|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量（台）** | **设备参数、性能指标** |
| 1 | 应用服务器 | 4 | 1、品牌： 浪潮2、外型：采用≤2U机架式服务器。 　★3、处理器：本次配置2颗Intel至强可扩展处理器，单处理器主频≥2.4GHz，单处理器物理核数≥10C。4、内存：主板集成≥24个内存插槽，以满足本次项目扩展要求；本次配置2\*16GB DDR4内存。5、硬盘：本次配置2块600GB 10K SAS硬盘，2块480GB固态硬盘。6、raid卡：配置≥1块SAS RAID卡。7、I/O扩展槽：支持≥7个PCI-E 3.0插槽，支持≥1个OCP卡。8、GPU扩展：最大支持≥4个双宽GPU。9、网络控制器：配置≥4口千兆网卡，2个万兆端口（含光模块），支持虚拟化加速、网络加速、负载均衡、冗余等高级功能，另有1个独立的千兆管理网口。10、电源：配置电源≥500W的冗余电源，具备智能冷却系统控制功能，已节约资源和保护计算机硬件设备。11、提供8个冗余热插拔风扇。由风扇控制器、风扇，独立风扇控制；采用双转子大尺寸风扇，支持免工具热插拔维护。12、要求部件支持高温耐腐蚀。★13、管理软件：配置中文版管理软件，，支持Windows/Linux系统跨平台管理；跨网段的集中管理；采用标准的IPMI等开放的协议，实现对服务器的带内带外统一管理。★14、支持安全可信模块，提供安全管理系统。1）采用B/S架构，由控制中心、系统中心、客户端三个模块组成防病毒体系。支持Windows Server 2012、Windows Server 2016、Windows Server 2019操作系统。2）提供直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。3）集反病毒、主动防御、防火墙“三合一”。4）可以定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等，可以根据部门需求定制不同的策略。5）提供反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力。6）提供黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免电脑遭到黑客入侵。直接从网络层防御Wanncry、MS 08-067等漏洞攻击；7）提供设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备。15、提供原厂3年质保服务。★16、采用原厂完整包装和配件，机器配置通过序列号可在厂家网站查询，机器及配件通过序列号能在厂商客户服务系统查真伪。 |
| 2 | 数据库服务器 | 2 | 1、品牌： 浪潮2、外型：采用≤2U机架式服务器。 　★3、处理器：本次配置2颗Intel至强可扩展处理器，单处理器主频≥2.4GHz，单处理器物理核数≥16C。4、内存：主板集成≥24个内存插槽，以满足本次项目扩展要求；本次配置64GB DDR4内存。5、硬盘：本次配置2块600GB 10K SAS硬盘，2块960GB固态硬盘。6、raid卡：配置≥1块SAS RAID卡。7、I/O扩展槽：支持≥7个PCI-E 3.0插槽，支持≥1个OCP卡。8、GPU扩展：最大支持≥4个双宽GPU。9、网络控制器：配置4口千兆网卡，2个万兆端口（含光模块），支持虚拟化加速、网络加速、负载均衡、冗余等高级功能，另有1个独立的千兆管理网口。10、电源：配置电源≥500W的冗余电源，具备智能冷却系统控制功能，已节约资源和保护计算机硬件设备。11、提供8个冗余热插拔风扇。由风扇控制器、风扇，独立风扇控制；采用双转子大尺寸风扇，支持免工具热插拔维护。12、要求部件支持高温耐腐蚀。★13、管理软件：配置中文版管理软件，支持Windows/Linux系统跨平台管理；跨网段的集中管理；采用标准的IPMI等开放的协议，实现对服务器的带内带外统一管理。★14、支持安全可信模块，提供安全管理系统。1）采用B/S架构，由控制中心、系统中心、客户端三个模块组成防病毒体系。支持Windows Server 2012、Windows Server 2016、Windows Server 2019操作系统。2）提供直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。3）集反病毒、主动防御、防火墙“三合一”。4）可以定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等，可以根据部门需求定制不同的策略。5）提供反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力。6）提供黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免电脑遭到黑客入侵。直接从网络层防御Wanncry、MS 08-067等漏洞攻击；7）提供设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备15、提供原厂3年质保服务。 |
| 3 | 文件服务器 | 2 | 1、品牌： 浪潮2、外型：采用≤2U机架式服务器。 　★3、处理器：本次配置2颗Intel至强可扩展处理器，单处理器主频≥2.4GHz，单处理器物理核数≥10C。4、内存：主板集成≥24个内存插槽，以满足本次项目扩展要求；本次配置2\*16GB DDR4内存。5、硬盘：本次配置2块600G 7.2K SAS硬盘，2块256GB固态硬盘。6、raid卡：配置≥1块SAS RAID卡。7、I/O扩展槽：支持≥7个PCI-E 3.0插槽，支持≥1个OCP卡。8、GPU扩展：最大支持≥4个双宽GPU。9、网络控制器：配置4口千兆网卡，2个万兆端口（含光模块），支持虚拟化加速、网络加速、负载均衡、冗余等高级功能，另有1个独立的千兆管理网口。10、电源：配置电源≥500W的冗余电源，具备智能冷却系统控制功能，已节约资源和保护计算机硬件设备。11、提供8个冗余热插拔风扇。由风扇控制器、风扇，独立风扇控制；采用双转子大尺寸风扇，支持免工具热插拔维护。12、要求部件支持高温耐腐蚀。★13、管理软件：配置中文版管理软件，支持Windows/Linux系统跨平台管理；跨网段的集中管理；采用标准的IPMI等开放的协议，实现对服务器的带内带外统一管理。★14、支持安全可信模块，提供安全管理系统。1）采用B/S架构，由控制中心、系统中心、客户端三个模块组成防病毒体系。支持Windows Server 2012、Windows Server 2016、Windows Server 2019操作系统。2）提供直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。3）集反病毒、主动防御、防火墙“三合一”且。4）可以定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等，可以根据部门需求定制不同的策略。5）提供反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力。6）提供黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免电脑遭到黑客入侵。直接从网络层防御Wanncry、MS 08-067等漏洞攻击；7）提供设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备15、提供原厂3年质保服务。 |
| 4 | 网络存储服务器 | 1 | 1、品牌： 浪潮2、外型：采用≤2U机架式服务器。 　★3、处理器：本次配置2颗Intel至强可扩展处理器，单处理器主频≥2.4GHz，单处理器物理核数≥10C。4、内存：主板集成≥24个内存插槽，以满足本次项目扩展要求；本次配置32GB DDR4内存。5、硬盘：本次配置4块4TB 7.2K SATA硬盘，2块600GB 10K SAS硬盘。6、raid卡：配置≥1块SAS RAID卡。支持建立大于4个raid17、I/O扩展槽：支持≥7个PCI-E 3.0插槽，支持≥1个OCP卡。8、GPU扩展：最大支持≥4个双宽GPU。9、网络控制器：配置4口千兆网卡，2个万兆端口（含光模块），支持虚拟化加速、网络加速、负载均衡、冗余等高级功能，另有1个独立的千兆管理网口。10、电源：配置电源≥500W的冗余电源，具备智能冷却系统控制功能，已节约资源和保护计算机硬件设备。11、提供8个冗余热插拔风扇。由风扇控制器、风扇，独立风扇控制；采用双转子大尺寸风扇，支持免工具热插拔维护。12、要求部件支持高温耐腐蚀。★13、管理软件：配置中文版管理软件，支持Windows/Linux系统跨平台管理；跨网段的集中管理；采用标准的IPMI等开放的协议，实现对服务器的带内带外统一管理。★14、支持安全可信模块，提供安全管理系统。1）采用B/S架构，由控制中心、系统中心、客户端三个模块组成防病毒体系。支持Windows Server 2012、Windows Server 2016、Windows Server 2019操作系统。2）提供直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。3）集反病毒、主动防御、防火墙“三合一”。4）可以定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等，可以根据部门需求定制不同的策略。5）提供反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力。6）提供黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免电脑遭到黑客入侵。直接从网络层防御Wanncry、MS 08-067等漏洞攻击；7）提供设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备15、提供原厂3年质保服务。 |
| 5 | 智能咨询服务器 | 5 | 1、品牌：浪潮 2、外型：采用≤2U机架式服务器。 　★3、处理器：本次配置2颗Intel至强可扩展处理器，单处理器主频≥2.4GHz，单处理器物理核数≥16C。4、内存：主板集成≥24个内存插槽，以满足本次项目扩展要求；本次配置64GB DDR4内存。5、硬盘：本次配置2块480GB固态硬盘。6、raid卡：配置≥1块SAS RAID卡。7、I/O扩展槽：支持≥7个PCI-E 3.0插槽，支持≥1个OCP卡。8、预装NVIDIA TESLA T4 GPU显卡。9、网络控制器：配置4口千兆网卡，2个万兆端口（含光模块），支持虚拟化加速、网络加速、负载均衡、冗余等高级功能，另有1个独立的千兆管理网口。10、电源：配置电源≥500W的冗余电源，具备智能冷却系统控制功能，已节约资源和保护计算机硬件设备。11、提供8个冗余热插拔风扇。由风扇控制器、风扇，独立风扇控制；采用双转子大尺寸风扇，支持免工具热插拔维护。12、要求部件支持高温耐腐蚀。★13、管理软件：配置中文版管理软件，支持Windows/Linux系统跨平台管理；跨网段的集中管理；采用标准的IPMI等开放的协议，实现对服务器的带内带外统一管理。★14、支持安全可信模块，提供安全管理系统。1）采用B/S架构，由控制中心、系统中心、客户端三个模块组成防病毒体系。支持Windows Server 2012、Windows Server 2016、Windows Server 2019操作系统。2）提供直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。3）集反病毒、主动防御、防火墙“三合一”。4）可以定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等，可以根据部门需求定制不同的策略。5）提供反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力。6）提供黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免电脑遭到黑客入侵。直接从网络层防御Wanncry、MS 08-067等漏洞攻击；7）提供设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备15、提供原厂3年质保服务。 |