1. **总体要求**
2. 本部分内容是根据本项目实际情况制定的。
3. 投标人必须仔细阅读本部分的全部条款。对本部分中存在的任何疑问、遗漏或相互矛盾之处，或是对于相关要求不清楚，认为存在歧视、限制的情况，投标人可以向采购中心寻求书面澄清。
4. 本部分所列明的工艺、材料和设备的标准以及参照的品牌或分类号仅起说明作用，并没有任何限制性，投标人在投标中可以选用替代标准，品牌或分类号，但这些替代应当等于或优于文件技术要求。
5. 付款方式：

（1）合同签订后15个工作日内，甲方向乙方支付合同金额的40%。

（2）硬件设备和服务项目到货并安装、调试合格试运行后15个工作日内，甲方向乙方支付合同金额的60%。

1. **技术服务需求**

**一、项目概述及需求一览表**

**1.需求一览表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **品目号** | **品目名称** | **数量** | **单位** | **交货期** |
| 智慧团建平台建设 | A01-01 | 四路服务器 | 5 | 台 | 合同签订后60日内 |
| A01-02 | 万兆交换机 | 2 | 台 |
| A01-03 | 千兆交换机 | 2 | 台 |
| A01-04 | 堡垒机 | 2 | 台 |
| A01-05 | 日志审计 | 1 | 套 |
| A01-06 | SAN存储系统 | 2 | 套 |
| A01-07 | NAS存储系统 | 2 | 套 |
| A01-08 | 虚拟化软件 | 20 | 套 |
| 智慧团建安全服务 | A01-09 | 安全服务 | 1 | 项 | 1年 |

\*品目A01-06、A01-07必须同一制造厂家产品

\*品目A01-01至A01-07须提供原厂售后服务承诺函（承诺函的内容包括：原厂提供技术服务期限为5年，从投入使用开始5年内，针对硬件使用过程中出现的技术问题，需要提供7\*24小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对软件的调节/优化提供建议，提供4小时带备件现场保修，五年原厂免费上门服务）

**2.项目概述**

**2.1项目背景**

“智慧团建”将建成覆盖全团全部团管理机关、基层团组织和团员的互联网工作平台，成为一个活跃用户达千万量级的巨型网络服务平台。从技术角度看，首先需要建成具有良好伸缩能力、能支撑千万量级活跃用户的数据中心基础设施。从软件开发和网络服务运营角度看看，为了按时间要求在全团有序推进“智慧团建”的相关业务，不仅需要建成承载业务的数据中心基础设施，而且需要开发专用的业务软件系统，并且从平台运维、内容建设、人员培训和业务督导等方面进行精心规划并作好充分的准备。从技术实施角度看，“智慧团建”系统建设主要有三个方面的工作：数据中心基础设施建设，“智慧团建”平台软件系统迭代开发和分阶段运营和推广实施。以下主要结合这三个方面就建设实施思路和成本预算进行说明。

**2.3建设内容**

本项目的建设内容为智慧团建平台建设。智慧团建平台建设内容主要包括硬件采购和安全服务两部分。

**二、技术规格、参数及要求**

**A01-01 四路服务器**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术要求及指标 |
| 1 | 处理器类型 | 主频：≥ 2.0GHz核心数：≥ 14核三级缓存：≥ 35M |
| 2 | 处理器数量 | **\*处理器配置数目:≥4个** |
| 3 | 内存 | 内存类型：ECCDDR4工作频率≥2133MHz |
| 4 | **\*内存配置容量：≥128GB,单条内存≥16GB** |
| 5 | 内存扩展能力：≥32个插槽，支持高级内存纠错、内存镜像、内存热备等高级功能 |
| 6 | 本地存储 | 内置硬盘类型：热插拔SAS/SATA/SSD硬盘 |
| 7 | 内置硬盘配置容量数目：≥5块，单块要求≥300GB，转速≥10Krpm转速 |
| 8 | 最大支持≥20块硬盘 |
| 9 | 配置独立RAID卡，缓存≥2GB，支持RAID0/1/5/6/50/60  配置掉电保护功能 |
| 10 | I/O扩展 | PCI-EI/O插槽总数≥12个 |
| 11 | 网卡 | 配置2个GE端口,2个10GE光口 |
| 12 | HBA端口 | 双16 GbpsFC端口 |
| 13 | 光驱 | 配置DVD驱动器 |
| 14 | 硬件远程维护支持 | 可以远程监控并操作主机的IPMI接口或其他技术 |
| 15 | 电源 | 配置不低于2+1冗余热插拔电源，并提供配套的电源连接线 |

**A01-02 万兆交换机**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术要求及指标 |
|  | 硬件规格 | **\*10G接口数≥48，40G接口数≥6，最大10G接口数≥72** |
|  | **性能参数** | 模块化电源冗余、模块化风扇冗余，电压及风扇支持热拔插。 |
|  | 交换容量≥2Tbps |
|  | 包转发率≥1000Mpps |
|  | **\*配置双电源、冗余风扇，配置万兆SFP+多模光模块48个。** |
|  | 产品功能 | 支持RIP、OSPF、BGP-4等三层路由协议 |
|  | 支持PIM-SM、IGMP 等组播路由协议 |
|  | 支持VXLAN routing 和VXLAN bridging，支持EVPN VXLAN |
|  | 实配支持VXLAN功能，无需另外购买授权 |
|  | 支持多虚一技术，可将多台物理设备虚拟化为一台逻辑设备统一管理，支持跨设备链路聚合及最快50ms 级故障链路收敛。 |
|  | 支持专门针对CPU的保护机制，能够针对发往CPU处理的各种报文进行流量控制和优先级处理，保护交换机在各种环境下稳定工作 |
|  | 支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行 |
|  | 支持端口镜像功能，支持多对一端口镜像及一对多端口镜像，支持跨交换机的远程端口镜像功能 RSPAN，支持聚合链路的镜像 |
|  | #支持软件定义网络SDN，符合OpenFlow 1.3协议标准，支持SDN和SDN Ready功能 |
|  | 支持IPv4/IPv6 |

**A01-03 千兆交换机**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 参数要求 |
|  | 硬件规格 | **\*固化端口：≥48个10/100/1000Mbps电口，≥4个SFP+光口，≥2个业务子卡扩展槽位** |
|  | 配置双电源、配置万兆SFP+多模光模块4个。 |
|  | 性能参数 | 交换容量≥590Gbps |
|  | 包转发率≥250Mpps |
|  | 支持48GE+8XS 100%线速转发 |
|  | 配置双电源、配置万兆SFP+多模光模块4个。 |
|  | 整机MAC地址≥64K，ARP表项≥20K，FIB表项≥12K |
|  | 产品功能 | 支持RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+ |
|  | 支持 IGMP v1/v2/v3，IGMP v1/v2/v3 Snooping |
|  | 支持基本的QinQ，支持灵活的QinQ |
|  | 支持PIM-DM，PIM-SM，PIM-SSM，PIM for IPv6 |
|  | 支持ARP防欺骗功能，能够禁止非法用户的ARP欺骗报文，保护合法用户免受其害，防止合法用户的数据被窃取 |
|  | 支持基于端口的出方向和入方向限速，限端口速粒度≤64Kbps；  支持基于流的出方向和入方向限速，且流限速粒度≤8Kbps； |
|  | 支持openflow 1.3协议 |
|  | 支持基本和灵活QinQ特性，且能够支持1：1和N：1 VLAN交换； |
|  | 支持模块化操作系统，支持针对单一模块打热补丁，故障模块升级中不影响其他进程的正常运行和业务转发 |
|  | 支持sFlow网络监测技术，可提供完整的第二层到第四层信息，可以适应超大网络流量环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。 |
|  | 支持虚拟化功能，最多可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms |
|  | 支持ITU-TG.8032ERPS |
|  | 支持端口休眠； |
|  | 符合国家低碳环保等政策要求，支持IEEE 802.3az标准的EEE节能技术 |
|  | 支持智能温控功能，支持风扇自动调速、风扇故障检测、风扇状态查询等操作； |
|  | 支持线缆检测，可对线路进行正常、短路、断路、半断开状态进行检测，且能够检测到线缆发生故障的具体位置； |
|  |  |
|  | 支持IPv4/IPv6 |

**A01-04 堡垒机**

| 序号 | 指标项 | 技术要求及指标 |
| --- | --- | --- |
|  | 产品外观 | 标准2U机架式 |
|  | 产品架构 | 软硬件一体化产品 |
|  | 部署方式 | 旁路部署，不影响原有网络结构 |
|  | 访问方式 | 采用B/S结构，采用HTTPS方式访问，无需安装任何代理 |
|  | 网络接口 | 6个10/100/1000自适应以太网口+4光插槽。1个Console口，支持Console口管理。 |
|  | 数据安全性和可靠性 | 专用千兆多核硬件平台和安全操作系统，MTBF不少于6万小时，支持双机热备。  #支持负载均衡（多协议代理服务器节点可访问相同资源时实现自动负载均衡） |
|  | 数据存储 | 系统标配3块4TB硬盘 |
|  | 节点数及并发连接数 | #3000个主机/设备审计节点许可，图形会话并发连接数>=800，字符会话并发连接数>=3000 |
|  | 基础功能 | 提供系统自身状态的监控功能，包括：cpu工作情况，内存使用情况，磁盘使用情况，网卡使用情况，系统自身数据库工作情况，系统自身WEB服务工作情况，系统自身其他关键组件工作情况等。 |
|  | 支持双机热备、冷备模式。 |
|  | 管理分权 | #业务管理组：分属不同业务管理组的业务管理员只能管理所在业务管理组内的用户、资源、策略和审计管理，适用于不同的管理部门有独立的管理员，运维人员，资源和审计管理要求的场景 |
|  | 字符文件传输协议审计 | #支持SSH协议服务端启用强加密算法hmac-sha2-256,hmac-sha2-512，提升SSH协议安全性 |
|  | 支持字符协议SSHv1、SSHv2、TELNET、RLOGIN和文件传输协议FTP、SFTP的协议审计，审计详细的操作语句和操作语句的执行结果 |
|  | 图形协议审计 | #支持RDP、VNC图形操作过程中键盘输入操作记录和鼠标点击行为记录，并支持开启或关闭键盘输入审计功能 |
|  | #支持RDP窗口标题审计，并支持通过窗口标题内容检索定位回放 |
|  | #支持对剪贴板拷贝文件行为和文本信息内容的记录，并支持通过搜索文本内容关键字定位审计回放 |
|  | #RDP协议支持windows服务端开启安全层SSL加密，加密级别符合FIPS标准，允许运行使用网络级别身份验证的远程桌面的计算机连接，以满足运维过程安全性的更高要求 |
|  | 资源管理 | 自动学习模式：可自动学习资产；对学习到的资产可以导入到资产列表中，并可根据导入的资产列表进行详情的编辑。 |
|  | 密码管理 | 支持改密的资源包括：Linux、Unix、Windows（采用RPC方式）、AIX以及数据库Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE |
|  | 审计查询和报表 | #支持通过账号核查报表统计幽灵账号、僵尸账号、孤儿账号，快速发现账号异常情况  幽灵账号报表，对资源账号进行统计分析，便于及时发现非法建立的资源账号。  支持僵尸报表，统计周期内登录次数低于某一阈值的用户账号和资源账号。  孤儿账号报表，统计未建立任何访问策略授权关系的用户账号和资源账号。 |
|  | 密码找回 | #支持用户忘记登录密码时，可通过邮件或短信方式获取验证码，验证通过后重置登录密码 |
|  | 对外接口 | 对所有审计日志提供外发接口，可通过FTP/SFTP外置，可选择性外发审计数据，也可配置外发所有审计，可配置对端端口等信息，同时可以直观显示审计日志外置导出的数量等详情。 |
|  | 系统扩展 | 支持4A扩展，可以将审计日志输出到4A平台。 |
|  | API接口 | 支持通过API接口进行资产添、删改，及策略的制定 |
|  | 运维方式 | 支持WEB H5，或者SSH网关等运维方式 |
|  | 产品资质 | 公安部《计算机信息系统专用产品销售许可证》 |

**A01-05 日志审计**

| 序号 | 指标项 | 技术要求及指标 |
| --- | --- | --- |
| 1 | 产品形态 | 软件产品，采用B/S架构，管理中心内嵌数据库，用户无需另外安装数据库管理系统；管理客户端基于浏览器，无需安装其他客户端软件，支持Windows、Linux等操作系统，并可根据实际环境需求进行定制。 |
| 2 | 事件采集性能 | 每秒采集≥50000条事件 |
| 3 | 事件分析性能 | 每秒实时关联分析≥12000条事件 |
| 4 | 事件采集丢包率 | 每秒采集≥10000条事件时，丢包率≤0.1% |
| 5 | 事件查询性能 | 百GB日志量查询平均响应时间≤1分钟 |
| 6 | 事件入库性能 | 事件入库性能可达每秒≥2万条； |
| 7 | 事件存储性能 | 存储容量仅取决于磁盘空间大小，可以在线分析≥800G的事件量 |
| 8 | 控制台并发数 | ≥500个 |
| 9 | 部署模式 | 支持支持级联部署。 |
| 10 | 用户使用模式 | 界面100%都是B/S模式，无需安装客户端，使用IE浏览器访问管理中心，浏览器端无需安装Java运行环境。 |
| 11 | 管理范围 | 能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 12 | 日志审计对象 | 支持对各类网络设备（路由器，交换机）、安全设备（包括防火墙，VPN，IDS，IPS，防病毒网关，网闸，防DDOS攻击，Web应用防火墙）、安全系统（Symantec、瑞星、江民、微软ISA、Windows防火墙）、主机操作系统（包括Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）、各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）、各种应用系统（邮件，Web，FTP，Telnet），网管系统告警日志、终端管理系统（或是内网管理系统、桌面管理系统）告警日志，网络综合审计系统告警日志，上网行为审计系统日志，以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。 |
| 13 | 日志采集方式 | 通过syslog、snmp trap、netflow、netscreem、jdbc、odbc、opensec lea、agent代理、wmi等多种方式完成各种日志的收集功能。对windows服务器（系统、应用和安全）日志和文件类型日志，可免日志代理或插件；支持用户环境中EVT格式的业务系统日志采集。对于保存在日志文件和数据库中的日志使用agent采集方便，无需定制开发采集。 |
| 14 | 日志归并 | 支持对事件名称、源地址、源端口、目的地址、目的端口相同的进行归并，条件可以多种组合；支持对指定设备发送的日志进行归并，其他设备发送的将不进行归并；支持对事件个数深度和事件时间深度进行归并。 |
| 15 | 事件可视化展现 | 支持通过世界地图定位IP地址，通过事件攻击图展示网络安全态势，通过行为分析图展示一段时间内的用户访问行为。 |
| 16 | 日志在线挖掘 | 系统具备事件挖掘能力可通过事件调查工具可以对某条感兴趣的日志中的源IP地址、目的IP地址、或者目的端口进行相关性日志检索。 |
| 17 | 事件分配 | 用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中。 |
| 18 | 趋势分析 | 可对收集的日志根据过滤条件，针对设备地址、源地址、目标地址等进行事件数量、流量等的趋势分析。 |
| 19 | 事件追溯 | 对于关联告警事件，用户可以进行追溯，查看导致该关联事件的所有原始事件。 |
| 20 | 日志关联分析告警 | 系统支持异常行为分析，维护一个与用户信息系统相关的合法账号的正常行为集合，以此区分入侵者的行为和合法用户的异常行为；系统应至少默认有50条告警规则，系统提供可视化规则编辑器，对告警规则进行增删改查。系统内置针对服务器和其他安全设备的访问ip地址、访问账户和访问时间的访问控制规则；告警规则可按照树型结构组织，并可在该树型结构上直接查看该规则的告警信息，对告警日志可按各告警字段进行分组排序。可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。 |
| 21 | 告警和响应管理 | 通过关联分析，对于发现的严重事件可以进行自动告警，告警内容支持用户自定义字段。告警方式包括邮件、短信、SNMP Trap、Syslog、MSN、飞鸽传书等。响应方式包括：自动执行预定义脚本，自动将事件属性作为参数传递给特定命令行程序。此外，还支持设备联动，即可以在告警后对防火墙/NIDS/网络设备下发联动策略，及时阻断威胁。 |
| 22 | 统一监控主页 | 系统应提供从总体上把握日志告警和日志统计分析的实时综合性监控界面。界面由多个监控组件组成，用户可以自定义监控主页。 |
| 23 | 日志分析 | 根据事件的级别、事件的累计发生次数等指标进行综合分析，从而对信息系统或信息系统中单个资源的风险等级进行评估；能够从大量的日志数据中提取隐含的、事先未知的、具有潜在价值的有用信息和知识，包括事件频繁发生的时间段、事件发生的因果关系以及根据共同特性和差异性特征揭发隐含事件的发生。 |
| 24 | 系统自身日志审计 | 用户对本软件系统的操作都记录日志并进行持久化存储，便于追踪、审核和告警。系统日志格式的属性包括：时间、源IP、用户名、操作类型、操作说明、操作结果（成功/失败）；审计日志支持导入和导入，加密导出日志。 |
| 25 | 系统认证 | 支持用户名密码认证方式，认证时需要提供验证码，用户身份鉴别失败的次数达到设定阈值时，产生系统告警消息，通知授权管理员；支持USB key双因子身份认证方式。支持动态口令认证。 |
| 26 | 级联管理 | 能够实现和现有日志审计产品的级联，包括上传监控信息和接收来自上级的控制指令。 |
| 27 | IPv6网络支持 | 系统支持IPv6网络环境。 |
| 28 | 与外部系统集成 | 可以与第三方的工单系统和工作流系统集成。 |
| 29 | 产品资质 | 公安部《计算机信息系统专用产品销售许可证》 |

**A01-06 SAN存储系统**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 指标项 | | 技术要求及指标 |
| 1 | 基本要求 | 体系架构 | #配置双控制器，控制器支持A/A模式，最大支持控制器≥16个，支持FCSAN、IPSAN |
| 2 | 阵列控制器硬件配置 | CPU | 64位多核处理芯片 |
| 3 | 前端主机端口 | 支持FC和IP两种主机连接，双控最大支持主机端口≥42个； |
| **\*实配主机16Gb FC接口≥8个，1Gb iSCSI主机接口≥6个，10GbiSCSI主机接口≥4个**； |
| 4 | 缓存容量 | 配置控制器缓存总容量≥256GB（非SSD硬盘、FLASH、NAS共享等方式扩展缓存） |
| 5 | 硬盘配置 | 磁盘类型 | 支持SSD、SAS、SATA、NLSAS硬盘 |
|  | 磁盘配置 | #双控最大硬盘数≥1000块，配置企业级1.8TB SAS 10000转硬盘54块，配置≥3.8TB SSD硬盘，单盘容量≤960GB，配置缓存软件 |
| 7 | 系统性能 | I/O处理性能 | SPC-1 Revision3.0以上版本提供不小于400000IOPS |
| 8 | 支持主机数量 | ≥256台主机 |
| 9 | 最大LUN数量 | ≥1024LUN |
| 10 | 可靠性 | RAID支持 | 支持优化raid技术，允许同一raid组内2块以上磁盘发生故障而raid不失效，数据不丢失  单块硬盘重建不超过20分钟 |
| 11 |  | Cache镜像功能 | 两条物理全冗余全双工的镜像通道，实现两个控制器的Cache数据通过相互镜像实现备份 |
| 12 | 掉电保护 | 掉电时Cache数据可安全写入硬盘永久保存，实现无限时断电保护Cache数据的目的 |
| 13 | 冗余组件 | 配置冗余控制器、电源、风扇、端口卡等，冗余部件全部支持在线热插拔维护 |
| 14 | 全局热备技术 | 可以实现热备盘跨框热备保护硬盘 |
| 15 | 后端硬盘通道冗余 | 硬盘物理通道要支持冗余，一条物理通道故障后要支持通过冗余通道来访问 |
| 16 | 兼容性 | 操作系统 | 兼容Linux、Windows、Unix操作系统，并提供这些系统下的多路径冗余软件 |
|  | 虚拟化 | 兼容VMware |
|  | 数据管理 | 兼容Veritas |
| 17 | 软件功能 | 阵列安全管理软件 | 配置基于存储阵列的安全控制管理软件，以保证在SAN环境下，不同主机系统对存储阵列访问的安全性，配置最大支持的主机组数许可(100主机组以上)，不得额外收取许可费用 |
| 18 | 数据快照 | 支持数据快照功能,单卷快照数量≥128 |
| 19 | 数据卷复制 | 支持LUN拷贝功能 |
| 20 | 数据消冗 | 支持数据消冗功能 |
| 21 | 数据压缩 | 支持数据压缩功能 |
| 22 | 远程复制软件 | 支持通过FC和IP链路进行远程卷复制功能，要求异步复制功能和现有生产存储直接进行数据复制，且无需添加网关实现数据复制。 |
| 23 | 存储双活功能 | #配置存储双活软件授权，将两台存储在非网关的模式下组成双活系统。当其中一台存储发生故障时，可自动切换到另一台存储上。切换过程自动完成，无需人工干预，业务不中断，数据零丢失； |
| 24 | 可维护 | 统一管理 | 支持基于WEB的GUI和可编程的CLI管理方式，图形化管理界面支持中文、英文两种模式 |
| 25 | 便捷的管理维护功能 | 支持管理界面告警与声光告警、支持Email告警与短消息告警、支持日志信息导出等 |

**A01-07 NAS存储系统**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 指标项 | | 技术要求及指标 |
| 1 | 架构 | 系统架构 | #全冗余架构，全Active并行集群模式，NAS集群节点必须实现共享存储空间并能同时访问同一目录 |
| 2 |  | 支持协议 | NFS,CIFS,FTP,HTTP |
| 3 | 访问控制 | 支持UNIX,NIS,AD,LDAP |
| 4 | 扩展性 | #配置2个NAS节点，最大可扩展至32个以上 |
|  | 每个文件系统可支持到≥256TB，每个文件系统内可以创建≥1000万个文件或目录； |
| 5 | 网络端口 | 系统配置访问NAS的千兆以太网接口≥2个，万兆以太网接口≥8个 |
| 6 | 单引擎可扩展至≥8个GE网口或≥6个10GE网口 |
| 7 | 系统内存 | 控制器内配置缓存总容量≥64Gb（非SSD硬盘、FLASH、NAS共享等方式扩展缓存单节点支持扩展至≥256GB |
| 8 | 消冗功能 | 支持数据消冗功能 |
| 9 | 压缩功能 | 支持数据压缩功能 |
| 10 | 镜像功能 | 支持文件系统镜像功能，实现存储单元间的数据保护，任意存储单元宕机，业务不中断，此次需实现2台磁盘阵列镜像，保证数据可靠性和业务连续性 |
| 11 | 管理软件 | 支持并提供功能全面的图形化管理软件，支持Web或其它图形化方式进行远程系统监控和管理，配置存储系统管理软件，可实现对SAN和NAS的统一管理，提供对整个存储系统各个部件模块的管理 |
| 12 | 存储双活功能 | 支持NAS环境的存储级双活容灾功能（非虚拟化网关实现方式），要求控制器之间可以跨域进行部署，实现关键数据自动实时双写到两个存储系统中，保证两份数据严格的物理隔离，同时保证两份数据自动实时同步； |
| 最远支持距离应不小于100公里； |
| 具备故障自动切换功能，减少人工干预，提升业务连续性。 |

**A01-08 虚拟化软件**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术要求及指标 |
| 1 |  | **\*配置20颗物理CPU授权，1套管理平台授权** |
| 2 | 基本要求 | #采用裸金属架构，无需绑定操作系统即可搭建虚拟化平台。 |
| 3 | 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。 |
| 4 | 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等。 |
| 5 | 能够提供性能监控功能，可以对资源中的CPU、网络、磁盘使用率等指标进行实时统计，并能反映目前物理机、虚拟机的资源瓶颈。 |
| 6 | 兼容性要求 | 支持现有市场上的主流x86服务器，具有双方认可的官方服务器硬件兼容性列表。 |
| 7 | 兼容现有市场上主流的存储阵列产品，具有双方认可的官方存储阵列兼容性列表，存储阵列类型包括SAN、NAS和iSCSI等。 |
| 8 | 兼容现有市场上主流厂商的多款不同型号的服务器配件、网卡和HBA卡产品。 |
| 9 | 兼容现有市场上x86服务器上能够运行的主流操作系统，具有双方认可的官方客户操作系统兼容性列表， 尤其包括以下操作系统：Windows XP、Windows Vista、Windows 2000、Windows 2003、Windows 2008、Windows 8、Redhat Linux、Suselinux、Solaris x86、FreeBSD、Ubuntu、Debian、Mac OS等，虚拟机上的操作系统不进行任何修改即可运行。 |
| 10 | 功能性要求 | 配置HA功能，当集群中的主机硬件发生故障时，该主机上的虚拟机可以在集群的其他主机上自动重启。当虚拟机的客户操作系统出现故障时，可以自动重启该虚拟机客户操作系统，保障业务连续性； |
| 11 | 配置容错机制，可以保证运行虚拟机的主机发生故障时，虚拟机会自动触发透明故障切换，同时不会引起任何数据丢失或停机，保障所有应用持续可用。 |
| 12 | 支持虚拟机的在线迁移功能，无论有无共享存储，都可以在不中断用户使用和不丢失服务的情况下在服务器之间实时迁移虚拟机，保障业务连续性。 |
| 13 | 支持虚机跨虚拟交换机进行在线迁移。 |
| 14 | 配置基础容灾功能，实现基于LAN或WAN的、独立于磁盘阵列的虚拟机级别的复制，可以对虚拟机数据进行基于多个时间点的复制。 |
| 15 | 支持虚拟机的在线迁移功能，无论有无共享存储，都可以在不中断用户使用和不丢失服务的情况下在服务器之间实时迁移虚拟机，保障业务连续性。 |
| 16 | 支持虚机跨虚拟交换机进行在线迁移。 |
| 17 | 配置基础容灾功能，实现基于LAN或WAN的、独立于磁盘阵列的虚拟机级别的复制，可以对虚拟机数据进行基于多个时间点的复制。 |
| 18 | 配置虚拟机的备份功能，能够利用重复数据删除技术对整个虚拟机或虚拟机单个磁盘快速进行无代理备份(全备份或增量备份)和恢复。同时配置备份接口，能够与第三方备份软件无缝兼容对虚拟机进行集中备份。同时配置对SQL server，Exchange和Sharepoint等关键应用备份。 |
| 19 | 配置高效的内存调度与保护机制，能够实现内存的过量使用，以此保证虚拟平台不会被暂时的物理内存耗尽而崩溃，同时实现虚拟内存可以超过物理内存。 |
| 20 | 虚拟机支持多路虚拟CPU（vSMP）技术，以满足高负载应用环境的要求。 |
| 21 | 可以为虚拟机创建一个或多个快照来保存虚拟机的基于时间点的运行状况和数据。 |
| 22 | 配置专用的P2V工具，实现在线物理机至虚拟机的无间断平滑转换。 |
| 23 | 虚拟化平台可以内建标准虚拟交换机，实现虚拟机之间或虚拟机与物理机之间的网络调度，支持同一物理机上虚拟机之间的网络隔离(支持VLAN)。 |
| 24 | 支持16 Gb端到端光纤通道。 |
| 25 | 配置物理主机级别的无状态防火墙，无需使用IPTABLES，管理员可以用命令行和图形化界面配置防火墙。 |
| 26 | 虚拟机支持直接访问裸设备，将虚拟机数据直接存储在LUN上。 |
| 27 | 具有存储精简配置能力，可以超额分配存储容量，提高存储的利用率，减少存储容量的需求。 |
| 28 | 配置虚拟机的存储在线迁移功能，无需中断或停机即可将正在运行的虚拟机从一个存储位置实时迁移到另一个存储位置。支持跨不同存储类型以及不同厂商存储产品之间进行在线迁移 |
| 29 | 无需中断或重启即可根据需要向虚拟机添加CPU，磁盘，内存和网卡。 |
| 30 | 支持跨多个LUN的共享数据文件系统，可以聚合至少32个异构逻辑卷（LUN），支持在线实时添加LUN以实现集群卷容量动态增长，可支持至少62TB容量集群卷。虚拟机文件系统也支持主流存储厂商的存储自动分层功能。 |
| 31 | 配置集中式自动管理物理主机和虚拟机补丁程序的功能。 |
| 32 | 扩展性要求 | 每台虚拟化主机至少支持480颗逻辑CPU |
| 33 | 每台虚拟化主机至少支持4096颗虚拟CPU(vCPU) |
| 34 | 每台虚拟化主机支持12TB内存。 |
| 35 | 每台虚拟化主机至少支持单个存储卷64TB大小容量。 |
| 36 | 每台虚拟化主机至少支持1024个虚拟机。 |
| 37 | 每个虚拟机至少支持62TB的虚拟磁盘容量。 |
| 38 | 每个虚拟机支持128个vCPU。 |
| 39 | 每个虚拟机的内存可以达到4TB。 |
| 40 | 每个虚拟机至少支持4个虚拟SATA适配器，每个虚拟SATA适配器的虚拟SATA设备数量至少可以达到30个。 |
| 41 | 每台虚拟化服务器的虚拟机在线迁移并发数量至少可以达到8个。 |
| 42 | 自动化管理 | 配置开发自动化和流程自动化平台 |
| 43 | 配置可扩展的工作流库，包括Http Rest，JDBC，AD，Powershell，SNMP，SOAP，SSH，使用该工作流库可以创建和运行可配置的自动规划流程来管理虚拟化基础架构以及第三方系统。 |
| 44 | 工作流可以调去虚拟化管理平台API中公开了的每一种操作，以便将这些操作集成到自动化流程中。 |
| 45 | 虚拟化管理 | 支持单点管理，可以从单个控制台对所有虚拟机的配置情况、负载情况进行集中监控，并根据实际需要实时进行资源调整。 |
| 46 | 每个控制台可管理至少1000台物理服务器、10000台已打开电源的虚拟机，15000台已注册的虚拟机，并可以通过链接至少10个控制台实例，跨10个实例管理30000个已打开电源的虚拟机和50000个已注册的虚拟机。 |
| 47 | 配置统一的图形界面管理软件，可以在一个地点完成所有虚拟机的日常管理工作，包括控制管理、CPU内存管理、用户管理、存储管理、网络管理、日志收集、性能分析、故障诊断、权限管理、在线维护等工作。同时能够直接配置、管理存储阵列，具有对存储阵列的多路径管理功能。支持QoS能力，支持基于应用程序的服务级别自动管理功能。 |
| 48 | 可以支持Web Client和命令行管理功能。 |
| 49 | 支持单点登录，用户只需登录一次，无需进一步的身份验证即可访问控制台并对集群进行监控与管理。 |
| 50 | 支持自定义角色和权限，可以限制用户对资源的访问，实现分级管理并增强安全性和灵活性。 |
| 51 | 支持AD域整合，域用户可以访问控制台，由AD来处理用户身份验证。 |
| 52 | 管理软件可实现多管理软件级别互通功能，支持多管理中心架构，并可实现分布式管理。 |
| 53 | 可以记录重大配置更改以及发起这些更改的管理员的记录，可以导出报告以进行事件跟踪。 |
| 54 | 配置自动报警功能，能够配置物理服务器或虚拟机的CPU、网络、 磁盘使用率等指标的实时数据统计，并能反映目前各物理服务器、虚拟机的资源瓶颈。 |
| 55 | 服务及其它要求 | **\*虚拟化软件的所有功能必须为同一家厂商提供，禁止借用第三方软件的整合，以保证功能的可靠性和安全性。** |

**A01-09 安全服务**

按照采购人要求完成咨询工作，按照采购人要求协助完成一年的一个三级应用系统的等级保护定级、备案、整改、测评等工作，所有测评费用由中标供应商承担。

等级保护测评服务内容包括：针对等保对应级别要求的自评估、自评估所发现问题的加固与整改、等保测评的实施及现场配合；

中标供应商应承诺协助采购人指定的系统通过等级保护测评机构的测评；

等级保护测评服务的提交物包括：《XX系统等级保护自评估报告》、《XX系统等级保护加固与整改计划》、《XX系统等级保护加固与整改报告》、《等级保护测评机构推荐报告》、《XX系统等级保护测评报告》等。

**三、售后服务**

**1. 软硬件产品安装及技术支持**

中标供应商提供软硬件的配置安装及集成工作，厂商提供设备安装的技术支持。中标供应商提供详细的安装规划文档包括系统补丁列表、系统参数调整列表、安装软件组件列表、以及系统环境变量列表。

硬件产品投标人提供技术服务期限为5年，从投入使用开始5年内，投标方针对硬件运行过程中出现的技术问题，需要提供5\*8小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对硬件的调节/优化提供建议。

软件产品投标人提供技术服务期限为1年，从投入使用开始1年内，投标方针对软件运行过程中出现的技术问题，需要提供5\*8小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对软件的调节/优化提供建议。1年服务支持期内发现的软件功能缺陷或安全漏洞，投标方应免费修补。

**2.培训要求**

培训计划内容周详、合理、培训范围广、有二次培训计划和持续培训计划安排，可实施，有针对性，包括但不限于系统管理员培训，安全培训及相关产品培训；

1、设备使用培训，说明培训计划、每种设备培训内容、使用培训达到预期结果；

2、设备教学培训，说明培训计划、每种设备实训项目内容、教学培训达到预期结果；

3、设备维护培训，说明培训计划、每种设备维护项目内容、维护培训达到预期结果；

4、所有培训必须有3-5名培训学员熟练掌握所培训内容，经过考核教师签字为准；

5、设备培训地点是培训师必须到采购方现场，如个别设备培训必须到供货方去，则费用全部由供货方负责

6、培训师须为原厂且工龄超五年以上的工程师；