自传播和转售

附录 A：阿里云不同服务模式下的典型产品

服务模式	一级类目	二级类目	产品名称	产品官网链接
IaaS 服务模式	云计算基础	存储服务	对象存储	https://www.aliyun.com/product/oss
			块存储	https://www.aliyun.com/product/disk
			归档存储	https://www.aliyun.com/product/oas/
		弹性计算	GPU 云服务器	https://www.aliyun.com/product/ecs/gpu
			超级计算集群	https://www.aliyun.com/product/scc
			弹性裸金属服务器	https://www.aliyun.com/product/ebm
			轻量应用服务器	https://www.aliyun.com/product/swas
			专有宿主机	https://www.aliyun.com/product/ddh
			云服务器 ECS	https://www.aliyun.com/product/ecs
		网络	NAT 网关	https://www.aliyun.com/product/nat
			弹性公网 IP	https://www.aliyun.com/product/eip
			负载均衡	https://www.aliyun.com/product/slb
			高速通道	https://www.aliyun.com/product/expressconnect
			云企业网	https://www.aliyun.com/product/cbn
			专有网络 VPC	https://www.aliyun.com/product/vpc
	安全	安全服务	云安全中心	https://www.aliyun.com/product/sas
PaaS 服务模式	云计算基础	存储服务	混合云备份服务	https://www.aliyun.com/product/hbr
			混合云存储阵列	https://www.aliyun.com/product/hgw
			混合云容灾服务	https://www.aliyun.com/product/hdr
			文件存储 NAS	https://www.aliyun.com/product/nas
			云存储网关	https://www.aliyun.com/product/hcs
			智能媒体管理	https://www.aliyun.com/product/imm
		弹性计算	弹性高性能计算	https://www.aliyun.com/product/ehpc
			函数计算	https://www.aliyun.com/product/fc
			批量计算	https://www.aliyun.com/product/batchcompute
			容器服务	https://www.aliyun.com/product/containerservice
			容器服务 Kubernetes 版	https://www.aliyun.com/product/kubernetes
		互联网中间件	企业级分布式应用服务	https://www.aliyun.com/product/edas
			全局事务服务	https://www.aliyun.com/aliware/txc
			消息队列 MQ	https://www.aliyun.com/product/ons
			消息服务	https://www.aliyun.com/product/mns
			性能测试	https://www.aliyun.com/product/pts
			应用配置管理	https://www.aliyun.com/product/acm
		视频	媒体处理	https://www.aliyun.com/product/mts
			全站加速	https://www.aliyun.com/product/dcdn

仅供阿里云用户参考使用，请勿私自传播和盲信

服务模式	一级类目	二级类目	产品名称	产品官网链接
			视频点播	https://www.aliyun.com/product/vod
			视频直播	https://www.aliyun.com/product/live
			音视频通信	https://www.aliyun.com/product/rtc
		数据库	Data Lake Analytics	https://www.aliyun.com/product/datalakeanalytics
			HybridDB for MySQL	https://www.aliyun.com/product/petadata
			表格存储	https://www.aliyun.com/product/ots
			分布式关系型数据库服务	https://www.aliyun.com/product/drds
			分析型数据库 MySQL 版	https://www.aliyun.com/product/ads
			分析型数据库 PostgreSQL 版	https://www.aliyun.com/product/gpdb
			数据管理	https://www.aliyun.com/product/dms
			数据库备份	https://www.aliyun.com/product/dbs
			云数据库 Memcache 版	https://www.aliyun.com/product/ocs
			云数据库 MongoDB 版	https://www.aliyun.com/product/mongodb
			云数据库 MySQL 版	https://www.aliyun.com/product/rds/mysql
			云数据库 POLARDB	https://www.aliyun.com/product/polardb
			云数据库 PostgreSQL 版	https://www.aliyun.com/product/rds/postgresql
			云数据库 PPAS 版	https://www.aliyun.com/product/rds/ppas
			云数据库 Redis 版	https://www.aliyun.com/product/kvstore
			云数据库 SQL Server 版	https://www.aliyun.com/product/rds/sqlserver
			云数据库 HBase 版	https://www.aliyun.com/product/hbase
	大数据	大数据计算	E-MapReduce	https://www.aliyun.com/product/emapreduce
			大数据计算服务	https://www.aliyun.com/product/odps
			实时计算（流计算）	https://data.aliyun.com/product/sc
		大数据搜索与分析	Elasticsearch	https://data.aliyun.com/product/elasticsearch
			Quick BI	https://data.aliyun.com/product/bi
			关系网络分析	https://data.aliyun.com/product/graphanalytics
			开放搜索	https://www.aliyun.com/product/opensearch
			DataWorks	https://data.aliyun.com/product/ide
		大数据应用	企业图谱	https://data.aliyun.com/product/eprofile
		数据开发	数据集成	https://www.aliyun.com/product/cdp

仅供阿里云用户参考使用，请勿私自传播和宣传

服务模式	一级类目	二级类目	产品名称	产品官网链接
		数据可视化	DataV 数据可视化	https://data.aliyun.com/visual/datav
	开发者服务	集成交付	CodePipeline	https://www.aliyun.com/product/codepipeline
		开发者平台	云效	https://www.aliyun.com/product/rdc
	企业应用	域名与网站	云虚拟主机	https://wanwang.aliyun.com/hosting/
			弹性 Web 托管	https://wanwang.aliyun.com/hosting/elastic
	物联网	云服务	时序时空数据库	https://www.aliyun.com/product/hitsdb
			物联网平台	https://www.aliyun.com/product/iot
			物联网无线连接服务	https://www.aliyun.com/product/olddyiot
SaaS 服务模式	安全	安全管理	堡垒机	https://www.aliyun.com/product/bastionhost
			操作审计	https://www.aliyun.com/product/actiontrail
			访问控制	https://www.aliyun.com/product/ram
			密钥管理服务	https://www.aliyun.com/product/kms
		数据安全	加密服务	https://www.aliyun.com/product/hsm
			数据库审计	https://www.aliyun.com/product/dbaudit
		网络安全	DDoS 高防 IP	https://www.aliyun.com/product/ddos
			游戏盾	https://m.aliyun.com/markets/aliyun/product/GameShield
			云防火墙	https://www.aliyun.com/product/cfw
		业务安全	内容安全	https://www.aliyun.com/product/lvwang
			实人认证	https://www.aliyun.com/product/cloudauth
		应用安全	SSL 证书（CA 证书服务）	https://www.aliyun.com/product/cas
			Web 应用防火墙	https://www.aliyun.com/product/waf
			漏洞扫描	https://www.aliyun.com/product/avds
			爬虫风险管理	https://www.aliyun.com/product/antibot
	企业应用	区块链	区块链服务	https://www.aliyun.com/product/baas
		移动云	移动测试	https://www.aliyun.com/product/mqc
			移动热修复	https://www.aliyun.com/product/hotfix
			移动推送	https://www.aliyun.com/product/cps
		应用服务	API 网关	https://www.aliyun.com/product/apigateway
			阿里邮箱	https://wanwang.aliyun.com/mail
			邮件推送	https://www.aliyun.com/product/directmail
			云 AP	https://www.aliyun.com/product/cloudap
			云投屏	https://www.aliyun.com/product/cd
		域名与网站	HTTP DNS	https://www.aliyun.com/product/httpdns
			域名	https://wanwang.aliyun.com/domain/
			云解析 DNS	https://wanwang.aliyun.com/domain/dns
		智能客服链	云呼叫中心	https://www.aliyun.com/product/ccc

仅供阿里云用户参考使用，请勿自行传播和复制

服务模式	一级类目	二级类目	产品名称	产品官网链接
		接	云客服	https://www.aliyun.com/product/ccs
			智能对话分析	https://www.aliyun.com/product/sca
	人工智能	人工智能产品	机器学习	https://data.aliyun.com/product/learn
			人脸识别	https://data.aliyun.com/product/face
			图像识别	https://data.aliyun.com/product/image
			图像搜索	https://ai.aliyun.com/imagesearch
			印刷文字识别	https://data.aliyun.com/product/ocr
			智能语音交互	https://data.aliyun.com/product/nls
			自然语言处理	https://ai.aliyun.com/nlp
	云计算基础	弹性计算	资源编排	https://www.aliyun.com/product/ros
		网络	共享带宽	https://www.aliyun.com/product/cbwp
			共享流量包	https://www.aliyun.com/product/flowbag
		运维管理	应用实时监控服务	https://www.aliyun.com/product/arms
			云监控	https://www.aliyun.com/product/jiankong

仅供阿里云用户参考使用，请勿私自传播和复制

附录 B：不同模式下云服务客户等级保护适用条款

B.1 网络安全等级保护基本要求（通用要求）

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；	●	--	--
		b）应保证网络各个部分的带宽满足业务高峰期需要；	●	--	--
		c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	●	--	--
		d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；	●	--	--
		e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性；	●	--	--
	通信传输	a）应采用密码技术保证通信过程中数据的完整性；	●	--	--
		b）应采用密码技术保证通信过程中数据的保密性；	●	--	--
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。	●	--	--
安全区域边界	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	●	--	--
		b）应能够对非授权设备私自联到内部网络的行为进行限制或检查；	●	--	--
		c）应能够对内部用户非授权联到外部网络的行为进行限制或检查；	●	--	--
		d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络；	●	--	--
	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	●	--	--
		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	●	--	--
		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	●	--	--
		d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	●	--	--
		e） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	●	--	--

仅供阿里云用户参考使用，请勿引用传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	●	--	--
		b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	●	--	--
		c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；	●	--	--
		d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	●	--	--
	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	●	--	--
		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	●	--	--
	安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	●	--	--
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	●	--	--
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	●	--	--
		d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	●	--	--
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。	●	--	--
安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	●	●	○
		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	●	●	○
		c）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	●	●	○
		d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	●	●	○
	访问控制	a）应对登录的用户分配账户和权限；	●	●	○

仅供阿里云用户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		b）应重命名或删除默认账户，修改默认账户的默认口令；	●	●	○
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	●	●	○
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离；	●	●	○
		e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	●	●	○
		f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	●	●	○
		g）应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。	●	●	○
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	●	●	○
		b）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；	●	●	○
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	●	●	○
		d）应对审计进程进行保护，防止未经授权的中断。	●	●	○
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	●	●	○
		b）应关闭不需要的系统服务、默认共享和高危端口；	●	●	○
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	●	●	○
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	●	●	○
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	●	●	○
		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	●	●	○
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	●	●	○
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。	●	○	○
	数据	a）应采用密码技术保证重要数据在传输过程中的完	●	●	○

仅供阿里云内部参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
	完整性	整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；			
		b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	●	●	○
	数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	●	●	○
		b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	●	●	○
	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	●	●	○
		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	●	●	○
		c）应提供重要数据处理系统的热冗余，保证系统的高可用性；	●	●	○
	剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	●	●	○
		b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	●	●	○
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	●	●	○
		b）应禁止未授权访问和非法使用用户个人信息。	●	●	○
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	●	●	●
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	●	●	●
	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	●	●	●
		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	●	●	●
	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；	●	●	●

仅供阿里云用户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	●	●	●
	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；	●	--	--
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；	●	--	--
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；	●	--	--
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；	●	●	●
		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；	●	●	--
		f）应能对网络中发生的各类安全事件进行识别、报警和分析；	●	●	--
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	●	●	●
	管理制度	a) 应对安全管理活动中的各类管理内容建立安全管理制度；	●	●	●
		b) 应对管理人员或操作人员执行的日常管理操作建立操作规程；	●	●	●
		c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。	●	●	●
	制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定；	●	●	●
		b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。	●	●	●
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	●	●	●
安全管理机构	岗位设置	a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；	●	●	●
		b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	●	●	●
		c) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	●	●	●
	人员配备	a) 应配备一定数量的系统管理员、审计管理员和安全	●	●	●

仅供阿里云客户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		管理员等；			
		b) 应配备专职安全管理员，不可兼任。	●	●	●
	授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	●	●	●
		b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；	●	●	●
		c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。	●	●	●
	沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	●	●	●
		b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	●	●	●
		c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	●	●	●
	审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；	●	●	●
		b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；	●	●	●
		c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。	●	●	●
安全管理人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用；	●	●	●
		b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；	●	●	●
		c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。	●	●	●
	人员离岗	a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；	●	●	●
		b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。	●	●	●
	安全意识教育和培训	a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；	●	●	●
		b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；	●	●	●
		c) 应定期对不同岗位的人员进行技能考核。	●	●	●
	外部人员	a) 应在外部人员物理访问受控区域前先提出书面申	●	●	●

仅供阿里云用户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
	访问管理	请，批准后由专人全程陪同，并登记备案；			
		b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	●	●	●
		c) 外部人员离场后应及时清除其所有的访问权限；	●	●	●
		d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。	●	●	●
安全建设管理	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	●	●	●
		b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	●	●	●
		c) 应保证定级结果经过相关部门的批准；	●	●	●
		d) 应将备案材料报主管部门和相应公安机关备案。	●	●	●
	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	●	●	●
		b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；	●	●	●
		c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。	●	●	●
	产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；	●	●	●
		b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；	●	●	●
		c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	●	●	●
	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	●	●	--
		b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；	●	●	--
		c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；	●	●	--
		d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；	●	●	--
		e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；	●	●	--
		f) 应对程序资源库的修改、更新、发布进行授权和批	●	●	--

仅供阿里云用户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		准，并严格进行版本控制；			
		g) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。	●	●	--
	外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；	●	●	--
		b) 应保证开发单位提供软件设计文档和使用指南；	●	●	--
		c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	●	●	--
	工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理；	●	●	--
		b) 应制定安全工程实施方案控制工程实施过程；	●	●	--
		c) 应通过第三方工程监理控制项目的实施过程。	●	●	--
	测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	●	●	--
		b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。	●	●	--
	系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	●	●	●
		b) 应对负责运行维护的技术人员进行相应的技能培训；	●	●	●
		c) 应提供建设过程文档和运行维护文档。	●	●	●
	等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	●	●	●
		b) 应在发生重大变更或级别发生变化时进行等级测评；	●	●	●
		c) 应确保测评机构的选择符合国家有关规定。	●	●	●
	服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定；	●	●	●
		b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；	●	●	●
		c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。	●	●	●
安全运维管理	环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	●	--	--
		b) 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；	●	--	--
		c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	●	●	●
	资产管理	a) 应编制并保存与保护对象相关的资产清单，包括资	●	●	●

仅供阿里云用户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		产责任部门、重要程度和所处位置等内容；			
		b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；	●	●	●
		c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	●	●	●
	介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	●	●	●
		b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	●	●	●
	设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	●	●	●
		b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；	●	●	●
		c) 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；	●	●	●
		d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。	●	●	●
	漏洞和风险管理	a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	●	●	●
		b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。	●	●	●
	网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	●	--	--
		b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	●	●	●
		c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	●	●	●
		d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	●	●	●
		e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	●	●	●
		f) 应指定专门的部门或人员对日志、监测和报警数据	●	●	●

仅供阿里云用户参考使用，请勿做宣传和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		等进行分析、统计，及时发现可疑行为；			
		g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；	●	●	●
		h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；	●	●	●
		i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；	●	●	●
		j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。	●	●	●
	恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	●	●	●
		b) 应定期验证防范恶意代码攻击的技术措施的有效性。	●	●	●
	配置管理	a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；	●	●	--
		b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。	●	●	●
	密码管理	a) 应遵循密码相关国家标准和行业标准；	●	●	●
		b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	●	●	●
	变更管理	a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；	●	●	●
		b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；	●	●	●
		c) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	●	●	●
	备份与恢复管理	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；	●	●	●
		b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；	●	●	●
		c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序	●	●	●

仅供阿里云用户参考使用，请勿私自传播和宣传

网络安全等级保护基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
		等。			
	安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；	●	●	●
		b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	●	●	●
		c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；	●	●	●
		d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	●	●	●
	应急预案管理	a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	●	●	●
		b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	●	●	●
		c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；	●	●	●
		d) 应定期对原有的应急预案重新评估，修订完善。	●	●	●
	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；	●	●	●
		b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；	●	●	●
		c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；	●	●	●
		d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。	●	●	●

仅供阿里云用户参考使用 请勿私自传播和宣传

注： “●”表示云服务客户适用条款，“○”表示云服务客户适用条款取决于云服务客户实际业务情况，“--”表示云服务客户不适用条款，其他未展示条款均为不适用条款。

B.2 网络安全等级保护基本要求（云扩展要求）

网络安全等级保护 2.0 基本要求			IaaS 服务模式	PaaS 服务模式	SaaS 服务模式
安全层面	控制点	要求项			
安全通信网络	网络架构	a)应保证云计算平台不承载高于其安全保护等级的业务应用系统；	●	--	--
安全区域边界	访问控制	a)应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；	●	--	--
		b)应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。	●	--	--
	安全审计	a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；	●	●	--
		b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。	●	●	--
安全计算环境	身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。	●	●	○
	数据完整性和保密性	a)应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；	●	●	○
	数据备份恢复	a)云服务客户应在本地保存其业务数据的备份；	●	●	●
安全管理中心	集中管控	c)应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；	●	●	○
		d)应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。	●	--	--
安全建设管理	云服务商选择	a)应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；	●	●	●
		b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标；	●	●	●
		c)应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；	●	●	●
		d)应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；	●	●	●
		e)应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。	●	●	●
	供应链管理	a)应确保供应商的选择符合国家有关规定；	○	○	○
		c)应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。	○	○	○

仅供阿里云用户参考使用，请勿私自传播和宣传

注：“●”表示云服务客户适用条款，“○”表示云服务客户适用条款取决于云服务客户实际业务情况，“—”表示云服务客户不适用条款，其他未展示条款均为不适用条款。

附录 C：阿里云等级保护基本要求安全能力对照表

C.1 网络安全等级保护基本要求（通用要求）

安全层面	控制点	等级保护基本要求条款	阿里云云产品	云产品安全能力	阿里云云安全产品	云安全产品安全能力
安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；	VPC、负载均衡	1）每个 VPC 由一个私网网段、一个路由器和至少一个交换机组成； VPC 控制台提供查询当前资源配额使用情况的能力，若某个资源的剩余配额不满足业务需求，可以直接申请增加配额； 2）负载均衡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。	——	——
		b）应保证网络各个部分的带宽满足业务高峰期需要；	云监控 弹性公网 IP	云监控通过监控弹性公网 IP 的流出流量、流入流量、流出数据包数、流入数据包数等监控项，帮助用户了解带宽使用情况。	DDoS 原生防护	DDoS 原生防护采用 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，通过一个 IP 实现不同运营商访问，各线路按最优策略调度，高可用性有保障。
		c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	VPC	VPC 为云服务客户提供自定义 IP 地址范围、网段、路由表和网关等安全能力，并根据业务需求自定义不同的安全域。	——	——
		d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段	VPC	1）不同 VPC 虚拟网络之间内部网络完全隔离，云服务客户根据业务需求通过对外映射弹性公网 IP 和 NAT IP 进行互连； 2）VPC 基于网络 ACL 和云服务器安全组进行区域间的访问控制。	云防火墙	云防火墙实现 VPC 间流量控制及主机间微隔离。

仅供阿里云用户参考使用，请勿私自传播和售卖

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
		e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性；	负载均衡	负载均衡采用全冗余设计，无单点，支持同城容灾和跨地域容灾，可用性高达 99.95%，支持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。	——	——
安全区域边界	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	VPC 安全组	1）不同 VPC 之间内部网络完全隔离，只能通过对外映射的 IP（弹性公网 IP 和 NAT IP）互连。 ； 2）安全组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。	云防火墙	云防火墙对 VPC 间的访问流量进行检测和控制。
		b）应能够对非授权设备私自联到内部网络的行为进行限制或检查；	安全组	安全组通过入口方向访问控制策略配置，限制云服务器非法内联。	云防火墙	云防火墙支持云服务器从内对外访问控制策略配置。
		c）应能够对内部用户非授权联到外部网络的行为进行限制或检查；		安全组通过出口方向访问控制策略配置，限制云服务器非法外联，允许或禁止云服务器实例对公网或私网的访问。	云防火墙、云安全中心	1）云防火墙支持云服务客户根据业务需求配置外对内访问控制策略，云防火墙支持对云服务客户南北向和东西向访问的网络流量分析，支持全网流量可视化，支持对主动外联行为的分析和阻断，配置开通、变更白名单策略； 2）云安全中心支持对云服务客户非授权联到外部恶意域名、IP 地址的行为进行检查和拦截。

仅供阿里云用户参考使用，禁止自传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	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。	云防火墙	云防火墙支持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，访问控制粒度可达端口级。
		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	安全组	安全组访问控制规则支持优先级设置，以及修改、克隆、删除，可实现云服务客户访问控制规则数最优。	云防火墙	云防火墙支持策略命中计数功能，确保没有无效的冗余策略，云防火墙访问控制策略可配置优先级，优化访问控制列表。
		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	安全组	安全组规则属性包括网络类型、网卡类型、规则方向、授权策略、协议类型、端口范围、优先级、授权类型、授权对象。	云防火墙	云防火墙支持对进出访问控制策略进行严格设置，访问控制策略包括源类型、访问源、目的类型、目的、协议类型、目的端口、应用协议、动作、描述和优先级。
		d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	——	——	云防火墙	云防火墙支持根据会话状态信息为数据流提供的访问控制能力。
		e） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	——	——	云防火墙、web 应用防火墙、DDoS 高防	1）云防火墙支持跨 VPC 数据流的应用协议、内容的访问控制； 2)WEB 应用防火墙支持应用级协议和内容访问控制; 3)DDoS 高防通过引流的方式对所有业务流量进行清洗，支持网络四层和七层防护。
	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	阿里云基础防护	阿里云基础防护支持实时地检测出各种攻击和异常行为，发现内部被控制的云服务器，对常见的 Web 应用攻击进行网络层拦截旁路阻断，并与其他安全防护模块联动防	云安全中心、云防火墙、web 应用防火墙	1）云安全中心通过大数据威胁检测、人工智能和病毒查杀引擎对网络流量和主机中的入侵行为和文件样本进行实时检测和防御； 2）云防火墙通过威胁检测引擎，对

仅供阿里云用户签考使用，请勿私自传播宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
				护。		互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截； 3）Web 应用防火墙支持将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器； 4）DDoS 高防支持抵御各类基于网络层、传输层及应用层的 DDoS 攻击，秒级启动流量清洗，过滤掉攻击流量支持全自动检测和攻击策略匹配，实时防护，清洗服务可用性 99.95%，可定制 99.99%。
		b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	阿里云基础防护	阿里云基础防护对云内部的恶意主机对外发起的攻击行为进行检测，及时发现内部已经被控制的云服务器。	云安全中心 云防火墙	1）云安全中心支持检测针对主机系统层和应用层的主动外联和恶意攻击行为，对进程、网络异常行为进行预警； 2）云防火墙能够检测东西向流量，配置相应的安全策略，阻断防止从内部发起的网络攻击行为。
		c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；	——	——	云安全中心 云防火墙	1）云安全中心基于主机、网络、云平台的安全数据进行分析，实现挖矿、勒索、蠕虫、DDoS 木马等基于新型网络攻击的攻击预警； 2）云防火墙对云上进出网络的恶意流量进行实时检测与阻断，支持防御挖矿蠕虫等新型网络攻击，并通过积累大量恶意攻击样本，形成精准防御规则；云防火墙入侵检测功能支持发现挖矿蠕虫感染事件。

仅供阿里云用户参考使用，请勿私自传播私宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
		d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	——	——	云安全中心、 云防火墙、 web 应用防火墙	1）云安全中心支持检测到威胁时，记录事件账号/源地址、攻击类型、攻击时间、事件级别以及处置建议，同时支持自动化攻击溯源，展示攻击过程； 2）云防火墙支持检测到攻击行为时，提供网络阻断功能，记录风险级别、事件名称、防御状态、源 IP、目的 IP、方向、判断来源、发生时间和动作； 3)Web 应用防火墙支持 HTTP 和 HTTPS 流量攻击，记录攻击事件类型、攻击 URL、来源 IP、目的 Host、时间、Get 请求内容和拦截动作; 4)DDoS 高防检测到 DDoS 攻击时，记录攻击类型、攻击目标、攻击时间、攻击流量峰值和清洗防护结果。
	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	阿里云基础防护	阿里云基础防护支持对互联网出口的恶意代码检测和清除，恶意代码规则库定期更新。	云安全中心、 云防火墙、 web 应用防火墙	1)云安全中心支持蠕虫病毒、勒索病毒、木马、网站后门等恶意代码的检测和隔离清除，定期升级相关恶意代码规则库; 2)云防火墙支持通过入侵防护和集成威胁情报支持防恶意代码，若传输样本的 MD5 的特征值匹配到威胁情报，则阻断该报文; 3)Web 应用防火墙流量恶意代码检测提供恶意代码检测功能，恶意代码规则库定期更新。

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	——	——	阿里云邮箱	阿里云邮箱支持垃圾邮件检测功能。
	安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	操作审计	操作审计（Action Trail）支持记录云账号对资源的操作日志，提供操作日志的查询和下载。	云安全中心、 云防火墙、 web 应用防火墙、 DDoS 高防、 堡垒机	1)云安全中心通过支持主机登录日志、进程启动、网络连接、端口快照、账户快照、暴力破解、网络会话、DNS 解析、WEB 会话、安全告警、漏洞和基线日志进行审计; 2)云防火墙支持通过日志审计模块记录所有流量日志、事件日志和操作日志; 3)Web 应用防火墙对攻击日志支持日志实时查询分析; 堡垒机支持对云端虚拟主机 ECS 资产进行运维权限管控及运维审计; 4)数据库审计支持对云上数据库访问行为进行监控，分析危险操作及可疑行为。
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	操作审计	操作审计（Action Trail）记录云账号用户云上操作日志，包括事件、用户名、事件名称、资源类型、资源名称和错误码。	云安全中心、 云防火墙、 web 应用防火墙、 DDoS 高防、 堡垒机	1)云安全中心检测到威胁时，记录事件账号/源地址、攻击类型、攻击时间、事件级别以及处置建议; 2)云防火墙支持日志记录事件被扫描到的时间、威胁类型、出/入方向、源 IP 和目的 IP、应用类型、严重性等级以及动作状态信息；流量日志记录访问流量开始和结束的时间、出/入方向、源 IP 和目的 IP、应用类型、源端口、应用、支持的协议、动作状态、字节数以及报文数等信

仅供阿里云用户参考使用，请勿做自传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
						息；操作日志记录云防火墙中的所有操作执行的时间、操作类型、严重性以及具体操作信息; 3)Web 应用防火墙记录攻击事件类型、攻击 URL、来源 IP、目的 Host、时间、Get 请求内容和拦截动作; 4)DDoS 高防检测到 DDoS 攻击时，记录攻击类型、攻击目标、攻击时间、攻击流量峰值和清洗防护结果; 5)堡垒机日志记录包括重要性、时间、日志类型、日志内容、用户、源 IP 地址和结果。
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	操作审计	操作审计（Action Trail）默认支持在线查询 90 天的操作日志，支持将操作日志保存在云服务客户指定的对象存储空间或日志服务中，自定义更长久的保存。保存的操作记录可以用作追踪资源变更行为和行为风险分析。	云安全中心、 云防火墙、 web 应用防火墙、 DDoS 高防、 堡垒机	云安全中心、云防火墙、Web 应用防火墙、DDoS 高防、堡垒机和数据库审计等安全产品支持日志分析功能，依托日志服务产品，可存储 6 个月内的日志数据提供实时日志分析能力。
		d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	日志服务	日志服务支持云服务客户操作审计进行单独审计，且提供审计数据分析能力。	云安全中心	云安全中心支持云服务客户所有资产安全事件的综合分析。
安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	——	——	堡垒机 云安全中心	1)堡垒机口令策略支持 8 个字符以上，必须包含大写字母、小写字母、数字及特殊符号，用户身份有唯一标识，口令 90 天定期跟换，新用户强制更改口令; 2)云安全中心支持对云服务客户登录的配置和密码复杂度进行定期安

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
						全检查，并提供安全建议并进行预警。
		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	阿里云控制台	阿里云控制台支持设置登录失败处理策略，可设置最大登录失败 5 次，失败后锁定 15 分钟，会话超时会自动中断。	堡垒机 云安全中心	1）堡垒机支持登录失败处理功能配置，建议配置云服务客户最大登录失败 5 次，临时锁定 30 分钟，登录连接超时时间为 30 分钟； 2）云安全中心支持登录失败防御配置，支持云服务客户配置最大登录失败 10 次数，临时阻断连接 1 天、3 天和 7 天。
		c）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	阿里云控制台	云服务客户控制台访问均通过 Https 加密协议来保证数据传输的安全。 云产品支持对外提供加密 Https 的 Endpoint API 调用，云产品访问采用加密协议。	堡垒机 云安全中心	1）堡垒机远程连接至云服务器时，采用安全的 SSH 方式进行远程登录； 2）云安全中心支持对远程管理的配置进行检查，防止不安全的配置导致传输被窃听。
		d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	MFA	阿里云控制台账户支持虚拟 MFA，支持主账号开启 MFA 安全检查，在登录云服务客户控制台时需通过用户名、口令可由虚拟 MFA 应用程序生成的动态安全码进行双因素认证，如使用用户名、口令和 Google Authenticator 等双因素认证登录到 RAM 控制台。	堡垒机 云安全中心	1）堡垒机支持作为唯一入口管理服务器，支持包括虚拟 MFA、短信验证码在内的多因子认证； 2）云安全中心支持对云平台配置提供基线核查，能够实时发现主账号双因素认证风险。
	访问控制	a）应对登录的用户分配账户和权限；	RAM	RAM 支持云产品接入，支持云服务客户通过开启 RAM 功能来完成授予 RAM 子云服务客户访问权限，	——	——

仅供阿里云用户参考使用，请勿私自传播宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
				权限的控制粒度可以细化到 API 级别。		
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	RAM	RAM 支持云服务客户对账户进行账户创建、删除和修改自行管理。	堡垒机 云安全中心	1）堡垒机支持云服务客户对无用、多余账户会锁定或删除管理； 2）云安全中心支持对平台账户进行安全配置检查。
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离；	RAM	RAM 支持子账号对云产品使用最小权限设置。	堡垒机 云安全中心	1）堡垒机支持基于用户角色分配权限，实现三权分立，角色分为超级管理员、审计员和运维员； 2）云安全中心支持对账户权限配置的安全检查，实现针对云服务客户权限分离的检查。
		e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	RAM	RAM 支持创建 RAM 子云服务客户并授予特定权限策略从账户权限上实现对云产品资源细粒度访问，如网络层面访问控制策略、安全组规则、开发与用户权限分离策略。	云安全中心	云安全中心支持对 RAM 用户提供高危风险配置的安全检查。
		f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	RAM 阿里云控制台	RAM 支持基于用户角色权限分配，授权主体为用户级，客体为云服务级别、操作级别和资源级别，云资源细粒度分配由云服务客户自行配置。 阿里云控制台支持主账号对子账号授权，可以控制到资源、接口和操作权限。	——	——
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	操作审计	操作审计（Action Trail）支持记录云账号对资源的操作日志，提供操作日志的查询和下载。	堡垒机 数据库审计 云安全中心	1）堡垒机支持对所有云服务客户的虚拟主机操作进行审计，系统自身日志本地保存；

仅供阿里云用户参考使用，请勿私自传播私自售卖

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
						2）数据库审计支持对数据库风险操作行为进行记录，提供细粒度审计数据库访问行为； 3）云安全中心支持对账户 9 登录进行记录，提供细粒度审计登录时间、登录账户、登录结果的记录，并通过报表进行实时监控预警。
		b）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；	操作审计	操作审计（Action Trail）记录云账号用户云上操作日志，包括事件、用户名、事件名称、资源类型、资源名称和错误码。	堡垒机 数据库审计 云安全中心	1）堡垒机日志记录包括重要性、时间、日志类型、日志内容、用户、源 IP 地址和结果； 2）数据库审计提供多维度线索分析，包括会话行为、SQL 行为、风险行为和政策性报表； 3）云安全中心日志记录包括主机登录日志、进程启动、网络连接、账户快照、端口快照、DNS、Web 访问、网站会话、云平台操作等日志结果。
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	操作审计	操作审计（Action Trail）默认支持在线查询 90 天的操作日志，支持将操作日志保存在云服务客户指定的对象存储空间或日志服务中，自定义更长久的保存。保存的操作记录可以用作追踪资源变更行为和行为风险分析。	堡垒机 数据库审计 云安全中心	1）堡垒机、数据库审计日志实时推送至日志服务，审计记录可按需调整存储空间，支持 6 个月以上保存期； 2）云安全中心支持日志记录保存期为 6 个月，同时支持对操作审计日志配置进行基线核查。
		d）应对审计进程进行保护，防止未经授权的中断。	操作审计、配置审计	阿里云控制台通过操作审计（Action Trail）记录云账号用户操作日志并基于日志审计，通过配置审计（Cloud Config）监控操作审计	堡垒机 数据库审计 云安全中心	1）堡垒机、数据库审计支持日志实时推送至日志服务； 2）云安全中心对操作审计日志配置进行基线核查。

仅供阿里云用户参考使用，请勿私自传播私自传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
				的有效运行状态，防止操作审计被误关闭。		
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	——	——	云安全中心	云安全中心客户端在上线前，均经过内部的安全审核，并进行安全加固，遵循最小化安装原则。
		b）应关闭不需要的系统服务、默认共享和高危端口；	——	——	云安全中心	云安全中心支持对主机、SLB、RDS、OSS 等云产品进行高危配置、端口的基线检查。
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	VPC、RAM、安全组	VPC 虚拟网络隔离技术和 RAM 账户策略可以对访问终端方式进行限制。 安全组支持云服务客户配置安全组规则，限制虚拟机的访问策略，包括端口、协议和 IP 地址等。	云安全中心	云安全中心支持联动云平台 IP 白名单、安全组的能力，对网络 IP、端口、协议进行管理和限制。
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	阿里云控制台 云产品	阿里云控制台和产品在上线前均已经过内部开发流程，支持对输入数据的有效性进行验证，过滤特殊字符。	——	——
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	——	——	云安全中心 漏洞扫描 渗透测试服务	1）云安全中心漏洞修复组件支持 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞和应急漏洞的一键修复功能，支持安全基线检测策略，支持平台安全配置等检查，能够实时检测已知漏洞； 2）漏洞扫描支持资产威胁检测，发现云服务客户业务系统关联资产，实现自动化漏洞渗透测试和敏感内容监测； 3）渗透测试服务支持通过模拟黑客

仅供阿里云用户参考使用，请勿作其他传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
						对云服务客户业务系统进行安全测试，发现安全缺陷和漏洞，并提出修复建议。
		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	——	——	云安全中心 Web 应用防火墙	1）云安全中心能够检测到对重要节点入侵行为并进行告警，主要包括异常登录检测、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； 2）Web 应用防火墙支持将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器。
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	——	——	云安全中心	云安全中心通过安全加固镜像部署代理，支持对恶意的代码实时拦截功能，在系统内核层面，识别恶意代码，并进行主动拦截。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。	可信计算云服务器	基于可信技术的云服务器正在部分区域试点，即将全面推出。	——	——
	数据完整性	a）应采用密码技术保证重要数据在传输过程中的完整性，包括	——	阿里云支持云服务客户基于 Https 的 API 访问点，允许云服务客户使	——	——

仅供阿里云用户参考使用，请勿私自传播私宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
		但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；		用 Access Key 以程序形式来调用 API。 阿里云支持标准 TLS 协议，支持提供 256 位密钥加密强度。		
		b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	对象存储	云存储产品支持自带完整性校验功能，OSS 通过上传 object 返回 CRC64 值，支持云服务客户在客户端与本地计算的 CRC64 值做对比，从而完成数据完整性验证，并支持在数据存储时进行校验码验证，实现数据进行细粒度的完整性校验保护。	KMS	密钥管理服务 KMS 支持云服务客户自主密钥管理，支持云产品接入 KMS 实现密钥管理，并对敏感资源和信息进行加密存储，实现云服务客户管理自己密钥并实现数据加解密过程。
	数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	——	阿里云支持云服务客户基于 Https 的 API 访问点，允许云服务客户使用 Access Key 以程序形式来调用 API。	——	——
		b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	——	——	KMS	密钥管理服务 KMS 支持密钥管理，支持提供 256 位密钥加密存储，满足加密存储需求。
	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	云服务器、云数据库、对象存储	1）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%； 2）云数据库通过数据备份和日志备份的备份方式，保证数据完整可靠。同时云服务客户可以随时发起数据库的备份，RDS 能够根据备份策略	——	——

仅供阿里云用户参考使用，请勿自行传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
				将数据库恢复至任意时刻，提高数据可回溯性； 3）对象存储采用多可用区机制，将云服务客户的数据分散存放在同一地域（Region）的 3 个可用区。		
		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	云服务器、云数据库、对象存储	1）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%； 2）云数据库通过数据备份和日志备份的备份方式，支持设置指定数据备份云数据库； 3）对象存储采用多可用区机制，将云服务客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。	——	——
		c）应提供重要数据处理系统的热冗余，保证系统的高可用性；	——	云产品基于飞天分布式操作系统高可用架构，存储产品支持高可用性，支持用于基于业务处理能力，按照需求动态调整资源，保证系统高可用。	——	——
	剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	——	阿里云对存储过云服务客户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖，对于重用或报废的物理设备，对存储介质进行覆写、消磁或折弯等数据清除处理。	——	——

仅供阿里云用户参考使用，请勿做宣传用途

安全层面	控制点	等级保护基本要求条款	阿里云云产品	云产品安全能力	阿里云云安全产品	云安全产品安全能力
		b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	——	阿里云支持不同云服务客户内存和持久化存储空间相对独立，当资源释放时，云服务客户空间会被释放和清除。	——	——
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	——	阿里云发布用户隐私政策声明，按照最小化原则采集和保存用户个人信息。	敏感数据保护	敏感数据保护支持对个人信息进行发现、分类和保护。
		b）应禁止未授权访问和非法使用用户个人信息。	——	阿里云发布用户隐私政策声明，按照最小化原则采集和保存用户个人信息，禁止未授权访问和非法、使用用户个人信息。	——	——
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	阿里云控制台、RAM、操作审计	阿里云支持账号管理，支持基于 RAM 授权系统管理员通过阿里云控制台进行系统管理，通过操作审计（Action Trail）记录管理员的操作日志。	堡垒机	堡垒机依赖云账号管理，支持对系统管理身份鉴别并对其操作进行审计。
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	阿里云控制台、RAM、配置审计	基于 RAM 授权系统管理员通过阿里云控制台对系统资源和运行进行配置，通过配置审计（Cloud Config）记录资源配置历史，并可基于资源配置数据完成合规性检测。	——	——
	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	阿里云控制台、RAM、操作审计	阿里云支持账号管理，支持基于 RAM 授权审计管理员进行安全审计，使用操作审计（Action Trail）记录管理的操作日志。	堡垒机	堡垒机依赖云账号管理，支持对审计管理员身份鉴别并对其操作进行审计。
		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策	操作审计	操作审计（Action Trail）支持短期审计记录和依托日志服务长期进行存储，支持操作时段、用户名、资	堡垒机、数据库审计	堡垒机依赖云账号管理，支持对审计记录进行查询、分析和管理，审计记录支持转存到日志服务中。

仅供阿里云用户安装使用禁止转载和宣传

安全层面	控制点	等级保护基本要求条款	阿里云云产品	云产品安全能力	阿里云云安全产品	云安全产品安全能力
		略对审计记录进行存储、管理和查询等。		源类型、资源名称、操作名称等维度来查询操作事件，对审计记录进行分析和管理。		
	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；	阿里云控制台、RAM、操作审计	阿里云支持账号管理，支持基于 RAM 授权安全管理员进行安全管理，通过操作审计（Action Trail）记录安全管理的操作日志。	安全产品管理	安全管理员基于安全控制台通过安全产品对云资源进行安全管理操作。
		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	——		安全产品管理 云安全中心	安全管理员可通过云安全中心进行基线核查、安全策略、访问控制策略统一配置。
	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；	VPC、RAM	通过云服务客户独立 VPC，建立独立安全管理区，基于 RAM 授权安全管理员对安全设备或安全组件进行管理和控制。	——	——
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；	——	阿里云支持全链路通信进行 SSL/TLS 安全加密处理，通过 Https 进行管理。	——	——
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；	云监控	云监控支持针对负载均衡、弹性 IP 地址、DDoS 高防、云服务器等运行状态创建监测规则，并进行集中监测和报警。	——	——
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；	操作审计、日志服务	操作审计（Action Trail）支持记录云服务客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云服务客户指定的日志服务中，可自定义留存时间。	云安全产品	云安全产品支持将自身采集安全审计记录在安全控制台上展示，并支持将审计记录统一保存到云服务客户指定的日志服务或存储空间，日志留存时间满足 6 个月。

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云 云产品	云产品安全能力	阿里云 云安全产品	云安全产品安全能力
		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；	配置审计	配置审计（Cloud Config）支持计算、存储、数据库、虚拟专用网络 VPC 等多类云产品的配置监控，持续记录资源的配置变更和配置历史，形成配置时间线。对资源的安全配置实现持续监控。	云安全中心	
		f）应能对网络中发生的各类安全事件进行识别、报警和分析；	——	——	云安全中心、 云防火墙、 Web 应用防火墙 DDoS 高防	1）云安全中心支持自动采集计算、数据库、负载均衡等等多种资产，收集多种日志数据，对重点安全威胁时管控，对各类安全事件进行识别、分析和告警，告警方式包括短信、邮件、钉钉等； 2）云防火墙通过威胁检测引擎，对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截； 3）Web 应用防火墙支持将 Web 流量引流到 WAF 上，由 WAF 将流量进行检测、过滤、清洗后再代理转发到应用服务器； 4）DDoS 高防通过引流的方式对所有业务流量进行清洗，支持网络四层和七层防护。

注：“--”表示无匹配该项基本要求条款的云产品和安全产品。

仅供阿里云用户参考使用，请勿私自传播和宣传

C.2 网络安全等级保护基本要求（云扩展要求）

安全层面	控制点	等级保护基本要求条款	阿里云云产品	云产品安全能力	阿里云云安全产品	云安全产品安全能力
安全区域边界	访问控制	a)应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； b)应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。	VPC 安全组	1）不同 VPC 间默认隔离，同一子网内默认互通，不同子网间可使用网络 ACL 进行安全控制， 2）不同 VPC 间默认隔离 ECS 安全组与 RDS/ECS/ SLB 的 IP 黑白名单支持虚拟网的隔离与访问控制。	云防火墙	1)云防火墙互联网边界防火墙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，访问控制粒度可达端口级; 2)云防火墙中 VPC 边界防火墙、互联网边界防火墙以及主机边界防火墙的访问控制用于检测和控制两个 VPC 间的通信流量、限制主机对内、外双向的未授权访问和 ECS 实例间的未授权访问。
	安全审计	a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；	操作审计 日志服务	操作审计（Action Trail）对云服务客户的云服务远程及本地管理进行审计，并基于日志服务保留审计记录。	堡垒机 云安全中心	1）堡垒机提供操作审计、职权管控、安全认证功能，记录所有运维操作记录、Linux 命令审计、Windows 操作录像； 2）云安全中心提供云服务客户所有资产安全事件综合分析的能力。
安全计算环境	身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。	RAM	云服务客户基于阿里云 RAM 授权和 AccessKey，通过密钥访问阿里云 API，如果双方均为合法证书则建立双向加密通道。	——	——
安全管理中心	集中管控	c)应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；	操作审计	操作审计（Action Trail）记录云账号对资源的操作日志，提供操作日志的查询和下载。	堡垒机 数据库审计	1）堡垒机对所有云服务客户的操作进行审计，操作系统自身日志本地保存； 2）数据库审计对数据库风险操作行为进行记录，提供细粒度审计数据库访问行为。

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	阿里云云产品	云产品安全能力	阿里云云安全产品	云安全产品安全能力
		d)应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。	云监控	云监控针对负载均衡、弹性 IP 地址、DDoS 高防、云服务器等运行状态创建监测规则，并进行集中监测和报警。	——	——
		b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标；	服务文本协议	阿里云各类云产品均为云服务客户提供服务等级协议。	——	阿里云各安全产品均提供服务等级协议。
		c)应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；			——	
		d)应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；			——	

注：“--”表示无匹配该项基本要求条款的云产品和安全产品。

仅供阿里云用户参考使用，请勿私自传播和宣传

C.3 网络安全等级保护基本要求（物联网扩展要求）

安全层面	控制点	等级保护基本要求条款	安全措施	阿里云物联网安全产品		阿里云物联网安全措施
安全区域边界	接入控制	a） 应保证只有授权的感知节点可以接入。	身份认证、访问控制	设备服务	IoT 设备身份认证（Link ID²）	1）ID²认证授权为物联设备/节点提供安全可信的身份认证服务； 2)ID²为每个感知节点设备分配唯一 ID，并生成唯一对应的 key，设备认证时同时提交 ID、使用 key 加密（挑战字/时间戳机制实现的唯一字段）后的密文，服务端进行可信验证，仅允许通过验证的设备接入。
	入侵防范	a） 应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。	访问控制、入侵检测	物联网安全服务	物联网安全运营中心（Link SOC）	1)Link SOC 安全基线检测支持识别超出设备行为预期的事件并采取相应的处置措施，阻止威胁事件； 2)Link SOC 支持限制接入设备的 IP 地址，并通过实时监测感知节点设备的网络行为，基于网络历史通信记录识别异常网络行为、提供分析工具自定义恶意行为模型、提供可视化分析工具生成感知节点的网络行为拓扑，限制与感知节点、网关节点通信的目标地址，在识别到陌生地址时，提供预警和防护措施，支持自动阻断。
		b） 应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。	访问控制、入侵检测		物联网安全运营中心（Link SOC）	
安全计算环境	感知节点设备安全	a） 应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。	授权	物联网安全服务	物联网可信执行环境-Link TEE（Trusted Execution Environment）	物联网可信执行环境 Link TEE（Trusted Execution Environment）在感知节点上提供独立于 OS 的可信环境，只允许授权用户/

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	安全措施	阿里云物联网安全产品		阿里云物联网安全措施
						授权应用通过 TA 对可信区域内的软件应用、数据进行访问、配置或变更。
		b） 应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力。	身份认证	设备服务	IoT 设备身份认证（Link ID²）	1）ID²认证授权为物联设备/节点提供安全可信的身份认证服务； 2）ID²为每个 IoT 设备提供唯一的身份标识，基于 ID²提供双向身份认证服务，为感知节点与网关节点的连接提供身份标识能力。
		c） 应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。	身份认证	设备服务	IoT 设备身份认证（Link ID²）	1）ID²认证授权为物联设备/节点提供安全可信的身份认证服务； 2）ID²为每个 IoT 设备提供唯一的身份标识，基于 ID²提供双向身份认证服务，为感知节点间的互联提供身份标识能力。
	网关节点设备安全	a） 应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力。	身份认证	设备服务	IoT 设备身份认证（Link ID²）	1）ID²认证授权为物联设备/节点提供安全可信的身份认证服务； 2）ID²支持为每个物联网节点设备（网关节点设备）分配一个全球唯一的 ID，并生成一个唯一对应的 key；节点设备认证的同时，节点设备认证的同时，提交 ID、使用 key 加密（挑战字/时间戳机制实现的唯一字段）后的密文，服务端进行身份验证和鉴别伪造设备。

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	安全措施	阿里云物联网安全产品		阿里云物联网安全措施
		b） 应具备过滤非法节点和伪造节点所发送的数据的能力。	身份认证	设备服务	IoT 设备身份认证（Link ID²）	1）ID²认证授权为物联设备/节点提供安全可信的身份认证服务； 2）节点设备认证通过后才可以与服务端建立起通信连接，未通过身份认证的节点不允许建立通信连接，提供阻断非法节点和伪造节点发送通信数据的能力。
		c） 授权用户应能够在设备使用过程中对关键密钥进行在线更新。	密钥更新	设备服务	IoT 设备身份认证（Link ID²）	1）ID²为 IoT 系统中的设备、应用、业务所使用的密钥提供集中管理，包括密钥生成、密钥销毁、端到端的密钥安全分发； 2）ID²支持基于设备的唯一 key 派生出数据加密的 key 和通信连接的 sessionkey，这些 key 支持用户根据业务需要进行在线更新。
		d） 授权用户应能够在设备使用过程中对关键配置参数进行在线更新。	配置参数更新	物联网安全服务	物联网安全运营中心（Link SOC）	Link SOC 安全基线检测支持对系统关键配置的周期性检查，监测系统关键配置的变更，授权用户通过从云端下发安全策略、自定义安全检查插件对设备的关键配置参数进行自定义配置。
	抗数据重放	a)应能够鉴别数据的新鲜性，避免历史数据的重放攻击。	身份认证	设备服务	IoT 设备身份认证（Link ID²）	KPM 基于 ID²主密钥派生的共享密钥，提供基于时间戳的动态密码服务，
		b） 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。	身份认证	设备服务	IoT 设备身份认证（Link ID²）	物联网设备身份认证系统 Link ID²（IoT Device ID），通过可信计算和密码技术为物联网系统提供设备安全认证能力。可信

仅供阿里云用户参考使用，请勿私自传播和宣传

安全层面	控制点	等级保护基本要求条款	安全措施	阿里云物联网安全产品		阿里云物联网安全措施
						根为每一次通信生成一条唯一的加密通道，每次通信使用不重复的派生 Session Key，防止非法节点的接入以及识别伪造节点、防止数据重放攻击。
	数据融合处理	a） 应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。	数据处理	物联网安全服务	物联网安全运营中心（Link SOC）	Link SOC 提供设备端的 SDK，支持 Linux、Android、RTOS 系统，基于 SDK 从感知节点、网络节点设备进行数据采集、数据整形处理，最终上传的数据都可以融合在同一平台中进行统一管理和使用。

注：基本要求物联网（第三级）扩展要求是针对物联网感知层提出特殊要求，包括 8 个控制点：感知节点设备物理防护、接入控制、入侵防范、感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理和感知节点管理，共计有 20 条基本要求项。

阿里云具备全面的物联网安全措施，附录 C.3 描述了阿里云物联网在网络等级保护 2.0 物联网扩展要求（安全技术）方面相关安全措施，更多详情可关注下列链接：

设备身份认证 **Link ID²**（Internet Device ID）：https://iot.aliyun.com/products/ID2

物联网安全运营中心 **Link SOC**（Security Operations Center）：https://iot.aliyun.com/products/linksoc

物联网可信执行环境 **Link TEE**（Trusted Execution Environment）：https://iot.aliyun.com/products/tee

仅供阿里云用户参考使用，请勿私自传播和宣传