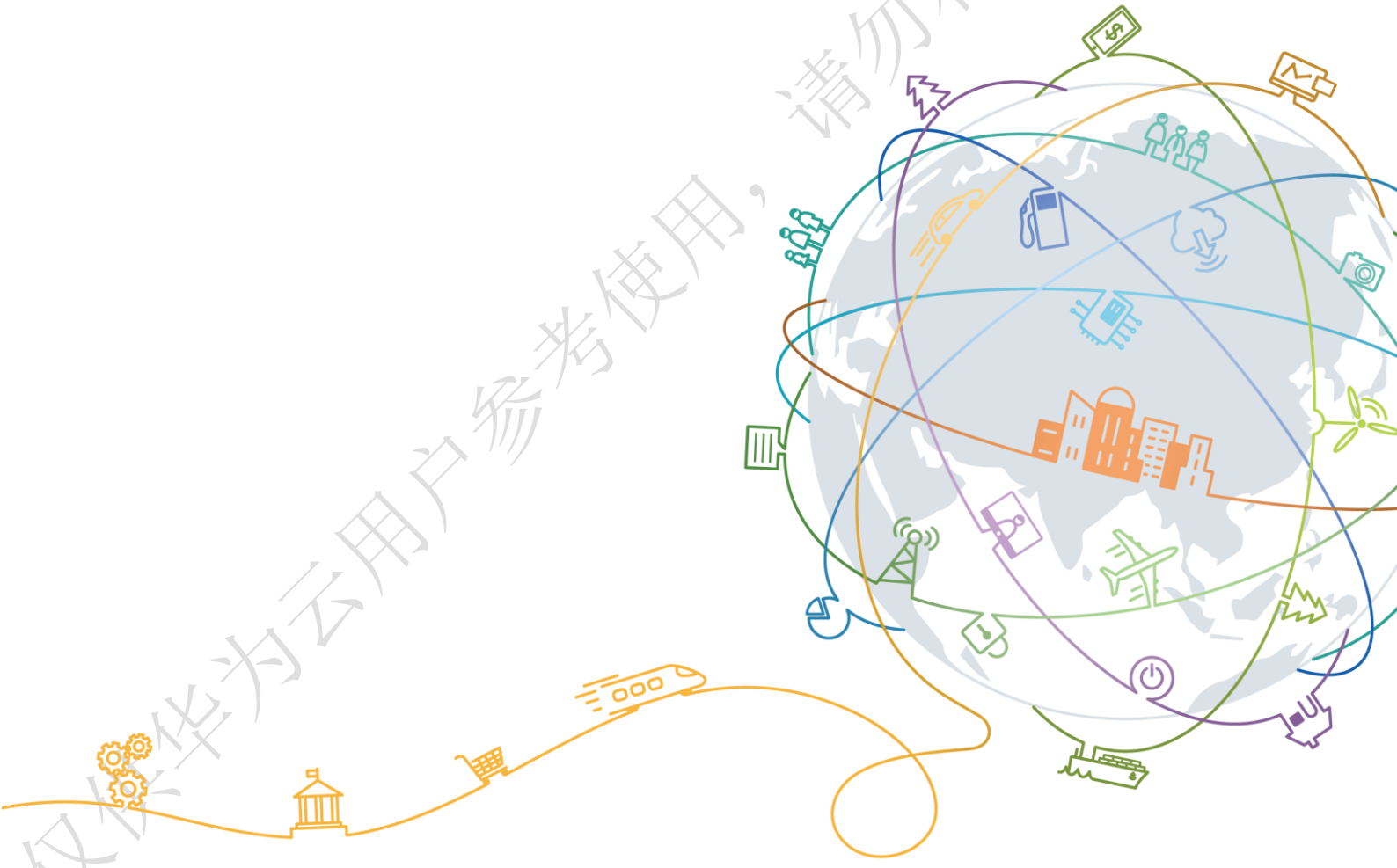
华为云网络安全等保 2.0 合规能力白皮书

文档版本 01

发布日期 2020-05-19



华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 总述 1
2 目的 2
3 安全合规责任 3
4 华为云安全合规与隐私保护能力模型 6
4.1 保护对象 6
4.2 安全措施 6
4.3 安全能力 8
4.3.1 云平台原生安全能力 8
4.3.2 云服务安全能力 8
4.3.3 云安全服务能力 9
4.3.4 云服务客户自建能力 9
4.4 安全合规评估 9
4.5 隐私保护 9
5 华为云对等保要求的解读 11
5.1 等级保护对象概述 11
5.2 等保基本合规要求分析（安全通用要求） 12
5.2.1 安全物理环境 12
5.2.2 安全通信网络 12
5.2.3 安全区域边界 16
5.2.4 安全计算环境 25
5.2.5 安全管理中心 43
5.2.6 安全管理制度 49
5.3 等保基本合规要求分析（云计算安全扩展要求） 49
5.3.1 安全通信网络 49
5.3.2 安全区域边界 52
5.3.3 安全计算环境 56
5.3.4 安全管理中心 65
5.3.5 安全建设管理 66
5.3.6 安全运维管理 70

6 华为云等保合规实践指引 71
6.1 等保实施指引 71
6.2 云服务客户在华为云上过等保的流程实践 74
6.3 云服务客户使用华为云满足等保要求的实践 75
6.3.1 安全区域边界 75
6.3.2 安全通信网络 76
6.3.3 安全管理中心 78
6.3.4 安全管理制度 78
7 附录 80
7.1 术语与定义： 80
7.2 参考标准与规范 83

主要撰写者

杨松、闻涛、赵洪日、李戬、魏宁、王欣洋、刘洪善

特别感谢

曹志源、宋好好、舒首衡、汤志明

1 总述

随着等保 2.0 的发布和执行，如何让业务在云上安全合规的运营成为网络运营者的刚需。借此，华为云推出《华为公有云网络安全等级保护 2.0 合规能力白皮书》（简称“白皮书”），将华为公有云（简称“华为云”）对等保 2.0 的理解和实践分享给用户和业界，以求相互了解，相互借鉴，共同推动云行业、云安全行业和等级保护合规领域的开放与发展。

2 目的

此白皮书适用于（但不限于）如下读者群体：

1. 上云或期望上云的企业的决策层，管理层，安全和隐私保护相关技术人员，以及其他相关岗位人员 (主要包括营销、采购/合同、合规审计等云服务相关人员)，以了解华为云如何满足客户上云后的等保需求；
2. 华为云的一般客户、生态伙伴，以了解华为云如何满足客户上云后的等保需求；
3. 安全从业者、等保从业者，以了解华为云在等保上的最佳实践；
4. 大中小型企业客户到个人用户，以了解华为云对等保的理解。

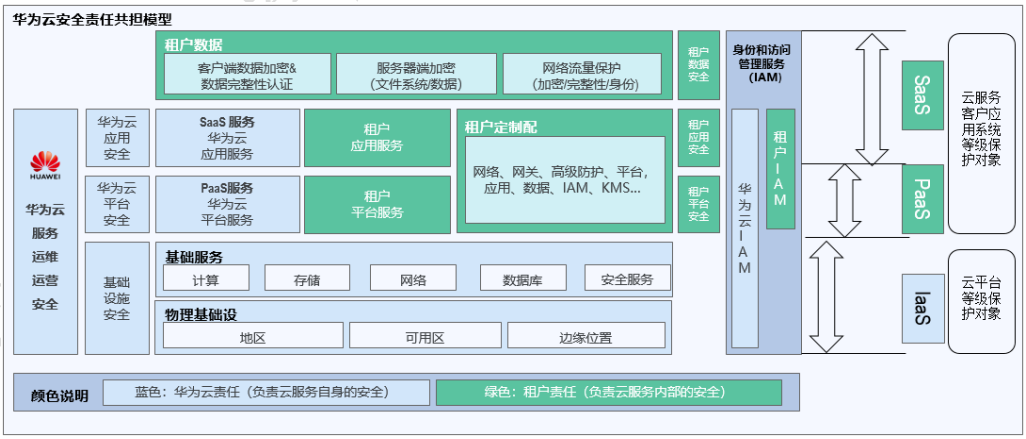
阅读本白皮书，你将会了解：

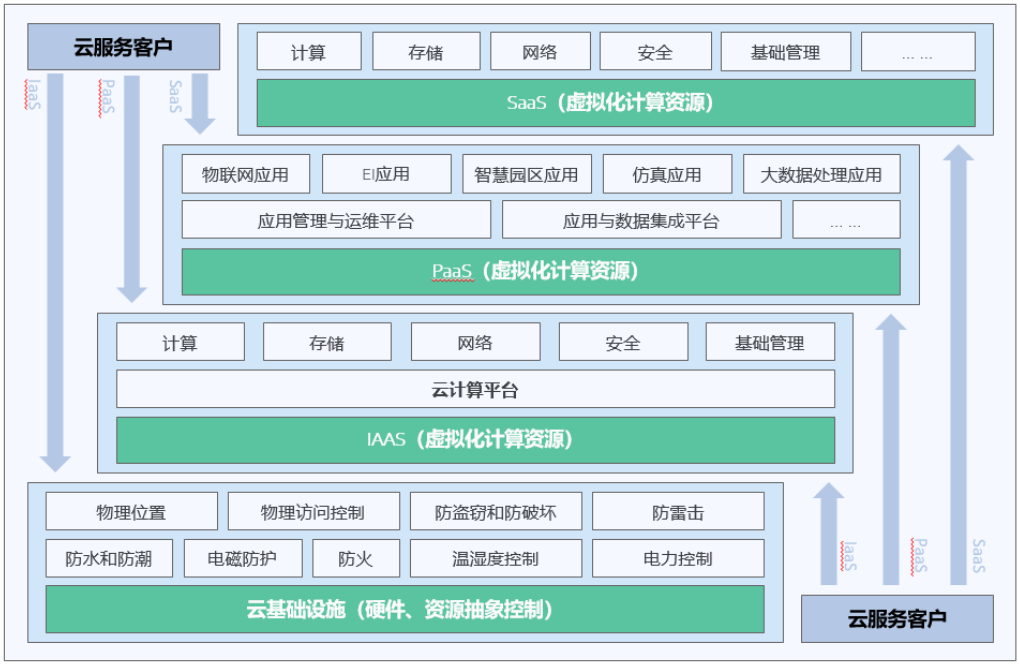
1. 如何确定不同云计算服务模式下的网络安全合规要求和责任边界；
2. 华为云为云服务客户提供的安全能力，包括云平台原生安全能力及云计算服务（包括云安全服务）提供的安全能力；
3. 云服务客户的业务系统，如何使用华为云提供的安全能力并根据业务系统自身的安全情况，满足等保要求；
4. 在合规的基础上，如何依托华为云的隐私保护体系和优秀实践，形成适合云服务客户业务需要的隐私保护体系。

3 安全合规责任

从传统数据中心的视角，云安全是指保护云服务本身在基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）中的技术资源的安全性，以确保各类云服务能够持续、高效、安全、稳定地运行。云服务与传统数据中心存在明显差异，前者对云安全整体设计和实践更侧重于为云服务客户提供完善的、多维度的、按需要任意定制、组合的各种安全和隐私保护功能和配置，涵盖基础设施、平台、应用及数据安全等各个层面。同时，不同的云安全服务又进一步为云服务客户提供了各类可自主配置的高级安全选项。这些云安全服务需要通过深度嵌入各层云服务的安全特性、安全配置和安全管控来实现，并通过可整合多点汇总分析的、日趋自动化的云安全运维运营能力来支撑。

华为云按业界常规做法定义的安全责任共担模型，云服务客户使用不同模式的云服务（IaaS、PaaS 或 SaaS）时，对资源的控制范围不同，如图 4-1 所示，图中两侧的箭头示意了华为云和云服务客户的控制范围。安全责任边界也根据控制范围的差异而有所不同。如下图：





如上两图所示，华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施、提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的立体安全防护体系，并保障其运维运营安全。

云服务客户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对云服务客户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，云服务客户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置、运维运营安全及用户身份的有效管理。

更详细的责任划分，见《华为云安全白皮书》。

技术/管理	大类	小类	三级条款数	IaaS模式	PaaS模式	SaaS模式
网络安全等级保护技术要求	通用部分	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
	云计算扩展	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
技术合计			133	83	71	67
网络安全等级保护管理要求	通用部分	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
	云计算扩展	安全建设管理	8	7	7	7
		安全运维管理	1	0	0	0
管理合计			124	122	119	118
技术+管理合计			257	205	190	185

依据上图所示，云服务客户在使用云计算的不同服务模式进行等级测评，各种服务模式下安全等级测评项数量分布有所不同， 云服务客户依据各服务模式的责任共担模型，需完成对应的测评项的安全建设与安全测评内容。

4 华为云安全合规与隐私保护能力模型

4.1 保护对象

4.2 安全措施

4.3 安全能力

4.4 安全合规评估

4.5 隐私保护

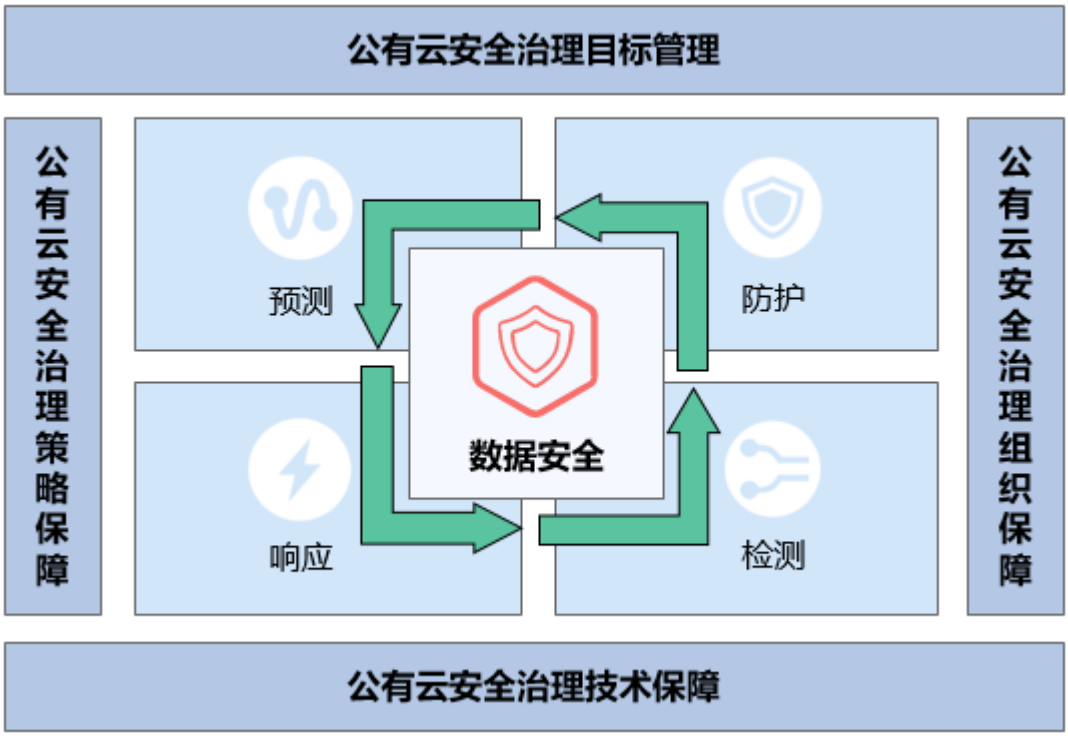
4.1 保护对象

根据云计算环境等级保护对象划分及公有云合规责任共担模型原则，云服务客户 可以基于部署的云计算服务模式确定业务系统的等级保护对象。

4.2 安全措施

华为云打造集预测、防护、检测、响应和恢复为一体的云数据安全保障体系，动态协同多种安全防御措施，保障云上数据安全。

图 5-1 华为云安全治理策略保障



预测

华为云构建了统一的分析和预警平台，全面掌握数据安全态势，快速识别、响应安全事件，同时通过对告警、事件、资产等信息的关联分析进行风险评估及安全态势预测，由此可预先制定安全防护策略，做到防范于未然。华为云构建了完善的漏洞管理体系，实现漏洞的感知、处置、披露等全流程的跟踪与管理，确保云计算平台各云服务和组件的漏洞得到及时的发现与修复，降低漏洞被恶意利用所带来的风险。

防护

- 物理和环境安全防护

  华为云严格遵从国际、国内相关标准要求，对数据中心进行合理的选址及设计施工，同时进行统一垂直管理，实施分层分级的安全防护，从围栏到 DC 建筑，从 DC 建筑到模块，从模块到机柜，从机柜到服务器，安全防护措施逐级增强，确保云数据中心的物理和环境安全。在严格执行物理访问控制的同时，通过智能的 7×24 小时监控，及时发现并修复安全隐患，确保数据中心稳定运行。

- 网络安全防护

  华为云帮助云服务客户构建网络安全防护体系，防止数据被窃取或泄露。

  华为云在互联网边界部署 Anti-DDoS 设备，来完成对异常和超大流量攻击的检测和清洗。同时在关键网络分区边界部署入侵防御设备，识别来自互联网及云服务客户间的攻击行为，并能够进行自动化、精确的阻断。

  所有云平台主机均安装安全防护软件，进行主机层面的弱密码检测、配置管理、入侵检测、应急响应等，构建合规、安全的主机环境。针对向外提供 Web 服务的系统，使用 Web 安全防护设备抵御应用层攻击行为，确保 Web 服务的安全。

- 运维管理

华为云制定并落实严格的规范、流程和管控措施，实现了运维操作的统一接入、统一认证、统一授权、统一审计。运维人员首先通过双因子认证接入运维环境，再集中从堡垒机跳转到目标机进行操作。目标机的口令被堡垒机回收并定期更新，确保运维人员无需也无法获取口令。严格的运维接入阻断了未授权的内部访问，是客户数据安全保护在关键环节。华为云对于运维人员实行基于角色的访问控制权限管理，限定不同岗位不同职责的人员只能对所授权的运维目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保运维人员不触碰云服务客户的数据。

检测

华为云联动分析各安全设备的告警信息，结合机器学习技术和专家经验构建相应的模型，检测未知数据安全风险，并及时采取有效措施进行防御。

华为云遵从法律法规要求，具备集中、完整的日志审计系统。内部人员运维操作均被日志平台采集并记录。华为云的日志审计系统有强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。华为云设置独立的内审部门，定期对运维流程各项活动进行审计，及时发现、纠正违规行为。

响应

华为云秉承快速发现、快速定界、快速隔离与快速恢复的“四快”原则，根据安全事件对全网及客户的影响，对事件进行分级响应。华为云设置 7*24 的专业安全事件响应团队及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会云服务客户，同时执行应急预案及恢复流程，降低业务影响。

4.3 安全能力

安全能力是指安全措施作用于保护对象而形成抵御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、云服务安全能力（包括云安全服务安全能力）及云服务客户自建安全能力。

4.3.1 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。

华为云云平台在物理安全、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良好基础。

4.3.2 云服务安全能力

云服务安全能力指云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）是云服务原生的，部分能力（如数据加密）需要云服务客户的开启和正确设置。

4.3.3 云安全服务能力

云安全服务安全能力主要指云服务提供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。

4.3.4 云服务客户自建能力

云服务客户自建能力指云服务客户基于业务需求对云服务能力的开启和正确配置及云服务客户根据自身业务需求自行建设的安全能力。

华为云为云服务客户提供的云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及时间响应等。

4.4 安全合规评估

华为云一如既往地确保其基础设施和云服务通过业界认可的独立第三方安全权威组织的测评及安全认证机构的审核，并且只向云服务客户提供运行于安全合规的基础设施之上的云服务。这些安全测评和认证向云服务客户展示华为云在基础设施和云服务的技术研发和运维运营中对流程、组织、技术等多方面制定的安全策略和安全风险管控措施，使得云服务客户能够深入了解华为云对用户数据保护和云上业务安全保障的有效管控能力。以华为云通过的云安全联盟 CSA STAR 金牌认证为例，该认证在 ISO/IEC 27001 的基础上，增加了云安全控制矩阵和其他安全要求，涵盖了风险治理、数据安全、应用安全、基础设施安全、开发和设计、身份和访问管理、数据中心安全、变更管理、配置管理、业务连续性管理、运营恢复能力、人力资源、供应链管理等方面的 16 个控制领域。

4.5 隐私保护

华为云秉承公司以网络安全和隐私保护为最高纲领，以国内外隐私保护的法律法规为基石，依托于华为公司的隐私保护体系，借鉴业界广泛认可的优秀实践，已形成适合华为云的隐私保护体系。华为云投入大量的专业人员和资源支撑新技术的研究和应用及保障隐私保护体系的有效运转，确保华为云的隐私保护处于行业领先的位置，实现华为云隐私保护的目标：遵守严格的服务边界，保护个人数据安全，助力云服务客户实现隐私保护。

华为云制定隐私保护七大原则（合法、正当、透明，目的限制，数据最小化，准确性，存储期限最小化，完整性与保密性，可归责），同时采用业界认可和先进的理念 PbD6（Privacy by Design）作为指导，结合华为云实际情况形成华为云隐私保护理念。隐私保护理念广泛应用在华为云的组织和人员管理、云平台个人数据安全管理及为客户提供的隐私服务等各个方面。同时，华为云使用 PIA7（Privacy Impact Assessment）识别隐私风险并采取恰当的方式消除或降低风险。华为云尊重用户的隐私权利，在官网明显处提供清晰的《隐私政策声明》及云服务客户反馈通道，帮助客户了解华为云隐私保护的信息。

说明

更多关于华为云隐私保护的政策和表述，可以在华为云的官方网站参考：
https://www.huaweicloud.com/securecenter/overallsafety.html。

5 华为云对等保要求的解读

5.1 等级保护对象概述

5.2 等保基本合规要求分析（安全通用要求）

5.3 等保基本合规要求分析（云计算安全扩展要求）

5.1 等级保护对象概述

等级保护对象是指网络安全等级保护工作中的对象。在华为云下基于安全责任共担模型及云计算环境网络安全等级保护的要求，云服务客户主要的安全责任包含：云服务客户业务系统网络边界、运维接入、应用安全、主机安全（包含虚拟机、数据库、中间件和镜像环境）、云服务客户应用系统的数据安全，云服务客户身份访问管理、云服务客户安全态势管理。

基于 IaaS 模式云服务客户业务部署典型合规场景下，华为云云服务客户开展等级保护安全能力建设时安全保护对象涉及到：

- 云服务客户网络边界：虚拟私有云 VPC，虚拟网络边界，负载均衡服务等；
- 云服务客户运维接入：云堡垒机接入；
- 云服务客户应用安全：云服务客户业务应用系统、云控制台；
- 云服务客户主机安全：虚拟机、操作系统、数据库；
- 云服务客户数据安全：业务数据、个人信息数据、业务配置数据、鉴别信息、审计数据等；
- 身份访问管理：云上业务场景的云服务客户、机构和公众用户的身份、访问级别和认证方式；
- 安全态势管理：云安全状态和安全威胁机制的全面监测和响应管理；
- 云服务客户安全管理：云服务客户系统运营单位主体安全管理机制情况。

5.2 等保基本合规要求分析（安全通用要求）

5.2.1 安全物理环境

华为云所有 Region 的安全保护等级为第三级。

华为云部分关键 Region、节点的安全保护等级为第四级。

云服务客户系统等级测评的安全物理环境部分可以沿用华为云平台安全保护等级测评报告结论。

请访问华为云工单系统申请最新的华为云云平台等级测评报告。

5.2.2 安全通信网络

网络架构

1. **应保证网络设备的业务能力满足业务高峰期需要**

- **【安全措施】**

  弹性负载均衡、网络弹性伸缩、网络性能监控。

- **【保护对象】**

  虚拟网络设备、云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  VPC 虚拟私有云：支持在云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务。

  弹性负载均衡：将访问流量根据转发策略分发到后端多台服务器的流量分发控制服务。弹性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，消除单点故障。

  云监控服务：为用户提供一个针对弹性云服务器、带宽等资源的监控平台。客户可监控云上的资源使用情况、业务的运行状况，并及时收到异常告警。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  通过 VPC、负载均衡进行网络资源配置，同时可通过云监控服务定期查看网络资源使用情况。

- **【合规满足度】**

  满足。

2. **应保证网络每个部分的带宽满足业务高峰期的需要**

- **【安全措施】**

  弹性负载均衡，网络带宽监控。

- **【保护对象】**

  云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  弹性负载均衡：将访问流量根据转发策略分发到后端多台服务器的流量分发控制服务。弹性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，消除单点故障。

  云监控服务：为用户提供一个针对弹性云服务器、带宽等资源的监控平台。客户可监控云上的资源使用情况、业务的运行状况，并及时收到异常告警。

- **【云安全产品满足度分析】**

  Anti-DDoS 流量清洗服务为弹性公网 IP 提供四到七层的 DDoS 攻击防护和攻击实时告警通知。同时，Anti-DDoS 可以提升用户带宽利用率，确保用户业务稳定运行。

- **【云服务客户自身安全能力建议】:**

  不涉及。

- **【合规满足度】**

  满足。

3. **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】**

  网络安全域划分、网络隔离。

- **【保护对象】**

  云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  VPC 虚拟私有云，VPC 支持在云上申请的隔离的、私密的虚拟网络环境。用户可以划分“DMZ”，“服务”，“数据”等区域，并使用安全组隔离 VPC 内的 IP 地址段、子网、安全组等子服务。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  用户需根据业务实际情况划分不同网络按区域，并配置 VPC 内的 IP 地址段、子网、安全组等。

- **【合规满足度】**

满足。

4. 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】**

  网络安全域划分、网络隔离、访问控制。

- **【保护对象】**

  云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  VPC 虚拟私有云：不同 VPC 之间通过隧道技术进行逻辑隔离，且不同 VPC 之间默认不能通信，但支持提供对等连接的方式，使用私有 IP 地址在两个 VPC 之间进行通信。

  同一 VPC 内支持用户定义安全组、VPN、IP 地址段、带宽等网络特性。用户可以通过 VPC 管理、配置内部网络，进行安全、快捷的网络变更。同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  用户需根据业务实际情况配置 VPC 内的 IP 地址段、子网、安全组等。

- **【合规满足度】**

  满足。

5. 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性

- **【安全措施】**

  网络设备冗余、网络链路冗余。

- **【保护对象】**

  云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  VPC 虚拟私有云：VPC 自身采用跨 Region，多节点方式部署，VPC 网络设备（如交换机、控制器等）采用集群部署确保所有链路冗余备份。

  弹性负载均衡：采用冗余设计，支持自动移除异常节点，并将流量在正常节点之间重新路由，确保云服务客户业务可用性。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

通信传输

1. 应采用校验技术或密码技术保证通信过程中数据的完整性

- **【安全措施】**

  数据传输加密。

- **【保护对象】**

  业务通信数据。

- **【云产品安全满足度分析】**

  虚拟专用网络（Virtual Private Network，以下简称 VPN）VPN，使用基于 Internet 的 IPsec 加密技术，构建 VPN 网关和用户本地数据中心的远端网关之间的加密的数据通信通道。

- **【云安全产品满足度分析】**

  SSL 证书服务可以提供 SSL 证书签发，便于用户部署对外发布基于 HTTPS 协议的 WEB 服务。

- **【云服务客户自身安全能力建议】**

  云服务客户需设置互联网访问加密配置（如 TLS），或使用 HTTPS 协议，加载网站 SSL 证书，保障互联网通信安全性和数据完整性。

- **【合规满足度】**

  满足。

2. 应采用密码技术保证通信过程中数据的保密性

- **【安全措施】**

  数据传输加密

- **【保护对象】**

  业务通信数据

- **【云产品安全满足度分析】**

  VPN 使用基于 Internet 的 IPsec 加密技术，构建 VPN 网关和用户本地数据中心的远端网关之间的加密的数据通信通道。

- **【云安全产品满足度分析】**

  SSL 证书管理服务可以提供 SSL 证书签发，便于用户部署对外发布基于 HTTPS 协议的 WEB 服务。

- **【云服务客户自身安全能力建议】**

  云服务客户需设置互联网访问加密配置（如 TLS），保障互联网通信安全性和数据完整性。

- **【合规满足度】**

  满足。

可信验证

1. **可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在应用程序的关键执行环境进行动态可信验证，并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**

   - **【安全措施】**

     不涉及。

   - **【保护对象】**

不涉及。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  非必选项，根据业内实际情况，此项暂不涉及。

5.2.3 安全区域边界

边界防护

1. **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】**

     网络访问控制。

   - **【保护对象】**

     虚拟网络设备、云服务客户业务系统网络边界。

   - **【云产品安全满足度分析】**

     VPC 虚拟私有云：VPC 支持在云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务。

     安全组：用户可配置具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     用户通过 VPC，及安全组的相关网络访问控制策略保证网络边界访问的安全性。

   - **【合规满足度】**

     满足。

2. **应能够对非授权设备私自联到内部网络的行为进行检查或限制**

   - **【安全措施】**

     网络访问控制。

   - **【保护对象】**

     云服务客户业务系统网络边界。

   - **【云产品安全满足度分析】**

     VPC 安全组：用户可配置具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则。

云堡垒机：可基于唯一身份标识的用户账户管理与访问控制策略，精细化的角色权限控制，与各服务器、网络设备、安全设备、数据库、应用系统进行连接管理，实现集中运维操作管理与审计。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户需部署云堡垒机针对运维场景下限制非授权设备连接内部网络行为进行限制和检查；同时配置 VPC 安全区进行相关非授权的网络连接。

- **【合规满足度】**

  满足。

3. **应能够对内部用户非授权联到外部网络的行为进行检查或限制**

   - **【安全措施】**

     网络访问控制。

   - **【保护对象】**

     云服务客户业务系统网络边界。

   - **【云产品安全满足度分析】**

     VPC 安全组：用户可在安全组中设置出方向规则，出方向规则会对安全组内部的云服务器出方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。

   - **【云安全产品满足度分析】**

     企业主机安全：可支持检测虚拟机的病毒木马非法外联到外部网络的异常链接，产生告警，并进一步阻断。

   - **【云服务客户自身安全能力建议】**

     云服务客户需配置 VPC 安全组进行相关非授权的网络连接限制。

   - **【合规满足度】**

     满足。

4. **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】**

     安全网络接入。

   - **【保护对象】**

     云服务客户业务系统网络边界。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】:**

     云服务客户根据业务系统实际应用场景和客户需求部署第三方无线网络控制相关产品保证无线网络接入的安全性。

   - **【合规满足度】**

云上系统不涉及，视客户实际业务场景而定。

访问控制

1. **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】**

     网络访问控制。
   - **【保护对象】**

     云服务客户业务系统网络边界。
   - **【云产品安全满足度分析】**

     VPC 安全组：用户可在安全组中设置网络出入方向规则，规则会对安全组内部的云服务器出入方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     云服务客户通过 VPC 及安全组的相关网络访问控制策略保证网络边界访问的安全性，同时建议在入方向不要配置 any-any 策略。
   - **【合规满足度】**

     满足。
2. **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】**

     网络访问控制。
   - **【保护对象】**

     云服务客户业务系统网络边界。
   - **【云产品安全满足度分析】**

     VPC 安全组：用户可以在安全组中定义各种访问规则，并支持安全组规则创建、删除、复制、导入/导出操作，实现访问控制规则的最优化配置。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     云服务客户通过安全组规则配置进行网络访问控制优化。
   - **【合规满足度】**

     满足。
3. **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**
   - **【安全措施】**

     网络访问控制。
   - **【保护对象】**

云服务客户业务系统网络边界。

- **【云产品安全满足度分析】**

  VPC 安全组：可支持基于出方向，入方向的源 IP 地址、目的 IP 地址、端口号、协议类型维度进行配置达到业务网络数据包的允许与拒绝进出。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户通过安全组规则配置进行网络数据包访问控制。

- **【合规满足度】**

  满足。

4. **应能根据会话状态信息为进出数据提供明确的允许/拒绝访问的能力。**

- **【安全措施】**

  网络访问控制。

- **【保护对象】**

  云服务客户业务系统网络边界。

- **【云产品安全满足度分析】**

  VPC 安全组：可支持基于出方向，入方向的源 IP 地址、目的 IP 地址、端口号、协议类型维度进行配置达到业务网络数据包的允许与拒绝进出。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户通过安全组规则配置（协议级）进行网络数据包访问控制。

- **【合规满足度】**

  满足。

5. **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】**

  网络访问控制。

- **【保护对象】**

  云服务客户业务系统网络边界。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  DDoS 高防（Advanced Anti-DDoS，AAD）可通过修改 DNS 解析或对外服务地址为高防 IP，将恶意攻击流量引流到高防 IP 清洗，保护对外 IP 地址不被攻击，确保重要业务不被攻击中断。支持四层和七层数据防护。

  WEB 应用防火墙通过将 HTTP 网络流量引入到 WAF 集群支持基于应用协议和应用内容的访问控制。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行 DDoS 高防和 WEB 应用防火墙的配置。

- **【合规满足度】**

  满足。

入侵防范

1. **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】**

     云服务客户业务系统网络边界。
   - **【云产品安全满足度分析】**

     不涉及。
   - **【云安全产品满足度分析】**

     WEB 应用防火墙通过将 HTTP 网络流量引入到 WAF 集群，通过 WAF 集群进行网络流量检测、防止或限制相关异常网络攻击。
   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行 DDoS 高防和 WEB 应用防火墙的配置。
   - **【合规满足度】**

     满足。
2. **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。
   - **【保护对象】**

     云服务客户业务系统网络边界。
   - **【云产品安全满足度分析】**

     不涉及。
   - **【云安全产品满足度分析】**

     态势感知（Situation Awareness）为用户提供统一的威胁检测和风险处置平台。态势感知能够帮助用户检测云上资产遭受到的各种安全风险。
   - **【云服务客户自身安全能力建议】**

     不涉及。
   - **【合规满足度】**

     满足。
3. **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】**

     云服务客户业务系统网络边界。
   - **【云产品安全满足度分析】**

不涉及。

- **【云安全产品满足度分析】**

  态势感知（Situation Awareness）支持检测出超过 20 大类的云上安全风险，包括 DDoS 攻击、暴力破解、Web 攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

4. **当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警**

   - **【安全措施】**

     入侵检测。

   - **【保护对象】**

     云服务客户业务系统网络边界。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     态势感知服务支持检测 DDoS 攻击、暴力破解、Web 攻击、后门木马、漏洞攻击、僵尸主机、异常行为、命令与控制等多种云上安全风险，同时“告警列表”提供告警威胁的统计信息列表，包括威胁告警的源 IP、攻击名称、攻击类型、攻击目标主机信息、攻击等级和攻击发生时间等信息。

     WEB 应用防火墙支持 HTTP/HTTPS 流量攻击检测，可支持记录攻击事件，攻击类型、攻击 URL，攻击源 IP 等信息，并产生相关告警。

     DDoS 高防（Advanced Anti-DDoS，AAD）在进行 DDoS 攻击防御时记录攻击事件、攻击类型、攻击 URL、攻击源 IP，攻击流量峰值，清洗防护结果等信息内容，并产生相关告警。

     企业主机安全支持检测 SSH、RDP、FTP、SQL Server、MySQL 等账户遭受的口令破解攻击，对识别出的攻击源 IP 封锁 24 小时，禁止其再次登录，防止主机因账户破解被入侵。根据账户破解防护信息，如“攻击源 IP”、“攻击类型”、“拦截时间”、“拦截次数”和“拦截状态”，您能够快速排查攻击主机的 IP，手动解除被拦截的可信 IP，同时产生相关告警。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

恶意代码和垃圾邮件防范

1. **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】**

  云服务客户业务系统网络边界。

- **【云安全产品满足度分析】**

  WEB 应用防火墙在防护引擎中预置丰富的攻击特征签名库，可检测多种通用 Web 攻击特征，并进行攻击拦击；攻击特征签名库根据攻击类型实时升级更新。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

2. **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】**

  云服务客户业务系统网络边界。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户可根据业务实际场景通过云市场购买部署第三方邮件服务相关产品。

- **【合规满足度】**

  视客户实际业务场景。

安全审计

1. **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】:** 云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  云审计提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

- **【云安全产品满足度分析】**

  WEB 应用防火墙可支持 HTTP 流量攻击防护，同时记录攻击事件，攻击类型、攻击 URL，攻击源 IP 等信息。

DDoS 高防（Advanced Anti-DDoS，AAD）在进行 DDoS 攻击防御时记录攻击事件、攻击类型、攻击 URL、攻击源 IP，攻击流量峰值，清洗防护结果等信息内容，并产生相关告警。

云堡垒机具备核心系统运维和安全审计管控功能，符合安全合规审查要求，提供安全统一的运维管理平台。

数据库安全审计提供旁路模式审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

2. **审计记录应包括事件的日期和时间、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】**

     云服务客户业务系统网络。

   - **【云产品安全满足度分析】**

     云审计服务提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。支持三类事件记录，包括全局事件、管理事件、数据事件。

   - **【云安全产品满足度分析】**

     WEB 应用防火墙可支持 HTTP 流量攻击防护，同时记录攻击时间、攻击事件、攻击类型、攻击源 URL、攻击源 IP、防护动作等日志审计信息。

     DDoS 高防在进行 DDoS 攻击防御时记录攻击事件、攻击类型、攻击 URL、攻击源 IP、攻击流量峰值、清洗防护结果等日志审计信息内容，并产生相关告警。

     云堡垒机具备核心系统运维和安全审计管控功能，支持记录相关操作审计信息包含：资源名称、类型、主机 IP、资源账户、起止时间、会话时长、会话大小、操作用户、操作用户来源 IP、操作用户来源 MAC、登录方式、运维记录、文件传输记录、会话协同记录等。

     数据库安全审计提供旁路模式审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警；包含记录用户行为审计操作记录及关联应用层和数据库层的访问操作记录。

   - **【合规满足度】**

     满足。

3. **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】**

     云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  云审计服务默认支持在服务界面中 7 天内的事件审计操作记录的存储和检索。同时可以支持操作审计日志记录转储至对象存储服务（OBS），转储后的事件文件将永久保存。

- **【云安全产品满足度分析】**

  WEB 应用防火墙，DDoS 高防，云堡垒机，数据库安全审计支持配套日志存储服务，支持服务的操作审计记录日志的永久存储和检索分析能力。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况使用华为云 OBS 进行相关日志的备份，同时控制删除权限。

- **【合规满足度】**

  满足。

4. **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】**

     云服务客户业务系统网络。

   - **【云产品安全满足度分析】**

     云审计服务提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

   - **【云安全产品满足度分析】**

     态势感知服务通过授权云日志服务（Log Tank Service，LTS）管理态势感知日志后，LTS 能提供准确实时采集、查询、分析和转储相关行为日志功能，帮助用户进行日志存储、导出、查询、分析等场景，满足日志存储 180 天及集中审计的要求。

     云堡垒机具备核心系统运维和安全审计管控功能，支持记录相关操作审计信息包含：资源名称、类型、主机 IP、资源账户、起止时间、会话时长、会话大小、操作用户、操作用户来源 IP、操作用户来源 MAC、登录方式、运维记录、文件传输记录、会话协同记录等。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行云服务的相关配置。

   - **【合规满足度】**

     满足。

可信验证

1. **可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在应用程序的关键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，并将验证结果形成的审计记录送至安全管理中心**

   - **【安全措施】**

     可信验证。

- **【保护对象】**

  云服务客户业务系统网络。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  非必选项，根据业内实际情况，此项暂不涉及。

5.2.4 安全计算环境

身份鉴别

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

   - **【安全措施】**

     身份认证，安全加固。

   - **【保护对象】**

     云服务客户业务计算环境。

   - **【云产品安全满足度分析】**

     统一身份认证提供华为云账户权限管理基础服务，支持云账号密码设置，如密码最小长度默认为 6 个字符，可以在 6~32 个字符之间设置；密码有效期策略，如用户在设置的时间内必须修改密码，否则密码将会失效，无法登录华为云；密码最短使用时间策略，如当用户密码修改后，再次修改密码时需要满足该策略设置的时间后才能修改。

   - **【云安全产品满足度分析】**

     云堡垒机支持相关密码配置，如密码长度必须为 8～32 个字符，且包含大小写字母、数字和特殊字符；强制新用户首次登录时修改密码；修改后的密码不能与前 N 次密码相同；配置账号密码的修改周期。

     态势感知服务支持主机口令复杂度策略检测，将主动检测主机中的口令复杂度策略，含有风险的账号及主机系统和关键软件中含有风险的配置信息。

   - **【云服务客户自身安全能力建议】**

     云服务客户需配置云服务器实例的账号安全策略，如配置登录凭证认证方式，SSH 密钥对登录，设置口令复杂度等。

     请参考云主机防暴力破解安全方案：
     https://www.huaweicloud.com/solutionattackPrevention/

   - **【合规满足度】**

   满足。

2. **应提供并启用登录失败处理功能，应配置结束会话、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】**

  身份认证，超时处理。

- **【保护对象】**

  云服务客户业务计算环境。

- **【云产品安全满足度分析】**

  统一身份认证提供华为云账户权限管理基础服务，支持配置会话超时策略，如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。

- **【云安全产品满足度分析】**

  云堡垒机支持登录失败处理，可以锁定登录失败账号，账号锁定一定时长后才能再次登录。

- **【云服务客户自身安全能力建议】**

  云服务客户需配置云服务器实例的账号安全策略，如配置登录失败处理措施等。

  请参考云主机防暴力破解安全方案：
  https://www.huaweicloud.com/solutionattackPrevention/

- **【合规满足度】**

  满足。

3. **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】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     华为云控制台，用户需使用 HTTPS 协议进行访问登录等操作。

     华为云提供基于加密 HTTPS 的 API Endpoint 调用。

     华为云内部服务之间的调用采用加密协议。

   - **【云安全产品满足度分析】**

     云堡垒机提供远程管理云服务器主机时，采用加密 SSH 方式进行远程登录。

     SSL 证书服务可以提供 SSL 证书签发，便于用户部署对外发布基于 HTTPS 协议的 WEB 服务。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

4. **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】**

     多因素认证。

   - **【保护对象】**

云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  华为云控制台支持虚拟 Multi-Factor Authentication(MFA)功能，此功能支持产生 6 位数字认证码的设备，遵循基于时间的一次性密码（TOTP）标准。华为云目前支持基于软件的虚拟 MFA，虚拟 MFA 应用程序可以在移动硬件设备（包括智能手机）上运行，用户可安装一个虚拟 MFA 应用程序后（例如：华为云 App、Google Authenticator 或 Microsoft Authenticator），绑定虚拟 MFA 设备。

- **【云安全产品满足度分析】**

  企业主机安全服务可开启云服务器实例的登录双因素认证，支持结合密码及验证码两种条件对用户登录云服务器实例的行为进行认证。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际需求，开启双因素认证相关服务和配置。

- **【合规满足度】**

  满足。

访问控制

1. **应对登录的用户分配账户和权限**

   - **【安全措施】**

     账号管理，权限管理。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据实际情况进行云控制台及业务系统的账号分配与权限管理。

   - **【合规满足度】**

     满足。

2. **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】**

     账号管理，权限管理。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

企业主机安全服务，支持检测主机系统中的账号，列出当前系统的账号信息，帮助用户进行账户安全性管理。

支持列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。

支持检测系统中的口令复杂度策略，并给出修改建议，帮助提升口令安全性。

支持检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改，防止账户口令被轻易猜解。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行重命名或删除默认账户，并修改默认账户口令。

- **【合规满足度】**

  满足。

3. **应及时删除或停用多余的、过期的账号，避免共享账号的存在**

   - **【安全措施】**

     账号管理，权限管理。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     企业主机安全服务，支持检测主机系统中的账号，列出当前系统的账号信息，帮助用户进行账户安全性管理；支持列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。

     云堡垒机支持对运维账号的管理，如删除无用账号，停用多余、过期运维账户。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行删除停用多余、过期账户避免共享账号的存在。

   - **【合规满足度】**

     满足。

4. **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】**

     账号管理，权限管理。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     企业主机安全服务，检测主机系统中的账号及账号权限信息，列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。

云堡垒机支持对云服务器主机、管理员账号、运维人员账号及权限变更的管理，能够细粒度地划分不同角色的权限，控制管理员对服务器的访问。

数据库安全服务，支持细粒度的帐户管理和权限控制，可以按照角色类型、表、视图对象、列等进行权限控制。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行账户的最小权限分配，并实现管理员账号的权限分离。

- **【合规满足度】**

  满足。

5. **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】**

  账号管理，权限管理。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

- **【云安全产品满足度分析】**

  云堡垒机支持对云服务器主机、管理员账号、运维人员账号及权限变更的管理，能够细粒度地划分不同角色的权限，控制管理员对服务器的访问。

  数据库安全服务，支持细粒度的帐户管理和权限控制，可以按照角色类型、表、视图对象、列等进行权限控制。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行访问控制策略设计与配置。

- **【合规满足度】**

  满足。

6. **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】**

  账号管理，权限管理。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

- **【云安全产品满足度分析】**

  云堡垒机支持对云服务器主机、管理员账号、运维人员账号及权限变更的管理，能够细粒度地划分不同角色的权限，控制管理员对服务器的访问。

数据库安全服务，支持细粒度的帐户管理和权限控制，可以按照角色类型、表、视图对象、列等进行权限控制。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行访问控制策略设计与配置。

- **【合规满足度】**

  满足。

7. **应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问**

- **【安全措施】**

  账号管理，权限管理。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  数据库安全服务，内置 PCI、HIPAA、SOX、GDPR 等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

安全审计

1. **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的安全事件进行审计**

- **【安全措施】**

  操作日志，安全审计。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  云审计提供对云服务客户账号的各种云资源操作记录的收集、存储和查询功能。

- **【云安全产品满足度分析】**

  云堡垒机提供提供针对云服务器实例的 Linux 命令审计和 Windows 操作录像来识别风险同时提供大数据智能审计功能，对所有运维操作进行审计、监控、控制和历史回放可追溯。

  企业主机安全服务支持检测并记录主机账户的异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。

  数据库安全审计提供旁路模式审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况开启并配置相关审计功能。

- **【合规满足度】**

  满足。

2. **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】**

  操作日志，安全审计。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  云审计服务提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。支持三类事件记录，包括全局事件、管理事件、数据事件。

- **【云安全产品满足度分析】**

  云堡垒机具备核心系统运维和安全审计管控功能，支持记录相关操作审计信息包含：资源名称、类型、主机 IP、资源账户、起止时间、会话时长、会话大小、操作用户、操作用户来源 IP、操作用户来源 MAC、登录方式、运维记录、文件传输记录、会话协同记录等。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况开启并配置相关审计功能。

- **【合规满足度】**

  满足。

3. **应对审计记录进行保护，定位备份，避免受到未预期的删除、修改或覆盖等**

- **【安全措施】**

  操作日志，安全审计。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  云审计服务默认支持在服务界面中 7 天内的事件审计操作记录的存储和检索，同时支持操作审计日志记录转储至对象存储服务（OBS），转储后的事件文件将永久保存。

- **【云安全产品满足度分析】**

  云堡垒机，数据库安全审计支持配套日志存储服务，支持服务的操作审计记录日志的永久存储和检索分析能力。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况开启并配置相关审计功能。

- **【合规满足度】**

  满足。

4. **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，安全授权。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  云审计服务支持对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

  通过**云监控服务**监控云上的资源使用情况、业务的运行状况，防止由于各种原因引起的进程中断，并及时产生异常告警。

- **【云安全产品满足度分析】**

  云堡垒机支持实时日志转储至日志服务或 OBS 对象存储，支持服务的操作审计记录日志永久存储和检索分析能力。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况开启并配置相关审计功能和监控告警功能。

- **【合规满足度】**

  满足。

入侵防范

1. **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】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     华为云镜像服务中公共镜像覆盖华为自研 EulerOS 操作系统，及 Windows Server、Ubuntu、CentOS 等多款主流操作系统，皆以正版授权，均经过严格测试，同时遵守业界统一规范，除了预装了初始化组件外，内核能力均由第三方厂商提供。

   - **【云安全产品满足度分析】**

     企业主机安全支持对主机系统进行安全评估，将系统存在的各种风险（账户、端口、软件漏洞、弱口令等）进行展示，提示用户及时加固，消除安全隐患；支持对常见的 Tomcat 配置、Nginx 配置、SSH 登录配置进行检查，帮助用户识别不安全的配置项。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况按照所需要的组件和应用程序。

   - **【合规满足度】**

     满足。

2. **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】**

  云服务客户业务网络环境，云服务客户业务计算环境。

- **【云产品安全满足度分析】**

  华为云镜像服务中公共镜像覆盖华为自研 EulerOS 操作系统，及 Windows Server、Ubuntu、CentOS 等多款主流操作系统，皆以正版授权，均经过严格测试，同时遵守业界统一规范，除了预装了初始化组件外，内核能力均由第三方厂商提供。

- **【云安全产品满足度分析】**

  企业主机安全支持检测主机系统中的端口，列出当前系统开放的端口列表，帮助用户识别出其中的危险端口和未知端口。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况关闭不需要的系统服务、默认共享、关闭高危端口。

- **【合规满足度】**

  满足。

3. **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】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

     VPC 安全组可支持基于出方向，入方向的源 IP 地址、目的 IP 地址、端口号、协议类型维度进行配置达到业务网络数据包的允许与拒绝进出。

   - **【云安全产品满足度分析】**

     云堡垒机支持对云服务器主机、管理员账号、运维人员账号及权限变更的管理，能够细粒度地划分不同角色的权限，控制管理员对服务器的访问。

   - **【云服务客户自身安全能力建议】:**

     云服务客户根据业务实际情况进行访问终端限制的配置。

   - **【合规满足度】**

     满足。

4. **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】**

     有效性校验。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  华为云提供的云控制台和基于加密 HTTPS 的 API Endpoint 调用，均支持对输入参数有效性校验等安全措施。

- **【云安全产品满足度分析】**

  WEB 应用防火墙支持对 URL 自动还原常见编码，识别变形攻击，所支持还原的编码类型：url_encode、Unicode、xml、C-OCT、十六进制、html 转义、base64、大小写混淆、javascript/shell/php 等拼接混淆。

- **【云服务客户自身安全能力建议】**

  云服务客户的业务系统需保证数据有效性检验功能，保证接口输入内容符合系统要求。

- **【合规满足度】**

  满足。

5. **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，漏洞修复。

- **【保护对象】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  华为云镜像服务中公共镜像覆盖华为自研 EulerOS 操作系统，及 Windows Server、Ubuntu、CentOS 等多款主流操作系统，皆以正版授权，均经过严格测试，同时遵守业界统一规范，除了预装了初始化组件外，内核能力均由第三方厂商提供。

- **【云安全产品满足度分析】**

  企业主机安全支持包括 Linux 软件漏洞和 Windows 系统漏洞的检测与修复；通过与漏洞库进行比对，检测出系统和官方软件（非绿色版、非自行编译安装版；例如：SSH、OpenSSL、Apache、Mysql 等）存在的漏洞，帮助用户识别出存在的风险。

  漏洞扫描服务支持针对服务器或网站进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理、自定义扫描多项服务。

  安全专家服务提供**网站安全体检**检测网站威胁，覆盖 SQL 注入、XSS 跨站、文件上传/下载/包含、敏感信息泄露、弱口令等。

  主机安全体检通过日志分析、漏洞扫描等识别主机威胁，通过基线检查发现主机 OS、中间件的错误配置、不合规项和弱口令等风险。

- **【云服务客户自身安全能力建议】**

  云服务客户需根据实际业务需求制定漏洞扫描策略进行漏洞扫描，并对扫描的漏洞进行修复。

- **【合规满足度】**

  满足。

6. **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】**

  云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  态势感知服务支持检测 DDoS 攻击、暴力破解、Web 攻击、后门木马、漏洞攻击、僵尸主机、异常行为、命令与控制等多种恶意代码检测，及隔离清除。

  WEB 应用防火墙通过将 HTTP 网络流量引入到 WAF 集群，通过 WAF 集群进行网络流量检测、防止或限制相关异常网络攻击。

  数据库安全防护支持用户自定义配置防火墙策略、自动学习策略及基于异常检测的 IDS/IPS 策略，当请求到达数据库防火墙且违反策略时，数据库安全防护会根据用户需求选择实时告警或阻断。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

恶意代码防范

1. **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】**

     恶意代码防范。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     企业主机安全支持通过程序特征、行为检测，结合 AI 图像指纹算法及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

可信验证

1. **可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在应用程序的关键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，并将验证结果形成的审计记录送至安全管理中心**

   - **【安全措施】**

可信验证。

- **【保护对象】**

  云服务客户业务计算环境。

- **【云产品安全满足度分析】**

  不涉及。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  非必选项，根据业内实际情况，此项暂不涉及。

数据完整性

1. **应采用检验技术或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】**

     数据传输加密。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     华为云控制台，用户需使用 HTTPS 协议进行访问登录等操作。同时支持访问密钥（Access Key ID/Secret Access Key，简称 AK/SK），通过开发工具（API、CLI、SDK）访问华为云时的身份凭证，系统通过 AK 识别访问用户的身份，通过 SK 进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

     华为云提供基于加密 HTTPS 的 API Endpoint 调用，接口之间调用使用消息认证码（MAC）对消息内容进行完整性保护，同时，对于重要的接口消息实现抗重放攻击机制。

     华为云内部服务之间的调用采用加密协议，保证数据传输过程中的数据完整性。

   - **【云安全产品满足度分析】**

     云堡垒机提供远程管理云服务器主机时，采用加密 SSH 方式进行远程登录。

     SSL 证书服务可以提供 SSL 证书签发，便于用户部署对外发布基于 HTTPS 协议的 WEB 服务。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据自身业务实际情况实现业务传输通道加密。

   - **【合规满足度】**

     满足。

2. **应采用检验技术或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】**

     数据存储加密。

   - **【保护对象】**

     云服务客户业务网络环境，云服务客户业务计算环境，云控制台。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     云硬盘支持对新创建的云硬盘进行加密。加密云硬盘使用的密钥由数据加密服务（DEW，Data Encryption Workshop）中的密钥管理（KMS，Key Management Service）功能提供。

     镜像服务支持创建加密镜像来提升数据安全性，加密方式为 KMS 的信封加密。外部镜像文件或者加密云服务器均可用来创建加密镜像。

     对象存储服务支持将数据加密后存储到 OBS 中，提高数据的安全性。OBS 提供 SSE-KMS 和 SSE-C 两种服务端加密方式。

     数据加密服务提供华为云上数据加密服务，提供专属加密、密钥管理、密钥对管理等服务，包含数据安全、密钥安全、密钥管理，及签名验签的相关功能，对于重要数据实现数字签名校验失败处理。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据自身业务实际情况实现业务数据存储加密功能。

   - **【合规满足度】**

     满足。

数据保密性

1. **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、重要商务数据和重要个人信息等；**

   - **【安全措施】**

     传输加密。

   - **【保护对象】**

     应用系统业务数据，重要个人信息。

   - **【云产品安全满足度分析】**

     华为云控制台，用户需使用 HTTPS 协议进行访问登录等操作。同时支持访问密钥（Access Key ID/Secret Access Key，简称 AK/SK），通过开发工具（API、CLI、SDK）访问华为云时的身份凭证，系统通过 AK 识别访问用户的身份，通过 SK 进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

   - **【云安全产品满足度分析】**

     云堡垒机提供远程管理云服务器主机时，采用加密 SSH 方式进行远程登录。

SSL 证书服务可以提供 SSL 证书签发，便于用户部署对外发布基于 HTTPS 协议的 WEB 服务。

数据加密服务提供华为云上数据加密服务，提供专属加密、密钥管理、密钥对管理等服务，包含数据安全、密钥安全、密钥管理的相关功能。

- **【云服务客户自身安全能力建议】**

  云服务客户根据自身业务实际情况实现业务传输通道加密。

- **【合规满足度】**

  满足。

2. **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】**

  数据存储加密。

- **【保护对象】**

  应用系统业务数据，重要个人信息。

- **【云产品安全满足度分析】**

  云硬盘支持对新创建的云硬盘进行加密。加密云硬盘使用的密钥由数据加密服务（DEW，Data Encryption Workshop）中的密钥管理（KMS，Key Management Service）功能提供。

  镜像服务支持创建加密镜像来提升数据安全性，加密方式为 KMS 的信封加密。外部镜像文件或者加密云服务器均可用来创建加密镜像。

  对象存储服务支持将数据加密后存储到 OBS 中，提高数据的安全性。OBS 提供 SSE-KMS 和 SSE-C 两种服务端加密方式。

- **【云安全产品满足度分析】**

  数据加密服务提供华为云上数据加密服务，提供专属加密、密钥管理、密钥对管理等服务，包含数据安全、密钥安全、密钥管理的相关功能。

- **【云服务客户自身安全能力建议】**

  云服务客户根据自身业务实际情况实现业务数据存储加密功能。

- **【合规满足度】**

  满足。

数据备份恢复

1. **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，数据恢复。

- **【保护对象】**

  应用系统业务数据，重要个人信息。

- **【云产品安全满足度分析】**

  云硬盘的存储系统采用三副本机制来保证数据的可靠性，即针对某份数据，默认将数据分为 1 MB 大小的数据块，每一个数据块被复制为 3 个副本，然后按照分布式存储算法将这些副本保存在集群中的不同节点上。

对象存储服务支持创建桶时开启多 AZ 属性，用户数据冗余存储至多个 AZ 中。同时支持通过跨区复制功能，用户可以将一个区域的桶中数据复制到另一个区域，实现云端备份；将 OBS 中的数据下载到本地进行本地备份数据。

云镜像服务支持备份系统盘。可以将本地或者其他云平台的服务器数据盘镜像文件导入至镜像服务中。

云数据库服务支持每天自动备份数据，上传到对象存储服务（Object Storage Service，简称 OBS）。备份文件保留 732 天，支持一键式恢复。用户可以设置自动备份的周期，还可以根据自身业务特点随时发起备份，选择备份周期、修改备份策略；支持按备份集和指定时间点的恢复。在大多数场景下，用户可以将 732 天内任意一个时间点的数据恢复到华为云关系型数据库新实例或已有实例上，数据验证无误后即可将数据迁回华为云关系型数据库主实例，完成数据回溯；华为云关系型数据库服务采用热备架构，故障秒级自动切换。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行数据备份。

- **【合规满足度】**

  满足。

2. **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，数据恢复。

- **【保护对象】**

  应用系统业务数据，重要个人信息。

- **【云产品安全满足度分析】**

  云硬盘的存储系统采用三副本机制来保证数据的可靠性，即针对某份数据，默认将数据分为 1 MB 大小的数据块，每一个数据块被复制为 3 个副本，然后按照分布式存储算法将这些副本保存在集群中的不同节点上。

  对象存储服务支持创建桶时开启多 AZ 属性，用户数据冗余存储至多个 AZ 中。同时支持通过跨区复制功能，用户可以将一个区域的桶中数据复制到另一个区域，实现云端备份；将 OBS 中的数据下载到本地进行本地备份数据。

  云镜像服务支持备份系统盘。可以将本地或者其他云平台的服务器数据盘镜像文件导入至镜像服务中。

  云备份功能可以为云内的云服务器、云硬盘、云下 VMware 虚拟化环境，提供简单易用的备份服务，针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点，支持跨 Region 复制备份数据，可在异地 Region 恢复，实现异地灾备。

  云数据库服务支持每天自动备份数据，上传到对象存储服务（Object Storage Service，简称 OBS），OBS 可以支持跨 Region 存储。备份文件保留 732 天，支持一键式恢复。用户可以设置自动备份的周期，还可以根据自身业务特点随时发起备份，选择备份周期、修改备份策略；支持按备份集和指定时间点的恢复。在大多数场景下，用户可以将 732 天内任意一个时间点的数据恢复到华为云关系型数据库新实例或已有实例上，数据验证无误后即可将数据迁

回华为云关系型数据库主实例，完成数据回溯；华为云关系型数据库服务采用热备架构，故障秒级自动切换。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行数据异地备份。

- **【合规满足度】**

  满足。

3. **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】**

  数据冗余处理。

- **【保护对象】**

  应用系统业务数据，重要个人信息。

- **【云产品安全满足度分析】**

  华为云依赖数据中心集群的二地三中心架构实现数据中心本身的容灾和备份，数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。同时，两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一数据中心故障的情况下，也可以将流量负载均衡到其他中心。

  华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。 每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

剩余信息保护

1. **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】**

  剩余数据删除与销毁。

- **【保护对象】**

  应用系统业务数据，重要个人信息。

- **【云产品安全满足度分析】**

  华为云平台数据删除与销毁机制：在用户确认删除数据后，华为云会彻底删除用户数据，确保数据不泄露。

内存删除：华为云在云操作系统将内存重新分配给用户之前，会对分配的内存进行清零操作，即写“零”处理，防止通过物理内存恢复删除数据造成的数据泄露。

加密数据防泄露：华为云建议云服务客户对要上云的重要数据进行加密存储，数据需要删除时，通过直接删除相关数据加密密钥，防止数据在被彻底删除前被恢复为明文后造成泄露。

存储数据删除：当云服务客户删除数据时，数据和对应的元数据在系统中一并删除，底层存储区域被回收以供系统重新覆盖写入，数据无法再被读取。但是针对客户误删除的操作场景，通过 EVS 服务的回收站功能、OBS 服务的多版本控制功能，用户可以最终决定数据的恢复或彻底删除。

磁盘数据删除：华为云对删除虚拟卷采用清零措施，确保数据不可恢复，有效防止被恶意云服务客户使用数据恢复软件读出磁盘数据，杜绝信息泄漏风险。

物理磁盘报废：当物理磁盘报废时，华为云通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户隐私和数据不受未授权访问。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

2. **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】**

  剩余数据删除与销毁。

- **【保护对象】**

  应用系统业务数据，重要个人信息。

- **【云产品安全满足度分析】**

  华为云提供云数据迁移服务（CDM），支持在多种类型数据源之间进行数据迁移，例 如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上 云、云中数据交换、数据回流本地数据中心等多种业务场景需求。

  客户内容数据销毁在客户内容数据的销毁阶段，华为云会对指定的数据及其所有副本进行全面的清除。 当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、 块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。 对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式 进行数据清除，确保其上的数据无法恢复。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】:**

  不涉及。

- **【合规满足度】**

  满足。

个人信息保护

1. **应仅采集和保存业务必需的用户个人信息**

   - **【安全措施】**

     个人隐私保护。

   - **【保护对象】**

     用户个人隐私数据。

   - **【云产品安全满足度分析】**

     华为云建立完善、规范和统一隐私保护体系确保云平台的隐私保护得以实现，并帮助客户实施隐私保护。华为云制定隐私保护七大原则（合法、正当、透明，目的限制，数据最小化，准确性，存储期限最小化，完整性与保密性，可归责），同时采用业界认可和先进的理念 PbD6（Privacy by Design）作为指导，结合华为云实际情况形成华为云隐私保护理念。隐私保护理念广泛应用在华为云的组织和人员管理、云平台个人数据安全管理及为客户提供的隐私服务等各个方面。同时，华为云使用 PIA7（Privacy ImpactAssessment）识别隐私风险并采取恰当的方式消除或降低风险。华为云尊重用户的隐私权利，在官网明显处提供清晰的《隐私政策声明》及客户反馈通道，帮助客户了解华为云隐私保护的信息。

     华为云研究团队同时致力研发各类隐私增强技术（PET－ Privacy Enhancing Technology），积累隐私保护工程技术能力，以满足客户不同需要实施隐私保护。华为云现已拥有的一系列 PET，包括等价类匿名、差分隐私、防跟踪技术、区块链私人支付及隐私保存计算等。

   - **【云安全产品满足度分析】**

     数据库安全防护服务内置 PCI、HIPAA、SOX、GDPR 等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据。一旦识别了敏感数据，用户就可以一键自动生成脱敏规则和审计规则。

   - **【云服务客户自身安全能力建议】**

     云服务客户应根据业务实际情况采集和保存业务必需的用户个人信息。

   - **【合规满足度】**

     满足。

2. **应禁止未授权访问和非法使用用户个人信息**

   - **【安全措施】**

     个人隐私保护。

   - **【保护对象】**

     用户个人隐私数据。

   - **【云产品安全满足度分析】**

     华为云建立完善、规范和统一隐私保护体系确保云平台的隐私保护得以实现，并帮助客户实施隐私保护。华为云制定隐私保护七大原则（合法、正当、透明，目的限制，数据最小化，准确性，存储期限最小化，完整性与保

密性，可归责），同时采用业界认可和先进的理念 PbD6（Privacy by Design）作为指导，结合华为云实际情况形成华为云隐私保护理念。隐私保护理念广泛应用在华为云的组织和人员管理、云平台个人数据安全管理及为客户提供的隐私服务等各个方面。同时，华为云使用 PIA7（Privacy ImpactAssessment）识别隐私风险并采取恰当的方式消除或降低风险。华为云尊重用户的隐私权利，在官网明显处提供清晰的《隐私政策声明》及客户反馈通道，帮助客户了解华为云隐私保护的信息。

- **【云安全产品满足度分析】**

  数据库安全防护服务内置 PCI、HIPAA、SOX、GDPR 等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据。一旦识别了敏感数据，用户就可以一键自动生成脱敏规则和审计规则。

- **【云服务客户自身安全能力建议】**

  云服务客户应根据业务实际情况建立响应个人信息保护机制。

- **【合规满足度】**

  满足。

5.2.5 安全管理中心

系统管理

1. **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】**

     身份鉴别，操作审计。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

     云审计提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

   - **【云安全产品满足度分析】**

     云堡垒机支持对云服务器主机、管理员账号、运维人员账号及权限变更的管理，能够细粒度地划分不同角色的权限，控制管理员对服务器的访问。

   - **【云服务客户自身安全能力建议】**

     云服务客户应根据业务实际情况对账户进行用户权限访问设计与管理。

   - **【合规满足度】**

     满足。

2. **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】**

  身份鉴别，操作审计。

- **【保护对象】**

  云服务客户业务计算环境，云服务客户业务网络环境。

- **【云产品安全满足度分析】**

  统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

- **【云安全产品满足度分析】**

  云堡垒机支持集中账号管理，建立基于唯一身份标识的全局用户账户管理，支持统一账号管理策略，实现与各服务器、网络设备、安全设备、应用系统和数据库服务器等无缝连接。同时支持集中访问控制，通过访问控制策略和命令控制策略，基于最小权限原则，实现集中有序的运维操作管控。

- **【云服务客户自身安全能力建议】**

  云服务客户应根据业务实际情况对业务系统进行系统资源管理。

- **【合规满足度】**

  满足。

审计管理

1. **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**

   - **【安全措施】**

     身份鉴别，操作审计。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境，云控制台。

   - **【云产品安全满足度分析】**

     统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

     云审计提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询和审计功能。

   - **【云安全产品满足度分析】**

     云堡垒机提供提供针对云服务器实例的 Linux 命令审计和 Windows 操作录像来识别风险同时提供大数据智能审计功能，对所有运维操作进行审计、监控、控制和历史回放可追溯。

   - **【云服务客户自身安全能力建议】**

     云服务客户应根据业务实际情况对账户进行用户权限访问设计与管理。

   - **【合规满足度】**

     满足。

2. **应通过审计管理员对审计记录进行分析，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】**

  操作审计。

- **【保护对象】**

  云服务客户业务计算环境，云服务客户业务网络环境。

- **【云产品安全满足度分析】**

  云审计提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

- **【云安全产品满足度分析】**

  云堡垒机，数据库安全审计支持实时日志转储至日志服务或 OBS 对象存储，支持服务的操作审计记录日志永久存储和检索分析能力。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行云服务的相关配置。

- **【合规满足度】**

  满足。

安全管理

1. **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**

   - **【安全措施】**

     身份认证，账号管理，操作审计。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     统一身份认证服务，支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

     云审计提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询和审计功能。

   - **【云安全产品满足度分析】**

     云堡垒机，可基于唯一身份标识的用户账户管理与访问控制策略，精细化的角色权限控制，与各服务器、网络设备、安全设备、数据库、应用系统进行连接管理，实现集中运维操作管理与审计

   - **【云服务客户自身安全能力建议】**

     云服务客户应根据业务实际情况对账户进行用户权限访问设计与管理。

   - **【合规满足度】**

     满足。

2. **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】**

     身份认证，账号管理。

- **【保护对象】**

  云服务客户业务计算环境，云服务客户业务网络环境。

- **【云产品安全满足度分析】**

  统一身份认证服务：支持公有云用户账号权限管理、安全访问、二次认证、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

- **【云安全产品满足度分析】**

  云堡垒机：可基于唯一身份标识的用户账户管理与访问控制策略，精细化的角色权限控制，与各服务器、网络设备、安全设备、数据库、应用系统进行连接管理，实现集中运维操作管理与审计。

  数据库安全服务：内置 PCI、HIPAA、SOX、GDPR 等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据

- **【云服务客户自身安全能力建议】**

  云服务客户应根据业务实际情况对账户进行用户权限访问设计与管理。

- **【合规满足度】**

  满足。

集中管控

1. **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】**

     管理域网络划分。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     VPC 虚拟私有云：支持用户定义安全组、VPN、IP 地址段、带宽等网络特性。用户可以通过 VPC 管理、配置内部网络，进行安全、快捷的网络变更；同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务自身情况设计并规划网络管理区域。

   - **【合规满足度】**

     满足。

2. **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】**

     传输加密。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境。

- **【云产品安全满足度分析】**

  华为云内部服务之间的调用采用加密传输通道(TLS/SSL)，同时提供基于加密 HTTPS 的 API Endpoint 调用。

- **【云安全产品满足度分析】**

  虚拟专用网络服务通过华为 VPN 专业设备，基于 Internet 搭建用户本地数据中心与华为云 VPC 之间的 IPsec 加密连接通道。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务自身情况开启并使用信息传输加密通道。

- **【合规满足度】**

  满足。

3. **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】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     云监控服务：为用户提供一个针对弹性云服务器、带宽等资源的监控平台。客户可监控云上的资源使用情况、业务的运行状况，并及时收到异常告警。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行云服务的相关配置。

   - **【合规满足度】**

     满足。

4. **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】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     云审计服务：默认支持在服务界面中 7 天内的事件审计操作记录的存储和检索分析，同时可以支持操作审计日志记录转储至对象存储服务（OBS），转储后的事件文件将永久保存。

   - **【云安全产品满足度分析】**

     WEB 应用防火墙，DDoS 高防，云堡垒机，数据库安全审计支持配套日志存储服务，支持服务的操作审计记录日志的永久存储和检索分析能力。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行云服务的相关配置。

- **【合规满足度】**

  满足。

5. **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】**

     安全管理。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     不涉及。

   - **【云安全产品满足度分析】**

     华为云安全服务控制台可支持针对于安全策略、恶意代码防范，漏洞分析详情，补丁升级，攻击事件、威胁告警和攻击源头进行集中呈现和管理。

     态势感知提供统一的安全态势总览、入侵检测、威胁分析、安全编排、漏洞扫描、应急漏洞、基线检查、告警设置等全局安全威胁态势，并提供防护建议。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行云服务的相关配置。

   - **【合规满足度】**

     满足。

6. **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】**

     安全监控。

   - **【保护对象】**

     云服务客户业务计算环境，云服务客户业务网络环境。

   - **【云产品安全满足度分析】**

     华为 PSIRT 和华为云安全运维团队已经建立了完善的漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务及运维工具等的自研漏洞和第三方漏洞都在 SLA 时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响云服务客户业务的风险。

   - **【云安全产品满足度分析】**

     态势感知服务支持检测 DDoS 攻击、暴力破解、Web 攻击、后门木马、漏洞攻击、僵尸主机、异常行为、命令与控制等多种云上安全风险，同时“告警列表”提供告警威胁的统计信息列表，包括威胁告警的源 IP、攻击名称、攻击类型、攻击目标主机信息、攻击等级和攻击发生时间等信息；

     WEB 应用防火墙支持 HTTP/HTTPS 流量攻击检测，可支持记录攻击事件，攻击类型、攻击 URL，攻击源 IP 等信息，并产生相关告警。

     DDoS 高防（Advanced Anti-DDoS，AAD）在进行 DDoS 攻击防御时记录攻击事件、攻击类型、攻击 URL、攻击源 IP，攻击流量峰值，清洗防护结果等信息内容，并产生相关告警。

   - **【云服务客户自身安全能力建议】**

云服务客户根据业务实际情况进行云服务的相关配置。

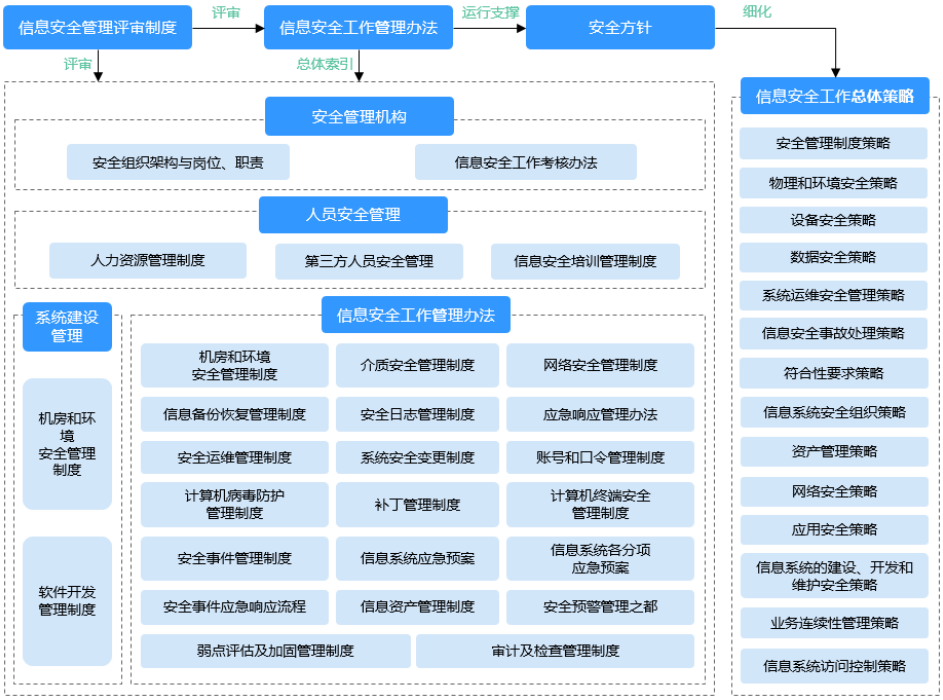
- **【合规满足度】**

  满足。

5.2.6 安全管理制度

华为公司建立了非常完善的安全管理制度框架和管理制度，也将此框架和制度实行于华为云的安全管理。

华为云协同第三方合作机构将相关经验和实践通过服务的方式提供给客户，共同提高客户的安全管理水平和能力。



5.3 等保基本合规要求分析（云计算安全扩展要求）

5.3.1 安全通信网络

网络架构

1. **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】**

     云平台安全保护等级定级。

   - **【保护对象】**

     云平台、云服务客户系统。

   - **【云平台原生安全能力满足度】**

     华为云所有 Region 的安全保护等级为第三级。

华为云部分 Region 节点的安全保护等级为第四级。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户所部署的应用系统定级需选择等于或高于其定级级别的云平台和相应的 Region。

- **【合规满足度】**

  满足。

2. **应实现不同**云服务客户**虚拟网络之间的隔离**

- **【安全措施】**

  网络隔离。

- **【保护对象】**

  云服务客户网络系统。

- **【云平台原生安全能力满足度】**

  虚拟私有云 VPC 采用网络隔离技术，实现不同云服务客户间在三层网络的完全隔离，云服务客户可完全掌控自己的虚拟网络构建与配置：一方面，结合 VPN 或云专线，将 VPC 与云服务客户内网的传统数据中心互联，实现云服务客户应用和数据从云服务客户内网向云上的平滑迁移；另一方面，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，满足云服务客户细粒度的网络隔离需要。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户需根据自身业务情况进行网络隔离设计和配置。

- **【合规满足度】**

  满足。

3. **应具有根据**云服务客户**业务需求提供通信传输、边界防护、入侵防范等安全机制的能力**

- **【安全措施】**

  网络边界防护，入侵防护等。

- **【保护对象】**

  云服务客户网络系统。

- **【云平台原生安全能力满足度】**

  不涉及。

- **【云安全产品满足度分析】**

  华为云构建纵深**云安全服务体系**，根据客户业务场景安全诉求提供相应的安全服务和解决方案。

  网络安全：DDoS 高防，Anti-DDoS 流量清洗。

  主机安全：企业主机安全，容器安全服务。

  应用安全：漏洞扫描服务，Web 应用防火墙。

数据安全：数据库安全服务，数据加密服务。

安全管理：安全专家服务，态势感知服务，SSL 证书管理，云堡垒机。

具体可参考如下链接：https://www.huaweicloud.com/product/security.html

- **【云服务客户自身安全能力建议】:**

  云服务客户根据业务实际情况部署配置安全服务。

- **【合规满足度】**

  满足。

4. **应具有根据**云服务客户**业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略**

   - **【安全措施】**

     安全策略。

   - **【保护对象】**

     云服务客户业务系统。

   - **【云平台原生安全能力满足度】**

     华为云构建纵深**云安全服务体系**，根据客户业务场景安全诉求提供相应的安全服务和解决方案；华为云提供的云安全服务可提供控制台进行安全策略的配置和统一可视化管理。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

5. **应提供开放接口或开放安全服务，允许**云服务客户**接入第三方安全产品或在云计算平台选择第三方安全服务**

   - **【安全措施】**

     能力开放，安全生态。

   - **【保护对象】**

     云平台安全能力，云服务客户业务系统。

   - **【云平台原生安全能力满足度】**

     华为云安全生态合作伙伴可以使用华为云云市场 Marketplace 平台展现自己的产品、解决方案和服务，与华为云共享云上潜在客户和销售机会。

     华为云向合作伙伴开放云服务技术接口， 支持合作伙伴开发面向各行业客户的安全方案，华为将帮助和支持这些方案走向市场，为客户带来价值，助力合作伙伴商业成功。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

- **【合规满足度】**

  满足。

5.3.2 安全区域边界

访问控制

1. **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】**

     云计算网络环境。
   - **【云平台原生安全能力满足度】**

     VPC 虚拟私有云，VPC 支持在云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     不涉及。
   - **【合规满足度】**

     满足。
2. **应在不同等级的网络区域边界部署访问控制机制，设备访问控制规则**
   - **【安全措施】**

     访问控制。
   - **【保护对象】**

     云计算网络环境。
   - **【云平台原生安全能力满足度】**

     华为云将网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为云服务客户数据平面、业务控制平面、平台运维平面、BMC（Baseboard Management Controller）管理平面、数据存储平面等，并在各平面之间设置访问控制规则以保证不同业务的网络通信流量得到合理且安全的分流， 便于实现职责分离。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     用户需根据业务实际情况划分不同网络按区域，并配置 VPC 内的 IP 地址段、子网、安全组等。
   - **【合规满足度】**

     满足。

入侵防范

1. **应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等**
   - **【安全措施】**

     网络攻击检测。
   - **【保护对象】**

     云计算网络环境。
   - **【云平台原生安全能力满足度】**

     华为云平台**网络入侵检测与拦截**（IDS/IPS-Intrusion Detection System / Intrusion Prevention System）：感知来自互联网及云服务客户虚拟网络之间东西向的攻击，并针对攻击实施阻断并记录相关，华为云在网络边界部署了 IPS 设备，包括但不限于外网边界、安全区域 边界和云服务客空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     不涉及。
   - **【合规满足度】**

     满足。
2. **应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；**
   - **【安全措施】**

     网络攻击检测。
   - **【保护对象】**

     云计算网络环境。
   - **【云平台原生安全能力满足度】**

     华为云在网络边界部署了边界部署 Anti-DDoS 设备来完成对异常和超大流量攻击的检测及清洗。Anti-DDoS 设备还可以为云服务客户提供精细化的 DDoS 防护服务，云服务客户可以根据业务的应用类型，配置流量阈值参数，并查看攻击和防御状态。

     华为云在网络边界部署了 IPS 设备，包括但不限于外网边界、安全区域边界和云服务客户空间边界等。IPS 具备网络实时流量分析和阻断能力，能记录并防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。
   - **【云安全产品满足度分析】**

     WEB 应用防火墙支持 HTTP/HTTPS 流量攻击检测，可支持记录攻击事件，攻击类型、攻击 URL，攻击源 IP 等信息，并产生相关告警。

DDoS 高防（Advanced Anti-DDoS，AAD）在进行 DDoS 攻击防御时记录攻击事件、攻击类型、攻击 URL、攻击源 IP，攻击流量峰值，清洗防护结果等信息内容，并产生相关告警。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况进行 DDoS 高防和 WEB 应用防火墙的配置。

- **【合规满足度】**

  满足。

3. **应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量**

   - **【安全措施】**

     网络检测。

   - **【保护对象】**

     云计算网络环境。

   - **【云平台原生安全能力满足度】**

     华为云平台**网络入侵检测与拦截**（IDS/IPS-Intrusion Detection System / Intrusion Prevention System）：感知来自互联网及云服务客户虚拟网络之间东西向的攻击，并针对攻击实施阻断并记录相关，华为云在网络边界部署了 IPS 设备，包括但不限于外网边界、安全区域 边界和云服务客户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

4. **应在检测到网络攻击行为、异常流量情况时进行告警。**

   - **【安全措施】**

     网络攻击检测、告警。

   - **【保护对象】**

     云计算网络环境。

   - **【云平台原生安全能力满足度】**

     DDoS 异常和超大流量清洗：华为云在每个云数据中心边界部署华为专业的 Anti-DDoS 设备来完成对异常和超大流量攻击的检测及清洗。Anti-DDoS 设备还可以为云服务客户提供精细化的 DDoS 防护服务，云服务客户可以根据业务的应用类型，配置流量阈值参数，并查看攻击和防御状态并产生相关告警。

     网络入侵检测与拦截（IDS/IPS-Intrusion Detection System / Intrusion Prevention System）：感知来自互联网及云服务客户虚拟网络之间东西向的攻击，针对攻

击实施阻断并记录相关日志，同时产生相关告警，华为云在网络边界部署了IPS 设备，包括但不限于外网边界、安全区域 边界和云服务客户空间边界等。IPS 具备网络实时流量分析和阻断能力，能防护异常协议攻击、暴力攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS 可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。

Web 安全防护：华为云部署了 Web 应用防火墙应对 Web 攻击，如 Web 应用层的 DDoS 攻击、SQL 注入、跨站脚本攻击（XSS-Cross-Site Scripting）、跨站请求伪造（CSRF-Cross-Site Request Forgery）、组件漏洞攻击、身份伪造等，以保护部署在 DMZ 区、面向外网的 Web 应用服务和系统，同时产生相关告警。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

安全审计

1. **应对云服务提供商和**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】**

     操作安全审计。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     华为云平台通过堡垒机进行管理云平台中的设备，当终端接入需要通过华为的网络防火墙 、身份鉴权平台对终端管控进行认证，终端认证后再通过堡垒机对用户进行身份鉴别。

     云审计提供云服务客户对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

   - **【云安全产品满足度分析】**

     云堡垒机可基于唯一身份标识的用户账户管理与访问控制策略，精细化的角色权限控制，与云服务客户服务器、网络设备、安全设备、数据库、应用系统进行连接管理，实现集中运维操作管理与审计。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

2. **应保证云服务提供商对**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】**

操作审计。

- **【保护对象】**

  云计算环境，云服务客户业务数据。

- **【云平台原生安全能力满足度】**

  华为云对云服务客户系统和数据需要云服务提供商进行任何操作时，需要云服务客户提交工单申请并进行授权，相关操作行为通过云服务客户管理平台进行记录并审计。

  云审计提供云服务客户对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

5.3.3 安全计算环境

身份鉴别

1. **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】**

     双向身份验证。

   - **【保护对象】**

     云计算平台。

   - **【云平台原生安全能力满足度】**

     华为云平台通过堡垒机进行管理云平台中的设备，当终端接入需要通过华为的网络防火墙、身份鉴权平台对终端管控进行认证，终端认证后再通过堡垒机对用户进行身份鉴别。

   - **【云安全产品满足度分析】**

     云堡垒机可基于唯一身份标识的用户账户管理与访问控制策略，精细化的角色权限控制，与云服务客户服务器、网络设备、安全设备、数据库、应用系统进行连接管理，实现集中运维操作管理与审计。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

访问控制

1. **应保证当虚拟机迁移时，访问控制策略随其迁移**

- **【安全措施】**

  访问控制。

- **【保护对象】**

  云计算环境。

- **【云平台原生安全能力满足度】**

  华为云平台支持虚拟机两种迁移方式：

  冷迁移：将虚拟机文件迁移后，系统扫描发现该虚拟机，同步更新其访问控制策略。

  热迁移：原虚拟机不变，拷贝该虚拟机至指定路径，同步数据后关闭原虚拟机。

- **【云安全产品满足度分析】**

  华为云**云数据迁移服务（CDM）**，支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

2. **应允许**云服务客户**设置不同虚拟机之间的访问控制策略**

- **【安全措施】**

  访问控制。

- **【保护对象】**

  云计算环境。

- **【云平台原生安全能力满足度】**

  VPC 虚拟私有云，VPC 支持在云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户根据业务实际情况配置虚拟机之间的访问控制策略。

- **【合规满足度】**

  满足。

入侵防范

1. **应能检测虚拟机之间的资源隔离失效，并进行告警**

- **【安全措施】**

  资源隔离。

- **【保护对象】**

云计算环境。

- **【云平台原生安全能力满足度】**

  华为统一虚拟化平台（UVP - Unified Virtualization Platform） 通过对服务器物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境，检测到虚拟资源隔离失效时进行告警。在中国可信云认证中，华为云平台的云主机获得最高级的五星+认证。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

2. **应能检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警**

   - **【安全措施】**

     操作授权，操作审计。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     云平台通过平台任务日志对非授权的操作如新建虚拟机、重启虚拟机、删除虚拟机等操作进行记录并支持审计。

   - **【云安全产品满足度分析】**

     云审计服务提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

3. **应能检测恶意代码感染及在虚拟机间蔓延情况，并进行告警**

   - **【安全措施】**

     恶意代码检测。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     华为云平台在宿主机部署了入侵检测能力，可检测恶意代码感染和传播情况，并进行告警。

   - **【云安全产品满足度分析】**

     云服务客户客户使用**企业主机安全服务**实现恶意代码检测，并提出告警。

   - **【云服务客户自身安全能力建议】**

不涉及。

- **【合规满足度】**

  满足。

镜像和快照保护

1. **应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务**

   - **【安全措施】**

     安全加固。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     镜像加固：华为云通过镜像工厂，由专业安全团队对虚拟机操作系统公共镜像进行安全加固，并及时修复系统安全漏洞，最终生成安全更新了的公共镜像，并通过镜像服务（IMS）持续提供给云服务客户。同时提供相关加固和补丁信息以供用户对 镜像进行测试、排除故障及其他运维活动时参考。由客户根据相关应用运行及安全运维策略，选择直接使用最新的公共镜像重新创建虚拟机或自行创建已安装 安全补丁的私有镜像。

     华为云安全加固服务：对主机服务器、中间件进行漏洞扫描、基线配置加固。提供对操作系统及应用面临的安全威胁分析，及析操作系统补丁和应用系统组件版本分析提供相应的整改建议，并在用户的许可下完成相关漏洞的修复和补丁组件的加固工作。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

2. **应提供虚拟机镜像、快照完整性检验功能，防止虚拟机镜像被恶意篡改**

   - **【安全措施】**

     虚拟镜像校验。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     华为云镜像服务基于华为云统一身份认证服务（IAM）来进行认证，支持镜像的传输和存储加密及完整性检测。IMS 的所有数据都存储于信任子网内的镜像仓库，并且采用对象存储分桶机制，也就是将公共镜像和私有镜像分别存放在不同的桶中。IMS 提供了安全的加密算法和功能，让用户选择对镜像进行加密存储。在基于镜像创建虚拟机时，系统会自动检查镜像完整性，以确保创建的虚拟机包含完整的镜像内容。

   - **【云安全产品满足度分析】**

     不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

3. **应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问**

   - **【安全措施】**

     虚拟镜像加密。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     华为云镜像服务基于华为云统一身份认证服务（IAM）来进行认证，支持镜像的传输和存储加密及完整性检测。IMS 的所有数据都存储于信任子网内的镜像仓库，并且采用对象存储分桶机制，也就是将公共镜像和私有镜像分别存放在不同的桶中。IMS 提供了安全的加密算法和功能，让用户选择对镜像进行加密存储。在基于镜像创建虚拟机时，系统会自动检查镜像完整性，以确保创建的虚拟机包含完整的镜像内容。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

数据完整性和保密性

1. **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】**

     个人数据信息存储。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     华为云国内基础设施和存储空间均位于中国境内，国内站点云上数据存储于中国境内，云服务客户数据是否存在数据处境情况需根据客户业务实际情况而定。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     云服务客户业务数据如果涉及出境，则需遵循相关法律合规要求。

   - **【合规满足度】**

满足。

2. **应确保只有在云服务客户授权下，云服务提供商或第三方才具有**云服务客户数据**的管理权限**

   - **【安全措施】**

     个人隐私保护。

   - **【保护对象】**

     个人数据。

   - **【云平台原生安全能力满足度】**

     华为云隐私政策声明描述了我们如何收集、使用和披露您的个人数据，及数据处理的法律依据和安全措施。它还表明在我们处理您的个人数据时，您控制个人数据的权利，及您在向我们提供个人数据之前需要了解的其他相关详细信息。

     华为云隐私政策声明链接：
     https://www.huaweicloud.com/declaration/sa_prp.html

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

3. **应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施**

   - **【安全措施】**

     完整性校验。

   - **【保护对象】**

     云计算环境。

   - **【云平台原生安全能力满足度】**

     华为云平台在启动虚拟机迁移时，支持带密钥启动，以保证虚拟机在迁移过程中的完整性。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

4. **应支持**云服务客户**部署密钥管理解决方案，保证**云服务客户**自行实现数据的加解密过程**

   - **【安全措施】**

     数据加密。

   - **【保护对象】**

云服务客户业务数据。

- **【云平台原生安全能力满足度】**

  不涉及。

- **【云安全产品满足度分析】**

  密钥管理服务可支持用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块（HSM －Hardware Security Module），为云服务客户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。HSM 是一种安全产生、存储、管理及使用密钥并提供加密处理服务的硬件设备。为保护云服务客户密钥安全，减少密钥外泄风险，华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云 HSM 供云服务客户选择，满足不同云服务客户的实际需求，例如通过 FIPS140-2 国际权威认证的第三方 HSM。KMS 对密钥的所有操作都会进行访问控制及日志跟踪，满足审计和合规性要求。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

数据备份恢复

1. 云服务客户**应在本地保存其业务数据的备份**。

   - **【安全措施】**

     数据备份。

   - **【保护对象】**

     云服务客户业务数据。

   - **【云平台原生安全能力满足度】**

     不涉及。

   - **【云安全产品满足度分析】**

     华为云数据库支持数据迁移和备份在指定的数据库对象中，并提供数据本地下载备份、数据本地导入导出功能。同时，华为云数据库实例支持每天定期执行全库备份，也可手动执行全库备份；定期进行一次增量日志备份。

   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务实际情况进行数据本地备份。

   - **【合规满足度】**

     满足。

2. **应提供查询**云服务客户数据**及备份存储位置的能力。**

   - **【安全措施】**

     数据查询。

   - **【保护对象】**

     云服务客户业务数据。

   - **【云平台原生安全能力满足度】**

华为云提供基于加密 HTTPS 的 API Endpoint 调用。

华为云 API Endpoint 可查询到华为云各服务应用区域和各服务的终端节点。包含存储服务，如云硬盘、对象存储、云备份、云数据库、内容分发服务 CDN 等。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

3. **云服务提供商的云存储服务应保证**云服务客户数据**存在若干个可用的副本，各副本之间的内容应保持一致**

   - **【安全措施】**

     数据冗余保护。

   - **【保护对象】**

     云服务客户业务数据。

   - **【云平台原生安全能力满足度】**

     云硬盘服务 EVS 使用多副本的数据冗余保护机制，采用副本同步写、读修复等措施保证数据一致性， 当检测到硬件故障能够自动后台修复，数据快速自动重建，数据持久性可达 99.9999999%。

     对象存储服务 OBS，客户存储数据分片后多份冗余存储在不同磁盘，后台自行检测一致性并及时修复受损数 据。数据持久性高达 99.9999999999%，服务可用性 达 99.995%。 同时会对存储前和存储后通 过 Hash 校验数据一致性，确保存入数据的完整性。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

4. **应为**云服务客户**将业务系统及数据迁移到其体云计算平台和本地系统提供技术手段，并协助完成迁移过程**

   - **【安全措施】**

     业务迁移、数据迁移。

   - **【保护对象】**

     云服务客户业务系统。

   - **【云平台原生安全能力满足度】**

     华为云**云数据迁移服务（CDM）**，支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

剩余信息保护

1. **应保证虚拟机所使用的内存和存储空间回收时得到完全清除**

   - **【安全措施】**

     数据清除。

   - **【保护对象】**

     云服务客户业务数据。

   - **【云平台原生安全能力满足度】**

     内存数据删除：华为云在云操作系统将内存重新分配给用户之前，会对分配的内存进行清零操作，即写“零”处理，防止通过物理内存恢复删除数据造成的数据泄露。

     存储数据删除：当云服务客户删除数据时，数据和对应的元数据在系统中一并删除，底层存储区域被回收以供系统重新覆盖写入，数据无法再被读取。但是针对客户误删除的操作场景，通过 EVS 服务的回收站功能、OBS 服务的多版本控制功能，用户可以最终决定数据的恢复或彻底删除。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

2. 云服务客户**删除业务应用数据时，云计算平台将云存储中所有副本删除**

   - **【安全措施】**

     数据清除。

   - **【保护对象】**

     云服务客户业务数据。

   - **【云平台原生安全能力满足度】**

     华为云在客户内容数据的销毁阶段，会对指定的数据及其所有副本进行全面的清除。当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。 对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式 进行数据清除，确保其上的数据无法恢复。

   - **【云安全产品满足度分析】**

不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

5.3.4 安全管理中心

集中管控

1. **应能对物理资源和虚拟资源按照策略做统一管理调度与分配**

   - **【安全措施】**

     虚拟机管理。

   - **【保护对象】**

     云计算环境、云服务客户业务计算环境。

   - **【云平台原生安全能力满足度】**

     华为统一虚拟化平台（UVP - Unified Virtualization Platform） 通过对服务器物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建 多个同时运行、相互隔离的虚拟机执行环境。在中国可信云认证中，华为云平台的云主机获得最高级的五星+认证。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

2. **应保证云计算平台管理流量与**云服务客户**业务流量分离**

   - **【安全措施】**

     安全区域划分。

   - **【保护对象】**

     云服务客户业务系统。

   - **【云平台原生安全能力满足度】**

     华为云将网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为云服务客户数据平面、业务控制平面、平台运维平面、BMC（Baseboard Management Controller）管理平面、数据存储平面等，以保证关乎不同业务的网络通信流量得到合理且安全的分流， 便于实现职责分离。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

- **【合规满足度】**

  满足。

3. **应根据云服务提供商和**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】**

     安全审计。
   - **【保护对象】**

     云服务客户业务系统。
   - **【云平台原生安全能力满足度】**

     云审计服务提供对各种云资源（包含网络设备，网络节点）操作记录的收集、存储和查询功能。支持三类事件记录，包括全局事件、管理事件、数据事件。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     不涉及。
   - **【合规满足度】**

     满足。
4. **应根据云服务提供商和**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**
   - **【安全措施】**

     安全监控。
   - **【保护对象】**

     云服务客户业务系统。
   - **【云平台原生安全能力满足度】**

     云监控服务：为用户提供一个针对弹性云服务器、带宽等资源的监控平台。客户可监控云上的资源使用情况、业务的运行状况，并及时收到异常告警。
   - **【云安全产品满足度分析】**

     不涉及。
   - **【云服务客户自身安全能力建议】**

     云服务客户根据业务自身情况使用监控服务进行云上资源和业务监控。
   - **【合规满足度】**

     满足。

5.3.5 安全建设管理

云服务提供商选择

1. **应选择安全合规的云服务提供商，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。

- **【保护对象】**

  云服务客户业务系统。

- **【云平台原生安全能力满足度】**

  华为云所有 Region 的安全保护等级为第三级。

  华为云部分 Region 节点的安全保护等级为第四级。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  云服务客户所部署的应用系统定级需选择等于或高于其定级级别的云平台和相应的 Region。

- **【合规满足度】**

  满足。

2. **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**

   - **【安全措施】**

     服务协议。

   - **【保护对象】**

     云服务客户相关权益。

   - **【云平台原生安全能力满足度】**

     华为云服务提供云服务等级协议（SLA）提供服务相关的协议，包含各云服务的服务内容及具体技术指标。

     华为云服务等级协议（SLA）请参考：
     https://www.huaweicloud.com/declaration/sla.html

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

3. **应在服务水平协议规定云服务提供商的权限与责任，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**

   - **【安全措施】**

     用户协议、服务协议。

   - **【保护对象】**

     云服务客户相关权益。

   - **【云平台原生安全能力满足度】**

     华为云与云服务客户之间协商并签订华为云用户协议，华为云用户协议中包含保密协议约定华为云与云服务客户云服务客户之间的管理范围、职责划分，访问授权、行为准则、违约责任等相关条款。

同时华为云服务提供云服务等级协议（SLA）提供服务相关的协议。

华为云用户协议请参考：https://www.huaweicloud.com/declaration/sa_cua.html

云服务等级协议（SLA）请参考：
https://www.huaweicloud.com/declaration/sla.html

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

4. **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**

   - **【安全措施】**

     数据清除。

   - **【保护对象】**

     云服务客户数据。

   - **【云平台原生安全能力满足度】**

     当客户主动进行数据删除操作 或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。

     华为云支持客户对账户进行注销。当客户提出账户注销的申请并通过华为云对账号的验证后，客户内容数据进入保留期，保留期内，客户不能访问及使用云服务，但对客户存储在云服务中的数据仍予以保留。保留期届满后，客户内容数据会得到彻底的清除，无法进行恢复。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

5. **应与选定的云服务提供商签署保密协议，要求其不得泄漏**云服务客户数据

   - **【安全措施】**

     保密协议。

   - **【保护对象】**

     云服务客户数据。

   - **【云平台原生安全能力满足度】**

     华为云与云服务客户之间协商并签订华为云用户协议，华为云用户协议中包含保密协议约定华为云与云服务客户之间的保密相关条款。

     华为云用户协议请参考：https://www.huaweicloud.com/declaration/sa_cua.html

   - **【云安全产品满足度分析】**

不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

供应链管理

1. **应确保供应商的选择符合国家有关规定**

   - **【安全措施】**

     供应商选择。

   - **【保护对象】**

     云计算平台。

   - **【云平台原生安全能力满足度】**

     华为云致力于构建开放、协作、共赢的安全生态体系，与业界领先的安全产品与服务供应商一起，基于责任共担模式，为云服务客户提供易部署、易管理、完善的安全解决方案，应对已知、未知的安全威胁，保障云服务客户的数据和业务安全。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

     满足。

2. **应将供应链安全事件信息或安全威胁信息及时传达到**云服务客户

   - **【安全措施】**

     威胁披露。

   - **【保护对象】**

     云计算环境，云服务客户业务系统。

   - **【云平台原生安全能力满足度】**

     华为云会将相关重要通知实时发布至官网，其中包括供应商的重要变更、产品变更公告、安全公告、升级公告、备案公告、其它公告等。同时，为保护最终用户和云服务客户，华为云秉承负责任的披露原则，对于涉及云平台、云服务客户服务等的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/云服务客户及时推送漏洞规避和修复方案和建议，与云服务客户共同面对安全漏洞带来的挑战。

   - **【云安全产品满足度分析】**

     不涉及。

   - **【云服务客户自身安全能力建议】**

     不涉及。

   - **【合规满足度】**

满足。

3. **应将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**

- **【安全措施】**

  风险通告。

- **【保护对象】**

  云计算环境。

- **【云平台原生安全能力满足度】**

  华为云会将相关重要通知实时发布至官网，其中包括供应商的重要变更、产品变更公告、安全公告、升级公告、备案公告、其它公告等。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

5.3.6 安全运维管理

云计算环境管理

1. **云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定**

- **【安全措施】**

  安全运维。

- **【保护对象】**

  云计算环境。

- **【云平台原生安全能力满足度】**

  华为云国内基础设施和存储空间均位于中国境内，国内云平台的运维操作地点也位于中国境内，并遵循国家相关规定。

- **【云安全产品满足度分析】**

  不涉及。

- **【云服务客户自身安全能力建议】**

  不涉及。

- **【合规满足度】**

  满足。

6 华为云等保合规实践指引

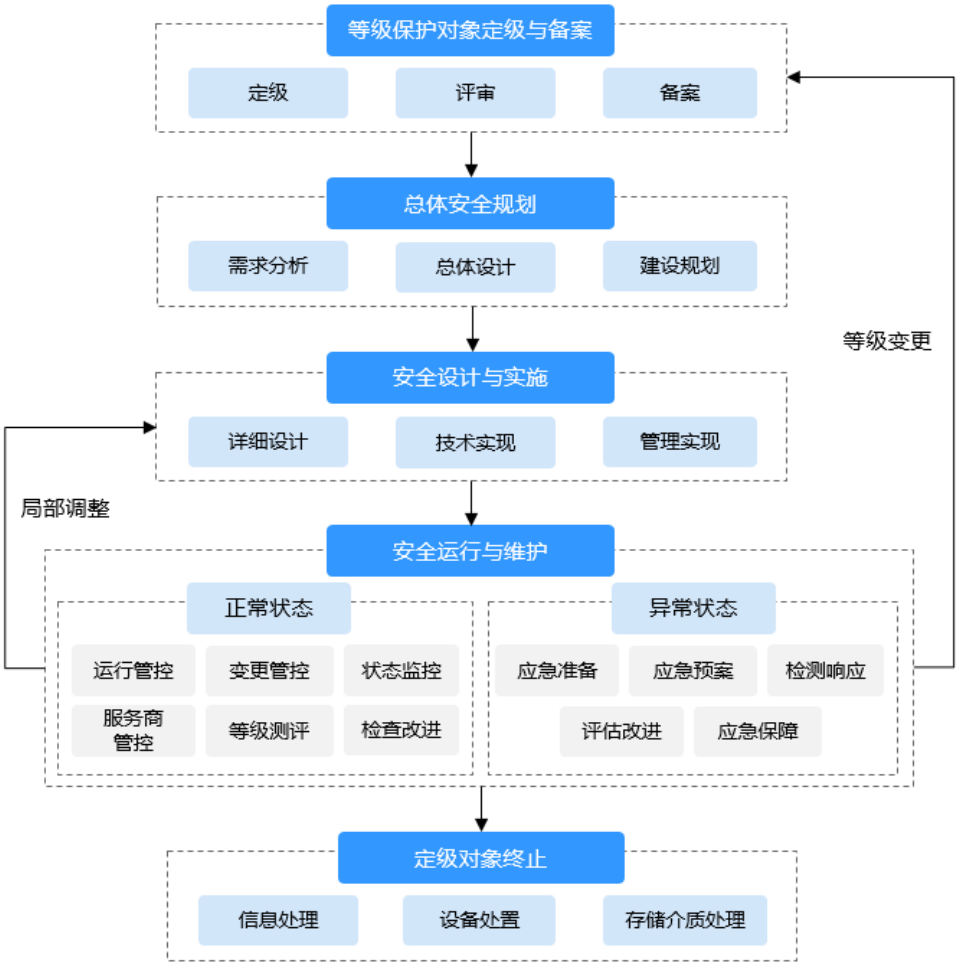
6.1 等保实施指引

6.2 云服务客户在华为云上过等保的流程实践

6.3 云服务客户使用华为云满足等保要求的实践

6.1 等保实施指引

根据《GBT25058-2019 信息安全技术网络安全等级保护实施指南》要求，等保实施基本流程包括等级保护对象定级阶段与备案、总体安全规划、安全设计与实施、安全运行与维护、定级对象终止。如下图所示：



- **等级保护对象定级阶段与备案**

  等级保护对象运营使用单位按照国家有关管理规范和定级标准，确定等级保护对象及安全保护等级，并经过专家评审。

  等级保护对象运营使用单位如有上级主管部门，应经上级主管部门审核、批准，并报公安机关备案审查。

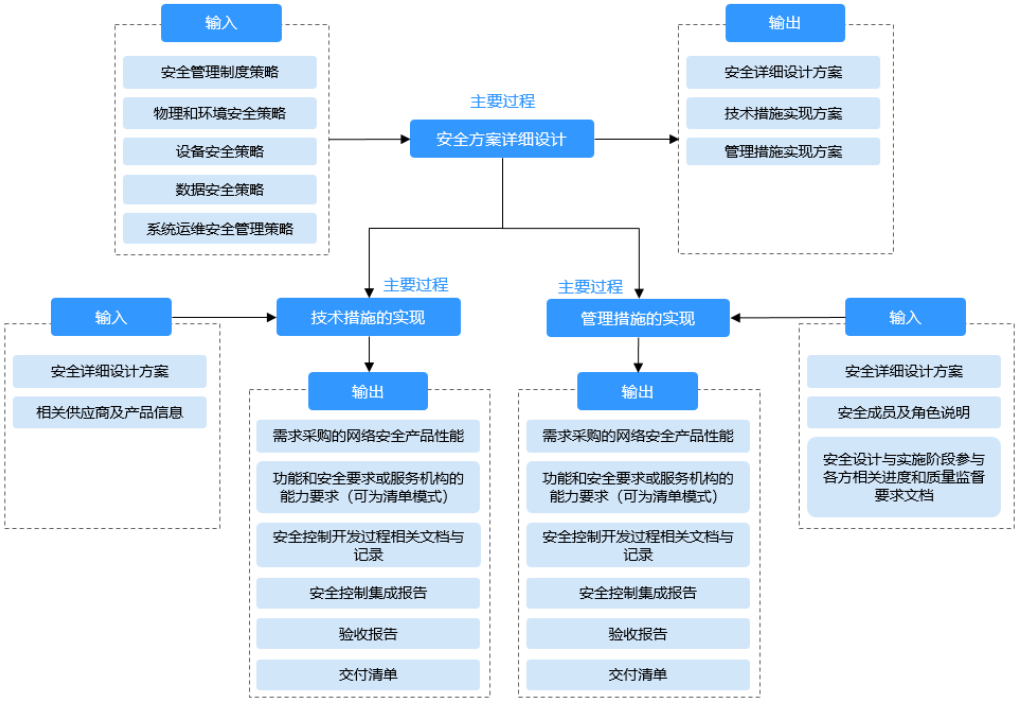
  定级标准可参考：《GA/T 1389-2017 信息安全技术 网络安全等级保护定级指南》。

- **总体安全规划**

  等级保护对象运营使用单位根据等级保护对象的划分情况、定级情况及承载业务情况，通过分析明确等级保护对象安全需求，设计合理的，满足等级保护要求的总体安全方案，并制定出安全实施计划，以指导后续的等级保护对象安全建设工程实施。

- **安全设计与实施**

  按照等级保护对象安全总体方案的要求，结合等级保护对象安全建设项目规划，分期分步落实安全措施。具体实施流程可参看如下图：



- **安全运行与维护**

  此阶段包含等级保护对象运营使用单位安全运行与维护机构和安全运行与维护机制的建立， 环境、资产、设备、介质的管理，网络、系统的管理，密码、密钥的管理，运行、变更的管理，安全状态监控和安全事件处置，安全审计和安全检查等内容。

- **定级对象终止**

当定级对象被转移、终止或废弃时，正确处理其中的敏感信息对于确保机构信息资产的安全是至关重要的。在等级保护定级对象生命周期中，定级对象并不是真正意义上的被废弃，而是改进技术或转变业务到新的定级对象，对于这些定级对象在终止处理过程中应确保信息转移、设备迁移和介质销毁等方面的安全。

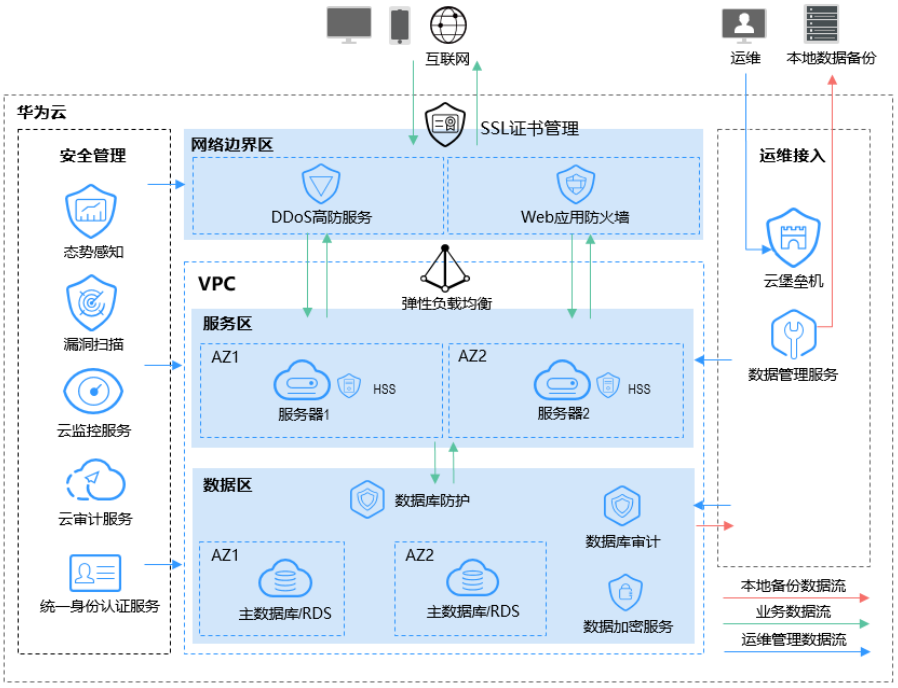
6.2 云服务客户在华为云上过等保的流程实践

按照等保测评实施指南的要求，等保工作中，各角色承担的工作内容，分步落实。华为云租户业务系统，通过等保测评工作，具体实施流程可参看如下图：

环节	建设/运营方	测评机构	行业主管/ 网信办与公安
定级	确定等级保护对象，确定安全保护等级，编制定级备案材料； 组织专家对等级保护对象的定级情况进行评审	协助进行等级保护对象定级备案，初步审核备案材料。协助提交或运营者自主提交公安	审查定级方法，工作过程，内容，结论等是否符合规定。
备案	政管理备案材料，向属地公安机关网监部门备案	协助进行等级保护对象定级备案初步审核备案材料。协助提交或运营者自主提交公安。	受理备案，实施备案审核，发放备案证明
建设整改	依据等级保护标准，开展安全技术和管理体系建设； 组织专家对等级保护对象的建设方案进行评审（三级及以上）	提出建设性整改建议，解答整改问题。	审查等级保护对象的安全建设整改工作； 对关键信息基础设施的安全建设工作重点审查
等级测评	定期选择具有资质的测评机构，开展等级测评工作	根据系统级别实施差距测评。对差距测评存在问题复测，确保等级保护对象整改后符合等保标准要求。	审查等级保护对象等级测评工作是否符合规定；对关键信息基础设施实行重点审查。
监督检查	接受并配合公安机关、上级主管部门的监督检查；定期开展安全自查		定期针对等级保护对象开展网络安全执法检查；关键信息基础设施实施重点保护

6.3 云服务客户使用华为云满足等保要求的实践

华为云为云服务客户提供全栈的安全防护体系和丰富的安全服务，帮助云服务客户高质量满足等级保护技术要求。如下图所示。这些服务往往能兼具满足数个等保测评项的要求，部署后，可集约化的满足等保要求。



6.3.1 安全区域边界

一、性能冗余

华为云提供各类规格的计算、存储、网络等资源，如各类规格的 CPU、内存、磁盘、带宽等，云服务客户可根据自己的业务需求，按需选用，且可弹性扩容，满足业务高峰期需要。

二、安全区域隔离与访问控制

华为云上网络区域隔离除了使用 VPC subnet 外，还提供安全组服务。安全组是虚拟防火墙，通过对 IP 和端口设置白名单访问策略，达到访问控制和隔离的目的，保证云上资源如云主机、RDS 等只能通过受控端口提供服务。

配置安全组前先梳理云上资源和通信矩阵，提供服务的端口和 IP，及对外发起访问的端口和 IP。

- 以资源为单位配置安全组：将相同类型的资源作为一个安全组，如提供 WebServer，且有相同通信矩阵的云主机，配置为一个安全组；
- 业务所需最小原则：安全组每一条策略，都明确备注其用途，如入方向策略中不出现 any 的 IP 或端口；

三、入侵防范

华为云提供纵深防御体系，针对四到七层的各类攻击行为进行监测并抵御：

Anti-DDoS 流量清洗服务，可抵御小流量的 DDoS 攻击；对大流量攻击，华为云 DDoS 高防服务提供 T 级流量清洗能力；

Web 应用防火墙，采用数十种以上的编码还原能力和业内领先的“AI+规则”双引擎，以较低的漏报率和误报率，为云服务客户提供 Web 攻击防护能力。

企业主机安全服务，入侵检测特性实时检测主机内部的风险异变，可识别并阻止入侵主机的行为，如暴力破解、异地登录、文件变更与篡改、恶意程序、网站后门等。

安全态势感知，针对各关键网络节点的攻击行为进行监测和分析，将云服务客户网络中所有安全事件进行集中展示、管理和关联分析，以进行攻击行为的追踪溯源；结合 AI 能力对新型攻击进行检测分析。

四、恶意代码防范

华为云企业主机安全服务，提供云主机的恶意代码防范能力，实时检测云主机上运行的程序，若发现主机可能存在恶意程序如病毒、木马蠕虫等，则会将其隔离查杀，并及时通知管理员。华为云安全团队 7*24 小时监控威胁情况，及时更新恶意代码特征库。

6.3.2 安全通信网络

一、安全区域划分

在公有云中使用 VPC、子网和 EIP 等服务，将网络从逻辑上划分为应用接入区、应用服务区、应用数据区和管理区。

- 网络接入区，通过华为云 ELB 服务（弹性负载均衡）提供互联网服务。建议仅 ELB 绑定 EIP（弹性 IP，公网 IP）作为业务唯一对外出口，云主机和数据库等不建议绑定 EIP。如有业务外联，建议通过 NAT 网关进行。
- 应用服务区，华为云主机组，在其上搭建 WebServer 等业务服务器，承接来自 ELB 分发的业务流量，建议采用多 AZ（可用区，即云服务提供商的不同机房）的集群部署，避免因单机房的不可控故障导致单点故障。
- 应用数据区，分为数据库和对象存储，使用华为云 RDS 高可用版本，主备实例选用不同的 AZ（可用区，即不同机房），华为云的不同 AZ 选址已达到同城双中心标准；对象数据，存储在华为云 OBS，华为云 OBS 本身提供多副本的高可用设计。
- 安全管理区，为逻辑上的分区，是云平台提供的一系列服务化的管理服务，满足集中管控的要求，包含资源管理、资源监控、身份管理、操作审计、安全管理中心等。
- 运维接入区，为云服务客户运维操作提供运维通道，并进行云上资产的运维操作的管理与审计。

二、安全通信协议

网络中使用安全的通信协议，特别是对外提供服务的协议，建议云服务客户使用安全协议，如使用 https 替代 http。华为云提供 SSL 证书管理服务，为云服务客户提供多品牌的 SSL 证书的购买和管理。

三、入侵防范

同 6.3.1 安全区域边界章节。

四、恶意代码防范

华为云提供针对云主机的恶意代码防范能力，以满足等保要求“应在关键网络节点处对恶意代码进行检测和清除”。依据责任共担模型，网络关键节点的安全责任主体为平台侧，云服务客户只用负责云主机的恶意代码防范。华为云平台在平台安全侧提供满足等保要求的恶意代码防范措施。

企业主机安全服务，提供入侵检测特性，实时检测主机内部的风险异变，可识别并阻止入侵主机的行为，如暴力破解、异地登录、文件变更与篡改、恶意程序、网站后门等。

一、主机安全

华为云服务客户的企业主机安全，提供入侵检测特性实时检测主机内部的风险异变，可识别并阻止入侵主机的行为，如暴力破解、异地登录、文件变更与篡改、恶意程序、网站后门等。

华为云同时提供“云主机防暴力破解解决方案”，结合华为多年运营商级别安全防护经验，为用户提供覆盖主流操作系统的主机加固&防护解决方案，提升云主机账户安全性，预防暴力破解风险，也满足了等保相关主机加固的要求。

二、应用安全

应用安全是云服务客户业务安全建设重点，云服务客户应参考等保标准对身份认证、访问控制、安全审计（业务管理员的审计）、入侵防范（安全编码、测试等）等进行严格的控制。

华为云 Web 应用防火墙（Web Application Firewall）对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，阻挡诸如 SQL 注入或跨站脚本等常见攻击，避免这些攻击影响 Web 应用程序的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险。

华为云漏洞扫描服务，对普遍采用的 Web 中间件和第三方开发框架，如 Apache、Tomcat、Nginx、thinkphp、struts2 等等进行 CVE 漏洞的定期扫描；对不安全配置项进行定期基线扫描。及时发现风险，提前处理。

华为云网页防篡改服务，可实时发现并拦截篡改指定目录下文件的行为，并快速获取备份的合法文件恢复被篡改的文件，从而保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。支持静态、动态网页及网盘文件的防篡改。

三、数据安全

华为云提供的云数据库服务，采用高可用跨 AZ 部署，将 RDS 的主备实例分布部署在不同可用区，华为云不同可用区距离超过 30KM，达到同城主备的能力。客户可根据实际业务情况配置云数据库的备份策略，如采取每天一次自动全量备份策略。华为云云数据库采用浮动 IP 策略，在故障时会自动切换，但 IP 不变，建议服务端设置自动重连机制。

华为云提供数据库审计服务，旁路模式，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。同时，数据库安全审计可以生成满足数据安全标准（例如 Sarbanes-Oxley）的合规报告，对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

针对敏感数据加密能力，可使用华为云的数据加密服务（DEW）。DEW 是一个综合的云上数据加密服务，可以提供专属加密、密钥管理等功能。其密钥由硬件安全模块（HSM） 保护。敏感数据加密的秘钥，可以通过 KMS（秘钥管理子模块）进行管理，加解密可调用华为接口实现；数据量较大时，可使用 DHSM（专属加密机，DEW 的子服务），该云化密码机符合国家密码局认证或 FIPS 140-2 第 3 级验证第级验证，能对高安全性要求的用户提供高性能专属加密服务，保障数据安全，规避风险。

6.3.3 安全管理中心

一、系统管理

华为云服务客户通过控制台进行资源的集中管控，通过 IAM（统一身份认证服务），对登录控制台的系统管理员进行身份鉴别和权限分配，满足对“系统管理”集中管控的要求。IAM 的“安全设置”可对管理员的口令强度、登录验证策略、密码策略等进行配置，可配置多因子认证，可对控制台的访问设置白名单策略。

二、审计管理

华为云提供云审计服务，对云控制台的操作记录，并可通过配置将审计记录转储到 OBS 中，以满足等保 180 天保存日期的需求。

华为云提供云堡垒机服务，对云主机的进行统一运维管理。堡垒机对所有运维操作均提供审计能力，日志记录保存在其数据库中。用户管理采用 RBAC 模式，提供审计管理员角色，可由运维审计员查看审计记录。

三、集中管理

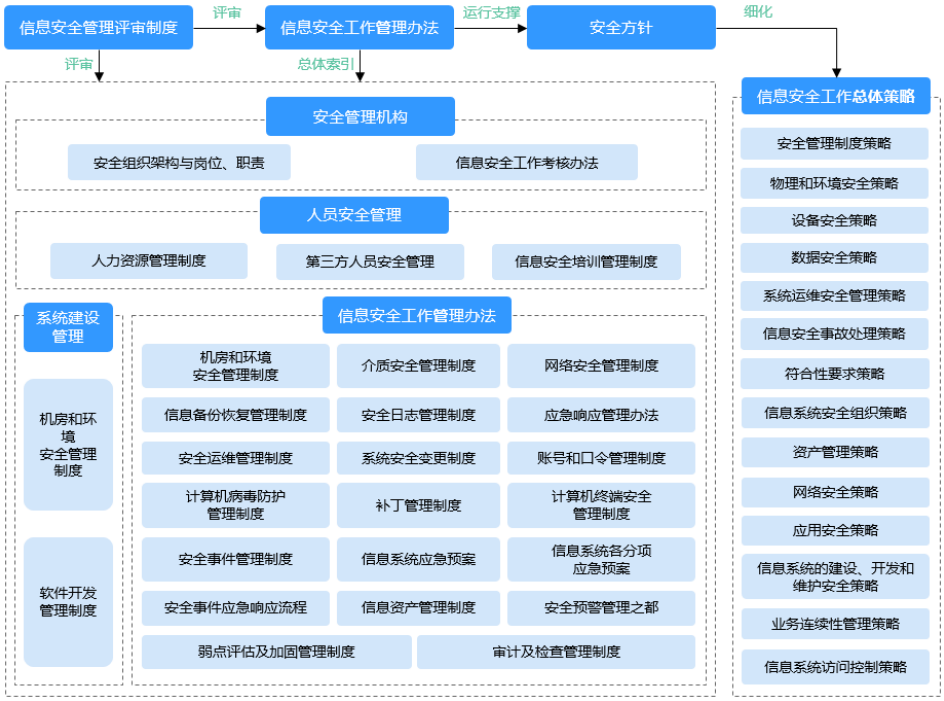
华为云提供云监控服务，对云主机、带宽、RDS 等资源的运行状态进行集中实时监控展示，并设置告警阈值，及时告警给管理员。

态势感知（Situation Awareness）为用户提供统一的威胁检测和风险处置平台。态势感知能够帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力。

6.3.4 安全管理制度

华为公司建立了非常完善的安全管理制度框架和管理制度，也将此框架和制度实行于华为云的安全管理。

华为云协同第三方合作机构将相关经验和实践通过服务的方式提供给客户，共同提高客户的安全管理水平和能力。



7 附录

7.1 术语与定义：

7.2 参考标准与规范

7.1 术语与定义：

部分术语引用于华为云产品术语列表：
https://support.huaweicloud.com/pcre_gls/index.html?product=consolehome

公有云

《GB/T 31167-2014 云计算服务安全指南》中 4.3 部署模式，根据云计算平台的客户范围的不同，将云计算分成私有云、公有云、社区云和混合云等四种部署模式。公有云，云计算平台的客户范围没有限制。公有云的云计算基础设施由云服务商拥有、管理和运营。

云服务商

《GB/T 31167-2014 云计算服务安全指南》中定义，云计算服务的供应方；云服务商管理、运营、支撑云计算的基础设施及软件，通过网络交付云计算的资源。

云服务客户/云租户/租户

《GB/T 31167-2014 云计算服务安全指南》中定义，为使用云计算服务同云服务商建立业务关系的参与方。*使用华为云 IaaS、PaaS、SaaS 的客户，*又称云租户、租户、客户

云计算服务

《GB/T 31167-2014 云计算服务安全指南》中定义，使用定义的接口，借助云计算提供一种或多种资源的能力。又称云产品、云服务产品、云产品服务。本文中统称云服务

云安全服务

用于做安全防护的云计算服务，又称云安全产品，

等级保护对象

《GA/T 1389—2017 信息安全技术 网络安全等级保护定级指南》中定义，网络安全等级保护工作的作用对象，主要包括基础信息网络、信息系统（例如工业控制系统、云计算平台、物联网、使用移动互联技术的信息系统以及其他信息系统）和大数据等。

云计算平台

《GB/T 31167-2014 云计算服务安全指南》中定义，云服务商提供给的云计算基础设施及其上的服务软件的集合

云计算环境

《GB/T 31167-2014 云计算服务安全指南》中定义，云服务商提供的云计算平台及客户在云计算平台之上部署 的软件及相关组件的集合

华为云控制台/管理控制台

华为云服务客户对所有云服务进行操作管理的控制台

弹性负载均衡 ELB

华为云服务。 ELB(Elastic Load Balance)将访问流量自动分发到多台云服务器，扩展应用系统对外的服务能力，实现更高水平的应用容错

虚拟私有云 VPC

华为云服务。VPC(Virtual Private Cloud)是云服务客户在华为云上申请的隔离的、私密的虚拟网络环境。云服务客户可以自由配置 VPC 内的 IP 地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性 IP 搭建业务系统

云监控服务 CES

华为云服务。CES（Cloud Eye Service）为云服务客户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。

Anti-DDoS 流量清洗

华为云服务。为华为云内资源（弹性云服务器、弹性负载均衡），免费提供基础 DDoS 防护，防护能力最高可达 5Gbps。本服务默认开启，实时检测攻击流量，秒级启动防御，并提供攻击实时告警（需配置告警通

虚拟专用网络 VPN

华为云服务。VPN(Virtual Private Network) 用于搭建云服务客户本地数据中心与华为云 VPC 之间便捷、灵活，即开即用的 IPsec 加密连接通道，实现灵活一体，可伸缩的混合云计算环境

SSL 证书管理服务 SCM

华为云服务。SSL 证书管理（SSL Certificate Manager）是华为联合全球知名数字证书服务机构，为您提供一站式证书的全生命周期管理，实现网站的可信身份认证与安全数据传输

安全组 SG

华为云服务。安全组（Security Group）是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。

云堡垒机 CBH

华为云服务。云堡垒机（Cloud Bastion Host）开箱即用，包含主机管理、权限控制、运维审计、安全合规等功能，支持 Chrome 等主流浏览器随时随地远程运维，开启高效运维新时代

企业主机安全 HSS

华为云服务。企业主机安全（Host Security Service）是服务器贴身安全管家，通过资产管理、漏洞管理、基线检查、入侵检测、程序运行认证、文件完整性校验，安全运营、网页防篡改等功能，帮助企业更方便地管理主机安全风险，实时发现黑客入侵行为，以及满足等保合规要求。

DDoS 高防

华为云服务。DDoS 高防是针对互联网服务器（包括非华为云主机）在遭受大规模 DDoS/CC 攻击后导致服务不可用的情况下，推出的付费服务。用户可通过华为云 T 级高防系统提供保护，确保关键业务连续性，广泛应用于政企门户、电商、游戏等场景。

Web 应用防火墙 WAF

华为云服务。Web 应用防火墙（Web Application Firewall）对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，阻挡诸如 SQL 注入或跨站脚本等常见攻击，避免这些攻击影响 Web 应用程序的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险

态势感知 SA

华为云服务。态势感知（Situation Awareness）为用户提供统一的威胁检测和风险处置平台。态势感知能够帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力

数据库安全服务 DBSS

华为云服务。数据库安全服务（Database Security Service）是一个智能的数据库安全防护服务，基于反向代理及机器学习机制，提供敏感数据发现、数据脱敏、数据库审计和防注入攻击等功能，保障云上数据库的安全

漏洞扫描服务 VSS

华为云服务。漏洞扫描服务（Vulnerability Scan Service）集 Web 漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测五大核心功能，自动发现网站或服务器在网络中的安全风险，为云上业务提供多维度的安全检测服务，满足合规要求，让安全弱点无所遁形

云审计服务 CTS

华为云服务。云审计服务（Cloud Trace Service）为您提供云账户下资源的操作记录，通过操作记录您可以实现安全分析、资源变更、合规审计、问题定位等场景。您可以通过配置 OBS 对象存储服务，将操作记录实时同步保存至 OBS，以便保存更长时间的操作记录

统一身份认证服务 IAM

华为云服务。统一身份认证服务（Identity and Access Management）提供身份认证和权限管理功能，可以管理用户（比如员工、系统或应用程序）账号，并且可以控制这些用户对您名下资源的操作权限

7.2 参考标准与规范

标准及规范编号	标准及规范名称
GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求
GB/T 25070-2019	信息安全技术 网络安全等级保护安全设计技术要求
GB/T 25058-2019	信息安全技术网络安全等级保护实施指南
GB/T 28448-2019	信息安全技术网络安全等级保护测评要求
GB/T 28449-2018	信息安全技术 网络安全等级保护测评过程指南
GB/T 31167-2014	信息安全技术 云计算服务安全指南
GA/T 1389-2017	信息安全技术 网络安全等级保护定级指南