

乌达区人民医院智慧医院云服务项目技术文件

总体要求

本次医院信息系统迁云项目是乌海市乌达区人民医院推进业务数字化转型的重要举措,通过将传统架构迁移至云架构,将显著提升系统的安全性、灵活性与运维效率。迁云后的系统将能够更好地满足医院业务发展的需求,为患者提供更优质、高效的医疗服务。同时,云架构的弹性扩展能力也将为医院应对业务峰值与未来发展提供有力支撑,助力医院实现数字化、智慧化转型的长远目标。

本次医院信息系统向云服务端迁移涵盖业务系统涉及的计算、存储、网络、安全、运维审计等全链路资源,具体包括:

- 1、计算资源:满足业务运行的弹性计算实例(云主机)
- 2、存储资源:高性能云硬盘及配套存储管理能力
- 3、网络资源:公网接入、专线连接及网络配置管理
- 4、安全资源:安全防护、漏洞管理、访问控制及日志审计系统
- 5、运维支撑:堡垒机、监控告警等运维工具

云计算服务配置

云计算服务资源必须满足医院服务器配置需求,医院服务器配置如下表如示。(所列服务器为我院现用服务器配置,作为上云需求参考)

乌海市乌达区人民医院服务器配置表

序号	服务器名称	数量(台)	处理器核数(C)	内存(GB)	存储(GB)
1	01 号服务器	1	8	32	1000
2	02 号服务器	1	8	16	500
3	03 号服务器	1	16	64	3000
4	04 号服务器	1	4	8	1000
5	05 号服务器	1	16	64	1000
6	06 号服务器	1	8	16	500
7	07 号服务器	1	8	16	200
8	08 号服务器	1	16	32	15000
9	09 号服务器	1	16	32	500
10	10 号服务器	1	8	32	500
11	11 号服务器	1	8	16	500
12	12 号服务器	1	4	8	200
13	13 号服务器	1	8	32	300
14	14 号服务器	1	16	32	500
15	15 号服务器	1	8	16	300
16	16 号服务器	1	8	32	1000
17	17 号服务器	1	8	32	1000
18	18 号服务器	1	4	8	200
19	19 号服务器	1	8	16	500
20	20 号服务器	1	8	16	500
21	21 号服务器	1	4	8	200

22	22 号服务器	1	8	32	500
23	23 号服务器	1	8	16	200
24	24 号服务器	1	8	16	200
25	25 号服务器	1	8	16	200
26	26 号服务器	1	8	16	200
27	27 号服务器	1	8	16	200
28	28 号服务器	1	8	16	200
29	29 号服务器	1	8	16	200
30	30 号服务器	1	8	16	300

技术参数

1. 云计算服务配置

序号	参数性质	技术参数与性能指标
1	★	生产环境云主机资源：提供不少于 264 核 VCPU、688GB 内存，总存储空间不少于 30TB,均支持在线扩充。 操作系统：支持主流操作系统（包含国产系统），确保兼容性与安全性。
2	★	混合云互联：为最大程度利用现有线下的超融合资源，本次方案需支持将线下超融合平台与线上云资源进行关联，通过混合云网络互联技术，构建统一的资源池、统一架构、统一管理、统一服务平台。实现对线上线下载资源的统一监控、统一运维管理，并具备混合云业务容灾能力。（提供加盖厂商公章的截图证明）
3		证明材料：投标方需提供与我单位线下超融合资源兼容对接且满足上述功能的承诺函，并加盖公章。
4		可靠性保障 合规性认证：云服务端需通过等保 2.0 三级认证。 服务可用性：云主机服务可用性≥99.9%，满足业务连续运行需求。 数据保护：提供宕机迁移、数据备份与恢复功能；备份数据以多副本形式存储，数据可靠性≥99.99%。 部署特性：支持物理机级别强反亲和性，避免单点故障风险。
5		核心功能支持 生命周期管理：支持创建、启动、停止、重启、释放等操作；支持强制操作、按需选型。 网络配置：支持绑定弹性 IP、弹性网卡，区分公网/私网 IP；限制弹性 IP 数量；支持 IPv4/IPv6 双栈网络，实例可自动获取 IP 地址进行内网通信。 监控能力：对 CPU、内存、硬盘等基础指标及系统进程的 CPU、内存、打开文件数进行监控等提供系统级、主动式、细粒度服务；支持监控数据导出及自定义导出参数。 存储管理：支持磁盘创建、删除、挂载/卸载；快照创建、删除、恢复及回滚；云硬盘批量操作、快照批量删除及自动快照策略；基于快照创建新云硬盘；支持自动/手动备份，备份恢复原盘或创建新盘，支持备份策略管理。 扩展能力：系统盘和数据盘均支持在线扩容，且具备无上限的容量扩展。 易用性：单台云主机创建时间需满足分钟级交付要求；支持基于已有实

		例快速创建相同配置主机及保存参数为模板进行批量复制；支持主流和常见镜像（如：RAW、VHD、QCOW2 等格式导入镜像）创建主机；支持密钥、密码、VNC 及远程软件登录。
--	--	---

2. 云网络资源配置

序号	参数性质	技术参数与性能指标
1	★	基础配置：部署点对点数据专线 2 条，并配置相关设施、设备接入医院网络，单条独享带宽≥1000Mbps，保障跨网络数据传输的稳定性与高效性。
	★	硬件独享与可视化：为了确保本次项目业务的数据安全性，本次采购的云服务需采用硬件独享的模式，云平台需提供给采购人（乌海市乌达区人民医院）专属的云资源，确保不与其他用户共用底层服务资源，满足物理隔离、安全合规等需求。需提供专属服务器大屏可视化管理界面，对于线下和线上混合部署的场景，提供资产检视、业务监控、故障快速定位等能力。云端智能大脑，可提供更加丰富的监控告警，并可以与工单联动，便于及时处置。
		证明材料：投标方需提供满足上述要求的证明材料（云服务商出具的部署架构说明及承诺函）并加盖公章。
2		服务能力：可按需选择接入地域、带宽等参数；支持 PTN、PON、OTN 方式接入。
3		与医院网络对接要求： 云服务对接医院内网是医疗信息化升级的重要环节，涉及数据安全、业务连续性、合规性等核心诉求。由于医院数据（如电子病历、患者信息、医疗设备数据）属于高敏感隐私数据，且医疗业务对稳定性、实时性要求极高，因此对接过程需满足严格的技术要求，需在“连通性”与“隔离性”之间实现精准平衡，需与其实现无缝对接，保障业务连续性。 除医院内网以外，还要确保云平台能与医院 5G 专网对接，实现数据在专网与云端的安全、高速传输。医护人员通过 5G 网络在手机、手持 PDA 等终端录入的患者信息、医嘱等数据，实时同步至云端存储、备份，确保终端与云端数据一致。云端与专网权限系统联动，仅授权医护人员可在专网内访问对应患者信息，操作全程留痕，保障业务连续性与合规性，最终实现医疗数据“可用不可见、可控可追溯”。

3. 云安全资源配置

序号	参数性质	技术参数与性能指标
1		云安全中心配置规模：部署 1 套云安全中心系统，覆盖全部核心资产。 核心能力： 安全评分：基于资产整体安全状态生成评分，展示补丁、系统、应用、账号风险检查结果及详情。 流量防护：具备流量微隔离功能，实时监控内网访问流量，控制横向渗透风险。 威胁检测：支持文件篡改监测，可定义告警事件类型及危险等级；支

		持恶意进程查杀（含勒索病毒、挖矿病毒等）。 资产管理：具备资产指纹功能，采集端口、进程、软件、账号、数据库、启动项、WEB 应用等信息。 附加功能：支持网络蜜罐部署，设置诱饵端口诱捕攻击；提供漏洞扫描（Linux/Windows 漏洞、安全补丁）及基线扫描（自定义策略、周期及目标）。
2		云防火墙配置要求：提供的防护带宽峰值$\geq 200\text{Mbps}$。 功能要求： ①支持 IPv4/v6 双栈；内置世界各国 ISP 地址库。支持不少于 8 种的选路算法，包括但不限于最小抖动、最小延迟、最小丢包率、轮询、加权轮询等。 ②支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT；支持 NAT 会话保持，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同。 ③支持 DNS 代理功能，能够把通过防火墙的 DNS 请求代理到指定的 DNS 服务器上做域名解析；能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率；同时支持通过配置多条 DNS 代理，实现内网资源服务器的负载均衡。 ④支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护。
3		Web 全栈防护基础配置：提供具备针对 WEB 的应用安全防护功能。 防护能力： 基于机器学习和语义分析的智能检测引擎，提升 SQL 注入和 XSS 检测精度。 支持 XML 防护，包括 XML 基础校验（包括最大树深度、元素名长度、元素个数、子节点个数等参数配置）、Schema 校验以及 SOAP 校验。 ③根据会话标识、浏览器标识进行会话跟踪，还原攻击场景。支持误分析功能，提升检测精度，减少告警噪音。 支持对 HTTP 协议合法性进行验证，提供 HTTP 协议防护功能，支持对 HTTP 协议的 URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理，且支持非法编码和解码的灵活控制与处理。 ⑤支持 ARP 攻击防护，支持 MAC 地址绑定。
4		增强漏洞扫描配置要求：支持 Web 和系统扫描。 功能要求： ①提供系统漏洞扫描和 Web 漏洞扫描功能，可扫描任意通过所有权认证的公网 IP，包括云资产和非云资产，能够全方位检测系统和 Web 网站存在的脆弱性问题，根据检测结果形成整体安全风险报告，及时进行漏洞修补。 ②支持以 SSH 方式登录 Linux 进行本地扫描。支持 SSH，TELNET 的扫描方式对目标主机全方位配置核查进行扫描。
5		日志审计系统配置规模：部署≥ 1套日志审计系统，支持不少于 20 个资产的日志采集与审计。 功能要求：①支持 HTTP / HTTPS 协议接口进行采集任务配置实现日志数据采集。

		②支持定制任务进行日志数据采集扩展，包括文本格式、目录下文本和数据库格式日志采集，支持编辑正则表达式和 SQL 语句进行日志采集，支持设置自定义任务时间。 支持对选中的事件日志提供在线/离线地图定位、支持源 IP 与目的 IP 分布走向的视网膜图展示、支持事件拓扑分析用于描述整个事件的访问关系及过程。 支持按事件等级、事件分类、系统事件、性能事件、设备类型等进行实时监测策略分组；并内置常用统计策略，内置策略至少包含网络设备操作事件、安全设备故障事件、主机成功登录事件、认证授权、访问控制、操作记录、信息刺探、恶意代码、攻击入侵、信息危害、设备故障等策略。 支持所有范式化事件字段参与关联；编辑规则支持针对事件属性引用规则、引用资产属性、引用资源仪表展现。 支持对正在发生的事件进行近实时关联分析，对过去发生的历史安全事件进行回溯关联分析。
6		云堡垒机配置规模：部署≥1 套云堡垒机，提供不少于 20 个资产的运维审计服务。 功能要求： 支持在 IPV4 与 IPV6 网络环境下部署。 支持添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能。 支持用户客户端 IP 和 MAC 限制，支持黑白名单两种工作模式。 支持资源管理功能，包括添加、删除、启用、禁用、移动、修改功能。 支持基于角色进行授权访问控制 RBAC (Role-Based Access Control)，包括系统管理员根据不同角色进行管理工作、运维人员根据不同角色进行运维工作，从而满足最小特权原则、责任分离原则和数据抽象原则。 支持僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况。 支持改密脚本。
7		抗 DDOS 配置要求：部署数量≥1 套；支持 1 个主域名的 DDOS 攻击防护，防护峰值不少于 5Gbps。 功能要求： ①支持防护 TCP SYN Flood、TCP SYN-ACK Flood、TCP FIN Flood、TCP ACK Flood、UDP Flood IP、Fragment Flood 等网络型攻击。 ②支持防护 CC 攻击、DNS 攻击、HTTP 攻击等应用型攻击支持检测阈值自定义配置。 支持防护对象的流量分析。 支持启动路由器的黑洞路由功能。 ⑤支持包流速和包流量维度的分析统计。
8		SSL 证书配置要求：提供一套 SSL 证书，证书类型为：企业型（OV）。 功能要求： 支持域名监控管理。 支持告警设置。

		支持查看证书相关操作记录。 ④支持国密证书品牌。
--	--	-----------------------------

4. 等保三级测评服务

序号	参数性质	技术参数与性能指标
1		依据《网络安全法》及《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019），本项目须按照等保 2.0 第三级要求进行建设，并通过具备资质的第三方测评机构评审。
2	★	对 3 个主要系统（His 系统/电子病历系统/服务号（掌上医院））进行定级与备案协助医院确定信息系统安全保护等级（第三级），编制《定级报告》，提交公安机关备案，出具测评报告并获得证书。
3		差距分析与整改对照等保三级要求，对云平台、网络架构、安全设备、管理制度等进行全面差距分析。 根据分析结果提出整改方案，并指导实施，确保技术和管理措施均满足测评要求。 重点覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五大技术层面，以及安全管理制度、管理机构、人员管理、建设管理、运维管理等五大管理层面。
4		正式测评委托具备国家网络安全等级保护测评资质的机构开展现场测评。 测评内容包括但不限于：漏洞扫描、渗透测试、配置核查、日志审计等。 测评完成后出具《网络安全等级保护测评报告》。
5		证书获取 协助医院完成测评报告的提交及备案手续，最终获得公安部门核发的《信息系统安全等级保护备案证明》（三级）及测评机构出具的合格测评报告。

5. 网络安全服务

序号	参数性质	技术参数与性能指标
1		渗透测试服务 网络渗透：检测防火墙/路由器端口暴露、弱密码、协议漏洞（如 SSH/Telnet 未加密传输），针对网络设备（防火墙、路由器等）及协议漏洞，识别开放端口、配置错误、MITM 攻击等风险。 Web 渗透：重点检测 SQL 注入、XSS、CSRF 等 OWASP Top 10 漏洞，覆盖前后端及组件安全。 无线网络渗透：破解无线加密协议，模拟恶意接入点攻击，验证无线网络安全策略。 客户端渗透：针对浏览器插件、邮件客户端等程序的安全测试，防范恶意文件执行和本地提权。 移动 APP：检查 API 接口鉴权漏洞、本地数据存贮明文风险、反编译防护有效性。 物理渗透：模拟非法物理入侵（如门禁破解、摄像头干扰），验证敏感区域物理安全措施。

		操作系统与服务器渗透：检测未打补丁的漏洞、权限提升缺陷及横向移动风险。 数据库渗透：验证 SQL 注入、弱密码配置等数据库层安全问题。 IoT 设备测试：针对物联网终端固件漏洞、通信协议缺陷的专项评估。 社会工程学测试：通过钓鱼邮件、电话欺骗等方式评估员工安全意识，测试组织对社交攻击的防御能力。
2		漏洞扫描服务 网络设备、安全设备扫描：（1）路由器/防火墙端口暴露、固件未更新漏洞（如 CVE-2023-39780）； （2）识别未更新的路由器/交换机固件版本（如华硕 RT-AC3200 存在身份认证绕过漏洞）、检测 IoT 设备固件供应链风险（如 Log4j 组件未升级引发 RCE 漏洞）； （3）.扫描开放高危端口（如 TCP 53282 端口 SSH 未授权访问风险）、验证协议实现缺陷（如 ICMP 协议重定向攻击路径）； （4）.检查访问控制列表（ACL）合理性，禁止非业务端口暴露（如关闭 135/445 端口）、验证 VPN 设备双因子认证策略有效性。 Web 应用扫描 主机系统扫描：弱口令、特权服务开放（如 SSH/Telnet）、补丁缺失（如 Windows/Linux 系统漏洞）。 网络层扫描：支持 16 种端口扫描模式，结合 NSE 脚本引擎实现漏洞探测，如检测永恒之蓝漏洞。 数据库扫描：通过 CNAS 认证，独创漏洞验证沙箱技术，可精准识别弱口令、权限溢出等数据库风险。 服务器扫描：（1）通过 SYN/TCP 握手探测开放端口（如 SSH 22、RDP 3389），识别异常服务暴露情况； （2）镜像网络流量检测隐蔽通信（如 ICMP 隧道、DNS 隐蔽信道）； （3）基于 CVE/NVD 漏洞库匹配系统组件指纹（如 Apache 2.4.49 路径穿越漏洞 CVE-2021-41773）； （4）操作系统内核漏洞（如 Windows 永恒之蓝漏洞 MS17-010）、提权漏洞（Linux dirty pipe 漏洞 CVE-2022-0847）； （5）Web 中间件配置缺陷（Nginx 错误配置导致目录遍历）、服务组件过期（Redis 未授权访问）； （6）核查密码策略复杂度、日志保留周期等是否符合等保 2.0 三级标准。 数据库扫描：默认配置风险（如 MySQL 空密码）、未加密传输、SQL 注入点。
3		安全加固服务：操作系统加固：重命名默认管理员账户（如 Windows 的 Administrator）并禁用 Guest 账户、设置密码复杂度策略：长度 ≥ 8 位，包含数字、大小写字母及特殊字符、关闭非必要服务（如 Telnet、FTP），禁用无业务需求的开放端口、启用防火墙策略，仅允许业务必需协议的出入站流量、清理系统中木马文件、修复系统漏洞。 网络设备加固：升级固件至最新稳定版本，修复已知漏洞（如 CVE-2023-39780）、配置 SSH 替代 Telnet，禁用 HTTP 管理接口，启用 ACL 访问控制列表、禁用 SSLv3/TLS 1.0，强制启用 TLS 1.3 协议。

		数据库加固：创建专用低权限账号（如 db_user），限制仅允许业务必需表的读写、禁用默认账户（如 MySQL 的 root 空密码账户）、启用透明数据加密（TDE），审计日志记录所有敏感操作。 应用程序加固：实施参数化查询防范 SQL 注入，对用户输入实施正则表达式过滤、配置 HTTP 响应头：添加 Content-Security-Policy 防 XSS 攻击、设置会话超时≤15 分钟，启用 JWT 令牌签名校验。
4		安全管理制度建设服务：建设安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

6. 技术服务要求：迁移实施计划

序号	参数性质	技术参数与性能指标
1		（一）前期准备 1. 环境调研：梳理现有系统架构、硬件配置、网络拓扑及数据量，明确与云资源的适配点。 2. 方案细化：根据调研结果，细化各模块配置参数，制定数据迁移工具选型及测试方案。 3. 资源确认：协调服务提供商完成云资源预配置，验证资源参数是否满足需求。
2		（二）迁移实施 1. 数据迁移：采用增量备份+全量同步方式，将现有系统数据迁移至云存储，同步过程中进行数据校验。 2. 应用部署：在云主机上部署应用程序，配置网络、安全策略及监控告警规则，与云专线、安全中心等系统联动调试。 3. 功能测试：验证云主机性能、网络连通性、安全防护有效性及运维工具功能，确保与需求一致。
3		（三）上线与优化 1. 灰度切换：分批次将业务流量切换至云环境，实时监控系统负载与响应时间。 2. 问题优化：针对迁移后出现的性能瓶颈、兼容性问题，调整资源配置或优化应用参数。 3. 运维交接：完成运维文档编写及团队培训，确保运维团队熟练操作云平台及配套工具。

7. 技术服务要求：风险与应对措施

序号	参数性质	技术参数与性能指标
1		数据迁移风险（迁移过程中数据丢失或损坏）：迁移前全量备份数据；采用校验机制（如 MD5）确保数据一致性；保留原系统 30 天作为应急回滚节点。
2		性能风险（云主机或网络带宽不满足业务峰值需求）：迁移前进行压力测试，预留 30% 资源冗余；配置弹性伸缩策略，自动应对流量波动。
3		安全风险（迁移过程中遭遇网络攻击）：迁移期间启用临时安全防护策略，限制外部访问；全程监控异常流量，及时拦截攻击行为。
4		兼容性风险（应用程序与国产化操作系统不兼容）：前期进行兼容性测试，对不兼容组件进行改造或替换；协调厂商提供技术支持。

8. 技术服务要求：服务能力

序号	参数性质	技术参数与性能指标
1		资源达标：云主机、网络、存储等资源参数满足方案要求，提供第三方检测报告或服务提供商证明材料。
2		功能验证：各模块功能（如宕机迁移、安全防护、日志审计等）通过实操测试，结果与需求一致。
3		性能达标：系统可用性、数据可靠性、网络带宽等指标达到承诺值，连续运行 30 天无重大故障。
4		灾备能力验收：需合理利用采购人现有机房设备和环境建立灾备机制，满足电子病历评级要求。需进行灾备切换演练，验证当云上业务出现故障时，保障不低于 10 个核心主要业务（具体业务清单待定）能够在 15 分钟内迅速从采购人线下灾备机房恢复，确保医院正常工作秩序。投标方需提供灾备方案及切换演练报告（或承诺函）。
5		等保合规验收：必须通过国家认可的第三方测评机构的等保 2.0 三级测评，并获得公安机关颁发的《信息系统安全等级保护备案证明》及合格的《测评报告》。该证明文件作为项目最终验收的必备材料之一。
6		文档完整：提供资源配置清单、测试报告、运维手册等文档，满足交付要求。
7		本方案基于业务需求制定，迁移过程中需要严格遵循行业最佳实践，确保系统平稳过渡至云环境，提升业务连续性与运维效率。

9. 技术服务要求：项目团队与职责

序号	参数性质	技术参数与性能指标
1		为确保系统迁云项目顺利实施，成立专门的项目团队，各成员职责如下： 项目经理：负责项目整体规划、进度管理、资源协调及跨部门沟通，把控项目质量与风险，定期向医院管理层汇报项目进展情况。
2		技术负责人：主导技术方案的制定与优化，解决迁移过程中的技术难题，确保各技术模块的兼容性与稳定性。
3		云平台工程师：负责云主机、存储、网络等云资源的配置与部署，进行云平台的日常运维与监控，保障云资源的正常运行。
4		安全工程师：负责云安全中心、Web 全栈防护系统、堡垒机等安全设备的部署与配置，进行安全漏洞扫描与风险评估，制定安全防护策略。
5		数据库工程师：负责数据迁移工作，包括数据备份、同步、校验及恢复，确保数据的完整性与一致性。
6		应用工程师：负责应用程序在云主机上的部署与调试，进行功能测试与性能优化，确保应用程序在云环境中正常运行。
7		运维人员：参与运维交接工作，学习云平台及配套工具的操作，负责系统迁移后的日常运维与监控告警处理。

10. 技术服务要求：培训要求

序号	参数性质	技术参数与性能指标
1		为使医院运维团队能够熟练操作云平台及配套工具,确保系统迁移后的稳定运维,制定以下培训计划: 1. 培训时间:项目上线前1周开始,持续2周,每天培训时长为4小时。
2		培训内容 云平台基础知识:包括云主机、存储、网络等云资源的概念与特点。 云平台操作技能:云主机的创建、启动、停止、重启等生命周期管理操作;存储资源的创建、挂载、快照等管理操作;网络配置的相关操作。 安全设备使用:云安全中心的安全评分查看、威胁检测与处理;Web 全栈防护系统的防护规则配置与攻击防护操作;堡垒机的账号管理与身份认证操作。 运维工具使用:日志审计系统的数据采集与分析;监控告警系统的指标查看与告警处理。
3		培训方式:采用理论讲解与实操演练相结合的方式,由服务提供商的技术专家进行授课,每位运维人员配备实操环境,确保掌握相关操作技能。
4		培训考核:培训结束后,通过理论考试与实操考核的方式检验运维人员的培训效果,考核合格后方可上岗进行运维工作。

11. 技术服务要求：应急预案

序号	参数性质	技术参数与性能指标
1		为应对系统迁移过程中及迁移后可能出现的突发情况,制定以下应急预案: 数据丢失或损坏应急处理: ①立即停止数据迁移或相关操作,启用迁移前的全量备份数据进行恢复。 ②检查数据损坏原因,采取相应的修复措施,如修复数据库漏洞、更换存储设备等。恢复数据后,进行数据校验,确保数据的完整性与一致性。
2		系统性能不达标应急处理: ①若云主机性能不满足需求,立即调整云主机的资源配置,如增加VCPU核数、内存容量等。 ②若网络带宽不足,联系服务提供商临时增加带宽,同时优化网络配置,减少网络拥堵。 ③对系统进行性能分析,找出性能瓶颈,进行应用程序优化或系统参数调整。
3		网络攻击应急处理 ①立即启用应急安全防护策略,如关闭不必要的端口、限制可疑IP地址的访问等。 ②安全工程师迅速对攻击行为进行分析与溯源,采取相应的拦截与防御措施。 ③若攻击造成系统故障,及时启动备用系统,确保业务的连续运行。
4		系统兼容性问题应急处理 ①若应用程序与国产化操作系统不兼容,立即将应用程序切换回原系

		统运行，避免影响业务开展。 ②组织技术人员对不兼容组件进行紧急改造或替换，协调厂商提供技术支持，尽快解决兼容性问题。 ③问题解决后，进行充分的测试验证，再将应用程序迁移至云环境。 ④本次医院信息系统迁云工程是乌海市乌达区人民医院推进业务数字化转型的重要举措，通过将传统架构迁移至云架构，将显著提升系统的安全性、灵活性与运维效率。迁云后的系统将能够更好地满足医院业务发展的需求，为患者提供更优质、高效的医疗服务。同时，云架构的弹性扩展能力也将为医院应对业务峰值与未来发展提供有力支撑，助力医院实现数字化、智慧化转型的长远目标。
--	--	--

响应说明：

序号	参数性质	技术参数与性能指标
1	★	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。
2	★	中标后需按照采购人要求进行逐条验收，不满足则予以废标，并依据《中华人民共和国政府采购法》等相关法律法规进行相应处罚。