（一）硬件资源平台要求

序号	指标	指标要求
1	硬件资源机房要求	拟提供硬件资源服务平台物理机房地址位于曲靖市内，满足同城灾备的要求，满足相关标准规范的要求。
2	服务资质	拟提供硬件资源平台满足等级保护三级和信息系统密三级评备案要求，同时还需满足相关标准规范的要求。
3	统一服务能力	硬件资源平台提供用户自助服务界面，用户能够通过自助服务门户完成资源申请、使用、修改、销毁等操作。
4	多资源池管理	满足对计算资源、存储资源、网络资源及安全资源等统一管理的需求。
5	监控功能	提供硬件资源监控管理的功能
6	网络接入	支持所有运营商数据链路接入，提供 100G/10G/1G 网络接入端口及相配套的服务
7	备份恢复	按照标准规范要求提供数据备份恢复服务

（二）计算资源服务要求

序号	指标	指标要求
1	计算资源	提供不少于 3000 vCPU，10TB 内存的计算资源。支持搭建内网区域平台和 DMZ 区域平台
2	主机创建	用户可以通过管理控制台批量申请主机。可自定义主机所需操作系统类型、镜像、规格、数据盘规格。可自定义主机网卡 IP 及安全组，主机支持配置 IPv6、IPv4 或双栈网络。可以为主机选择自定义密码、随机密码或密钥对登录。
3	主机全生命周期管理	支持主机生命周期管理，包括批量创建、关闭、重启、删除等操作。
4		提供主机详情页，主机具体信息可在线查看，并监控各项运营数据，提供图形化展示。

（三）存储资源服务要求

序号	指标	指标要求
1	规格要求	提供不少于 50TB 容量的双活 SSD 存储资源服务;不少于 200TB 容量的 SDD 存储资源服务；不少于 100TB 容量的备份服务。
2	存储兼容性	同一 AZ 内支持同时使用 FC SAN 协议和 IP SAN 协议，同时支持不同 AZ 分别使用 FC SAN 协议和 IP SAN 协议。
3	存储冗余	存储需支持副本或纠删码（EC）的数据冗余技术。
4	快照	支持快照功能，单块云硬盘最多拥有 64 个快照额度。

5	数据安全	支持 IQN 认证，CHAP 鉴权等数据访问隔离和鉴权等安全机制。
6	备份	备份数据可用率不低于 99.99%。

（四）网络资源服务要求

序号	指标	指标要求
1	网路接入要求	支持所有运营商数据链路接入，提供 100G/10G/1G 接入所需的所有配套服务
2	VPC 技术要	支持自定义 DNS 服务器地址，可实现云服务器在 VPC 子网内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网 DNS 访问云上服务。
3	公网 IP 技术要求	支持公网 IP 绑定主机、裸金属、负载均衡、NAT 网关、辅助网卡、高可用虚拟 IP 等资源。
4	VPC 拓扑	支持 IPv4/IPv6 双栈，在 VPC 详情支持查看 VPC 内拓扑。

（五）安全资源服务要求

序号	指标	指标要求
1	规格要求	提供不少于 2 套云防火墙服务；
		提供不少于 1 套 SSL VPN 接入服务，用户数量不低于 1000；
		提供不少于 1 套网页防篡改服务；
		提供不少于 1 套主机防病毒服务；
		提供不少于 1 套数据库审计服务；
		提供不少于 1 套漏洞扫描服务；
		提供不少于 1 套堡垒机服务；
		提供不少于 1 套日志审计服务；
		提供不少于 1 套态势感知服务；
		提供不少于 1 套云 WAF 服务。
		密码应用安全服务
2	网页防篡改技术要求	支持网页文件防护和网络攻击防护，通过 web 防攻击模块、防篡改模块（系统内核层的文件驱动），对动态和静态网页文件进行保护。可自定义设置网站目录、文件的读写权限，限制文件目录的增、删、改等操作行为，确保网页文件不被非法篡改。支持记录并展示所有防篡改日志信息。日志信息字段包括：日期和时间、Web 名称、设备名称、进程名、文件名、攻击类型。满足相关标准规范的要求。
3	主机防病毒技术要求	支持安全体检：检测的项目包括系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门等。支持对恶意进程及软件进行查杀，并提供隔离、信任等操作。满足相关标准规范的要求。能满足所有主机防病毒需求，满足相关标准规范的要求。

4	数据库审计技术要求	支持 Oracle、Sybase、DB2、Mysql、SQL server、Informix 等主流数据库，达梦、金仓、南大通用、神通等国产数据库，Postgresql、Cache、Teradata、Mongo、Redis 等专用数据库，以及 Telnet、Ftp、Vnc、Rdp、Ssh 等其它应用的审计。支持监测业务系统监听正常情况、设备运行健康度、今日数据库数据、今日 WEB 数据、今日告警数据库事件数、今日告警 WEB 事件数、数据库会话统计、系统连续运行时间等设备状态。能满足对 20 套数据库进行审计的需求。满足相关标准规范的要求。
5	漏洞扫描技术要求	支持以下资产类型的漏洞扫描：web 系统：支持 http、https 协议；数据库系统：支持 SSH、Telnet、SMB、MYSQL、Oracle、SqlServer、DB2、informix、Sybase、DM 协议；操作系统：支持 SSH、Telnet、SMB、SNMP 协议。支持查看资产历史漏洞变化趋势，新增、减少漏洞情况；支持不同资产组资产总数和漏洞情况的对比统计。支持对 500 台以上主机进行漏洞扫描。定期形成漏洞扫描报告。满足相关标准规范的要求。
5	堡垒机技术要求	支持操作审计：支持图形、字符、文件传输、数据库操作审计。支持事件审计：登录日志审计，支持对登录人员进行审计，记录登录时间、登录用户、登录 IP、登录方式、登录是否成功等日志信息；配置日志审计，支持对管理员操作行为进行细粒度审计；审计行为审计，支持对审计管理员审计行为进行细粒度审计。堡垒机可管理主机数量不低于 500，用户数量不低于 200。满足相关标准规范的要求。
6	日志审计技术要求	支持收集云内服务器（Windows、Linux、Unix 等）、各类应用（MySQL、SQL Server、Oracle、WebLogic、Tomcat 等）的日志进行存储、审计、分析和展示。支持实时展示各个等级的日志上报趋势和丰富后的日志信息，为用户展现每种日志等级详细的日志信息。日志信息展示方式包括：日志上报趋势图：通过折线图展示一段时间内，各等级的日志上报趋势。日志列表：通过列表展示一段时间内各个等级的日志信息，如日志类型、日志产生时间、日志等级等。支持对 500 台以上主机进行日志审计。定期形成报告。满足相关标准规范的要求。
7	态势感知技术要求	支持以列表的形式展现整网资产的安全风险分析结果，包括展示资产名称、IP 地址、所属区域、级别、TOP3 安全事件名称标签。支持对单个风险资产遭受的安全事件进溯源，以路径的形式展示威胁过程
8	云 WAF 技术要求	支持 XSS 攻击,SQL 注入攻击，CC 攻击等常见攻击方式的防护。展示当前登录用户所有 WAF 实例下各种类型攻击数量统计，主要包括 web 访问、web 攻击、ddos 攻击、安全情报攻击。
9	密码应用安全服务	达到密码应用三级水平，满足相关标准规范的要求。