宁波市北仑区滨海新城医院数据安全服务采购需求文件

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 采购内容 | 采购需求 | 采购预算金额 |
| 1 | 数据安全服务 | 详见采购文件 | 4.95万/年。 |

# 一、数据运维技术服务要求

## 1.1维护范围及要求

本项目建设旨在充分保障宁波市北仑区滨海新城医院核心数据库安全稳定运行，针对系统已存在或未来可能出现的问题，进行维护和业务连续性建设保障服务，投标方应结合招标方的现状和未来的发展需要，制定出全面、科学的解决方案，并提出相应的实施方案，以保证整个系统的平稳发展。

## 1.2现有系统维保范围及要求

为了保障各业务系统数据库的正常稳定运行，及时处理出现的各类故障，应对灾难发生，保障核心数据的安全，拟对宁波市北仑区滨海新城医院现有核心业务数据库服务进行招标采购。

维保设备范围：宁波市北仑区滨海新城医院现有核心业务数据库

维保时间要求：一年（合同到期前，经双方协商，如院方对服务商提供的服务满意的，该合同可自动续签）

响应时间要求：7\*24小时响应。

|  |  |  |
| --- | --- | --- |
| 序号 | 技术服务内容 | 服务期限 |
| （一） | 数据库技术服务要求 | 一年 |
| 1.1 | 7\*24小时400电话、远程不间断支持 | 一年 |
| 1.2 | 故障管理和查询回顾 | 一年 |
| 1.3 | 现场应急保障服务 | 4天/年 |
| 1.4 | 数据库日常巡检服务 | 4次/年 |
| （二） | 防统方服务 | 一年 |

投标人应根据以上要求提供系统维保的详细方案、服务内容以及响应时间。

人员上应选派招标方熟悉的或认可的人员，若服务期间工程师需要更换，需提前一个月通知招标人，并做好交接工作。

**数据库技术服务要求****7\*24小时400电话、远程不间断支持**

对数据库系统故障或与数据库系统相关联的系统故障，投标人提供7\*24小时不间断非现场(可以是400电话、e-mail、VPN、QQ等形式)支持服务，通过以上方式直接联络服务商的技术工程师，寻求问题的解决方案、技术文档以及技术指导，提供故障处理案例。

★投标方在接到招标方故障申告后应于5分钟内响应，如故障未能在15分钟内通过远程支持得到解决，投标方承诺根据招标方要求派指定服务工程师在1小时内赶到招标方现场，提供不间断故障处理服务。

**故障管理和查询回顾**

投标人必须为招标方建立Oracle故障处理档案，投标人工程师应把用户所有故障问题记录在档，并建立故障ID，可以让投标人随时跟踪故障ID的处理状况。故障报告包括故障ID、故障ID的严重等级、故障ID及问题解决的状态、处理该问题的Oracle技术支持工程师、问题说明、问题进展等。

投标人必须为招标方设定固定的专职的主备责任工程师提供服务响应支持。主责工程师需定期进行数据库状况检查，同时提供系统健康检查顾问服务以及协助客户建立ORACLE数据库日常管理规范。

投标人为招标方建立的系统健康档案。详细记录用户系统发生的事故及解决方案，为招标方提供技术案例知识库更新服务，时时关注招标方系统的安全状况，Oracle数据库、服务器操作系统官方网站更新信息，及时为用户提供系统补丁更新、软件升级服务。

**现场应急保障服务**

当遇到复杂性问题，需要到现场进行综合诊断或者用户要求现场支持服务的时候，要求服务团队人员乃至专家后援服务团队人员在1小时内到达支持现场，同时要求在路途中不中断电话支持以求快速解决问题。

当由于各种原因引起数据库不可用或者部分不可用的状况，要求服务团队精通灾备技术，快速恢复各种灾难性故障。熟悉招标方的备份机制和模式，利用备份机制实现快速故障恢复，针对数据灾难情形提供强有力的挽救技术或工具。

★服务期内要求现场服务根据实需求提供，并且不少于4天。

**数据库日常巡检服务**

日常检查至少包括以下内容：

* 检查相关软硬件、数据库配置和SGA、PGA的配置情况；
* 检查数据库、备份结果集、各表空间的变化情况等，并对数据变化情况作评估；
* 统计当前表空间、文件系统和数据文件的使用情况；
* 检查数据库alert.log日志文件和相关trace文件；
* 检查操作系统用户、数据库用户、系统本身的安全性；
* 收集数据库运行期间的负载情况和Instance各性能指标；
* 检查数据库备份是否正常；

★提供一年4次的日常巡检服务。

**防统方服务**

为促进卫生事业的全面、协调、可持续发展，根据国家和省市卫计委的要求，治理医药购销中的不正之风，保障医疗活动正常规范，制止违规统方行为。需要为宁波市北仑区滨海新城医院提供一年的防统方系统服务。

防统方系统服务技术要求如下：

|  |  |
| --- | --- |
| 指标项目 | 技术指标要求 |
| 功能要求 | 防统方系统管理服务控制台,以Web方式提供访问。  配置统方数据库行为审计模块，实时获取操作系统内存段的获取方式。 |
| 部署管理 | 防统方系统不需要改变现有应用程序和数据库的设计，无需改变应用程序代码，无需应用做二次开发，编写接口等，对医院现有系统无影响 |
| ▲同时支持旁路镜像部署模式和探针部署模式；（提供产品功能截图） |
| ▲在探针模式下，通过探针将数据库的所有操作传送到防统方设备；探针支持自动推送安装，且支持探针性能的限制，防止对数据库性能产生影响。（提供产品功能截图） |
| 可支持防统方系统集中化管理功能，基于Web的管理方式和SQL管理接口，B/S架构模式。 |
| 审计对象范围 | ▲全面支持Oracle、SQL Server、MySQL、DB2、DM、Hive、Informix、Sybase、PostgreSQL、MariaDB、KingBase、GBase、hbase、优炫（UXDB）、HANA、cache、神通、greenplum、GaussDB（高斯）、tibero、MongoDB等数据库。以满足未来信息化发展需要（提供产品功能截图） |
| ▲支持从网络流量中自动发现数据库信息，并添加到防统方平台；支持自动扫描IP地址段，发现数据库信息，并可添加到平台。（提供产品功能截图） |
| 事件处理能力 | 内置大数据搜索引擎，支持模糊检索，亿级数据检索速度在秒级别实现。 |
| 统方审计功能 | 实现SQL语句的细粒度审计，并记录详细的用户行为信息，包括该语句执行的时间、机器名、用户名、IP地址、交换机端口、MAC地址、客户端程序名以及SQL语句、执行结果、执行时长、返回行数、结果集等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控。 |
| ▲支持通过数据库绑定变量方式的防统方审计能力。（提供产品功能截图） |
| ▲支持按数据库进行白名单、黑名单审计策略配置，按客户端IP、应用程序、数据库用户配置黑白名单，过滤审计流量，可降低探针网络带宽压力，减小审计存储压力。（提供产品功能截图） |
| ▲内置丰富的风险引擎特征库，对于SQL注入攻击、数据库漏洞攻击进行精准识别并智能告警。（提供产品功能截图） |
| 实现数据库登录操作的审计，并记录详细的成功登录行为和失败登录行为信息，能够识别暴力破解等非法登录行为。 |
| 支持应用系统三层架构审计，可以精确的识别操作人，可以精确的识别来自于B/S架构的浏览器终端信息；能精确识别到操作人和应用程序账户，可以精确定位到人。 |
| ▲支持Oralce、MySQL数据库本地审计；支持客户端SSH隧道代理访问数据库审计；支持本地命令行访问数据库审计。（提供产品功能截图） |
| ▲对于疑似威胁的操作记录，能够基于会话进行追踪溯源，根据人（用户名、账户）进行追溯，在同一界面展现跟其相关的从登录、访问到退出的全过程（提供产品功能截图）。 |
| ▲SQL语句提供直译和意译的不同翻译引擎，支持英文翻译成中文，统方代号翻译成常规名称，增加易读性，便于纪委等非技术人员理解报警内容（提供产品功能截图）。 |
| 告警策略 | 根据IP地址、机器名、时间、程序名，sql语句等精细组合对统方表操作行为预设警报策略，并能够为特定的审计需求自定义审计警报规则。 |
| 提供多种安全响应措施，包括数据库记录、邮件报警、短信报警、syslog等。通过这些监控和防御措施，对招标方统方信息进行有效的监控、预防和保护。 |
| 模型分析策略：以操作语句为原型，根据获取的审计内容字段、表名称、条件字段、操作频率等条件设定分析策略； |
| 对于首次出现的终端（IP）、人（用户名、账户），进行高级告警。 |
| 安全告警必须支持基于订阅的模式，每个人可以订阅自己的安全告警事件，页面的安全告警事件必须区分开当前30分钟的安全告警事件和过去的安全事件以方便阅读，支持任意组合的规则订阅，实现人员的个性化订阅管理。 |
| 报表管理 | 定期自动生成：日、周、月、年度综合报表； |
| 支持按时间、范围、报表模板自定义生成报表； |
| ▲支持下载法规性报表，如SOX法案、PCI报表、等级保护报表；（提供产品功能截图） |
| 综合报表展现形式具有多样性，如使用表格、柱状图、饼状图、折线图等多种方式进行展现分析； |
| 所有报表都支持下载；文档支持格式：包括WORD\HTML\PDF\EXCEL等； |
| 定期生成的报表可配置邮箱，定时收取最新生成的报表。 |
| 配置管理 | ▲支持事件FTP服务器自动备份功能，备份记录支持恢复到平台。（提供产品功能截图） |
| ▲支持查询结果下载，自定义设置下载字段，下载审计查询的结果。（提供产品功能截图） |
| ▲提供事件审阅和自动审阅，自动审阅的审计信息后续出现将不需要再行审阅；依赖于审计信息的访问规则的单键生成,依赖于审计信息的订阅规则的单键生成；（提供产品功能截图） |
| 产品资质 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 原厂资质要求 | 原厂商具有ISO27001信息安全管理体系认证证书；  具有ISO20000信息技术服务管理体系认证证书；  具有ISO9001：2008质量管理体系认证证书；  具有省级重点企业研究院证书。 |
| 原厂售后服务 | 本项目提供原厂项目管理和售后实施服务，要求项目经理同时具备PMP证书和OCM证书，实施工程师需要同时具备OCP和CISP证书。提供相关证书原件复印件。 |
| 原厂商在宁波本地拥有分公司或服务机构，遇到产品自身问题时，可以提供2小时以内的上门服务。提供营业执照等相关证明材料原件复印件。 |

## 1.3服务团队要求

基本要求

（1）具有丰富的数据库经验

具有强有力的远程支持能力以快速解决问题。具有丰富的数据库运行维护支持经验和性能优化经验，特别对于Oracle RAC具有丰富的运行维护支持经验和性能优化经验。具有丰富的重大故障和灾难性故障处理经验。具有丰富的数据库安全管理经验。

（2）具有丰富的操作系统维护经验

宁波市北仑区滨海新城医院的核心系统架构在LINUX上，服务团队需要具有丰富的主机操作系统知识，更好的保障数据库的稳定运行。

（3）具有密码猜测检测和防御实现的技术能力

数据安全管理是招标方运行维护改善的持续性方向之一，数据安全分析服务可以全面评估安全漏洞、安全威胁、潜在风险，同时还能审计操作行为，降低安全风险。

数据库密码尝试，能轻易导致数据库用户被锁死，业务受到极大影响。在服务周期内，要求服务商提供具备一种运行在Oracle数据库上的密码猜测检测和防御工具，一旦宁波市北仑区滨海新城医院出现类似问题，可以提供相关工具使用，以方便用户快速解决问题。

请仔细描述密码猜测检测工具的基本原理和实现思路。

要求服务团队精通数据安全管理方法和技术，尤其在分权管理和DBA访问控制上，提供有针对性的解决方案，要求提供丰富的安全管理案例。

（4）数据库安全评估能力

数据库与业务系统的接口，是进入数据库的一大门户，黑客常常通过对业务系统的页面分析、攻击尝试，而获得数据库系统的控制权，如SQL数据库代码注如攻击，因此，接口设计必须充分考虑数据库的安全性，接口设计必须具有良好的抗攻击能力，万一业务系统出现问题也不会影响数据库的安全。因此要求投标公司具备数据库安全评估能力，能够在用户需要建设数据库安全时帮助用户梳理并且评估数据库所存在的安全隐患，并且提出合理的安全评估建议。

（5）具有业务系统中间件诊断支持技术能力

业务系统中会遇到各种问题，要求服务团队熟悉招标方业务，针对Oracle数据库遇到的业务类疑难问题和性能问题提供有效支持。

当业务运行在B/S三层架构下，数据库无法识别出终端IP地址或用户信息，无法实现数据库优化、开发和诊断支持，一旦用户出现类似技术问题，要求服务商有能力提供基于TOMCAT、JBOSS等中间件的Oracle数据库终端捕捉，可以在数据库内识别终端的IP地址和用户名等信息。

在故障跟踪或优化服务中，需要定位终端信息，基于Oracle SQL Trace或者10046事件的SQL跟踪，可以正确的运行在TOMCAT、JBOSS等环境下, 清晰识别SQL语句来自于哪个终端。

（6）本项目配备厂家Oracle数据库支撑专家组要求

▲要求配备5人及以上的OCM认证，3名10年以上OCP认证，2人及以上的Oracle ACE Associate称号的技术服务团队，组成宁波市北仑区滨海新城医院Oracle数据库二线支撑专家组，设置宁波市北仑区滨海新城医院的主责工程师以更好的协调宁波市北仑区滨海新城医院维保工作。

▲为宁波市北仑区滨海新城医院指定一名数据库顾问，要求该顾问具备Oracle数据库专家ACE PRO荣誉资质。

（7）主责工程师要求

▲要求主责工程师常驻宁波本地，并且具备OCP认证，要求提供宁波本地分公司证明和本地主责工程师社保证明。

## 1.4其他要求

1）节假日保障服务：在每次国定长假前提供系统健康检查服务，投标人在长假期间提供响应的7\*24小时值班人员及联系电话，根据客户的实际、客观需要，提供假日现场服务。

2）技术支持服务：对于用户单位因本项目涉及设备出现技术上的问题或其他项目涉及本项目设备需要配合时，提供远程电话或现场技术支持服务。第三方服务配合：当用户问题涉及第三方服务商时，承担协调工作。当用户问题需要配合时, 承担配合工作。