国家癌症中心运维平台技术需求

## 1.采购产品一览表

运维平台一套。

## 2.采购需求

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标项要求** |
| 1       | 硬件配置 | 2U机架式（专用硬件平台），冗余交流电源，2\*GE板载管理口，4\*GE板载接口，2×接口板卡插槽。32GB内存，1×4TB硬盘。 |
| 标配30个数据库(ip+port)授权。最高扩展数据库个数50个 |
| 标配50个运维账号数量，最高可扩展至100个 |
| 2U机架式（专用硬件平台），冗余交流电源，2\*GE板载管理口，4\*GE板载接口，2×接口板卡插槽。32GB内存，1×4TB硬盘。 |
| 2       | 协议支持 | 支持国际数据库类型：Oracle、SQL Server、MySQL、PostgreSQL； |
| 支持国产数据库：DM、CirroData、TeleDB、TelePG、GBase 8a；支持HIVE，Impala等 |
| 3       | 密码代填 | 基于系统内运维自然人身份关联数据库账号，使每一个运维人员都具有专属的运维账号密码，实现数据库账号及密码对运维人员保密的前提下开展数据库运维和管理工作。且不需要进行软件安装部署。支持批量录入数据库账号。数据库账号可按组织机构关联；支持批量创建数据库账号与运维人员对应关系。 |
| 4       | 运维申请审批 | 支持运维人员提交运维申请，选择对应审批人，并根据操作时间指定执行时间段。 |
| 支持运维人员按实际操作的语句行为提交运维申请，包括访问来源（IP、数据库用户、客户端工具），可对全部对象或指定对象进行SQL操作行为申请。 |
| 支持运维人员以完整SQL语句形式提交运维操作申请；在提交语句申请时，可选择一次申请单条或多条语句。 |
| 支持多级审批账户对提交的运维申请动作进行审批； |
| 5       | 运维流程审计 | 支持对运维人员的申请类型、申请内容、申请时间、审批人、审批状态进行查看。支持审批人快捷查看所有待审批申请。支持将申请审批信息与执行语句进行关联分析。 |
| 6       | 防护能力 | 支持两种防护模式：会话阻断：支持依照策略配置对存在风险的会话进行阻断；拦截语句：支持依照策略配置对会话中的风险语句进行拦截，但不影响会话原有的连接状态。支持通过数据库名称、数据库实例、Schema、表名、字段名、函数等关联信息解析和设置防护规则；内置默认规则，支持场景：高危操作、权限变更、批量数据泄露或篡改、撞库、无where更新或删除、SQL注入、系统表非法操作、错误码提示等。"支持进行敏感访问操作行为防护：定义非法访问：通过客户端IP、数据库用户、客户端工具、客户端MAC、OS用户、主机名、时间等；管控高危操作、权限变更行为：通过全部对象或指定对象的ALTER TABLE、DROP TABLE、TRUNCATE等高危操作行为拦截；防止大量数据修改、删除、泄露：通过精细化管控受影响数据行数(阀值)，超出阀值的行为进行阻断；拦截no where引起的整表更新、整表清空的误操作；支持数据库攻击行为防护：支持口令攻击防护，可基于频次判断失败登录风险；支持SQL注入、XSS跨站攻击等外部行为防护。支持数据库漏洞攻击防护：提供针对利用已公开的数据库漏洞攻击行为进行拦截的虚拟补丁功能；漏洞分类应涵盖：缓冲区溢出、权限提升、拒绝服务攻击等，至少提供450个以上虚拟补丁；漏洞补丁规则管理维度，包括：漏洞名称、CVE标识、CNNVD标识、漏洞类型和影响范围。支持防护白名单，信任特定行为或语句，可以设置为放行审计，也可以设置放行不审计。支持为单防护规则设置白名单，白名单可设置内容与防护规则所属类型可配置项相同。支持针对SQL语句配置防护规则。支持通过“SQL语句关键字”“SQL语句模板关键字”等条件控制，防止敏感操作执行。支持返回错误码、响应时间控制。支持结果集内容作为规则判定的条件，结果集包含敏感数据，则直接拦截或阻断。 |
|   |
|  |
| 7       | 敏感数据识别 | 内置针对符合特征的敏感数据发现规则，规则包括：身份证、通用证件号、银行卡号、电话号码（手机、座机）、中文姓名、中文地址、企业名称、日期、税号、Email地址、统一社会信用代码、证券号、海关编号等。支持发现任务的创建，针对指定的数据库进行敏感数据的自动发现，并对任务进行管理。支持对发现敏感数据的匹配率调整，在满足一定比例条件下即可识别为敏感数据。支持将资产梳理结果导入到敏感字段梳理中，实现敏感数据联动发现；支持自定义发现敏感数据规则，包括正则、数据字典、复合匹配等方式。对核实完成的敏感数据类型，可一键新建敏感规则或加入到原有敏感数据脱敏，并根据敏感数据类型自动匹配最优的脱敏算法。支持对数据库驱动进行管理，在敏感发现任务中使用自定义的驱动进行连接并执行发现任务。 |
| 8       | 数据脱敏功能 | 支持SQL改写和结果集脱敏两种方式进行动态脱敏包括：随机替换：使用随机产生的相同含义的数据替换原有的敏感数据；数据遮蔽：将原数据中部分或全部内容，用“\*”或“#”等字符进行替换，遮盖部分或全部原文。"支持遮蔽算法自定义，包括遮蔽起始位置、遮蔽长度、替换字符可自定义； |
| 9       | 风险分析 | 系统具有语句模板抽象能力，能够将语句结构相同但参数不同的语句，抽象为语句模板，并能够根据语句模板配置语句的黑白名单规则，进行拦截和阻断。支持按风险语句模板统计具体某一种风险模板语句产生次数、最后执行时间、以及所命中规则。支持风险统计：统计全局和单库的风险命中情况；支持风险源分析：基于客户端IP、数据库用户、工具分析风险来源。 |
| 10     | 告警与外送 | 支持规则命中后的风险告警；风险告警内容支持触发规则风险内容，并支持根据风险等级进行告警通知。支持告警与规则和数据库关联，实现不同规则、数据库的告警发送给不同收件人，方便进行风险的排查。告警方式包括：邮件、短信平台、SYSLOG、SNMP、企业微信、钉钉群助手、防护系统前台界面；支持SYSLOG方式进行数据外送，可外送审计数据、会话信息、新型语句模板、系统审计日志；支持自定义编辑外送模板。 |
| 11 | 报表 | 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式。支持各类报表展现，针对风险、性能、访问源、账户等信息做专项报表展现。支持按日、周、月等时间周期生成综合报表；支持将报表按指定的时间推送至指定管理员的邮箱。报表支持以Word、PDF、HTML、CSV等格式保存到本地。 |
| 12    | 产品资质 | 主流国产数据库的官方兼容性证明，如Kingbase、达梦、OceanBase、南大通用等； 国产操作系统官方兼容性证明。 |

## 3.服务要求

软硬件三年维保服务；三年5\*8小时线上技术支持；三年不定期线下技术支持。