

序号	技术参数指标要求
1	GPU 服务器 6 台，每台参数如下：
●1.1	规格：高度 \geq 4U。
★1.2	处理器：配置 \geq 2 颗复杂指令集处理器，每颗 CPU 核心数 \geq 28 核，每颗 CPU 主频 \geq 2.0GHz，缓存 \geq 42MB，TDP \geq 205W，支持 AVX-512 指令集、同时 FMA 寄存器 \geq 2。
●1.3	内存：配置 \geq 12 个 64GB DDR4 3200 内存，最大可扩展内存数量 \geq 32 个内存插槽。
●1.4	硬盘：配置 \geq 2 块 480GB SATA SSD、配置 \geq 1 块 1.92TB SATA SSD。
●1.5	阵列卡：配置 \geq 1 块阵列卡，支持 Raid 级别 0/1/10。
▲1.6	硬盘支持：支持采用 NVMe SSD 硬盘，硬盘 MTBF \geq 250 万小时。
★1.7	GPU 卡：提供 \geq 4 颗 GPU 卡。单 GPU 卡 FP64 算力 \geq 9.7TFLOPS，FP32 算力 \geq 19.5TFLOPS，FP16 算力 \geq 312 TFLOPS，HBM2e 显存容量 \geq 80GB，支持通过桥接器实现两卡 600GB/S 互联。
●1.8	配置 \geq 2 个 GE 电口。
●1.9	配置电源 \geq 4 块，单电源功率 \geq 2000W，2+2 冗余。
●1.10	集成 BMC 管理芯片，支持 IPMI2.0、Redfish、SOL、KVM、虚拟媒介等功能。
▲1.11	冗余可靠：支持 BMC flash（ROM）硬件冗余、升级失败后自动回退或切换至另一片 Flash 启动。
▲1.12	操作系统：配置商用正版授权服务器操作系统，支持基于模块流的软件包源管理功能，支持模块安装与更新功能，可实现应用软件及其依赖组件的安装与更新功能。
▲1.13	主机入侵检测：支持轻量化的主机入侵检测功能，可内置入侵检测规则，支持对 Rootkit 攻击、无文件执行、内核模块加载、LD_PRELOAD、计划任务修改等可疑行为进行监控的功能，监测到可疑行为后可实时告警。
▲1.14	轻量组件：配备的安全防御组件，对 CPU 和内存性能影响均需小于 5%以内，性能测试工具需采用 Linux 主流开源工具测试（如：sysbench, stream）。（提供具备 CMA 资质的第三方测评报告）
▲1.15	防御暴力破解：需支持实时检测 SSH、RDP、SMB 服务的快速和慢速暴力

	<p>破解行为,可以自定义单位时间内登录失败阈值(同一 IP 连续暴破次数)、暴破攻击处置方式(上报和自动封堵)、封堵时长等配置项。支持暴力破解威胁事件一键信任、一键忽略、加入黑名单等操作。支持 IP 地址白名单(信任名单)设置,不做暴破日志上报和自动封堵,防止产生误报;支持 IP 地址黑名单设置,可以对攻击源 IP 地址进行永久封堵。</p>
▲1.16	<p>性能监控:支持服务器全方位性能监控,包括总功率、CPU 温度、磁盘介质错误、电压、出入风口温度、风扇转速;CPU 利用率、内存使用率、SWAP 使用率、TCP 重传率及套接字个数、UDP 连接数、文件句柄数及使用率、磁盘读写速率、分区使用率等。</p>
★1.17	<p>虚拟化软件:配置 CPU 虚拟化软件,软件授权终身有效,1 年免费维保服务。</p>
●1.18	<p>支持虚拟机全生命周期管理能力,包括但不限于开机、关机、强制关机、重启、强制重启、暂停、恢复、克隆为模板、重置密码、重装系统、整机快照、迁移、批量创建虚拟机、虚拟机列表导出等。</p>
●1.19	<p>支持虚拟机故障 HA 功能,可配置 HA 接入控制策略,HA 最大尝试次数、HA 资源预留,且支持 HA 故障切换主机设置,达到故障隔离的效果,并支持配置虚拟机自启动策略和启动优先级,提供截图证明材料。</p>
●1.20	<p>提供全局分布式 SDN 功能,支持 VLAN/VXLAN 模式。无需单独的网络节点及 SDN 虚拟机,以避免 SDN 控制节点故障。支持支持分布式防火墙、支持分布式路由器、分布式 NAT 网关等功能。提供截图证明材料。</p>