



2025 年南网云深圳分节点扩容及边缘节点 建设项目（云平台管理软件） 技术条件书

深圳供电局有限公司

2025 年 7 月

目 录

1 项目概况	4
2 工作范围	5
2.1 供货范围	5
2.2 服务界限	6
2.3 项目工期	6
3 引用标准	6
4 技术要求	6
5 资料管理	42
5.1 文档范围	42
5.2 投标方的责任	42
5.3 文档种类	42
6 售后服务及技术培训	42
7 质量保证	43
8 试验与调试	43
8.1 验收要求	43
8.2 现场安装和现场试验	44
8.3 验收时间与地点	44
9 技术性能偏差表	44
10 投标方需说明的其他问题	44

总则

1.1 本技术条件书适用于 2025 年云平台管理软件采购，以及相关产品的功能、性能、安装等方面的技术要求。

1.2 本技术条件书提出的是最低限度的技术要求，并未对一切技术细节做出规定，也未充分引述有关标准和规范的条文，投标方应提供符合本技术条件书和工业标准的优质产品。

1.3 如果投标方没有以书面形式对本技术条件书的条文提出异议，则意味着投标方提供的设备(或系统)完全符合本技术条件书的要求。如有异议，不管是多么微小，都应在报价书中以“对招标技术文件的意见和同招标技术文件的差异”为标题的专门章节中加以详细描述。

1.4 本技术条件书所使用的标准如遇与投标方所执行的标准不一致时，按较高标准执行。

1.5 本技术条件书经招、投标双方确认后作为订货合同的技术附件，与合同正文具有同等法律效力。

1.6 投标方在应标技术文件中应如实反映应标产品与本技术条件书的技术差异。如果投标方没有提出技术差异，而在执行合同的过程中，招标方发现投标方提供的产品与其应标技术文件的条文存在差异，招标方有权利要求退货，并将对下一年度的评标工作有不同程度的影响。

1.7 投标方应在应标技术部分按本技术条件书的要求如实详细的填写应标设备的标准配置表，并在应标商务部分按此标准配置进行报价，如发现二者有矛盾之处，将对评标工作有不同程度的影响。

1.8 投标方应充分理解本技术条件书并按本技术条件书的具体条款、格式要求填写应标的技术文件，如发现应标的技术文件条款、格式不符合本技术条件书的要求，则认为应标不严肃，在评标时将有不同程度的扣分。

1.9 本技术条件书未尽事宜，由招、投标双方协商确定。

1 项目概况

深圳供电局有限公司以为“双区”建设发挥南网力量为己任，充分挖掘自身丰富的数据要素价值，全面聚合内、外部数据，全中心积累数据量达 100TB，记录数达 1000 亿条。为了加强数据资产运营，满足十四五规划建设新型电力系统和建立完善的数据资产管理体系要求，贯彻落实南网数字化转型战略部署，支撑深圳供电局数据供给服务中心体系构建，打造“高质量建设数据供给服务中心”，需要实现生产运行数据的实时全量采集供给，进一步加强公司数据供给服务能力，打造管理更有序、接入更广泛、处理更实时、数据更准确、运转更高效、服务更开放的数据供给服务中心，同时为了向一线业务的开展进行数据赋能，更大程度赋能公司高质量发展。

为了达成目标，公司在南方电网数字化部指导下，遵循“分层分区、全面感知、实时高效”原则，于网公司统一架构下建设III区数据中心深圳分节点，并与网级III区数据中心互通、与深圳IV区数据中心协同，为深圳业务提供数据采集、存储、计算及工具能力。至 2025 年，将实现IV区管理大区底座全域数据采集率 100%，数据规模达百 PB 级，处理能力达 TB/秒。同时，紧扣“全、快、好”三字，强化数据资产管理，全景展示数据链路，优化敏捷开发工具，提升数据质量监测与智能治理，推动数据赋能，激发全员数据应用创作热情，落实基层减负，提升全员数字化素养，以进一步完善提升底座基础能力。

落实公司《南方电网公司“十四五”数字化规划》指导要求，针对新型电力系统海量高速、灵活多样、突发弹性等特点，依托“3+1+X”数据中心云平台架构升级示范应用，中心算力与边缘算力协同建设，形成物理分布、逻辑统一的南网云“算力一张网”：

（1）扩建南网云深圳分节点，构建跨思明、新洲、深南三个机房的分布式云平台，具备数据中心水平扩展能力。

（2）建设基于云边协同的分布式边缘算力平台与区局边缘节点，以云基座对计算、存储和网络资源服务化，通过虚拟机或容器方式提供标准化计算资源，提供云侧（中心）向边缘赋能的技术基础，同时提供云边协同组件，边缘节点可通过云边协同技术，往边缘侧延伸能力，快速为本地电力作业智能化提供技术支撑，结合边缘云管平台实现对资源的统一管理，形成立体化资源配置管理，提升监控能力，打造良好的边缘侧云服务与支撑环境。

（3）为满足公司关键核心业务系统异地灾备需求，开展异地灾备环境云平台建设。

（4）结合人工智能大模型多模态威胁检测与上下文感知推理能力开展应用系统运行时安全风险识别管控及智能辅助决策，通过与各系统平台 API 深度解析适配、多源日

志语义关联分析、动态应用行为图谱构建、安全风险智能推理，辅助运维人员对异常活动识别、未知威胁检测、未经授权访问拦截等事件的处置决策支撑，全面提升应用系统安全响应及保障能力。

2 工作范围

2.1 供货范围

本技术条件书要求采购的云平台管理软件供货范围包括：

物资名称	规格型号	单位	数量
云平台管理软件	云平台管理软件（云基座软件 license）	套	72
	云平台管理软件（云安全组件 license）	套	72
	云平台管理软件（边缘算力云化服务组件 license）	套	120
	云平台管理软件（云边协同组件 license）	套	120
	云平台管理软件（边缘云安全组件 license）	套	120
	云平台管理软件(GPU 资源虚拟化平台 license)	套	44
	云平台管理软件（IaaS 平台授权许可）	套	93
	云平台管理软件（容器平台授权许可）	套	3000
	云平台管理软件（微服务平台授权许可）	套	2
	云平台管理软件（分布式存储软件授权许可）	套	23
	云平台管理软件（管理节点）	套	12
	云平台管理软件（网络节点）	套	6
	云平台管理软件（计算节点）	套	25
	云平台管理软件（安全节点）	套	62
	云平台管理软件（裸金属节点）	套	10
	云平台管理软件（块存储节点）	套	4
	云平台管理软件（应用安全风险识别管控智能辅助组件）	套	1
	云平台管理软件（网络性能监控组件）	台	318
	云平台管理软件（运行日志监控组件）	节点	700
	云平台管理软件（用户行为监控组件）	个	20
	云平台管理软件（业务流程监控组件）	个	20
	云平台管理软件（应用安全风险探测组件）	节点	700
	云平台管理软件（安全自动化响应平台授权）	套	1
	云平台管理软件（DHCP 系统软件）	套	1

2.2 服务界限

从生产厂家至招标方指定交货点的运输和装卸全部由投标方完成；

现场安装和试验在投标方的技术指导和监督下由招标方完成，投标方协助招标方按标准检查安装质量，处理调试投运过程中出现的问题。

2.3 项目工期

自合同签订之日起至 2026 年 6 月 30 日（具体实施期限以合同签订为准）。

3 引用标准

除本招标书另有说明外，投标方提供的所有设备均应按照下列标准进行设计、制造、检验和安装。所用的标准必须是最新版本。如果这些标准的内容有不同之处时，应按照最高标准的条款执行或按双方协商同意的标准执行。如果投标方选用本条件书以外的标准时，需提交这种替换标准相当于或优于本条件书规定的标准的说明。标准如下：

- (1) ISO-----国际标准化组织标准
- (2) IEC-----国际电工委员会标准
- (3) ITU-T----国际电信联盟标准
- (4) IEEE-----美国电气电子工程师协会标准
- (5) EIA-----电子工业协会标准
- (6) GB-----中华人民共和国国家标准
- (7) DL-----中华人民共和国电力行业标准
- (8) 《南方电网公司管理信息系统安全等级保护标准》
- (9) 《关键基础设施网络网络安全防护能力评价方法》
- (10) 《信息安全技术网络安全等级保护基本要求》
- (11) 其它招标方指定的规约

4 技术要求

其中★项目为关键参数。▲项目为重点评分项，如优于指标要求需提供证明材料并加盖公章。

1、★本项目采购的设备须满足自主可控要求，满足 IPv4/IPv6 协议双栈要求，提供承诺函。

2、★产品到货后按照国家及南网的要求，如需开展系统入网安评、商用密码应用安全性评估、信息系统安全等级测评及备案等合规性审查工作，以及如需开展数认平台、统一密码平台等安全管控系统接入集成工作，涉及相关系统集成及网络安全测评费用且无其他相关项目支撑的，由投标方承担所投产品的集成与测评费用，提供承诺函。

3、★采购设备在并网投运时应确保不存在弱口令风险，在维保期内发现弱口令风

险应按合同和技术协议要求整改，提供承诺函。

4、参数指标

云平台管理软件（云基座软件 license）（72 套）

指标项	指标子项	指标要求
分布式云基座	数字原生基座	▲具备自动部署、节点管理、快速扩容和在线升级能力。（需提供产品功能截图，并加盖厂商公章）
	自动化中心	管理员可以通过自动化中心实现云环境的管理，如日志导出、关闭环境、环境详情、存储配置、服务器硬盘维护、节点管理等功能，为用户提供易用的管理界面。
	计量服务	通过计量服务功能管理员在概览页可以查看云主机情况及资源使用情况，包括计算节点状态、存储集群 IOPS 等；在告警管理页，支持针对云主机进行自定义监报告警、通过设置 CPU 、内存、磁盘、网络资源的监控阈值进行自定义告警，支持选择通知列表；同时支持统一的日志收集和导出平台，包平台操作日志、系统日志、节点日志等。
	定时服务	定时服务提供多种常用的定时备份任务，提供便捷的自动化运维能力。同时定时备份支持多条备份链，最大限度满足对数据备份的细粒度控制。
	内置常用操作	数据备份常用的云主机快照、云硬盘快照、云硬盘备份等高频操作都已经内置到服务中，开箱即用。
多元算力调度组件	/	▲提供计算资源池管理、存储资源池管理、网络资源池管理、容器算力调度等能力。（需提供产品功能截图，并加盖厂商公章）
分布式云资源及应用编排组件	/	采用可视化编排服务根据用户的业务需求情况，通过可视化界面任意拖拽图元，快速完成计算、存储、网络、应用等资源的自动化部署，并作为一个整体为用户服务，支撑业务快速上线。同时编排部署提供了通过编排模板快速部署复杂环境的服务，可以使用平台创建可视化编排模板，也可以通过上传 YAML 文件完成编排部署，实现业务的快速上线。
性能要求	分布式存储	分布式存储集群提供单盘读写性能不低于 100 IOPS, 10GB/s。
	集群规模	集群可支持 10000 个计算节点。
		单节点支持虚拟机不少于 1000 个。
	虚拟机创建性能	在并发 1000 个虚拟机创建请求条件下，创建完成时间不超过 10 秒。
	网卡性能	虚拟机的网卡性能损失小于 5%。
其它要求	软件许可	★每套组件许可支持 1 台服务器永久授权，并提供承诺函。

云平台管理软件（云安全组件 license）（72 套）

指标项	指标要求
总体要求	▲云安全组件支持兼容主流云厂家，包含但不限于华为云、阿里云、天翼云。（需提供第三方测试报告证明）
云安全管理平台	云安全管理平台统一管理云防火墙、云 web 应用防护系统、云堡垒机、云日志审计、云数据库审计、云漏洞扫描、云主机安全、云容

	器安全等安全网元。
云防火墙	能够精确识别用户、应用和内容，支持完整的 L2-L7 层安全防护体系。 支持静态路由、RIP 和 OSPF 动态路由、策略路由等多种路由协议；支持 IPv4/IPv6 双栈工作模式。
入侵防御系统	通过对网络流量的深度解析，可及时准确发现各类非法入侵攻击行为，并执行实时精确阻断，主动而高效的保护用户网络安全。 支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。 ▲支持内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。(需提供产品功能截图证明，且加盖厂商公章)
云主机安全	支持针对云主机的全网资产细粒度清点、全面的入侵行为检测、风险评估（弱密码检测、漏洞检测、基线检查）、轻量级病毒查杀、威胁统一处置相关能力。 支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直接看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析。
云 WEB 应用防护系统	专注于网站及 Web 应用系统的应用层专业安全防护，有效地缓解网站及 Web 应用系统面临的常见威胁，并且可以快速地对恶意攻击者对 Web 业务带来的冲击，实现 Web 业务应用安全与可靠交付。 全面实施并严格遵守 OWASP TOP10 的安全防护措施，以确保系统的安全性。
云堡垒机	能够提供集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计为一体的运维安全审计服务。能够对服务器、网络设备、安全设备、数据库等资产的运维操作过程进行有效的运维操作审计，使运维审计由事件审计提升为操作内容审计。 支持以下协议：SSH(V1、V2)、TELNET、RDP、VNC、FTP、SFTP、ORACLE、MSSQL、Sybase、Mysql、DB2 数据库远程访问审计。
云日志审计	能够实时不间断地采集汇聚云主机、操作系统和业务系统的日志信息，协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及违规事件。 支持以下协议：SSH(V1、V2)、TELNET、RDP、VNC、FTP、SFTP、ORACLE、MSSQL、Sybase、Mysql、DB2 数据库远程访问审计。
云数据库审计	能够实时监控对数据库服务器的操作流量，智能解析出各种操作，并提供日志报表系统分析，为进行事后的分析、取证提供证据。 可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。
云漏洞扫描	能够准确、快速、及时地发现、汇总不同主机、数据库、中间件和网络及安全产品的安全配置问题、漏洞情况。 支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫

	描、WEB 漏洞扫描、弱口令扫描同时执行。
云容器安全	支持镜像软件供应链安全、容器运行时工作负载安全、容器平台环境基础设施安全、容器网络应用安全保障。 ▲支持自定义添加仓库并配置需要扫描的镜像，至少兼容 8 种镜像仓库，包括 Docker Registry、Harbor、JFrog、华为云 SWR、腾讯云 Coding、Nexus、阿里云 ACR、火山引擎 Vestack 敏捷版 CR 等主流镜像仓库。（需提供产品界面截图，并加盖厂商公章）
软件许可	★每套组件许可支持 1 台服务器永久授权，并提供承诺函。

云平台管理软件（边缘算力云化服务组件 license）（120 套）

指标项	指标子项	指标要求
软件规格	软件要求	▲支持 X86、ARM 架构 CPU 算力设施混合部署，支持不少于 2 种国产化 CPU。（需提供功能截图，并加盖原厂公章）
边缘云基座	总体要求	提供容器、虚拟机运行环境，具备算力、网络、存储资源的基础管控能力。为边缘侧提供稳定的算力轻量化云环境。具备分布式存储能力，提供统一存储，实现同一套存储系统为上层应用提供块、文件和对象三种数据服务，满足业务对结构化和非结构化数据的存放需求，并且内置数据保护功能，如：备份、容灾等，同时提供多种企业级特性，包括快照、自动备份、压缩等，帮助企业轻松应对业务快速变化时的信息灵活、可靠存取需求。 支持计算存储资源融合部署，支持块存储、文件存储。 支持不超过三个物理服务器部署。 ▲支持与南网云平台对接，满足南网云平台远程实时监控云基座运行状态等相关指标；（需提供承诺函，并加盖原厂公章）
	存储能力	至少同时支持副本、纠删码两种以上数据可靠性保证技术；支持全闪存和混闪两种部署模式。 提供存储容量在线动态伸缩功能。 支持 NFS/FTP/S3 协议互通。 支持存算分离能力，提供以 virtio-blk 接口为裸金属服务器提供硬盘读写能力。 支持在线快照，秒级虚拟机创建快照，不影响现有业务，性能无损失。 支持 iSCSI、CSI、RBD 等多种协议对接访问。 支持一致性组快照管理；支持创建、编辑、删除一致性组，创建组快照、一致性组回滚、一致性组快照复制。 支持多协议互通。NFS/CIFS/FTP/S3/HDFS 协议互通，任意一个协议写入的文件，其他协议无需搬迁，可直接读写同一份数据，性能无损访问。 支持在线对存储进行动态调整，如添加或删除磁盘，对磁盘进行扩容缩容。

		<p>支持集群高可用部署,单集群至少允许三分之一节点或不同节点任意 2 块硬盘同时故障,存储服务不中断,数据不丢失,持续提供数据服务。</p> <p>▲支持块存储卷 CSI-iSCSI 功能,为容器提供持久化存储卷并支持扩容功能。（需提供功能截图,并加盖原厂公章）</p> <p>4K 随机读 IOPS 不低于 90000,时延不高于 6ms。</p> <p>4K 随机写 IOPS 不低于 40000,时延不高于 4ms。</p> <p>1MB 顺序读速率不低于 2500MB/s。</p> <p>1MB 顺序写速率不低于 800MB/s。</p> <p>1MB 顺序读写混合速率不低 1200MB/s。</p>
本地运维监控	总体要求	提供无人化/少人化运维,实时管控边缘各组件以及监控地市边缘节点节点和服务的运行状态,提高边缘运维效率,降低边缘的运维成本。
	运维能力	<p>▲支持对中心侧（南网云平台）下放的业务服务（标准 docker 镜像）进行本地部署操作。（需提供功能截图,并加盖原厂公章）</p> <p>支持边缘本地实时查看业务服务的运行状态。</p>
	监控能力	<p>支持监控云主机的负载情况,如当前 CPU 和内存使用率等。</p> <p>支持监控边缘集群核心服务的运行状态,和相关性能指标。</p> <p>支持纳入中心云监控。</p>
其它要求	软件许可	★每套组件许可支持 1 台服务器永久授权,并提供承诺函。

云平台管理软件（云边协同组件 license）（120 套）

指标项	指标子项	指标要求
软件规格	总体要求	支持云边的资源协同、制品协同、应用协同、安全协同以及数据协同,打造与中心侧平台体验一致的云服务与支撑环境,保持云边能力一致性,为多场景应用提供统一管理。
		支持 arm64 和 x86 架构环境下部署。
		支持容器化部署。
		组件自身的持久化数据支持两种及以上数据库存储
		应用协同服务接口响应时间小于 2 秒。
		▲监控协同数据同步到中心云延时时间不超过 10 秒。（需提供功能截图,并加盖原厂公章）
		支持按需从中心侧下放各类技术或应用组件到边缘进行本地化部署。
资源协同	资源监控采集	支持收集边缘集群资源信息,如边缘主机运行指标、边缘组件运行指标和边缘应用运行指标。
	监控数据上报	支持将边缘集群的相关资源监控指标上送到中心侧的监控中心。
		边缘集群通过资源协同代理作为边缘侧资源监控数据的统一出口,向云端监控协同服务上报资源监控数据。

安全协同	统一安全管控	提供中心侧统一管控各地边缘节点的安全管控方式，收缩边缘安全管控面。支持南网云安全中心的统一管控调度，实时上送安全运行信息，形成分布式的数字安全防护体系，保障中心和边缘的整体安全。
应用协同	集成要求	提供边缘一个统一的外部访问出口，与中心云（南网云平台）的应用交互服务对接，实现了中心云和边缘集群的应用接口交互能力。
	交互策略	支持通过安全管道和云端保持长链接通信能力。能够根据云端下发的交互策略启动相应的交互策略服务，为边缘应用提供和云端通信能力的访问地址。
数据协同	数据同步	支持通过云边数据通道，实现边侧数据汇聚至云端进行数据分析挖掘，以及云端数据下发至边侧进行控制。
	数据共享	支持边端数据在云端共享与开放，实现对云端业务场景的决策支撑。
其它要求	软件许可	★每套组件许可支持 1 台服务器永久授权，并提供承诺函。

云平台管理软件（边缘云安全组件 license）（120 套）

指标项	指标要求
总体要求	<p>▲云安全组件支持兼容主流云厂家，包括但不限于华为云、阿里云、天翼云。（需提供第三方测试报告证明）</p> <p>支持基于边缘云基座轻量化部署。</p> <p>支持边缘安全组件受中心侧统一部署和安全策略管理。</p> <p>支持边缘安全组件受中心侧统一运行状态实时监控。</p>
云防火墙	<p>能够精确识别用户、应用和内容，支持完整的 L2-L7 层安全防护体系。</p> <p>支持静态路由、RIP 和 OSPF 动态路由、策略路由等多种路由协议；支持 IPv4/IPv6 双栈工作模式。</p>
入侵防御系统	<p>通过对网络流量的深度解析，可及时准确发现各类非法入侵攻击行为，并执行实时精确阻断，主动而高效的保护用户网络安全。</p> <p>支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。</p> <p>▲支持内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。（需提供产品功能截图证明，且加盖厂商公章）</p>
云主机安全	<p>支持针对云主机的全网资产细粒度清点、全面的入侵行为检测、风险评估（弱密码检测、漏洞检测、基线检查）、轻量级病毒查杀、威胁统一处置相关能力。</p> <p>支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直接看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析。</p>
云 WEB 应用防护系统	<p>专注于网站及 Web 应用系统的应用层专业安全防护，有效地缓解网站及 Web 应用系统面临的常见威胁，并且可以快速地对恶意攻击者对 Web 业务带来的冲击，实现 Web 业务应用安全与可靠交付。</p> <p>全面实施并严格遵守 OWASP TOP10 的安全防护措施，以确保系统的</p>

	安全性。
云堡垒机	能够提供集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计为一体的运维安全审计服务。能够对服务器、网络设备、安全设备、数据库等资产的运维操作过程进行有效的运维操作审计，使运维审计由事件审计提升为操作内容审计。 支持以下协议：SSH(V1、V2)、TELNET、RDP、VNC、FTP、SFTP、ORACLE、MSSQL、Sybase、Mysql、DB2 数据库远程访问审计。
云日志审计	能够实时不间断地采集汇聚云主机、操作系统和业务系统的日志信息，协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及违规事件。 支持以下协议：SSH(V1、V2)、TELNET、RDP、VNC、FTP、SFTP、ORACLE、MSSQL、Sybase、Mysql、DB2 数据库远程访问审计。
云数据库审计	能够实时监控对数据库服务器的操作流量，智能解析出各种操作，并提供日志报表系统分析，为进行事后的分析、取证提供证据。 可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。
云漏洞扫描	能够准确、快速、及时地发现、汇总不同主机、数据库、中间件和网络及安全产品的安全配置问题、漏洞情况。 支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。
云容器安全	支持镜像软件供应链安全、容器运行时工作负载安全、容器平台环境基础设施安全、容器网络应用安全保障。 ▲支持自定义添加仓库并配置需要扫描的镜像，至少兼容 8 种镜像仓库，包括 Docker Registry、Harbor、JFrog、华为云 SWR、腾讯云 Coding、Nexus、阿里云 ACR、火山引擎 Vack 敏捷版 CR 等主流镜像仓库。（需提供产品界面截图，并加盖厂商公章）
软件许可	★每套组件许可支持 1 台服务器永久授权，并提供承诺函。

云平台管理软件(GPU 资源虚拟化平台 license)（44 套）

指标项	指标要求
资源注册与注销	支持 GPU 资源注册与注销，用户可以通过统一界面进行纳管服务器、推理加速资源（GPU）。 支持手动注销指定的 GPU 资源。
资源聚合	提供 GPU 资源聚合功能，包括单机多卡、多机多卡等应用场景。满足对 GPU 需求量较大的场景。并支持限制和隔离单个服务容器所占用的 GPU 资源数。（需提供功能截图，并加盖原厂公章）
资源拆分	提供 GPU 单卡资源算力拆分功能。多个服务容器可共享单张 GPU 卡，并支持限制和隔离每个服务容器所占用的 GPU 算力、显存额度。保障服务间互不干扰，保障服务性能。（需提供功能截图，并加盖原厂公章）
远程 GPU 调度	支持提供 GPU 资源远程调度的能力，即 AI 训练或推理服务部署在非

	GPU 主机上，借助集群内其他 GPU 主机实现远程 GPU 的加速能力，并保障服务性能。
支撑深度学习框架	▲支持基于多种深度学习框架的训练、推理等 AI 应用，深度学习框架包括但不限于 TensorFlow、pytorch、caffe2、mxnet、paddlepaddle、MindSpore 等。（需提供功能截图，并加盖原厂公章）
动态调整	支持 GPU 资源动态调整功能，确保业务服务容器所分配的资源量可动态的调整。
资源超售	支持 GPU 资源超售功能，业务服务使用 GPU 资源时允许按一定比例超过配额。在不扩容硬件 GPU 资源的前提下，允许更多用户共享 GPU 资源池的算力资源。
配额管理	支持为基于 Docker 的容器，基于 KVM 的虚拟机和基于 Linux 操作系统的 AI 应用提供 GPU 资源配额（虚拟 GPU），并且资源配额是动态可调的。
资源调度策略	支持为业务服务分配 GPU 资源时，用户可根据实际需求，选择更合理的调度策略，包括随机调度、本地优先、远程优先以及组合调度策略等。
兼容 Kubernetes 容器集群	支持为 kubernetes 容器集群提供 GPU 资源的功能，并能够与南网现有 Kubernetes 容器集群无缝对接，不影响 Kubernetes 容器集群业务。
系统兼容性	支持 NVIDIA P40、V100、A100、T4、A10、A30 等 GPU 卡。 ▲支持华为昇腾 910B、昆仑芯 P800、Atlas 300I 等国内主流 GPU 卡。 支持 CUDA 9 及以上版本。（需提供承诺函，并加盖原厂公章） 支持 Kylin V10 及以上版本。 支持 Docker 1.13 及以上版本，支持 Kubernetes 1.10 及以上版本。
监控服务	对系统纳管的 GPU 资源，提供相应的监控服务，包括资源池纳管的 GPU 资源总体情况统计，业务服务所申请的 GPU 资源利用率等情况统计，保障申请的 GPU 资源更加贴近实际需要，从总体上提升 GPU 资源利用率。
软件许可	★每套许可支持至少 1 个 GPU 卡永久授权。（需提供承诺函，并加盖原厂公章） ▲在质保期内可免费解绑并重新绑定任意型号的 GPU 卡。（需提供承诺函，并加盖原厂公章）

云平台管理软件（IaaS 平台授权许可）(93 套)

指标项	指标子项	指标要求
分布式云基座	数字原生基座	▲具备自动部署、节点管理、快速扩容和在线升级能力。（需提供产品功能截图，并加盖厂商公章）
	自动化中心	管理员可以通过自动化中心实现云环境的管理，如日志导出、关闭环境、环境详情、存储配置、服务器硬盘维护、节点管理等功能，为用户提供易用的管理界面。
	计量服务	通过计量服务功能管理员在概览页可以查看云主机情况及资源使用情况，包括计算节点状态、存储集群 IOPS 等；在告警管理页，支持针对云主机进行自定义监报告警、通过设置 CPU、内存、磁盘、网络资源的监控阈值进行自定义告警，支持选择通知列表；同时支持统一的日志收集和导出平

		台，包平台操作日志、系统日志、节点日志等。
	定时服务	定时服务提供多种常用的定时备份任务，提供便捷的自动化运维能力。同时定时备份支持多条备份链，最大限度满足对数据备份的细粒度控制。
	内置常用操作	数据备份常用的云主机快照、云硬盘快照、云硬盘备份等高频操作都已经内置到服务中，开箱即用。
多元算力调度组件	/	▲提供计算资源池管理、存储资源池管理、网络资源池管理、容器算力调度等能力。（需提供产品功能截图，并加盖厂商公章）
分布式云资源及应用编排组件	/	采用可视化编排服务根据用户的业务需求情况，通过可视化界面任意拖拽图元，快速完成计算、存储、网络、应用等资源的自动化部署，并作为一个整体为用户服务，支撑业务快速上线。同时编排部署提供了通过编排模板快速部署复杂环境的服务，可以使用平台创建可视化编排模板，也可以通过上传 YAML 文件完成编排部署，实现业务的快速上线。
性能要求	分布式存储	分布式存储集群提供单盘读写性能不低于 100 IOPS, 10GB/s。
	集群规模	集群可支持 10000 个计算节点。
		单节点支持虚拟机不少于 1000 个。
	虚拟机创建性能	在并发 1000 个虚拟机创建请求条件下，创建完成时间不超过 10 秒。
	网卡性能	虚拟机的网卡性能损失小于 5%。
其它要求	软件许可	★每套组件许可支持 1 台服务器永久授权，并提供承诺函。

云平台管理软件（容器平台授权许可）（3000 套）

指标项	指标要求
跨可用区部署	支持将一个容器集群跨可用区部署。
容器运行时	支持多种容器运行时组件，包括 docker、containerd。
网络	▲支持和 VPC 网络、云负载均衡、分布式云存储、云监控、权限管理等云产品和功能模块进行无缝集成。（需提供产品功能截图，并加盖厂商公章）
	支持多种容器网络插件，能够直接分配 VPC 地址给到 POD
弹性伸缩	支持 Worker Node 节点的自动弹性伸缩。
软件许可	★每套许可适用于 1 核 VCPU 配置，软件永久授权，并提供承诺函。

云平台管理软件（微服务平台授权许可）（2 套）

指标项	指标要求
软件许可	★每套许可适用于 100pod，软件永久授权，并提供承诺函。
安全策略	支持用户访问安全策略（包括密码安全、用户禁用、用户锁定、访问控制策略等）设置，防范恶意用户的安全威胁（如恶意登录、账号长期不登出等），满足用户访问安全性增强的业务场景需求。
微服务治理能力	应用支持无损发布，实现应用确定已经能提供服务之后，应用实例才会被注册到注册中心。
	▲支持服务熔断配置。允许服务消费者针对服务提供者的接口、实例、

	服务进行熔断处理。可以根据请求错误率、延时等进行熔断。（ 需提供产品功能截图，并加盖厂商公章 ）
	支持与资源解耦，提供灵活的部署方式，支持部署在虚拟机和容器上
	支持单元化架构，对应用进行单元化切分，按规则进行单元路由；支持可视化单元管理、单元切换。
监控能力	支持多维度界面化监控视图，如平台视角、集群视角、集群主机视角、应用视角、容器视角。
	支持平台组件的健康状态自动检测。
兼容性要求	支持与第三方容器集成，支持对接开源 K8S 和基于 K8S 的商业化产品。

云平台管理软件（分布式存储软件授权许可）（23 套）

指标项	指标要求
存储组件 License	★容量授权不区分磁盘介质、存储服务类型，不限制节点数量，可灵活分配容量授权到不同的存储需求。每套许可适用于 1 个存储节点配置，软件永久授权，并提供承诺函。
可信安全	▲满足信创要求，一个存储池可以同时支持多种架构 CPU（鲲鹏，飞腾，海光，Intel），同时提供块、文件、对象和大数据服务。（ 需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章 ）
	支持基于国产操作系统部署，至少支持兼容银河麒麟 V10、统信 UOS v20，并提供兼容性互认证证书。
全协议	同一个存储池支持 iSCSI/RBD/FC/NFS/CIFS/FTP/HDFS/S3 存储协议。
块存储要求	支持卷管理操作，精简配置，在线扩容。
	支持 iSCSI，FC，CSI 和 RBD 原生访问。
	支持卷 QoS，支持在线调整 QoS，实时生效。
	支持卷回收站，防止数据误删除，可设置回收策略。
	▲支持块存储卷 CSI-iSCSI 功能，为容器提供持久化存储卷并支持扩容、快照、克隆功能。（ 需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章 ）
文件存储要求	支持日志审计，提供文件系统操作日志功能，日志类型可以开启或关闭。
	文件系统支持在线整池扩容。
	支持目录 QoS，可以为单个目录配置 IOPS 或带宽上限。
	支持目录快照，支持手动快照和定时快照，支持快照回滚。
	支持文件 WORM 功能，文件在保护期内不能篡改或删除。
	▲支持 NFS/CIFS/FTP/S3/HDFS 协议互通。（ 需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章 ）
	支持目录配额，支持容量配额，文件数配额，硬配额，软配额等。
	支持目录回收站，可以设置保留时间。
对象存储要求	支持 Amazon S3 标准接口，兼容 S3 生态体系。
	对象压缩加密，支持给桶设置压缩率阈值功能，达到压缩率阈值的对象会被正常压缩，未达到压缩率阈值的对象不会被压缩。
	支持桶快照，支持快照回滚。
	支持桶回收站功能，桶删除后会进入桶回收站，可以从桶回收站恢复被删除的桶。
	数据生命周期管理，可以根据前缀、元数据、标签、拥有者等过滤条

	件定义不同的数据集，数据集按规则实现数据流动；对数据集设置过期时间，支持按设定天数过期，也支持按指定时间点过期，到期后自动删除对象。
	支持在集群内不同数据存储类别间分层流动，从热层转换为温层，或从温层转换为热层，双向都能转换。
	支持重定向、代理、镜像、CDN 回源配置，当本地集群出现灾难时，可以通过分层数据反向重建集群，实现灾难重建。
	▲支持数据纳管，从第三方存储反向重建对象索引到本集群，纳管第三方存储上的数据。（需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章）
	支持按桶或业务设置 QoS。
	支持指定顺序将多个对象快速合成一个大对象。
运维要求	支持自动重平衡，发现集群容量不均衡的时候，会自动重平衡。
	系统盘故障后，重装系统只重构差异数据，不用全量重构，减少恢复时间。
	以可视化的视图展示硬盘的基本信息及从属关系，基本信息包括：硬盘名称、状态、容量、已使用容量、数据恢复情况、硬盘介质、IO 利用率等。从属关系包括从属服务器视图和从属存储池视图。
	可视化硬件网络拓扑，直观展现集群网络情况、数据中心、机架、服务器、网卡信息。同时可以可视化展现集群网络中各个模块的异常情况。支持不同网卡的监控信息及监控历史。
	支持集群内所有资源的告警，支持自定义告警通知，告警会显示告警原因和建议解决意见，当故障恢复之后，告警自动恢复。
	触发告警之后，当告警解除之后，界面自动标记该告警为已解决状态，告警自动恢复。
数据保护要求	▲支持副本和 EC，块、文件和对象全场景 EC，支持精简 EC。（需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章）
	配置存储卷级别的异步复制功能，基于快照级别的分钟级异步复制，实现与备份集群数据容灾。
	▲支持双活数据中心功能。（需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章）
	支持按前缀、后缀、标签、对象类型等定义数据集，不同的数据集按策略配置桶复制，复制过程中可以执行 QoS 控制。
	系统全冗余架构，控制器之间必须是高可用架构。任何一个控制器出现故障，不影响数据的正常访问。
	支持多级故障域，在线升级故障域，从节点升级到机架，机房。
	在数据处于降级状态时，系统会自动触发数据重建恢复。可根据业务压力自动调整数据恢复带宽，最小化对业务的影响。
	支持磁盘亚健康，对于故障盘或慢盘，即时检测告警，自动隔离并可解除隔离。
	支持网络亚健康，对于故障盘或慢盘，即时检测告警，自动隔离并可解除隔离。
灵活性要求	▲支持缓存池和数据池解耦，独立部署，缓存池和数据池独立扩容，互不影响。（需提供具备 CMA 或 CNAS 标识的第三方测试报告，并加盖厂商公章）
	支持在线动态扩容。支持通过增加访问节点、存储节点、存储磁盘等

	方式实时对存储容量进行扩充，动态扩容期间服务不中断，对外服务能力不下降。扩容完成后，无需人工迁移数据，数据会自动均匀平衡数据到新增存储节点或磁盘。
--	---

云平台管理软件（管理节点）（12套）

指标项	指标要求
用户管理	支持用户的创建、删除、修改、查询、禁用、重置密码等操作，并可限定每个用户操作的资源范围；用户忘记密码后，可以通过邮箱、短信找回密码。
权限管理	支持按资源空间、企业项目模型进行授权管理；支持按操作授权，包括按组织、服务、应用、计量、审批等操作进行精细化授权控制。
虚拟数据中心	提供虚拟数据中心（VDC）管理能力，支持 5 级 VDC 管理，匹配用户的组织架构。每个 VDC 有独立的资源访问权限，有独立的云服务管理权限。
租户管理	提供的灵活组织模型管理能力，包含租户、多级 VDC、企业项目、资源空间、用户组等。
配额管理	▲支持对 VDC 使用的资源进行配额限制，包括但不限于虚拟机、裸金属、镜像、云硬盘、VPC、弹性 IP、网络 ACL、VPN、虚拟负载均衡等服务。（需提供功能截图，并加盖厂商公章）
	支持提供云服务配额明细统计，支持提供云服务配额明细统计，支持按照 VDC、资源空间、云服务、区域维度的详细统计，支持基于区域、服务、资源池、可用分区的配额使用 Top 统计图表。
标签管理	为方便资源统一管理和快速检索，支持用户创建自定义标签并关联到各类云资源，支持在运营管理侧创建、删除标签，支持在云资源申请时打标签。
服务自定义	▲支持自定义服务目录，包括自定义云主机、云硬盘、网络等基础云服务、自定义组合的应用服务。（需提供功能截图，并加盖厂商公章）
	支持服务的白名单能力，可以指定服务对组织的可见度设置。
统一资源管理	▲支持统一资源管理，包括各类云资源、脚本资源、软件资源，支持查看已分配资源和资源回收站。（需提供功能截图，并加盖厂商公章）
	支持提供丰富的脚本类型，包括安装、配置、启动、故障自愈等脚本分类，默认预置 30+脚本资源。
应用管理	支持为应用添加或删除云主机、裸金属等资源。应用管理所管理的对象是由一组云服务实例编排组合而成的，承担某种业务系统的业务单元。
	支持自动生成应用拓扑，当应用中加入、删除资源后，应用拓扑支持自动刷新。
	支持在云服务资源上部署软件、执行脚本，能够在界面上可视化编排软件部署流程。
流程审批	支持将产品或服务跟审批流程关联，关联后该产品或服务的订单需要按照该审批流程进行审批。
代维管理	为提升云资源运维效率，云管平台支持跨租户代维管理，支持跨一级 VDC 代维，代维账号可以进入被代维的多个一级 VDC 进行代维。

日志审计	支持统一的操作日志管理能力，操作日志记录用户对云平台各类资源所做的操作以及操作的结果，用于日志审计、日志分析。
回收站	支持用户删除资源后保留到回收站，允许误删除后恢复资源，支持资源冻结期设置。支持的回收站的资源包括云主机、云磁盘等。
集中监控	支持对类资源的告警、性能指标等进行全方位监控，及时了解资源运行状态。
告警管理	支持云平台下物理资源和虚拟资源的统一监控管理。物理资源管理包括监控服务器、网络设备（交换机、路由器、防火墙、负载均衡等）、存储设备的位置信息、告警信息以及性能信息等。
	虚拟资源管理包括可按 VDC 统计服务使用情况、按资源池统计资源总量、云内虚拟网元对象性能监控信息（包括虚拟负载均衡的连接数等监控指标）等。
报表管理	支持容量、资源、设备统计、资源利用率、告警统计报表。支持报表自定义呈现，管理员可对已有指标进行重新组合、过滤以实现自助式业务分析。
日志分析	提供运维侧管理日志和租户操作日志的统一汇聚和查询，帮助管理员了解系统运行状况，了解用户行为，排查系统故障，识别并消除安全威胁。
	提供统一运行日志中心，支持按需下载各云服务管理面和租户面运行日志，辅助故障定位。通过查看运行日志，可以及时发现影响系统运行状态的因素，以采取相应措施，保证系统的正常运行。
容量管理	支持资源容量分析，管理员可按照不同维度（数据中心/区域、不同资源池、不同的可用分区、不同主机组/集群）查看计算、存储、网络资源的使用情况和分配情况。
	▲支持资源闲置分析，支持根据具体的业务需求，设定需要的闲置资源判定规则。支持灵活的闲置规则设置，包括资源创建时间、持续闲置时长、使用率算法、闲置条件等，其中闲置条件支持 CPU 使用率、内存使用率。（需提供功能截图，并加盖厂商公章）
	▲支持资源瓶颈分析，支持根据具体的业务需求，设定需要的瓶颈资源判定规则。支持针对需要扩容 vCPU、内存、磁盘给出容量扩容建议。支持灵活的瓶颈规则设置，包括资源创建时间、持续瓶颈时长、使用率算法、瓶颈条件等，其中瓶颈条件支持 CPU 使用率、内存使用率。（需提供功能截图，并加盖厂商公章）
自动化运维	支持自定义运维脚本，将运维脚本批量下发到指定虚拟机、裸金属、计算/管理节点并执行。
	支持将不同脚本按照一定逻辑、流程编排成运维任务，管理员可以选择定时执行、周期执行、手动执行等多种方式调度运维任务。
	自动化作业执行策略支持手动执行、定时(单次)执行、周期执行和告警触发。
智能巡检	支持创建自定义巡检任务，支持日常巡检和升级前巡检，日常巡检支持实时任务、定时任务、周期任务，支持导出巡检报告，报告包含巡检任务的基本信息、检查结果和处理建议等。
大屏能力	支持自定义多种不同的大屏展示内容，自定义内容包括容量、性能、资源统计、告警等对象。可定义每个内容的不同呈现形式，包括柱状图、饼图、仪表盘等。

云平台管理软件（网络节点）（6套）

指标项	指标要求
虚拟私有网络	支持用户自助创建私有、隔离的虚拟网络环境，每个虚拟网络环境包含一套虚拟出口路由器、若干虚拟防火墙以及子网网络等。用户可以独立配置自己的网络环境，包括自助创建子网（IPv4、IPv4&IPv6）、指定子网网段/网关/掩码、子网使用的 DNS 等参数，支持为子网中云服务器配置静态路由。
	支持添加多段地址空间，支持在地址扩容场景添加容器或者 IaaS 扩展地址空间，一个 VPC 支持添加一个主网段和 3 个扩展网段。
	为保障业务组网灵活性，VPC 和子网创建时无需指定 AZ 可用域，天然支持跨 AZ 网络能力。
	为保障业务组网灵活性，云主机和裸机支持共用一个 VPC 子网，无需为裸机单独创建专用网络。
	▲支持虚拟机网卡 QoS 限速，避免虚拟机网络风暴或负载过高影响其他业务。支持将 QoS 限速规则批量设置到多个网卡和云主机。（需提供功能截图，并加盖厂商公章）
	支持为云主机在线添加网卡并设置 IP 地址，支持单台云主机配置不少于 15 个网卡。
	支持不同租户子网设置不同 NTP 服务源、DNS 服务源，方便不同租户应采用不同的 NTP 和 DNS 配置。
安全组	支持 VPC 拓扑，支持图形化拓扑展示当前 VPC 的子网信息，以及使用该子网的云服务信息。
	支持安全组服务，可以对进出虚拟机端口的网络报文进行安全过滤规则设置。虚拟机端口与安全组关联后，安全组规则可对进出虚拟机端口的网络报文进行过滤，只有规则允许的报文可通过。
	支持安全组规则的导入、导出操作。
	支持安全组绑定到不同 VPC 的云主机，支持关联安全组到辅助网卡。
	支持快速添加安全组入方向规则和出方向规则，界面提供常见协议端口可视化勾选，包括远程登录和 ping、Web 服务、常见数据库端口、常见网络协议、权限控制端口。
	▲支持安全组克隆，快速复制原安全组出入方向规则。（需提供功能截图，并加盖厂商公章）
NAT 网关	安全组内支持对 TCP、UDP、ICMP、ANY 协议进行配置。支持指定安全组出/入方向过滤的对象，过滤对象可以为 IP 段（可以指定 TCP/UDP 的源/目的 IP 及端口）、其它安全组等。
	支持在管理界面上进行 NAT 网关实例创建、修改和删除，每个 NAT 网关实例可配置 SNAT 规则和 DNAT 规则。
	支持自定义 SNAT 规则使用的公网 IP 和子网，可以增加，修改和删除规则。
	支持 SNAT 绑定多个 EIP，一条规则可以配置多个弹性 IP。

	支持自定义 DNAT 规则使用的公网 IP 和服务端口，私网 IP 和服务端口，端口可以用指定单个，也可以指定范围，支持增加、修改和删除单个规则，支持批量删除规则。
弹性 IP	支持将 EIP 与弹性云服务器、裸金属服务器、弹性负载均衡、虚拟 IP 等对象进行绑定。支持弹性 IP 地址的绑定、解绑定以及释放功能。
	支持租户界面批量申请弹性 IP 地址，可以自行选择弹性 IP 地址所属的地址池、分配方式（自动分配或者手动分配）等策略。
负载均衡	支持负载均衡服务，负载均衡服务基于软件方式实现，不依赖于特殊硬件设备。可以将用户业务访问流量自动分发到多台云服务器，扩展应用系统对外服务能力。
	▲支持用户通过云平台在已有的负载均衡上创建监听器，支持四层、七层的监听策略。支持配置监听器的监听协议/端口，支持四层以及七层协议；支持负载的加权轮询算法、加权最少连接、源 IP 算法等分配策略；支持 IP 地址、HTTP cookie、应用程序 cookie 等会话保持策略。（需提供功能截图，并加盖厂商公章）
	▲支持多种转发规则配置转发策略，支持基于 HTTP 请求头、域名、URL、网段多种规则进行转发，实现基于业务的灵活调度。（需提供功能截图，并加盖厂商公章）
	支持开启高级转发策略功能。开启高级转发策略功能之后，支持转发策略排序，支持单条转发规则中添加多个条件，支持添加重定向至 URL 和 URL 重写动作类型。
	支持后端服务器组离线主动 RESET，提升故障场景快速响应能力。
	后端云服务器组支持界面添加多种后端类型，包括云服务器后端、IP 后端、辅助网卡后端，每种后端类型均支持设置端口和权重，提供功能截图证明。
	支持针对 member 粒度的健康检查探测状态、应答时间、错误码等监控指标呈现，提升负载均衡监控易用性。
	支持用户为监听器配置健康检查策略，用于检查后端服务器的状态，支持四层以及七层检测方式，并可以设置检查周期、检查超时时间、重试次数等，对于七层 HTTP/HTTPS 协议，支持设置协议与后端服务器交互的方法、服务器响应的状态码以及 URL。
	支持一个负载均衡实例绑定多个 EIP，满足 ELB 使用不同网段 EIP 对外提供服务的业务场景。
	支持对访问负载均衡的客户端 IP 进行白名单安全控制，如果使用访问控制能力，则只有被允许的 IP 能通过 ELB 访问后端云服务器/物理机；如果不使用，则任何 IP 都可以访问该负载均衡。

	支持 QoS 功能，支持 TCP/UDP、HTTP/HTTPS 协议进行限速，支持针对不同的业务类型配置不同的规格，其中规格涉及并发连接数、每秒新建连接数、每秒查询请求数、吞吐带宽等指标。
	支持跨 VPC 负载均衡能力，支持跨 VPC 添加后端服务器，支持通过专线添加云外后端服务器的能力。
	支持深度健康检查，提供基于响应内容的深度健康检查。TCP 支持指定请求字符串和期望的响应字符串，HTTP 支持指定期望的响应字符串。支持响应字符串的精确匹配和模糊匹配。
	支持灰度发布，基于不同服务器组实现灰度发布，将老版本应用与新版本应用分别作为不同的后端服务器组，让一部分请求继续使用老版本应用，一部分请求开始使用新版本应用，然后根据具体情况逐步提升新版本流量权重，最终迁移到新版本应用。
	▲支持租户对负载均衡实例的并发连接数、活跃连接数、非活跃连接数、新建连接数、流入数据包、流出数据包、网络流入速率、网络流出速率、异常主机数、正常主机数、访问异常返回 4xx 响应次数、7 层协议返回码（5XX）等指标进行监控。（需提供功能截图，并加盖厂商公章）
	负载均衡器支持开启修改保，开启修改保护后，负载均衡、监听器、后端云服务器对应资源其它修改/删除按钮灰化。
云解析 DNS	支持内网域名解析功能，支持 VPC 内生效的内网域名与私网 IP 进行关联，为云上资源提供 VPC 内的域名解析服务。用户可以自己在管理界面上进行记录集的创建，修改和删除。支持 A、AAAA、CNAME、MX、TXT、SRV、PTR、NS、SOA 类型的域名记录。
	支持一个域名可以关联多个 VPC，方便统一管理部署，减少管理员的配置工作。
网络 ACL	支持网络 ACL 服务，用户可以在管理界面上进行网络 ACL 的申请、修改、删除操作，支持对规则创建、修改、删除操作。
	支持用户自助创建安全规则，支持定义出、入方向的安全规则定义，支持 TCP、UDP、ICMP、ANY 等几种类型的规则定义，可以执行允许、拒绝以及驳回操作，源、目的地址支持单 IP、IP 段的定义策略，源、目的端口支持单端口和端口范围的定义，并支持安全规则的导入/导出操作。
	支持 ACL 导入规则时支持指定优先级，网络 ACL 界面搜索功能支持状态、类型、描述、源/目的端口范围。
	支持单条规则聚合功能，可在一条安全规则中支持多个网段/多个端口，并聚合为一条规则减少规则数量、提高运维效率。
跨 VPC 私网通信	支持同区域下跨 VPC 间的资源通信。支持在 VPC 中创建应用程序，将其配置为终端节点，同一区域下其他 VPC 内创建的终端节点可以与该终端节点服务建立连接和进行通信。无需考虑地址重叠、访问限制等问题，无需配置 EIP 服务，占用公网 IP。

	支持用户在管理界面上进行终端节点/终端节点服务的创建，修改和删除，终端节点服务支持配置弹性负载均衡、云服务器两类资源类型，支持开启连接审批配置支持用户在管理界面上进行终端节点/终端节点服务的创建，修改和删除，终端节点服务支持配置弹性负载均衡、云服务器两类资源类型。
--	--

云平台管理软件（计算节点）（25 套）

指标项	指标要求
云主机服务	支持创建虚拟机时，配置外网接入能力即 EIP，配置虚拟机创建完成后为关机状态，指定非管理员账号（linux 下的非 root，windows 下的非 administrator）的用户名、密码，配置高级功能，包括配置标准 IPMI 的软件狗检测能力，配置开启或关闭虚拟机的 HA 功能，配置亲和性和反亲和性，配置用户注入数据。
操作系统兼容	云主机支持丰富的国产操作系统类型，至少包括中标麒麟、银河麒麟、统信 OS 等国产操作系统。
一云多芯	支持管理 X86、鲲鹏、飞腾、海光服务器，支持同一个 Region 管理多个异构资源池。
亲和反亲和	支持用户申请虚拟机时为虚拟机配置亲和性、反亲和性、弱亲和性、弱反亲和性。
自定义配置	支持云服务器的个性化初始配置，用户申请弹性云服务器时增加数据盘以及网卡，可以分别设置每块数据盘的容量以及每块网卡的网络。
	支持为云服务器指定 IP 地址创建云主机，方便运维人员进行 IP 的统筹管理。
外网 IP 管理	支持申请云服务器时绑定弹性 IP，为特定虚拟机提供申请后即可访问外网环境的能力。
自定义脚本	▲支持申请云主机时自定义开机执行的命令、脚本或注入文件。 （需提供功能截图，并加盖厂商公章）
云主机迁移	支持 x86 场景下 CPU 跨代共集群和热迁移，充分利旧资源池，未来支持使用新一代 CPU 进行持续扩容。
	支持虚拟机跨存储设备迁移，支持虚拟机跨 AZ 整机冷迁移，支持界面化执行迁移操作，支持由用户指定迁移到的目标可用区和主机。
云主机检索	支持通过名称、私有 IP 地址、弹性 IP 地址、ID 或 CPU 厂商筛选与搜索云主机，方便快速查找指导云主机。
登录云主机	支持多种云主机登录认证方式，包括密钥登录、密码登录、VNC 登录，方便云服务器的配置、管理等操作。
操作系统切换	支持已发放云服务器重装操作系统或切换操作系统，方便在云主机系统故障或不满足业务诉求时自助进行重置。
整机快照	▲支持云主机整机快照，保障包括系统盘和多块数据盘之间的崩溃一致性，避免单个盘快照导致系统数据不一致。（需提供功能截图，并加盖厂商公章）

云主机克隆	支持以云主机的系统盘和数据盘为模板，克隆新的弹性云主机，支持在线或者离线克隆，除了 ID、MAC 地址、IP 地址、VIP、EIP、密码或密钥外，其余属性及参数与原云服务器完全一致。支持克隆时修改网络配置，包括配置新的 VPC、网卡、安全组等。
在线规格变更	支持云主机在线规格变更 CPU 和内存，变更过程中无需停止正在运行的业务，变更完成后无需重启云主机即可生效。
云主机高可用	▲支持云服务器或云服务器所在主机故障，系统会自动在其他主机上重建云服务器，保证业务的连续性。（需提供功能截图，并加盖厂商公章）
	▲支持防群体性故障 HA，防止虚拟机被攻击反复 HA 引起的故障传染。（需提供功能截图，并加盖厂商公章）
	支持 HA 过程信息自动收集，提供界面化 HA 信息收集作业，实现 HA 全链路实现关键进程监控和告警上报信息收集，提升 HA 场景运维效率。
安全隔离	支持云平台管理和业务网络平面物理隔离，管理面网络故障不影响业务面，支持虚拟机 HA 迁移时通过管理网络，无需占用和影响业务网络流量。
	支持云主机重置密码的功能仅由虚拟机创建者修改，避免其他用户误重置密码影响业务安全。
性能监控	▲支持云主机监控管理，提供性能监测分析、异常告警等功能，支持监控指标包括 CPU 使用率、内存使用率、网络流入/流出速率、云硬盘 IO 速率、GPU 利用率等。（需提供功能截图，并加盖厂商公章）
自动化升级编排	自动计算冗余主机数并预估升级时长，支持自动编排和迁空主机，满足宿主机滚动升级。

云平台管理软件（安全节点）（62 套）

指标项	指标要求
安全云脑	支持全局安全大盘展示，包括不同风险资产数量统计、资产安全风险评估、资产威胁告警统计&TOP 排名、漏洞统计&TOP 排名、安全基线检查结果&TOP 排名和近 7 天安全评分数据趋势等统计信息。
	支持态势感知大屏，集中呈现资产防护率、基线合规统计、风险资源分布、漏洞趋势、威胁趋势、告警统计、待办工单统计、安全事件响应闭环统计与趋势分析。
	支持集中展示所有租户和平台的全局安全态势供云平台全局管理员了解全局使用；支持仅供单租户使用，了解自身的安全态势。
	支持安全运营日报、周报、月报，统计关键运营指标。
	支持自动同步云主机资产、防护网站域名或 IP、VPC 资产；支持资产应用/归属部门/责任人挂载。支持预置的资产类型包括主机、域名、IP、VPC。
	支持展示资产之间的关联关系：网络关系、IP 与主机、IP 与域名、IP 与数据库等；支持展示资产与安全风险要素关系：资产与弱配置、资产与漏洞、资产与威胁告警、资产与入侵事件等。每周统计客户资产防护状态，同时发送邮件/短信通知。

	支持对资产进行基线检查，弱配置项支持定位到资产；支持弱配置详情解读，及修复指导，支持自动扫描，无法自动检查项，提供问卷归档；支持自定义基线；支持导出检查报告。
	支持威胁检测模型，可以从安全日志中发现威胁、生成告警；同时，提供安全响应剧本，可以对告警进行自动研判、处置，并对安全配置自动加固。
	支持安全事件和告警管理，事件和告警统计信息列表包括事件的名称、类型、等级、影响资产、责任人和发生时间等，可对事件和告警进行处置。支持通过自定义过滤条件，快速查询到相应的统计信息。支持统计未关闭告警并进行通知。
	支持情报管理，情报信息列表包括指标名称、威胁度、置信度、责任人和发生事件等，可对情报进行处置。支持通过自定义过滤条件，快速查询到相应的指标信息。
	支持告警时自动关联多方情报，同时将 IP 的情报同步到情报管理中。
	支持基于模板快速构建威胁分析模型，可关联资产信息、租户信息、地理位置信息等进行统计建模分析；支持模型启停、增删改查、状态及业务量监控。
	▲支持威胁分析，通过内置威胁模型身份及运维安全威胁、网络安全威胁、应用安全威胁、主机安全威胁、数据安全威胁分析。（需提供功能截图，并加盖厂商公章）
	支持多种安全日志数据源接入的方式，如 TCP、UDP、KAFKA、OBS 等。支持多种日志格式解析，如 json、prune、KeyValue、csv、等，此外对于用户自定义的格式，还支持正则表达式匹配和解析。
	支持数据源中的安全事件在满足触发条件时，自动或人工启动剧本编排处理安全事件，以达到安全事件的智能响应和闭环处理。
	支持流程编排能力，可拖拽式编排、流程定义，即时生成针对安全事件的定制处理剧本。
平台堡垒机	▲支持按照用户、用户组、资源账户、账户组，建立用户对资源的访问控制授权，支持通过配置访问控制策略、双人授权、命令控制策略实现对资源不同维度的控制。（需提供功能截图，并加盖厂商公章）
	支持设置用户访问资源的权限，包括访问有效期、登录时间段、IP 限制、是否允许上传/下载、文件传输、剪切板、显示水印等。
	支持设置命令或数据库控制策略对关键操作进行管控，当进行敏感、高危操作时，触发的系统响应需至少包括动态授权、强制阻断、告警及二次复核。
	支持通过自动发现、一键同步云上资源、从文件批量导入等方式纳管弹性云服务器资源。
	支持自动改密，可设置改密策略的执行时间和改密方式，支持手动、定时和周期的执行方式，支持改密日志查看与下载。
	支持对 Linux 命令审计、Windows 操作审计全程录像记录，回放录像视频可自动过滤空闲时间。支持生成视频文件，一键下载会话视频。
	支持集中可视化呈现运维统计信息，包括运维时间分布、资源访问次数、会话时长、双人授权、命令拦截、字符数命令、传输文件数等信息。支持一键导出运维报表。
	▲支持双人授权模式，配置双人授权后，运维人员若需访问核心资源，要求管理员现场授权认证，通过认证后才能访问核心资源。（需提供功能截图，并加盖厂商公章）

	支持将历史会话日志远程备份至 Syslog 服务器、FTP/SFTP 服务器，实现系统日志容灾备份。
	支持使用浏览器上传文件到堡垒机或从堡垒机下载文件，并可共享堡垒机的文件到被运维云主机。
	支持一键登录多个授权资源，多个资源可同时在一个浏览器页签运维，开启群发键，能够对多个资源访问同步命令输入。
	支持邀请多人进入同一会话，协同进行运维工作、技术共享。
	支持第三方客户端运维，包括 SecureCRT、Xshell、Xftp、WinSCP、Navicat 、Toad for Oracle 等工具。
	支持在线管理脚本，以及通过配置命令执行、脚本执行、文件传输的运维任务，可定期、批量、自动执行预置的运维任务。
	支持国密算法，可在传输、存储环节使用国产算法加密，支持使用国密智能密码钥匙做身份认证。
平台应用 防火墙、	▲支持对 OWASP Top 攻击进行安全防护，支持包括 XSS、SQL 注入、命令注入、代码注入、远程溢出攻击、Webshell 检测等。（需提供功能截图，并加盖厂商公章）
	支持 CC 防御，支持基于 IP、Cookie、Referer 的源和目的限速，限速的防护动作至少要支持设置验证码、动态阻断 IP/用户一段时间，限速的响应页面支持用户自定义。
	支持目录攻击防护（支持对目录的访问控制，支持路径遍历攻击防护）。
	支持恶意扫描防护，至少包括防爬虫、防扫描工具恶意扫描、防应用扫描。
	支持自定义 IP 黑白名单、精准访问防护规则。
	支持网站静态页面防篡改能力。
	支持防止返回页面的敏感信息泄漏，如用户的身份证号码、电话号码、电子邮箱等。
	支持查看昨天、今天、3 天、7 天或者 30 天内所有防护网站和指定防护网站的防护情况，包括请求与各攻击类型统计次数，QPS、带宽，以及事件分布、受攻击域名 Top10、攻击源 IP Top10、受攻击 URL Top10 等防护数据。
	支持记录防护日志，日志中至少包括攻击发生时间、源站 IP、域名、URL、事件类型、防护动作等信息，支持按照攻击事件、命中规则、防护动作、源站 IP、URL 等多维度条件查询防护日志。
	支持用户自定义隐私屏蔽策略，对隐私参数进行匿名化处理，当隐私数据（如用户名、密码）出现在攻击负载中，也不会被平台侧记录，最大化保障用户隐私。
平台主机 安全	资产管理支持清点并展示平台侧主机账号权限、所属用户组、用户目录、启动 Shell 等信息；支持清点并展示进程路径、文件权限、开放端口、软件版本等信息。
	漏洞管理支持检测平台侧主机软件漏洞，漏洞信息显示包括漏洞名称、风险程度、漏洞描述、修复建议和漏洞详情，漏洞处置一般包括忽略、取消忽略、验证等。
	基线检查支持口令复杂度策略检测，并使用弱口令字典对系统帐户进行扫描，检测出弱口令后展示弱口令存在时长并提示用户修改。
	支持检测策略的修改和查看，可以自定义检测策略配置，便于精细化安全运营。
	安全基线配置支持对安全基线检测库进行管理，为管理员展示当前使用的检测库文件版本、更新时间等信息。

平台数据库审计	支持实时记录用户访问平台数据库行为，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。
	支持生成合规报告，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。
	支持实时审计用户对数据库系统所有操作（插入、删除、更新、用户自定义操作等），还原 SQL 操作命令包括源 IP 地址、目的 IP 地址、访问时间、用户名、客户端程序名、数据库操作类型、数据库表名、字段名、字段值、数据库响应时间、返回行数、返回码等信息。
	支持展示会话的终端信息、会话的主机信息、会话的其它信息、操作信息等。
	支持多数据库聚合报表展现和单数据库综合性报表展现。
	支持基于总体概况、性能、会话、语句、风险多层面展现报表。
	支持用户通过内置规则或自定义规则对审计平台存储和展示的敏感信息脱敏。
平台漏洞扫描	支持资产分组管理能力，可按照分组批量快速启动扫描。支持主机资产授权信息管理能力，支持授权信息的新建、编辑、删除等操作，支持授权信息复用。
	支持系统安全配置核查功能，能够对主流操作系统、中间件的安全配置项目进行检查、报告。
	支持漏洞库管理功能，支持漏洞库离线更新，可展示漏洞库版本信息、更新时间等信息。
	支持按照漏洞类型、漏洞风险等级筛选漏洞，支持对漏洞结果进行确认和标记。
	支持生成专业的扫描报告，并提供专业的修复建议；支持导出漏洞扫描报告；支持汇总报告、单台主机报告，支持 PDF、Excel 报告格式。
密码服务	提供统一身份认证、运维登录口令保护、云服务内部敏感数据加密、镜像机密性、镜像完整性、操作日志完整性、运维接入通道加密、服务接入通道加密和 API 接入通道加密等服务。
证书签发服务	支持国际、商密 CA 的管理能力，包括创建 CA、导入外部签发的 CA，支持协议配置和白名单等机制。支持证书的签发、下载、更新、查询、吊销等生命周期管理，支持证书模板管理功能，支持商密 SM2 证书（支持 SM2、SM3、SM4 算法）。支持证书吊销列表 CRL 能力。

云平台管理软件（裸金属节点）（10 套）

指标项	指标要求
裸金属服务生命周期管理	通过管理界面申请物理服务器运行业务，支持常见的 windows、Linux 操作系统，可以指定要申请的物理服务器的规格、所使用的镜像、所使用的网络、网络所属的安全组、需要绑定的弹性 IP 以及指定服务器登陆信息等，发放过程中支持用户数据注入，完成主机名、密码注入等 OS 系统初始化配置。
	支持裸金属服务器的生命周期管理以及相关业务操作，包括裸金属服务器的开关机、重启、删除、监控以及重置密码等操作，同时可以自动完成服务器的操作系统安装、IP 地址配置、弹性 IP 绑定等。删除裸金属时，可以选择是否删除裸金属的数据盘。

网络能力	支持裸金属服务器与云主机共用同一个 VPC 和子网,无需单独设置 VPC 或子网。
	支持裸金属服务基于硬件交换机的增强型网关方案,提供高性能、高带宽的网络访问。
存储能力	支持基于 HDD 和 SSD 磁盘的本地磁盘发放裸机实例,支持本地 SSD 磁盘实例的数据快速擦除和实例重新发放。

云平台管理软件（块存储节点）（4 套）

指标项	指标要求
云硬盘生命周期管理	支持云硬盘的新建、扩容、挂载、卸载、申请快照、重命名、删除、变更类型等基本操作。
自助查看	支持云硬盘的管理,用户可以查看系统中已有的硬盘列表,可以查看磁盘名称、状态、容量、挂载到的服务器、创建时间等基本信息。
	支持快速搜索磁盘,可以通过磁盘名称或者磁盘是否挂载等条件搜索目标磁盘/磁盘组。
数据加密	支持数据的软件加密,采用计算内核侧加密,支持 XTS-AES-256,国密 SM4-XTS 加密算法。
QoS 限速	▲支持磁盘 QoS 限速,能对指定磁盘类型的 IO 性能进行限制,包括磁盘的 IOPS 上限、带宽防止某些业务抢占存储性能资源,保障所有业务性能均衡。（需提供功能截图,并加盖厂商公章）
磁盘快照	▲支持快照服务,可以通过管理平台为自己的虚拟机/虚拟机磁盘创建快照,单磁盘支持不少于 64 个快照,支持自助完成快照恢复。（需提供功能截图,并加盖厂商公章）
共享盘	支持创建共享盘,满足集群系统共享存储诉求,单个共享盘支持挂载不少于 12 台云主机。
大规格云盘	支持单个云磁盘不低于 32TB,支持单个云主机挂载不少于 32 块云磁盘,满足大容量和大规格云主机业务场景。
平滑扩容	支持系统盘和数据盘在线扩容,扩容不中断业务。

云平台管理软件（应用安全风险识别管控智能辅助组件）（1 套）

指标项	指标子项	指标要求
应用安全风险识别	网络风险识别	<p>（1）多源数据融合</p> <p>支持与主流 WAF、IPS 审计、API 安全监测、全流量威胁监测、主机安全防护系统等安全设备或平台对接,统一采集其日志与告警信息。</p> <p>通过自适应解析引擎和预定义映射规则,实现对不同格式的流量日志、攻击事件记录的结构化转换,形成统一的网络安全事件库。</p> <p>（2）大模型智能检测</p> <p>基于深度学习与特征工程的方法,对常见网络威胁（如 DDoS、扫描、漏洞利用、恶意流量等）进行多维度识别与风险评分。</p> <p>针对“攻击特征分析”智能分析类别,可自动提取并匹配潜在攻击链的特征（如 IP 多次切换、同一 IP 对多端口的探测行为等）,并在监测面板中做重点标注。</p>

		<p>（3）异常流量识别与基线管理</p> <p>构建对 HTTP、TCP、UDP 等多协议的流量基线，能在日常业务“正常流量模式”下捕捉平均包速率、连接频次、流量波动区间等关键指标。一旦发生 DDoS、恶意扫描、暴力探测或其他异常激增/递增流量，即可与正常基线做快速比对，显著提高对突发型或渐进式网络攻击的识别度。</p> <p>支持与蜜罐监测联动，当识别到可疑流量时，将其引流至蜜罐进行进一步验证与行为记录，丰富后续威胁情报。</p>
	应用风险识别	<p>（1）多层级应用审计</p> <p>支持读取现有应用审计工具的分析内容，根据管控项深度检查应用账号、角色以及相关业务访问控制，识别是否存在未授权操作、角色越权或异常账号状态等高风险隐患。</p> <p>结合应用审计日志自动判断访问行为是否符合预期规则（如仅允许特定角色访问的敏感操作，是否由其他角色频繁调用），从而快速定位潜在应用安全缺陷。</p> <p>（2）应用漏洞关联</p> <p>在识别到越权访问或异常操作等问题时，自动推断可能涉及的应用漏洞类型（例如逻辑漏洞、弱认证配置等），并与已知漏洞库进行对比溯源分析。</p>
	数据权限风险识别	<p>（1）多重权限关联</p> <p>能综合应用、服务器、本地账号的分配情况，识别同一人员是否在多个系统均拥有超管理权限，或存在权限过度集中等问题。</p> <p>具备针对“服务器账号”与“应用账号”映射关系进行验证，确保不存在越权级联（如同一账号可在数据库、服务器和应用层面同时执行高危操作）。</p> <p>（2）违规数据访问追踪</p> <p>当检测到异常大量数据读取、敏感字段访问，系统可自动回溯相关操作的主体信息、访问方式及操作来源。</p> <p>具备结合“服务器登录日志”、“服务器历史命令”等信息，判断是否为内部人员违规或外部攻击造成的可疑数据导出。</p>
	风险分析与整改辅助	<p>（1）安全态势综合研判</p> <p>集成网络攻击、应用越权、数据访问违规等多条风险线索，使用大模型进行关联分析，输出“应用安全总览”或“风险雷达”视图。</p> <p>建立风险事件索引体系，支持按时间、主机、攻击类型、业务系统等进行分层溯源，提升安全分析效率。</p> <p>（2）风险矩阵与优先级排布</p> <p>通过多维指标（影响范围、敏感度、攻击成功率等）为风险事件赋予优先级标签，辅助安全运营团队在修复或加固过程中合理分配资源。</p> <p>支持分析结果与第三方漏洞库（如 CVE、CNVD）进行智能映射，帮助快速确认风险场景的严重程度。</p>
风险行为管控	账号与访问风险识别	<p>（1）统一账号智能分析与监控</p> <p>支持“应用系统”、“服务器账号”、“服务器登录日志”等多维度智能分析类别，对各层账号的状态、登录历史和权限范围进行纵深审计。</p>

		<p>支持对账号批量导入或自动同步 CMDB/LDAP 信息，保持智能分析数据的高一致性与实时性。</p> <p>（2）异常登录行为分析</p> <p>识别短时间内的多次失败登录、跨区域或跨系统频繁登录、管理员账号 IP 异常等登录行为。</p> <p>支持借助历史行为基线与行为分析图谱，对同一终端或账号在多个系统上的快速切换操作进行聚合，判断是否存在撞库、拖库或其他非法登录意图。</p> <p>（3）高风险事件聚类</p> <p>使用聚类算法及 NLP 处理，对大批量登录失败、异常用户自定义脚本、不同服务器间关联操作等进行聚合，形成可视化的风险行为群组。</p> <p>在安全运营视图中提供访问风险的分布图，帮助安全运营人员快速锁定重点安全事件。</p>
	风险预警与控制	<p>（1）实时告警与分级管理</p> <p>根据大模型分析结果设定分级阈值（高、中、低），当检测到高风险或批量异常行为时，系统自动发送告警通知至安全控制台；支持按事件类别、主机、账号等进行精细化筛选和分级，以减少误报并确保关键威胁得到及时关注。</p> <p>（2）联动策略与管控闭环</p> <p>支持与公司内其他安全平台进行 API 集成（如防火墙、SDP 控制端、身份管理系统等），在必要时触发自动化响应过程；支持在处置过程中同步更新风险状态，形成完整的监控—识别—响应—审计闭环。</p>
智能辅助能力	统一日志采集与处理	<p>（1）多源日志对接</p> <p>支持通过 API、Agent、文件导入等方式对接应用系统、安全平台（IPS、WAF、蜜罐、全流量分析等）日志。</p> <p>支持多源日志采集与平台化分析，覆盖主机操作系统日志、应用安全审计日志及网络安全设备日志等关键数据来源，实现日志的统一接入、结构化处理与集中存储，为后续风险识别与审计追溯提供可靠的数据支撑。</p> <p>（2）标准化与结构化</p> <p>针对海量原始日志进行标准化、去重、归并及索引，加速后续的检索与关联分析。</p> <p>内置可扩展的日志解析规则库，便于持续引入新型设备或自定义日志格式。</p>

	深度解析与多源语义关联分析	<p>(1) 跨平台 API 适配</p> <p>▲支持为不同系统平台提供通用适配层，将多样化的日志字段、协议格式映射至统一的安全事件模型。</p> <p>自动完成字段标准化与上下文合并，消除多平台、多协议间的数据割裂，为大模型分析奠定基础。</p> <p>(2) 语义级关联与行为画像</p> <p>▲利用自然语言处理、知识图谱等技术，对日志中的账号、IP、URL、进程、命令等要素进行语义分析与可视化关联。</p> <p>在交互界面中生成事件脉络或攻击链示意图，展示关键节点与风险分布，帮助安全人员快速定位可疑点。</p>
	风险与业务关联	<p>在安全监测结论的基础上，提供业务影响分析模块，帮助安全研发团队初步了解风险事件对关键业务流程的影响程度。</p> <p>面向开发、安全运维、业务负责等不同角色，生成相应层次的分析摘要和风险提示。</p>
	集中管理与可视化	<p>系统提供多维度图表、趋势报告、风险列表等视图展示，可嵌入企业内部看板或运维平台。</p> <p>支持与 DevSecOps 流程集成，将高风险事件标记为待修复任务，帮助开发与安全团队在迭代中持续完善安全防护。</p>
	自动化分析与闭环管理	<p>允许根据风险评估结果和运维策略，自动调度或周期性执行检查分析任务，将识别到的风险上报至集中管理平台。</p> <p>日志与风险检测结果保持持续更新，为长期安全规划及数据驱动的安全决策提供扎实支撑。</p>
扩展性	可扩展性	<p>具备可扩展性功能，支持用户自定义智能分析场景和智能编写脚本。</p>
		<p>▲产品具备 5 个以上 mcp 场景工具，并且支持 mcp 工具扩展。</p>
性能指标	平均分析耗时	平均每 15 个检查点分析时间不多于 600 秒。
	并发任务	系统支持不低于 20 并发任务。
	自主修正	智能管控分析模型自主修正后命令执行成功率不低于 80%。

云平台管理软件（网络性能监控组件）（318 台）

指标项	指标子项	指标要求
数据采集管理	插件管理	支持多种类型、协议的插件在线制作，包括 Script、SQL、Exporter、DataDog、JMX、BK-PullL、SNMP 类型。
	网络监控	<p>▲提供硬件采集能力，支持 SNMP、IPMI、SMI-S 协议。其中 IPMI 插件开箱即用；SNMP 插件可基于 MIB 库在线制作自定义插件，自定义扩展插件支持设备类型。</p>
数据监测	异常检测	<p>支持丰富的异常检测能力：</p> <ul style="list-style-type: none"> ➢可选择监控对象的指标、事件、设置监控目标范围、检测算法、触发/恢复条件、无数据告警等。 ➢▲支持 8 种异常检测算法，支持异常防抖收敛，支持无数据异常检测和异常恢复检测，满足企业各种场景下的监控需求。
	指标计算	<ul style="list-style-type: none"> ➢支持单指标函数计算。 ➢支持多指标表达式四则运算。 ➢PromQL 表达式

	告警等级管理	支持告警等级配置，支持致命、预警、提醒三种级别的告警配置。
监控管理	监控目标管理	<ul style="list-style-type: none"> ➤支持策略的监控目标管理，支持以 CMDB 模型实例、云资源实例、容器对象等作为监控目标。 ➤支持指定静态目标实例、或指定动态组进作为目标进行下发。动态组分为动态分组和动态拓扑两种模式。
	监控策略配置	<ul style="list-style-type: none"> ➤监控策略包含采集配置、检测配置、告警配置、一体化配置，减少重复工作内容。 ➤支持基于实例、基于数据两种配置模式，前者使用门槛低，直接根据目标进行策略下发；后者自由度高，直接基于数据本身进行检测配置。 ➤支持策略应用模式管理，默认监控目标策略按关联的策略生效，且支持单个目标自行修改策略配置，且修改配置仅对单个个体生效。
可视化	拓扑管理	➤支持全局网络拓扑的手动绘制，针对不同类型设备、对象提供内置图标，支持设备间连线设置，支持设备、连线属性设置，支持拓扑节点绑定 CMDB 实例。
	拓扑可视化	➤支持拓扑展示、支持拓扑链路展示，支持拓扑节点和链路告警展示，支持链路悬浮卡片信息概览，支持拓扑全屏、放大、缩小、分层展示隐藏、端口展示隐藏。
	拓扑发现	➤支持通过 SNMP 协议对网络设备进行发现，自动扫描基于 SNMP 协议获取设备上的 ARP 表、IFTable 表、IP 地址表进行拓扑绘制。支持拓扑的全量扫描和增量扫描。
	链路管理	➤支持拓扑自动生成链路，支持手动添加链路，支持链路两端接口信息设置，支持专线链路带宽设置。
	链路流量监控	➤支持链路流量指标定义和计算，支持流量指标告警。
告警汇聚	告警源插件开发	<ul style="list-style-type: none"> ➤以开发 python 脚本插件方式，自定义对接其他监控系统。 ➤内置鲸眼监控和 REST API 推送告警源插件。 ➤可提供详尽的插件开发文档，供客户自行开发，自主可控。 ➤提供插件开发服务，帮助客户完成插件开发。 ➤支持导入导出，实现一次开发，多次复用。
	对接监控系统	<ul style="list-style-type: none"> ➤控制已上线告警源接入告警的启停；查看已启用告警源的接入状态是否正常。 ➤根据接入指引，完成告警源的接入配置。 ➤内置鲸眼监控和 REST API 推送告警源。 ➤提供开箱即用的标准告警源插件：ZABBIX、Prometheus、vCenter、solarwinds、自定义 REST API 推送。
告警丰富	CMDB 丰富	<ul style="list-style-type: none"> ➤★将产生告警的实例的维护在 CMDB 的各项属性信息，自定义补充到告警中以便用户排障分析。 ➤若监控系统未和 cmdb 打通，即告警原始信息未携带 cmdb 模型、实例信息，可根据对原始告警字段的匹配规则，实现模型匹配、实例匹配，找到告警对应的实例，并完成实例属性信息的丰富。
	常规丰富	<ul style="list-style-type: none"> ➤方案应用范围：设置常规丰富方案的适用范围，满足规则的告警才执行该常规丰富。 ➤字符替换：用户选定一个或多个字段，将这些字段里的文本进行替换。 ➤字符提取：用户选定一个字段，通过正则表达式将信息提取为多部分，然后将相应内容替换为不同的告警字段。 ➤字段调整：当告警的某些字段满足用户设定条件，那么执行另一些指定字段的更新。
告警收敛	内置去重	➤抑制由于告警未恢复而持续产生的重复告警（根据告警事件 ID 去判定）。

	防抖抑制	<ul style="list-style-type: none"> ➤抑制抖动类指标偶发性产生的告警事件，如：CPU 使用率、内存使用率、磁盘 IO、网卡流量等。
	关联聚合	<ul style="list-style-type: none"> ➤将部分告警字段相同的告警聚合，如：将 10 分钟内“告警指标+CMDB 业务”相同的告警聚合为 1 条有效告警。
	告警合并	<ul style="list-style-type: none"> ➤可创建合并规则，当符合合并规则的告警同时出现，会被收敛并生成一条新的告警。如：当主机、拨测、组件等告警同时产生时，可以生成一条业务不可用的告警。
	告警屏蔽	<ul style="list-style-type: none"> ➤抑制由于已知事件导致的产生了无需关注的告警事件，如：系统维护期内、固定任务窗口内。 ➤抑制由于依赖关系影响而导致的关联告警事件，如：A 进程依赖 B 进程运行，B 进程故障会导致 A 进程的运行。 ➤抑制由于告警对象有 CMDB 关联关系而导致的关联告警事件，如：组件安装、运行于主机的关系；主机磁盘挂载了存储提供的存储盘等。 ➤查看某条告警的详情时，可点击快捷屏蔽此条告警事件及后续屏蔽时间内，相同的告警（根据告警事件 ID 去判定）。
告警处理	告警自动化	<ul style="list-style-type: none"> ➤对于不关注的告警，某些特定场景下可以配置自动关闭，某些非紧急告警（高可用某个节点异常、测试机器的性能告警等），工作日内处理，非工作日自动关闭。 ➤★对于常见的告警，有固化处理流程的场景，可配置告警自愈策略，如：日志文件过大，自动清理日志；磁盘空间满，自动清理指定目录的文件；服务异常自动重启进程；支持手动审批是否执行自愈处理；支持配置告警自愈完成后是否关闭告警。 ➤▲对于需要二线专家介入的复杂告警处理，可以通过工单系统流转给对应的小组或专家进行处理，并留下完整的处理记录；支持通过插件扩展对接各类工单系统；内置对接嘉为 IT 服务管理中心。 ➤将告警分配给指定人处理，会计算 MTTA 和 MTTR 指标，衡量指定人的告警响应及时率和告警处理效率 支持分派升级、根据业务/模型通知组完成动态分派 支持延迟通知：设定时间内未恢复/关闭再通知，减少打扰；支持分派给值班组。
	告警手动处理	<ul style="list-style-type: none"> ➤手动处理告警：认领、响应、转发、审批通过/拒绝、关闭；支持批量操作。 ➤支持告警添加标签，用于对告警进行标记。 ➤支持对流程设置多套模板，手动处理告警时可以选择流程参数模板以减少重复工作量。
告警通知	全局通知	<ul style="list-style-type: none"> ➤当有告警未响应时，定期通知这些告警的当前处理人去及时响应。 ➤当有告警未分派时，定期通知指定的负责人去手动分派告警。
	通知模板	<ul style="list-style-type: none"> ➤支持配置多套通知模板，每一套通知模板覆盖全部通知渠道，可配置不同的通知内容（全部通知内容可自定义）。 ➤实现对不同筛选条件的告警、不同的通知场景（如分派告警时、恢复通知时、转工单失败时）选用不同的通知模板。
	页面通知	<ul style="list-style-type: none"> ➤设置告警处理策略的通知方式，当告警匹配到对应策略后，会在当前处理人登录的系统页面上收到弹窗提示和音频示警（音频可以播报告警内容）。
	移动端	<ul style="list-style-type: none"> ➤移动端告警管理：接收并（批量）处理告警（手动认领/响应/手动转工单/转自愈流程/转发/审批/关闭）；实现时间屏蔽策略的创建、启停、管理。
	通知渠道	<ul style="list-style-type: none"> ➤默认支持短信/邮件。 ➤全局控制各通知渠道的启停。 ➤设置各通知渠道失败重试机制。

	自定义扩展通知渠道	<ul style="list-style-type: none"> ➤可在 API 网关的通道管理/自助接入，自定义开发和注册新的通知渠道。
告警查看分析	告警详情	<ul style="list-style-type: none"> ➤从告警信息、对象信息、其他信息三个层面分层展示所有的告警字段。 ➤可以添加/批量添加告警标签，对告警进行标记，便于后续的分析 and 治理。 ➤▲关联拓扑：基于 CMDB 的模型关联关系，以当前告警事件的关联对象为核心，展示周边关联的其它的对象及其告警状态和告警事件；业务拓扑：基于 CMDB 的业务拓扑关系，以当前告警所在业务为核心，展示该对象在该业务全貌中的位置。 ➤和当前告警相关联的，被自动去重、被防抖收敛、被关联聚合、被依赖屏蔽的告警会出现在关联告警处。 ➤支持展示当前告警事件的指标趋势图。 ➤展示当前告警事件流转的每一步，包括告警入库、告警丰富、告警策略（可查看快照、详情）、手动操作等，以及此过程中告警分派的具体人员和每种通知方式具体的通知结果（成功/失败），转工单/自愈可以直接通过任务 ID 跳转到对应系统页面；展示已恢复告警的恢复记录及信息。
	关联分析	<ul style="list-style-type: none"> ➤按业务（CMDB 业务）或按对象（对象模型实例）进行告警事件的聚合查看。 ➤按告警指标、告警等级进行统计查看。 ➤按 CMDB 业务，分析查看业务拓扑：展示该业务的所有集群、模块、主机、关联实例的告警分布情况。 ➤按对象模型实例，分析查看实例关联拓扑：基于 CMDB 的模型关联关系，从对象出发，展示周边关联的其它的实例及其告警状态和告警事件。
	报表	<ul style="list-style-type: none"> ➤有效告警数、关闭告警数、未响应告警数、未关闭告警数、MTTA、MTTR。 ➤告警压缩占比图、告警处理事件数变化趋势图、告警级别/告警状态/告警分析（我的告警/有效告警）。 ➤告警接入量变化趋势图，告警等级分布图，告警接入方式分布图，告警来源分布图。 ➤人员分析（不同用户所认领、被分派的告警数量、MTTA、MTTR）。

云平台管理软件（运行日志监控组件）（700 节点）

指标项	指标子项	指标要求
日志采集	采集日志	<ul style="list-style-type: none"> ➤★支持日志类型：单行文本日志、多行文本日志、Windows 事件日志、Syslog。 ➤★支持数据源：操作系统、网络设备、安全设备、业务系统、中间件、数据库。 ➤★支持操作系统类型：支持采集大部分主流麒麟、Linux、Windows 操作系统。 ➤支持日志编码：共支持 50 多种编码，支持采集大部分常见编码的日志。 ➤支持采集中英文路径下的日志。 ➤▲支持使用模板，复用采集规则，降低重复工作量。
	字段提取	<ul style="list-style-type: none"> ➤支持清洗方式：JSON、分隔符和正则表达式。 ➤支持清洗的日志格式：除了不规则的 xml 格式日志，其他格式的日志都可以支持。 ➤自动提取关键字段（标准字段），例如 cloudId、dtEventTimeStamp, gseIndex, iterationIndex, log, path,

		<p>serverIp, time。</p> <ul style="list-style-type: none"> ➤自动提取 Windows 事件日志和 Syslog 日志内容，无需用户进行字段提取操作。 ➤支持预览清洗结果，提前检查清洗效果。 ➤支持手动将某个字段设置为整条日志的时间字段，系统以时间字段为时间维度对数据进行管理。 ➤支持使用模板，复用字段提取规则，降低重复工作量。
日志存储	存储日志	<ul style="list-style-type: none"> ➤使用 ES 作为存储源，支持将采集到的日志数据以索引的形式存储到 ES 集群中，支持自定义过期时间（采集到的日志数据多少天后过期）。 ➤支持接入企业已有 ES 集群，在日志管理中心查询并使用 ES 上的数据。 ➤支持对不同业务/应用下的日志数据，自定义其存储的 ES 集群，以实现数据隔离。 ➤索引自动拆分，分片路由 ES 集群。
	ES 温热集群	<ul style="list-style-type: none"> ➤温热集群：近期的数据放在配置高的热节点上，查询速度快，较远历史数据放在配置低的冷节点上，查询速度慢，降低存储成本。 ➤支持界面化将指定 ES 集群设置为温热集群。 ➤支持自定义温、热数据存储时间。
日志检索	日志查询	<ul style="list-style-type: none"> ➤查询语法：支持全文检索，QueryString 语法和正则匹配。支持查询指定字段、模糊查询指定字段、数值范围查询、通配符查询、逻辑运算符查询、基本正则表达式查询、特殊字符查询。 ➤支持通过索引集，跨系统或跨应用日志联合查询。 ➤表格展示检索结果，支持自定义展示字段。 ➤展示日志数量直方图，展示各字段数量统计。 ➤支持查看近 10 条历史查询记录，支持自定义检索时间范围。
	快速过滤	<ul style="list-style-type: none"> ➤IP 过滤：选择 IP/拓扑节点/服务模板/集群模板，精确控制日志检索范围。 ➤▲字段匹配：添加字段匹配条件可以更精确的定位到日志内容。支持的字段匹配方式有等于、不等于、包含、不包含、大于、大于等于、小于、小于等于、该字段为空、该字段非空。
	实时日志	➤▲支持滚动查看实时上报的日志。
	上下文查看	➤▲支持查看指定日志在原始文件中的上下文信息。
	收藏查询	➤将需要重复使用的检索条件（索引集、查询语句、IP 选择、字段匹配、字段显示）设置为收藏查询语句。
	日志数据导出	➤支持指定检索条件、检索时间范围将采集到的日志数据导出至本地查看。
日志监控	日志监控	<ul style="list-style-type: none"> ➤支持日志关键字监控和日志指标监控，支持通过监控策略周期性评估查询和分析结果。 ➤丰富的策略配置能力，支持自定义异常检测规则，如检索语句、汇聚方法、汇聚周期、监控维度、监控条件、检测算法等。 ➤支持 8 种异常检测算法。 ➤支持无数据异常检测和异常恢复机制。 ➤实时展示监控视图，辅助用户检查监控策略。 ➤支持使用模板，复用监控规则，降低重复工作量。
	异常告警	<ul style="list-style-type: none"> ➤支持自定义告警配置，如通知间隔、通知时间段、告警组等。 ➤支持自定义告警推送，支持多种告警通知方式。

		➤告警信息收敛处理机制，将处理好的告警信息发送到相应的告警组。 ➤支持配置告警组。
	事件管理	➤查看告警事件生命周期，展示流转记录、视图信息。 ➤支持确认、关闭告警事件，支持查看告警事件的关联日志。 ➤支持屏蔽告警事件，支持自定义屏蔽时长。 ➤告警事件详情展示告警级别、首次异常事件、事件产生事件、监控策略、关联索引集、告警内容等。

云平台管理软件（用户行为监控组件）（20 个）

指标项	指标子项	指标要求
探针管理	探针管理	支持以低侵入的 JS 脚本方式，进行用户体验用户的采集。
用户体验 web 端应用概览统计	前端应用全景统计	➤提供以单个前端应用为维度，提供关键指标，包括访问、性能、异常，并对应用表现进行评分，快速进行表现不良的应用定位。 ➤提供指定时间范围的筛选及下钻能力。
	用户访问分析	➤★根据会话信息，支持自动采集并以关键访问指标进行统计分析，展示访问该网站的真实用户情况。如 PV、UV、会话数、周活、月活、访问量 TOP 等。 ➤提供指定时间范围对访问量的筛选及下钻能力。
	性能分析	➤▲支持自动采集并以关键性能指标进行统计分析，量化真实用户在该网站上的体验。如 APDEX、页面加载时间、core web vitals 等。同时支持性能访问优劣 TOP 排名及下钻能力。阐明构成性能不良的明细及会话上下文。 ➤提供指定时间范围的性能表现筛选及下钻能力。
	异常分析	➤▲支持自动采集并统计分析系统的脚本错误（JS 异常），统计其影响会话数、发生数，并支持下钻追踪。从明细角度阐明异常的上下文及明细信息。 ➤支持自动采集并统计分析系统的资源请求异常，统计其影响会话数、发生数，并支持下钻追踪。从明细角度阐明异常的上下文及明细信息。 ➤提供指定时间范围的异常发生筛选及下钻能力。
	终端分布	➤提供以多种系统终端维度进行筛选过滤，查看异常、性能、用户访问的分布情况。 ➤提供以用户自定义的阈值进行警示并下钻至明细的能力，包括异常阈值、性能阈值。 ➤提供指定时间范围的异常发生筛选及下钻能力。
用户体验 web 端应用明细数据分析	单用户轨迹追踪	➤★提供以用户的单次会话为粒度进行统计的能力，支持展示用户轨迹及相关具体明细源数据（attribute）。 ➤提供指定时间范围内的会话筛选及下钻能力。 ➤支持根据会话访问过的视图进行筛选及下钻能力。
	页面加载瓶颈定位	➤▲支持以单次视图为粒度进行统计的能力，支持以瀑布图形式展示该页面加载资源、用户操作、发生异常等事件的时序图。 ➤提供指定时间范围内的视图筛选及下钻能力。
	搜索器	➤支持根据会话/视图的属性，如会话 ID、会话开始时间、会话经过的页面数等；以及进行会话的真实用户终端数据，如用户浏览器、设备类型等进行搜索、筛选过滤及下钻的能力。
	调用链 TRACE 追踪	➤▲支持根据前后端单次调用产生的唯一凭证 traceID 进行调用链追踪，查看其前端消耗时间、网络连接时间、后端处理时

		<p>间。</p> <p>➤支持根据资源请求地址搜索其关联的所有 traceID。</p>
	代码异常定位	<p>➤针对 JS 异常信息，支持根据用户上传的反混淆文件，对用户发生异常的 JS 异常信息进行解析，定位发生异常文件名及行数。</p> <p>➤在未完整上传反混淆文件的时候，支持进行分解解析，并标记未完成解析的部分。</p>
	资源请求异常分析	<p>➤根据请求类资源所反应的前端逻辑时间与响应时间，对发生资源请求异常解析多个环节耗时问题。</p> <p>➤通过 traceID 和接口服务识别前后端责任分工。</p>
用户体验 web 端应用管理	应用管理	<p>➤▲支持根据用户需求，调整前端应用监控的名称、快捷一键启停等功能。</p> <p>➤支持根据用户业务需求，调整性能、异常预警的阈值。</p>
告警管理	活动告警	<p>➤列表展示所有活动告警。</p> <p>➤支持活动告警详细信息查看，包含告警名称、告警指标、告警对象、告警状态、告警等级、通知情况等多个字段信息</p>
	历史告警	<p>➤展示历史告警事件。</p> <p>➤支持活动告警详细信息查看，包含告警名称、告警指标、告警对象、告警状态、告警等级、通知情况等多个字段信息</p>
监控管理	监控管理	<p>➤支持自定义策略，对前端应用数据进行监控告警配置。</p> <p>➤支持在一个监控策略中，支持监控多个前端应用用户体验指标，并设置阈值检测配置和告警通知配置。</p>

云平台管理软件（业务流程监控组件）（20 个）

指标项	指标子项	指标要求
业务看板	全业务看板	<p>➤★展示所有的业务面板，支持下钻，查看业务资源监控汇总、业务全局拓扑。</p>
	业务监控覆盖率	<p>➤展示业务下所有监控对象资源的监控覆盖率，反映业务系统接入观测体系的完成度。</p>
	告警汇总视图	<p>➤环状图展示指定业务的告警汇总信息，包括（各等级）活动告警数、有效告警总数、MTTA/MTTR</p> <p>➤支持下钻业务告警列表，查看业务下所有活动告警关键信息。</p>
业务纵览	资源分类看板	<p>➤★分组展示业务下所有的监控资源对象，包括业务、容器、应用服务、数据库、物理机、中间件、网络设备。</p>
	对象模型看板	<p>➤展示业务下所有监控对象模型的资源情况，包括资源数量、告警汇总。</p> <p>➤支持下钻告警列表，展示指定业务、指定监控对象所有活动告警关键信息。</p> <p>➤支持下钻资源列表，展示指定业务、指定监控对象实例列表，实例详情信息。</p>
观测拓扑	拓扑展示	<p>➤★展示业务下所有监控对象实例的架构拓扑，包括 APM 应用、组件、基础资源、硬件资源等八大类分层架构。</p> <p>➤根据各资源内置/自定义聚合资源实例节点，反映更真实的业务运行架构。</p> <p>➤自定义聚合支持 CMDB 字段聚合以及自定义实例聚合两种规则。</p> <p>➤可根据节点名称进行模糊搜索，精确匹配目标资源实例。</p> <p>➤可高亮指定资源实例上下游关联路径，一键定位资源影响范围。</p> <p>➤根据业务资源实例监控情况对节点进行染色，区分未监控与已监控资源。</p> <p>➤告警视图：根据告警情况对节点进行染色，展示业务实时告警态势。</p>

		<ul style="list-style-type: none"> ➤支持节点下钻资源详情，查看指定对象实例观测详细数据。
监控详情	拓扑信息	<ul style="list-style-type: none"> ➤▲支持展示指定监控对象实例上下游架构拓扑。
	告警常驻	<ul style="list-style-type: none"> ➤支持展示指定对象告警列表。 ➤支持展示上下游关联资源告警列表。 ➤支持下钻告警列表页，查看指定时间范围内告警关键信息。 ➤支持告警回溯功能，可按照告警流转实际情况动态染色拓扑节点，回溯历史告警发展历程。
	基础监控	<ul style="list-style-type: none"> ➤支持查看指定监控对象指标视图。
	日志监控	<ul style="list-style-type: none"> ➤支持查看主机关联日志数据。 ➤支持下钻日志检索页面，使用日志高级功能。
	监控配置	<ul style="list-style-type: none"> ➤支持查看指定监控对象策略配置。
	实例详情	<ul style="list-style-type: none"> ➤▲支持查看指定监控对象配置（CMDB）信息。
告警拓扑分析	告警拓扑分析	<ul style="list-style-type: none"> ➤支持查看当前告警所属业务的全景观测-告警态势拓扑图。 ➤▲支持查看业务的全景观测-告警态势拓扑图，或告警对象的上下游告警拓扑图。

云平台管理软件（应用安全风险探测组件）（700 节点）

指标项	指标子项	指标要求
软件对象风险探测	软件探测	<ul style="list-style-type: none"> ➤支持对主机对象进行风险探测，包括大部分主流麒麟、Linux、Windows 操作系统。 ➤支持对数据库对象进行风险探测，包括 Oracle、MySQL、MSSQL、达梦。 ➤支持对中间件对象进行风险探测，包括 Weblogic、NGINX、Tomcat。 ➤实现操作系统信息获取、组件软件信息获取、服务与进程信息获取、系统日志信息获取、系统安全与权限获取、补丁信息获取、环境变量与配置获取。
硬件设备风险探测	硬件探测	<ul style="list-style-type: none"> ➤支持对网络设备进行风险探测，包含多品牌的路由器、交换机。 ➤▲支持网络风险探测脚本管理，网络设备风险探测指标库、网络设备风险探测模板。 ➤▲支持 IP 地址统一管理，创建 IP 扫描任务，扫描到的 IP 进行智能化分析，识别异常 IP、异常网段、未分配责任人 IP。 ➤支持网络设备的配置定期备份，设置网络配置基线，定期使用基线进行对比核查，发现异常改动的网络配置。
系统接口信息风险探测	接口信息探测	<ul style="list-style-type: none"> ➤调用目标 API 接口，获取接口返回的数据进行风险探测，包括常见的 restful api 方式、webservice 方式。 ➤配置 API 调用所需的请求参数，如 URL、请求头、请求体。 ➤解析 API 接口返回的响应数据，提取关键信息，对 API 返回的数据进行校验，确保数据的完整性和正确性。 ➤实现 API 风险探测任务的自动化调度，定期执行风险探测任务。
应用界面 UI 风险探测	应用界面 UI 探测	<p>支持进行应用系统界面风险探测，详细功能如下：</p> <ul style="list-style-type: none"> ➤★支持创建界面风险探测脚本，包含界面模拟登录、界面元素捕捉、界面截图、截图标准输出。 ➤★支持捕获和解析系统/平台界面内容，输出界面内容风险探测解析结果，展示在任务历史。 ➤★风险探测任务执行获取脚本截图内容，在风险探测任务历史中查看风险探测截图，导出风险探测报告中能看到风险探测截图内容。 ➤支持引用自动化运维平台的通知模块，实现多种方式通知，包含邮件、短信。 ➤支持业务保障策略，严格控制风险探测时间，在业务高峰期无法

		<p>风险探测减少业务影响。</p> <ul style="list-style-type: none"> ➤支持凭据管理，对平台的账号使用国密算法加密，保证安全。 ➤▲支持审批策略，风险探测脚本/流程更新会触发审批，只有经过审核通过的脚本/流程才能上线使用。
风险统一管理	指标库管理	<p>支持根据脚本内容配置风险探测指标和维度，主要包含以下内容：</p> <ul style="list-style-type: none"> ➤风险探测指标库列表的展示支持卡片和表格展示。 ➤风险探测指标库的新增、删除、编辑、上传图标。 ➤提供指标库名称和指标库类型的高级搜索。 ➤根据风险探测对象和风险探测脚本、脚本编写类型、脚本编写内容设置风险探测的指标和维度。 ➤脚本输出类型分为标准脚本输出（prometheus），非标准脚本输出。 ➤风险探测指标提供指标模板、导入、下载当前风险探测指标。 ➤风险探测指标的自定义分类。 ➤配置完的指标库需经过脚本测试，待测试成功后才可以进行保存。
	探测模板	<p>支持对多个对象引用不同的风险探测指标库，详细参数要求如下：</p> <ul style="list-style-type: none"> ➤风险探测模板的新增、克隆、编辑、删除、导出、导入。 ➤风险探测模板名称和对象的高级搜索。 ➤新增模板可以选择多个对象，并对其引用不同指标库。 ➤支持对不同指标设置对比方式和影响级别。 ➤自定义配置风险探测报告布局。
	探测脚本管理	<p>支持脚本的新增、删除和版本管理，详细功能如下：</p> <ul style="list-style-type: none"> ➤脚本语言支持 Shell、Bat、Perl、Python、Powershell。 ➤可通过脚本上、下线，对脚本进行版本管理。 ➤脚本的版本管理中提供脚本克隆和对已下线的脚本编辑。
	参数集管理	<ul style="list-style-type: none"> ➤▲支持对象的参数管理，新增、编辑、删除。
	探测任务管理	<p>支持根据基线模板选择风险探测目标，并执行后输出任务报告，详细功能如下：</p> <ul style="list-style-type: none"> ➤风险探测任务的新增、执行、编辑、克隆、删除。 ➤任务名称、风险探测模板、任务类型的高级搜索。 ➤根据风险探测模板选择风险探测的目标。 ➤执行时间可以设置为立即、定时、周期、自定义。 ➤风险探测任务类型可以为基础风险探测和业务风险探测。 ➤支持分别为风险探测模板中的指标库选择执行目标。
	任务历史管理	<p>支持展示风险探测任务的结果，详细功能如下：</p> <ul style="list-style-type: none"> ➤支持风险探测任务历史记录高级搜索、按时间范围搜索、任务历史详情查看和删除。 ➤任务历史中包括，任务信息、实例统计、问题统计、结果总览、问题汇总、风险探测对象列表，业务风险探测已业务维度展示数据。 ➤可查看执行日志、对象指标详情。 ➤任务报告导出。

云平台管理软件（安全自动化响应平台授权）（1套）

技术指标	指标要求
功能要求	安全自动化响应平台 3 年授权，包含 7*24 小时软件技术支撑服务，涵盖 20 个以上自动化安全运营场景、升级运营数据展示功能等在内的软件升级服务授权，完成设计、调试、部署相关剧本场景。
安全场景剧本实现的功能要求	▲威胁检测与响应：通过威胁情报平台（如微步在线）检测病毒、木马、蠕虫、挖矿、僵尸网络等威胁，并根据情报结果触发事件单，进行病毒扫描或通知相关人员处理。

	适用场景：病毒事件、木马事件、蠕虫事件、挖矿事件、僵尸网络事件等。
	▲自动化封堵与通知：当检测到异常行为（如 WIFI 远控自动化、外网威胁、远控工具使用等），通过防火墙或 K01 自动封堵 IP 地址，并通过短信或邮件通知相关人员。
	适用场景：WIFI 远控自动化、外网威胁阶梯式封堵、远控事件等
	资产与策略管理：定期校验和管理资产信息（如堡垒机资产、CMDB 平台资产），处理零命中策略、高危命令策略等，确保策略合规性和资产完整性。
	适用场景：堡垒机资产校验、安博通零命中策略、堡垒机高危命令策略等。
编排与自动化流程引擎功能	安全漏洞管理：定期校验漏洞整改情况、网络策略开通情况等，通过扫描和日志分析优化安全策略，确保系统安全性和策略有效性。
	适用场景：漏洞复核、网络策略校验等
	▲通知与事件跟踪：针对各类告警事件（如信息泄露、暴力破解、弱口令等），创建事件单并通知相关人员，同时跟踪事件处理状态，确保问题及时解决。适用场景：信息泄露事件、暴力破解事件、弱口令研判、不明 IP 自动化等
	流程设计器：提供图形化拖拽式的流程建模界面，支持所见即所得的操作方式；
	流程引擎：支持异步并发执行、多线程调度，具备强健的流程运行管理能力；
告警管理与分析	条件分支逻辑：支持流程中根据上下文状态设置条件判断、循环、分支等控制逻辑；
	流程模板管理：支持流程模板的导入导出、版本控制、回滚、共享与复用；
	流程审计与追踪：记录流程执行日志、参数变化、结果状态，支持全过程审计与回溯。
	告警聚合能力：具备多源告警收集、标准化、去重、归并、压缩等聚合功能；
	威胁智能融合：支持对接第三方威胁情报平台，结合威胁情报自动增强告警内容；
自动化响应与闭环处置	告警分类与打分：对接 SIEM、IDS/IPS、防火墙等告警来源，实现自动分类与风险评分；
	场景化告警识别：通过告警上下文、行为链条等规则构建威胁场景，实现攻击路径还原
	响应动作库：内置多种安全处置动作，如阻断 IP、禁用账户、隔离主机、提交沙箱分析等；
	联动处置能力：支持与主流安全产品（如防火墙、VPN、堡垒机、EDR、WAF 等）联动执行；
	处置流程执行：支持自动执行、半自动执行、人工确认执行三种模式，灵活匹配不同场景；
集成与可视化能力	事件工单联动：与工单平台集成，自动生成事件工单并跟踪处置状态；
	处置结果反馈：响应结果可自动回传至告警源平台，实现闭环记录和态势更新。
	平台集成能力：支持 RESTful API、Webhook 等主流集成方式，便于与外部平台对接；
	数据对接能力：支持与日志平台、SIEM、CMDB、情报平台、工单平台等平台集成；
	可视化仪表盘：提供可配置的监控看板，支持多维度展示流程运行状态与响应效率；
	报表统计功能：支持自定义报表模板，生成响应次数、平均处置时间、告警分类等统计图表。

云平台管理软件（DHCP 系统软件）（1 套）

技术指标	指标要求
基本要求	采用 3 节点部署方式，HA+Failover 方式部署，Failover 主节点通过 2 个节点组建 HA 架构部署，同时作为管理节点，Failover 备节点独立部署，由主节点集中管理；单服务节点 LPS 不低于 800。
部署方式	<p>提供全中文 Web 操作界面多节点统一管理（支持对服务节点的统一纳管不需要单独登录系统进行管理），能够实现同一管理页面下的可视化配置管理。</p> <p>▲支持 IPv4 及 IPv6 的 DHCP failover 部署方式，failover 支持自定义设置 MCLT、负载比例、端口等，可实现跨区域的 DHCP 冗余建设要求，实现 DHCP 节点快速切换，提供 DHCP 服务备灾的功能，当一台异常时，另外一台支持一键接管全部租赁服务。</p> <p>支持 HA 高可靠架构、Failover 集群部署等多种架构的 DHCP 负载地址分发，提升终端入网稳定性。</p>
IPAM 管理	<p>图形化地址管理：网络地址支持图形化展示，支持以图形和列表的形式展示网络、IP 地址，便于进行直观的网络地址管理。</p> <p>支持创建 IPv6 地址规划方案，可基于组织架构创建进行父子方案设计，方案绑定为固定 IPv6 前缀；支持在地址台账中应用 IPv6 规划方案，便捷添加 IPv6 网络；支持通过规划地图直观展示全网的 IPv6 地址规划情况。</p> <p>支持方案的地址空间规划，可按照图形化方式拖拽规划 IPv6 地址空间，每个空间标记不同的业务类型；支持为各地址空间配置空间标识，同时关联与上级标识，形成可落地的 IPv6 编址方案。</p> <p>支持手动创建 IP 地址基线数据或同步当前台账数据作为基线，支持针对基线信息与当前台账数据进行比对，可形成基线差异报告并支持导出。</p> <p>支持 IPv4 定制报表，可统计重要网络的网络平均使用率趋势、最近 7 天在线 IP 的日环比统计（且可以查看日环比新增/减少具体 IP）。</p> <p>动态地址管理：支持 DHCP 动态地址分配、续租，支持地址池、固定地址、保留地址、僵尸地址。支持标识地址冲突，并支持一键进行冲突地址的管理操作，可一键进行固定、保留地址的转换，方便快速进行 IP 和 MAC 的固定化使用。</p> <p>地址池管理：支持对地址池进行分组，方便根据使用目的不同进行地址池归类管理，支持手动创建分组和基于自定义属性自动分组两种方式，并以树形方式展示分组信息。</p> <p>僵尸地址管理：可以针对长期未在线的固定地址或手动地址在“僵尸地址条件天数+自动回收延时天数”天后自动设置为其之前的地址类型。</p> <p>IPV6 地址管理：支持通过 IPAM 系统自动生成 IPV6 地址，在指定的地址区间内正序、倒叙、随机的生成地址，并支持设置生成的 IP 地址个数。</p> <p>地址管理支持多种类型的识别和管理，包括但不限于未使用、冲突、未管理、活跃地址、地址池、保留地址、僵尸地址、手动地址、固定地址、僵尸地址回收。</p> <p>地址状态审计：支持地址审计，具备完整的 IPAM 在线状态日志，不是通过 DHCP 分配的 IP 也能记录历史在线状态，方便审计回溯网内 IP 历史在线状态、支持对 IP 地址变更历史进行审计。</p> <p>支持基于 ARP、ICMP、NETBIOS 的网络协议扫描发现，可周期性的自动执行，获知网内 IP 在线状态。</p> <p>支持冲突处理，可一键进行冲突地址的管理操作。</p> <p>搜索功能，可以对全局 IP/网络进行搜索，用户可以定制查询条件；支持通过 excel 导入、导出网络、IP 地址、MAC 地址等信息。</p>
地址分配	<p>支持对 IPV4/IPV6 网路多级拆分，拆分时可选择 CIDR 和网络数量及目标分组。拆分后的网络可根据设置的模板自动创建地址池，降低运维复杂度。支持对 IPV4/IPV6 地址配置生命周期管理，该 IP 地址到达使用截期时可以自动回收再分配给其他用户。</p> <p>支持网络 IP 使用率、已经使用地址数和地址总数的统计展示。</p>

	支持 DDNS，可基于主机名生成动态域名对应，也可以自定义某终端的完整域名。
	支持针对 DHCP 选项(Option)匹配进行 Option 配置下发，满足复杂场景需求，包括 Option 60 61 66 67 77。
	支持共享网络功能，把多个不同网段绑定在一个组里解决单个网段内地址不足的问题；支持最大租约、最小租约、正常租约，合理控制终端租约使用，可手动进行租赁清除。
	支持双栈地址分配，可创建双栈地址池，将 IPv4 后地址嵌入 IPv6 后 64bit 中进行地址分配。
安全功能	地址准入控制：支持基于指纹（内置指纹库可通过管理页面升级指纹库）、MAC、Options 的访问控制列表，识别终端并进行接入控制；根据不同的终端类型来选择接入的网络控制判断其属于哪个 DHCP 域。提供截图。
	支持自动识别并丢弃非法的 DHCP 报文，使之不影响 DHCP 地址分配性能。提供证明文件。
	▲支持 Discover 和 Request 攻击防护。支持地址池使用率告警，告警内容可携带自定义属性。
	支持地址分配预先 ping 检测，在地址分配前判断地址是否可用，避免分配地址冲突。
用户管理	支持设置密码复杂度、最小密码长度、密码使用期限、历史密码使用次数、密码过期提醒等；支持设置账号锁定时长、锁定重试次数、IP 锁定时长、IP 锁定次数、系统锁定时效、是否允许用户多处登录；双因子认证功能，可以设置邮箱+账号的认证方式登录系统。
	支持设置访问会话超时时间，支持超时自动退出，即管理员一定时间不操作时，管理平台自动退出，再次操作需重新登录。
	支持密码验证保护，同一账号密码连续多次错误一段时间内禁止登录，账户的禁止状态可手动解除。
	用户登录支持双因子认证，至少支持密码+邮箱认证方式。提供截图。
	支持管理账号源地址访问控制，只有设定的来源 IP 能使用对应账号登录管理系统。
	支持账户分权，可设定基于网络/地址池的隐藏/只读/读写权限。
	支持为指定用户组设定权限，权限至少分为 WEB 管理权限、CLI 权限、API 权限，任一权限可不依赖其它权限单独指定，也可与其它权限组合分配。
	可设定操作日志、系统日志对某些管理员不可见，对记录的日志信息保密。
系统管理	支持通过 Web 前台查看集群内所有节点的设备型号、序列号、识别码、内存大小、磁盘数量/容量、RAID 级别、RAID 磁盘总数、CPU 主频/内核/线程数量、电口/光口信息；内存、磁盘、扩展卡等扩容结果可以直接查看，无需进行人为手动数据注入操作；硬件资源如 CPU、内存使用率状态需动态展示，无需手动点击刷新。
	▲系统支持分析监控展示包括但不限于网卡流量、内存、CPU、CPU 温度、磁盘、LPS、Leases 总量统计、DHCP 使用率、报文统计、指纹统计等，系统资源数据提供实时更新，业务数据提供 1 分钟更新粒度。
	支持通过 Web 界面设置各种阈值、事件告警，支持邮件告警、回调告警、SNMP 告警、syslog 告警、短信告警及声音告警。告警记录内容包括但不限于告警时间，节点名称及 IP、告警事件原因。
	支持对 IPV4 的 DHCP 报文类型 discover、offer、request、ack、decline、nak、release 报文实时统计，可查看近三个月的统计结果，统计结果支持导出为 PDF 或 CSV 格式文件。
	支持对 IPV6 的 DHCP 报文类型 solicit、advertise、request、confirm、renew、rebind、reply、release、decline、information 报文实时统计，可查看近三个月的统计数据，统计结果支持导出为 PDF 或 CSV 格式文件。
	DHCPV4 日志要求体现时间、MAC 地址、主机名、类型、DHCPrelay 网关、网关地址 IP、Request 源地址、服务器回复 IP、租期开始时间、租期结束时间

	等关键指标，并支持 syslog 发送和手动导出功能。
	DHPCV6 日志要求体现时间、MAC 地址、类型、DHCPrelay 网关、客户端源地址、服务器回复 IP、租期开始时间、租期结束时间等关键指标，并支持 syslog 发送和手动导出功能。
	支持标准 API 接口，可与第三方运维平台对接，实现自动化运维。
产品资质	投标产品需为自主可控产品，具有软件相关著作权登记证书，以及国产操作系统兼容性认证证明。
	投标产品需连续五年在国内 DDI 市场占有率为前五名，提供 IDC 市场报告证明。
	产品具备第三方权威机构（公安部、中国信息安全测评中心）的安全测试报告。

5 资料管理

5.1 文档范围

- 1) 投标方提供的文档包括系统技术资料、维护手册、培训资料、和用户手册等。
- 2) 提供的文档还应包括由投标方采购供货的产品的技术手册及相关资料。

5.2 投标方的责任

投标方应对其所提供的全部文档的准确性和完整性负责。所有由投标方采购供货的产品的技术手册的准确性由投标方负责。

5.3 文档种类

投标方必须至少提供以下文档（所有文档提供电子文档一份）：

项目	说明	数量
1	用户手册	24
2	管理员手册	24
3	运维手册	24
4	产品安装和配置手册	24

6 售后服务及技术培训

6.1 软件类产品技术服务要求

- 1) 提供 1 年原厂质保服务，包含：
 - 提供 7×24 小时技术支持服务，指定相对固定的技术负责人及联络电话、传真、e-mail 等。
 - 重大故障时，投标方应在接到故障电话后，需 1 小时内到达现场处置。
 - 提供安全漏洞补丁更新服务，确保中高危漏洞整改率 100%。
- 2) 确保产品生命周期大于 5 年，5 年内提供中高危漏洞补丁。

6.2 技术培训

1) 投标方应由资深专家为招标方的技术人员开设现场培训课程。招标方的技术人员应在产品使用、维护等各方面得到培训，熟悉和掌握运行、检查和维护相关产品。

2) 投标方应提出对受训者最为有利的培训计划(包括培训时间、地点、内容)。

3) 投标方应向招标方提交培训时间表和课程表，投标方应定出培训大纲，培训大纲和计划应提交招标方确认，根据招标方实际需求进行修改。

4) 免费提供培训，甲方选派人员参加；培训内容为相关系统的现场安装、调试、维护、使用、故障诊断等；

6.3 在系统频繁出现故障、或遇重大节假日等特殊情况下，需要提高系统维护等级的情况下，应招标人要求，应提供技术人员提供现场技术支持，及时处理各类故障。

6.4 一旦发现系统运行不稳定，而与合同产品有关，须免费提供合乎原厂商规定的合同产品的更新或版本升级，或对系统进行维修、维护，直至问题得到解决。

6.5 免费进行必要的软件更新和版本升级。当招标人准备对合同产品进行升级或扩容时，须提供咨询服务，并提交相关方案。

6.6 向招标人提供合同产品相关的新技术的日常技术咨询服务。

7 质量保证

7.1 投标方所提供软件类货物的质量保证期为从投标方所提供货物通过验收后 1 年；投标方所提供边缘算力信创超融合机柜的质量保证期为从投标方所提供货物通过验收后 5 年。

7.2 在投标方所提供货物质量保证期内，如发现投标方提供的货物有缺陷，不符合招标方规定，投标方应按照甲方要求进行免费修理或更换。

7.3 投标方应遵守本规范书中各条款和工作项目的 ISO9000、GB/T1900 质量保证体系，该质量保证体系已经过国家认证和正常运转。

8 试验与调试

8.1 验收要求

1) 投标方将负责对现场安装和测试进行指导，投标方的工程师将协助进行现场试验验收。

2) 在现场验收完成后 20 天内，双方的代表将签署验收报告。

3) 验收计划由投标方准备，交给招标方审查同意。

4) 为有利于软件产品的安装、投运和测试, 投标方应派出有经验的专家提供技术服务。

5) 所交付的产品、文档资料均作为验收的一部分。

8.2 现场安装和现场试验

1) 产品现场安装完毕, 招标方应通知投标方人员到场参加调试。

2) 在调试过程中, 若发现软件存在不正常工作情况, 投标方应负责维护直至问题解决。

8.3 验收时间与地点

1) 验收时间: 在完成项目合同约定内容后, 报价方按照合同约定时间提交验收申请, 经采购方确认提交资料满足采购方项目验收标准, 可以开展验收。

2) 验收地点: 双方具体约定。

9 技术性能偏差表

投标方应将所供设备与本招标书技术文件有差异之处, 无论优于或劣于本招标书技术文件要求, 均汇集至以下表中。

技术差异表

序号	采购技术条件书		投标文件	
	条目	简要内容	条目	简要内容

10 投标方需说明的其他问题

如有需说明的其他问题, 投标方应通过书面形式提交, 并加盖公章。