医院IT技术运维服务2025年度

|  |  |
| --- | --- |
| 服务需求 | 信息化资产梳理服务及标注服务  1）对单位信息化资产信息进行了全面梳理，对服务器、存储设备（含光纤交换机）、网络与安全设备及虚拟化平台业务虚拟机等设备和系统的信息化资产梳理。最终形成包括位置信息、设备类型、型号配置、IP地址、端口号、操作系统、应用系统、责任人等信息的信息资产清单。对照清单，对现有系统和机房设备进行规范化的标注，查漏补缺；如有变动及时更新清单。  2）收集整理并形成网络拓扑图、SAN拓扑图等图表以及各重要业务系统的架构图。  3）各设备标签的打印及标注；其它附属设备的统计记录。 |
| 系统维护资料  拓扑图、ip配置、基础配置、资产安装、设备手册资料、常见问题处理文档资料，建立项目知识库档案，详细记录与项目相关的服务交付信息和项目管理信息。 |
| 技术咨询支持服务  技术咨询支持服务，为甲方机房数据中心所有设备提供技术支持，包括日常技术交流、网络架构调整和信息建设咨询服务等技术支持。 |
| 设备应急响应服务  提供7\*24小时应急响应服务，确保将客户损失减少到最小。甲方系统（包括硬件和软件）出现问题或故障，自接到报修电话后10分钟电话响应，对于系统严重问题，经验丰富的技术人员将在1小时内赶赴现场。根据故障的具体情况进行故障诊断，尽快排除故障。重大事故完成故障排除后输出完整的故障报告给到甲方。故障报告详细分析故障的现象、原因以及优化建议。 |
| 周巡检服务  1、每周对机房所有设备的硬件资源的运行状态、运行性能、资源分配使用情况进行监控，以便了解其是否满足运行要求。适时采用合适的装备与手段进行设备监控。监控内容如下：  1）设备的健康状况、整体运行状态、各项硬件资源开销状况；  2）链路健康状况如端到端时延变化、链路端口工作稳定性、链路负载百分比、部署路由策略情况下端到端选路变化、路由条目变化；  2、主动问询是系统运行过程中是否有问题 |
| 季度巡检服务  1、每季度巡检服务，巡检整个系统相关设备运行状态。包括设备状态的检测、监测各端口的工作状态保障所有端口畅通运行、提取设备运行的日志并记录分析、对整个网络的性能进行测试。巡检完毕后输出完善的巡检报告。并且每次巡检完毕，输出检测报告，分析设备当前状况，提供相应的解决方案，寻求避免问题的再次出现最佳方案。  2、对各系统一段时间的运行进行分析，给出整改意见及建议。  3、对整个交换网络、中心机房、数据中心、安全体系进行评估，从整体运行方面给出调整和优化建议。 |
| 年巡检服务  1、每年开展子系统全面巡检  2、对发现的问题，制定整改方案，与客户核对后，开展整改，优化提升系统稳定性。  3、对整个业务系统和院方需求进行分析，给出提升整改意见和建议。  4、年度巡检报告，各子系统全面巡检信息;对维护维保服务进行总结，并提出改进建议;对各子系统一年的运维情况进行总结，开展自评评价，并给出改进提升建议;对各系统进行评估，提出整改意见及建议。 |
| 信息安全巡检服务  利用客户现有提供病毒扫描报告、日志审计报告、数据审计报告、漏洞扫描报告，每季度统计一次，统计后输出给甲方。 |
| 驻场服务  1、安排技术工程师每周不少于2天驻扎在客户现场，按客户现场需求进行工作排班，驻场人员保持关注设备状态，一旦出现问题可以即时跟进解决，保证了对故障问题的快速跟进及即时处理。  2、驻场人员长期和维护设备打交道，建立了一套具体的设备资料库，保证对于每台设备出故障的原因都很熟悉，保证了对故障的快速处理能力。 |
| 优化改进服务  1、根据应用系统特点和运行需求，对物理资源进行调整，如路由策略调整、设备或链路负载调整、安全策略调整与优化、监控对象覆盖与范围调整、局部交换优化、局部冗余优化等。  2、根据应用系统的特点和运行需求，通过对物理资源的运行记录、趋势的分析，对物理资源进行调整、扩容或升级，包括但不限于：硬件容量变化，如网络设备硬件、软件升级、带宽升级等；整体网络架构变动；网络架构容量变化，如网络子系统的增减等；系统功能变化，如新增功能区、新增安全系统、新增审计系统等；路由协议应用及部署调整；整体安全策略收紧；交换优化；冗余优化。  3、按厂商配置最佳实践，针对客户日常实际问题，由工程师进行设备的配置梳理检查，把不合理的配置整改规范，把全网配置标准化。 |
| 设备升级及维护服务  根据要求对设备数据的配置、规划、调整、备份等。设备的版本升级及补丁安装等。新增设备网络参数及IP规划、割接入网、业务调整等。架构变动时的设备迁移，设备升级、打补丁等。 |
| 现场值守技术保障服务  当遇到重大活动（如两会、国庆、攻防演练等）需要提供临时性的保障服务时，按要求提供保障值守服务，保障服务范围内的系统正常运行。同时，在需要现场保障服务的三天前，提前对所有网络设备进行临时性健康检查，排除安全隐患，杜绝网络安全事件发生。 |
| 信息安全应急支持服务  信息安全紧急事件应急处理服务。甲方出现信息安全紧急事件，乙方将第一时间提供技术支持进行威胁清除、漏洞修复和相应处理。 |
| 应急演练服务  演练内容包括网络及系统可靠性，信息安全等。配合客户制定应急演练计划，并对急预案计划进行演练和验证。 |
| 培训服务  1、通过日常对基础环境、资产梳训，着力提高人员的运维技术能力，通过言传、带教、操作文档等多手段对甲方运维人员进行培训。提升信息化部门整体的技术能力。  2、提供对甲方运维人员进行培专题培训课，培训内容可以是网络、安全、服务器、存储、虚拟化、数据库内容。 |
| 监控软件  1、提供一套运维监控平台，对机房内所有必要的服务器、存储设备、操作系统、交换机设备、安全设备、虚拟化平台、业务系统以及所有类型数据库的运行情况进行实时监控，按时间输出资源使用情况与性能图表，告警信息可发送钉钉、微信提醒。实现集业务、软件（包含数据库、中间件、虚拟化软件、负载均衡、消息队列、Webservice等）、网络、硬件设备的多维度立体化统一运维监控及数据分析。  2、要求平台运行于国产Linux操作系统之上，且保证平台稳定性和安全性。  3、平台监控对象授权数量不做限制，支持无限扩容。同时，在服务期限内，免费提供产品售后及升级服务。  4、提供平台的安装部署服务，负责把医院的IT设备添加到平台中进行监控，并制定大屏展示功能，实时界面展示监控整体运行情况。  5、要求平台支持对支撑业务系统正常运行的重要端口、服务、进程的可用性进行监控。当状态出现异常时，第一时间发出报警信息。  6、要求平台支持对Oracle（含RAC）数据库的监控，包括如：数据库监听、表空间、会话、进程、阻塞、作业、RMAN、AWR、DG、SGA、实时Top SQL等的监控。支持对Oracle数据库阻塞的监控，支持对主从阻塞的识别，可定位导致阻塞的会话，及引起阻塞的SQL语句。 |
| 保密和廉洁要求 | 成交人必须如约承担合同履行时所应该尽的一切保密、廉洁义务。成交人对项目实施过程中的资料、数据进行保密，未经采购人书面同意不得泄露，且保密责任不因合同的中止或解除而失效，否则，需承担相应的法律责任。 |
| 商务条款 | 1、年度的维护费用总金额包含税费、合同寄送费及工程师差旅费等完成本项目服务期限内工作全部费用的总合；除非另有明确约定，甲方无需向乙方支付额外任何价款、费用或报销。  2、甲方应自本合同生效之日且乙方开始服务半年，并收到乙方开具的全额发票起3个月内将前述系统维护费用的50%，汇入乙方指定帐户，合同维护期满且考核合格后、甲方应在3个月内将前述系统维护费用剩余的50%，汇入乙方指定帐户。  3、违约责任：如乙方未按要求提供服务，甲方有权拒付服务费，且乙方应退回甲方已付金额的50%的款项，并向甲方赔偿因乙方未按要求提供服务所导致的损失。 |
| 服务期限 | 甲乙双方约定维护服务期限为签订日期起一年。 |
| 预算价格 | 74000元 |