## 项目概述

1、项目名称：

2、服务期限：合同签订之日起12个月

3、服务地址：采购人指定地点

4、项目概况：

肿瘤医院医计划依托“上海肿瘤疾病人工智能工程技术研究中心”建设智能运营体，深度集成至管理核心场景，推动医院运营向“数据驱动、智能决策”模式转型。本项目通过租赁云、网、算服务打造国产化AI大模型基座，对接院内智能影像平台、医院患者服务平台、数据中台、OA协同办公系统、钉钉移动端等系统，为医院医疗服务的提质增效提供关键助力，为患者提供更高效、更精准的诊疗服务。

5、建设内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 服务内容 | 量纲 | 数量 |
| 1 | 算力资源 | GPU裸金属服务器 | 台/年 | 2 |
| 2 | 通算资源 | 8 vCPU 16G云主机，系统盘50GB及以上，数据盘1TB及以上 | 台/年 | 1 |
| 3 | 公网IP+带宽 | 50M公网带宽 | 个/年 | 1 |
| 4 | 云防火墙 | 基础版 | 套/年 | 1 |
| 5 | 主机安全 | 可管理1资产 | 套/年 | 3 |
| 6 | 堡垒机 | 可管理1资产  | 套/年 | 3 |
| 7 | 云VPN网关 | 20M | 个/年 | 1 |
| 8 | 网络资源 | 100M点对点专线 | 条/年 | 1 |

## 二、技术参数要求

本技术规格书中标注“▲ ”号的为关键技术参数。

“▲”标注的服务需求为重要服务需求，若不满足将按照评分标准相关规定处理。

**1、算力资源应满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 算力资源 | 智算节点 | ▲CPU：国产单颗CPU物理核数48核及以上，2.6GHz及以上，4颗；▲内存：2048GB DDR4及以上▲GPU：配置不少于8块GPU卡，单卡显存不低于64GB，单卡半精度浮点算力不低于376TFLOPS▲硬盘：系统盘采用SSD介质，按RAID1配置，可用容量900GB及以上，数据盘采用NVMe SSD介质，总容量6.4T及以上▲网卡：200G RoCE网卡\*8，双口100G RoCE网卡\*1，双口25G网卡\*2 |
| 2 | 算力服务平台 | 集群管理 | 支持对集群资源的全生命周期的管理 |
| 平台可支持纳管不同GPU型号的服务器，实现资源的共享复用 |
| 节点管理 | 节点生命周期的管理，同时还提供远程访问，重启、密码重置，重置操作系统等能力 |
| 权限管理 | 提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 |
| 算力调度 | ▲支持多策略算力调度算法，匹配算力资源的合理化利用（需提供算力调度平台软著） |
| 资源监控 | 支持查看资源的CPU使用率、内存使用率、磁盘使用率、磁盘读/写带宽、磁盘读/写IOPS、流入速率、流出速率，GPU使用率等监控信息。 |
| 审计服务 | 提供云服务资源的操作记录，记录内容包括从管理控制台或者openAPI发起的云服务资源操作请求以及每次请求的结果，供查询、审计和回溯使用，可支持查看最近90天的事件记录。 |
| 安全管控 | 支持对算力服务的安全访问控制，例如添加访问策略等 |

1. **网络资源需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 专线网络 | 提供1条100M点对点专线，连接肿瘤医院与算力中心。投标人负责调通院内专网到算力中心的网络。 |
| 2 | 专线传输 | ▲需采用电路交换，基于二层网络VC硬管道进行传输，确保带宽刚性固定分配 |
| 3 | 专线安全 | ▲承载点对点专线的传输网络，应具备网络全程双路由保护及50ms的保护倒换时间； |

1. **云主机需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 云主机资源 | 8 vCPU 16G内存，系统盘50GB及以上，数据盘1TB及以上 |
| 2 | 登录方式 | 支持密码、密钥对方式登录。 |
| 3 | 多架构支持 | 支持x86计算、arm架构、异构计算GPU。 |
| 4 | 实例管理 | 1）支持对云服务器的创建、删除、变更规格、开机、关机、重启、重置远程连接密码、挂载云硬盘、变更安全组、变更操作系统、绑定/解绑EIP，创建镜像、创建快照，同步云平台数据等； |
| 2）支持对创建的实例在控制台进行管理，可通过IP、ID进行查看、检索。 |
| 5 | 镜像可选 | 支撑创建时可选镜像，支持私有镜像上传。 |
| 6 | 数据盘挂载 | 支持挂载多块数据盘。 |
| 7 | IPv4/IPv6 | 支持IPv4/IPv6双栈，支持绑定、解绑。 |
| 8 | 反亲和性 | 支持虚拟机组管理功能，可以将虚拟机创建到不同宿主机。 |
| 9 | 资源组 | 支持创建资源组，通过资源组功能可管控不同用户管理不同的云服务器资源。 |
| 10 | 专属宿主机 | 创建云服务器时支持选择专属宿主机。 |
| 11 | 网卡管理 | 支持绑定/解绑辅助网卡，更改辅助网卡对应的安全组策略，或针对未关联实例的网卡进行销毁操作。 |
| 12 | 资源动态调整 | 支持在线虚拟机资源热添加，可以在线调整虚拟机的CPU、内存、硬盘等资源。 |
| 13 | 安全组 | 提供安全组管理功能，创建安全组，灵活配置安全组规则，并支持查看安全组所关联的云服务器 ECS 实例信息、辅助网卡信息；支持导入/导出安全组规则。 |
| 14 | 虚拟机回收站 | 支持虚拟机回收站功能，防止用户误删除，虚拟机在回收站中不占用系统资源。 |
| 15 | 监控功能 | 支持查看云服务器 ECS 的 CPU 使用率、内存使用率、云盘使用率、云盘读/写带宽、云盘读/写 IOPS、流入速率、流出速率监控信息。 |
| 16 | 操作日志 | 支持区分时间段、区分云产品查看、导出操作日志。 |

1. **云存储需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 基本功能 | 1）用户可以将单独创建的数据盘挂载到ECS实例上。 |
| 2）用户可以将数据盘从ECS实例上卸载下来。 |
| 3）当云盘容量不满足业务需要时，用户可进行弹性扩容。 |
| 4）云盘、快照创建完成后可以修改名称。 |
| 2 | 快照 | 1）用户可以创建快照来快速保存指定时刻云盘的数据。 |
| 2）用户可以通过快照创建新云盘，新云盘在初始状态就具有快照中的数据。 |
| 3）一旦升级或迁移过程中出现问题，用户可以通过快照及时将业务恢复到快照创建点的数据状态。 |
| 4）用户可以删除不再需要的快照。 |
| 3 | 性能监控 | 提供包括云盘读写带宽、IOPS等基本性能监控信息。 |
| 4 | 单盘最大IOPS | 高效云盘3000、全闪云盘25000。 |
| 5 | 最大吞吐量（MB/s） | 高效云盘60、全闪云盘260。 |
| 6 | 访问时延 （ms） | 高效云盘 10~12 、全闪云盘4~6。 |
| 7 | 超大容量需求 | 可提供超数据盘最大可支持32T。 |
| 8 | 高可靠性 | 采用三副本机制，数据存储的持久性可达99.9999999%，服务可用性99.95%。 |
| 9 | 弹性可扩展 | 支持通过单台云服务器挂载多块云硬盘的方式扩展存储空间，同时支持对单块云硬盘进行在线扩容。 |

1. **弹性公网IP需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 基础能力 | 1）支持在线创建弹性公网IP，创建时可选择云区域、带宽值以及设置实例名称。 |
| 2）支持对创建的弹性公网IP在控制台进行管理，进行查看、检索； |
| 3）支持IPv4 以及 IPv6 带宽功能，最大带宽值可达 1000Mbps。 |
| 4）支持对弹性公网 IP 公网流入速率以及流出速率的监控。 |
| 5）支持在用户创建资源的配额到达规定的上限后，通过工单形式，可调整配额大小，满足不同客户对于资源的需求量。 |
| 2 | 管理功能 | 1)支持调整带宽值（升配或降配）。 |
| 2)支持绑定/解绑云服务器ECS、裸金属服务器、负载均衡SLB。 |
| 3)支持续费、退订弹性公网IP。 |
| 3 | 权限管控 | 提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 |
| 4 | 网络性能 | 支持带宽值范围为1-1000M。 |
| 5 | 弹性灵活 | 支持与云服务器、负载均衡等实例灵活地绑定和解绑，支持带宽灵活调整，应对各种业务变化。 |
| 6 | 实时监控 | 使用提供弹性公网IP以及IPv6 带宽的监控数据，了解实例状态。 |

1. **云防火墙需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 网络支持 | 路由协议 | ▲产品需支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。 |
| 产品需支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试。 |
| 产品需支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试。 |
| 地址转换 | 产品需支持全面的NAT转换配置，包括包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式。 |
| 产品需支持在会话的源、目的地址同为IPv4地址时，可将目的地址转换至指定服务器地址，同时可探测服务器是否存活。 |
| 产品需支持在源地址转换过程中，对SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过SNMP Trap、邮件、声音、短信等方式告警。 |
| 2 | 访问控制 | 访问控制 | 产品需支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制， 并支持地理区域对象的导入以及重复策略的检查。 |
| 流量管理 | 产品需支持多调度类相互嵌套最大5级的带宽管理设置。支持设置每IP最大或最小带宽，支持对每IP进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。 |
| 支持配置基于IP、用户、应用的流量管理规则，且至少支持对2900种应用定制流量管理规则。 |
| 3 | 攻击防护 | 网络攻击防护 | 产品需支持基于不同安全区域防御DNS Flood、HTTP Flood攻击，并支持警告、阻断、首包丢弃、TC反弹技术、NS重定向、自动重定向、手工确认等多种防护措施。 |
| 产品需支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥。 |
| 产品需支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率。 |
| 产品需支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片等；并可在设备页面显示每种攻击类型的丢包统计结果。 |
| 产品需支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入。 |
| SSL 解密 | ▲产品需支持IPv4和IPv6流量的HTTPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，并可同时基于安全域、IPv4和IPv6地址进行例外设置。 |

1. **主机安全需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 文件防护要求 | 产品除支持一般性病毒木马查杀外，还应支持例如：宏病毒、敲诈勒索软件、注册表病毒、间谍软件、僵尸远程软件等特定恶意文件的查杀；除落地在本地文件系统中的文件外，对网络映射驱动器、移动存储路径、共享目录、局域网路径等扩展路径也能够进行扫描查杀。 |
| 产品应内置webshell扫描引擎，针对网站系统恶意webshell、后门等文件进行扫描防护。 |
| 提供快速扫描、全盘扫描、指定扫描等多种扫描防护模式，支持自定义路径、指定引擎、自定义处理动作的个性化扫描防护。 |
| 提供主动防御保护，智能监控系统文件操作行为，利用文件审计关联技术，实时对病毒木马及恶意相关文件进行拦截和防护。 |
| 产品应支持对病毒文件进行手动加白置黑操作，对目录、文件、扩展名进行信任操作，以提升查杀效率和降低误杀率。 |
| 产品应支持对病毒扫描查杀进行资源占用限制和任务并发控制，防止引发启动风暴、扫描风暴，修改资源利用方式无需重启。 |
| 2 | 网络隔离和防护要求 | 产品应支持双向状态防火墙，提供对出入主机流量进行访问控制与隔离；防火墙支持从IP、端口、方向、协议、优先级方面进行策略控制；支持防火墙策略的批量复制、删除、修改、停用等操作。 |
| 产品应支持入侵防御，可对来自网络层的拒绝服务、缓冲区溢出、木马后门、web攻击、恶意网络扫描、恶意入侵提权等各类威胁流量的检测与防护。提供截图证明。 |

**8、堡垒机需要满足以下要求：**

|  |  |  |
| --- | --- | --- |
| **编号** | **功能/特性** | **设计指标** |
| 1 | 资源管理 | 支持SSH、RDP、VNC、Telnet、FTP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin等协议。 |
| ▲可通过应用发布实现对MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql等应用程序/客户端的扩展支持。 |
| 支持对资源（包括主机、应用、应用服务器和资源账户）及账户批量导入、导出。 |
| 支持内置常用的系统类型，包括Linux、Windows、H3C、Huawei、Cisco。 |
| 支持资源按标签管理，每个用户可以给每个资源打10个标签、支持批量添加和删除标签。 |
| 支持TELNET、SSH协议资源使用普通账户自动切换到root（或enable）账户。 |
| 支持支持SSH、RDP、VNC、Telnet、FTP等协议。 |
| 无需安装任何客户端，便可windows、linux、MAC OS等类操作系统登录堡垒机，并访问管理资源。 |
| 支持IE、Edge、Chrome、FireFox、Safari等主流浏览器。 |
| 2 | 资源运维 | 支持SSH、RDP、TELNET、VNC协议资源的批量登录功能，并且支持混合协议的批量登录，支持同时在一个页面运维不同协议的资源。 |
| 支持运维IPv6地址的主机，主机协议类型包含：SSH、RDP、TELNET、FTP、SFTP、SCP。 |
| 支持RDP、SSH、VNC协议类型主机的文件上传和下载，并进行审计。 |
| 访问图形协议资源时，支持分辨率设置。 |
| 支持SSH key方式登录SSH资源。 |
| 支持多台SSH、TELNET协议资源批量执行操作指令。 |
| 支持将运维资源列表导出成XShell和SecureCRT格式的配置。 |
| 支持XShell、putty、MAC terminal等客户端和Remote Broswer（HTML5）访问目标资源。 |
| 支持通过标签筛选资源。 |
| 会话协同过程中，支持参与者控制会话，同时支持创建者强制获取控制权。 |
| 支持字符协议预置命令功能，可添加至少15个经常使用的命令在系统当中。 |

## 三、服务要求：

1. 运营支持

快速响应对操作系统和GPU驱动、计算框架等定制化配置，满足业务的多样性需求；

提供远程算力使用技术支持，快速响应在使用算力和平台时的问题；

提供模型部署等支持和优化方案，协助解决算力使用难题，保障大模型部署顺利进行；

2、运维响应

提供稳定高效的云平台AI算力资源，提供全天候技术支持，专业团队具备丰富运维经验，能迅速响应突发事件；

提供算力资源管控，实时监控资源状态，定期巡检硬件，预警异常保障业务稳定；

系统故障响应时间及时，维修时限短、效率高；

## 四、售后服务响应

1、配备专业化的售后服务团队和专业技术人员7\*24小时维护。当发现故障发生时，能在15分钟内向用户方通告故障情况，每15分钟通告故障处理情况，直到故障消除，并在故障消除后30分钟内通知用户。对于主用设备故障，尽快完成故障处理，使应用系统快速恢复。

2、对于平台运行故障，必须在收到故障告警15分钟内发现上报，并每15分钟反馈处理进展。硬件设备出现故障时，应进行紧急备件更换，保证用户方的业务系统正常运行。对于影响业务的故障，需在故障处理完毕后三个工作日内向用户方提供纸质文件方式的故障处理报告。

## 五、培训要求

由报价人对使用单位选派的相关人员（人数不限）进行培训，内容为安全、监控及高可用服务的使用，并派专门的经验丰富技术人员到现场，提供完善的现场培训。报价人负责对招标人的技术人员和维护操作人员进行培训，以保证参加培训的人员能完全独立的对该类服务进行操作、运行、维护。对于报价人在本项目中提供的所有软件系统，报价人均应详细制定人员培训方案，培训方案应包括培训目的、培训时间安排、人数、次数、教材编写、培训课程、培训组织方式等。培训方案作为评判整体解决方案优劣的重要因素之一。报价人应为所有被培训人员提供文字资料和讲义等相关用品,所有的资料应是中文书写。培训时间不少于1天。

## 六、履约验收

完成业务及应用数据上云后，报价人应自行组织设备和人员，并在招标人监查下现场进行测试和功能验证，由招标人根据使用情况在交付后15个工作日内完成验收。具体依据项目合同中的履约验收方案执行，合同中的履约验收方案将明确履约验收的主体、时间、方式、程序、内容和验收标准等事项。

## 七、保密与责任

1、报价人严格遵守国家有关法律、行政法规和管理规章；严格执行信息安全管理规定《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《互联网电子公告服务管理规定》、《互联网网络安全应急预案》、《电信业务经营许可管理办法》、《木马和僵尸网络监测与处置机制》（工信部保【2009】157号）等有关法规和行政规章制度，不得利用相关业务服务从事危害国家安全、泄露国家秘密、违法犯罪、妨碍社会治安等活动。

2、报价人负有保密义务，承担保密责任。报价方不得出于非法目的泄露招标方业务系统信息，不得损害招标方业务系统数据安全，未经招标方书面同意不得披露、更不得转卖招标方的任何数据与信息。若一经发现，招标方有权要求立即删除、限期整改、暂停甚至终止合作，并要求承担相应法律责任。