附件3

日志分析管理系统扩容

需求及技术要求

一、技术标准和要求

（一）项目概况及要求

根据我社生产运维工作对日志数据的管理应用需求以及监管部门对日志数据的审计存储要求。我社与上海七牛信息技术有限公司采购日志分析管理系统（软件产品为：七牛云机器数据分析平台软件[简称：Pandora]）10TB/天日志数据处理能力产品容量授权（含系统标配的软件产品、定制化开发、现场实施等服务）。目前，日志分析管理系统已完成核心系统、黔农云网络金融服务平台、贷款核算系统等15套重要交易类业务系统日志统一采集、查询、管理、备份、审计、分析和告警等日志应用能力建设，系统总体运行状况良好。

为进一步提高我社信息系统运维能力，提升应用系统运行保障水平，有效防范系统运行风险，切实保障业务连续性，实现对业务系统、基础软硬件产品的日志分析、监控与统一备份，我社拟扩容日志分析管理系统，该系统建设目标是实现日志统一收集管理，日志的安全审计、基于日志进行分析、监控和告警，日志异常数据通过API对外供数已满足我社后续智能运维平台建设要求。

本次日志采集管理扩容范围包含：114套业务系统日志；1500余台网络和安全设备日志；4200余套操作系统、1000余台主机及100余台存储设备运行日志；400余套数据库运行日志；1000余套中间件运行日志及部分系统冗余规划。

需满足行内每天30TB的日志吞吐量以及该产品的部署架构必须考虑到跨数据中心的应用场景并保证高可用性。

（二）建设内容

1.收集并细化我社日志分析管理系统的扩容建设需求，包括但不限于制定存量业务系统的日志管理规范和对接、基础软硬件产品运行日志的管理规范和对接、日志系统存储规划和性能优化、日志分析统计、日志模式识别、日志告警、基于日志数据的系统运行报表等，并结合省农信实际环境，分析与评估建设重点及难点。

2.完成我社日志分析管理系统扩容规划设计和实施方案，包括但不限于概要设计、详细设计等，提供本次招标所需的软件产品安装介质和授权文件，提供软硬件资源需求，配合我社将系统安装部署完成，同时自测功能通过。

3.中标方事前需充分评估实施风险,实施监控纳管后不能影响现有业务正常运行。中标方需根据招标方工作计划并结合各技术条线实际情况分步骤、分时间段或业务停机窗口对日志进行分批采集纳管,计划实施时间为12个月,期间中标方需派人进行现场实施,采集纳管操作完成后实施人员需至少现场对资产运行情况进行一周时间观察。

4、对接行内CMDB、统一告警平台、一体化智能运维平台等运维系统接口，使日志分析管理系统融入行内运维体系。

二、功能需求

4.1一般性需求

（1）投标方必须提供符合要求的成熟软件产品。投标方提供的所有产品必须具有在中华人民共和国境内的正式合法使用权。

（2）投标方必须承诺保证提供的所有软件产品为在中华人民共和国境内销售的正式版本；具有很好的开放性和扩展性，支持主流的技术标准和规范；支持主流的操作系统和硬件平台。

（3）投标方必须保证任何功能模块的维护和更新都不影响软件的其他模块，软件升级具备容错能力。

（4）投标方必须承诺保证不同时期的日志分析管理系统版本应能向下兼容，软件版本易于升级，且在升级的过程中不影响集群节点的使用，保证运维工作的连续性。

（5）投标方必须承诺及时提供最新稳定版本的日志分析管理系统软件，且该软件是经过测试正式推出的，其可靠性、稳定性是经过严格验证的。

（6）投标方应必须承诺日志分析管理系统软件升级时免费更新软件版本，并提供相应的新版本软件功能中文说明及操作运维说明手册。

（7）投标方必须承诺保证提供的所有软件产品都具有完整的技术资料和介质。

（8）投标方必须承诺提供的日志分析管理系统软件为当前软件产品的最新稳定版本。

4.2功能性需求

日志分析管理系统应至少包括，但不限于如下功能：

4.2.1数据采集功能

（1）支持linux、windows、AIX、中间件、数据库、业务应用、容器docker、kafka、prometheus日志采集。

（2）采集方式支持kafka/mq消息队列， syslog上传，文件目录监听，snmptrap接收，snmpget接收，脚本上传，web上传，数据库采集，对接flume数据源，对接hdfs数据源，对接redis数据源，数据源，对接netflow数据源，对接Docker数据源，对接logstash数据源，beats上传，压缩文件采集，systemd-journald日志上传，对接H3Csessionflow数据源，对接MongoDB数据源。

（3）支持通配符匹配文件采集路径，递归采集子目录下白名单日志文件。

（4）支持正则表达式模式对多行日志合并处理。

（5）日志采集agent需支持传输限流功能, 避免对生产环境服务器的网络带宽造成影响。

（6）agent配置支持全web界面管理，包括黑白名单,字符集, 最后修改时间等配置通过这些配置,可对日志采集过程进行细粒度的控制。

（7）agent采集配置参数支持批量agent下发。。

4.2.2日志解析功能

（1）平台应内置各种设备的字段解析模版，对于新遇到的日志样例，可以通过划选辅助功能自动生成正则表达式，降低维护人员数据清洗难度。

（2）支持正则表达式，kv/xml/json自动解析，数值转化，url解码，user agent解析，时间戳识别，字段分拆，syslog pri解析，geo地理位置信息解析，固定电话归属地解析，手机号归属地解析，字段脱敏配置，内容替换，新增扩展字段，自定义字典，时间生成，事件统计，流式统计等常用解析组件，解析规则可以嵌套使用。

（3）支持通过智能辅助划选字段自动生成正则表达式。

（4）内置IP解析库,如将IP地址解析为地理位置(省市)的IP地址库, 手机号码和固定电话归属地解析等。

（5）通过自定义字典对查询字段进行翻译，如将错误码或者业务码翻译成更容易理解的语句描述。

4.2.3数据检索功能

（1）支持全文检索、短语(多个词中间空格)搜索、字段过滤、逻辑运算搜索、数值范围搜索、通配符搜索、简单正则表达式，命中结果高亮显示。

（2）支持搜索结果保存成定时任务。

（3）支持提前设置不同日志数据集别名，在搜索界面点击别名自动搜索需要的日志，如中间件日志数据集设置包含nginx、apache、tomcat等，不需手动编写写查询条件。

（4）支持随时终止运行中的搜索任务，支持对搜索结果下载（txt，csv或json格式）。

4.2.4数据分析功能

（1）支持管道符、产生新增字段、分组查询、子查询、联合查询、字段挑选、条件过滤、结果排序、数据量过滤、字段重命名、分桶查询、统计查询、移动标准差、移动均值、时序预测、去重、行列转换、自动回归、动态提取，json提取，序列映射，多值拆分，多值归并，时序图，制造结果，输入映射，输出映射，事件排序。

（2）能够求和、最大值、最小值、平均值、最新的值等数学计算。

（3）支持数据库式的join操作实现多个日志的关联。

（4）支持搜索时日志关联行内自定义字典数据进行关联分析。

（5）搜索可调用脚本获取脚本执行结果数据，并对数据结果进行二次分析。

4.2.5可视化展示功能

（1）能支持常规饼图、条带图、折线图、区域图、柱状图、散点图、单值图、区线图、和弦图、迷你图、桑基图、玫瑰图、力引导图、和弦图、循序图、旭日图、雷达图、漏斗图、矩阵热力图、调用链表格等任意形态进行数据可视化等展示方式。

（2）能实现多个不同维度类型指标如交易量、耗时在同一时间轴的多Y轴趋势图对比展示。

（3）能自定义组合图表形成仪表盘，可自定义仪表盘过滤项，过滤项支持与特定图表绑定。

4.2.6定制报表功能

（1）搜索结果、统计数据能组成各种图表，可自定义展示图表布局。

（2）报表支持富文本，为了方便用户在报表内添加个性化说明内容，报表支持可自定义字体、字号、颜色、标题设置，支持在输入的文本内嵌入图表。

（3）报表支持以PDF、XLSX、HTML等格式发送或下载，支持报表定时发送。

4.2.7监控告警功能

（1）支持对事件数、字段值、动态基线、复杂告警。

（2）支持告警抑制功能，触发告警之后固定时间段内（或者倍增式时间段抑制）不再发送告警，以免产生告警风暴。

（3）支持告警按高、中、低不同优先级配置，分等级推送。

（4）支持邮件、短信、http转发等多种告警方式，支持脚本自定义告警发送方式，与行内告警平台接口集成。

4.2.8知识库功能

（1）为将遇到的错误日志以及解决方案积累成排障经验，需提供知识库功能，通过引导式流程添加知识。

（2）运维人员搜索到报错信息时，能点击关联对应知识库解决方案。

4.2.9平台自监控管理功能

（1）为提升平台的稳定性，即使发现平台异常，需要对平台自身各模块的性能进行监控，包括但不限于CPU、内存、队列、IO等并能发送邮件告警。

（2）平台各模块的日志可以通Web界面进行查询，无须登录后台服务器进行故障排查。

4.2.10敏感信息脱敏功能

（1）日志包含身份证号码、手机号码、邮箱、地址敏感信息，通过正则表达式匹配日志中的敏感信息，对查询结果自动进行脱敏处理，有效防止敏感信息泄漏。

（2）同一条日志，有敏感数据查看权限的用户，能查看敏感信息原文，没有敏感数据查看权限的用户，查看结果为脱敏后的数据，同时脱敏的部分内容如手机号都能正常搜索使用。

4.2.11平台权限管理功能

（1）支持赋予角色不同数据、功能、资源权限。

（2）管理员账户可查看全部日志数据，部门经理账户能查看本部门全部日志数据，部门普通账户只能查看个人管理日志数据。

（3）管理员账户可查看、编辑、删除所有账户，部门经理账户能查看、编辑、删除本部门账户，并修改角色权限，部门普通账户只能查看自己账户，不能修改自身角色权限。

（4）管理员账户可查看、编辑、删除全部采集代理，部门经理账户能查看、编辑、删除本部门全部采集代理，部门普通账户只能查看本部门全部采集代理。

（5）管理员账户可查看、编辑、删除全部资源，部门经理账户能查看、编辑、删除本部门全部资源，部门普通账户只能查看本部门全部资源，资源包括仪表盘、监控告警、报表等所有内容。

4.2.12平台安全性功能

（1）可配置密码锁定时间、密码有效时间、密码长度，禁止使用过去几次用过的重复密码，忘记密码可通过管理员重置，保障平台登录安全。

（2）长时间跨度搜索会占用较多资源,为防止某用户误操作把集群资源耗。光，要求能控制最大搜索时长

4.2.13日志生命周期管理功能

（1）agent侧日志备份功能，日志可以无需入库，能通过agent将原始日志文件压缩后备份到分布式存储平台，备份完成后自动删除原始日志文件

（2）数据索引路由功能，对业务日志、主机日志、数据库等日志在线保存时长要求不同，可以设置不同保存时间和占用存储空间上限，例如业务日志保存360天、数据库日志保存180天，主机日志保存180天，不同日志类型的存储周期要求需和招标方共同确定配置。

4.2.14日志报文上下文聚合分析功能

（1）多行日志合并功能，多行顺序打印日志能按要求将多行日志合并成一条日志。

（2）多线程交叉打印日志，在搜索时可通过线程号、起始标识对多行日志进行自动聚合分析, 可展现以时间顺序一笔交易从头到尾的所有日志, 并进行进一步的统计分析。

（3）自动聚合计算量大，需要通过定时任务将聚合后的日志写入独立的日志索引，索引可直接用于二次搜索分析，提升查询分析效率。

4.2.15内置日志经验模板功能

（1）平台需内置丰富的日志处理模板，覆盖常见主机、中间件、数据库、网络安全设备日志类型，除行内自行开发应用外的设备日志，能实现自动字段提取、分析报表视图、监控告警。

（2）模板支持以资源包方式上传下载，自研业务日志分析模板可以下载后，在生产、测试等多环境快速复用。

4.2.16告警合并功能

（1）为减少告警重复发送，支持对告警进行抑制，触发告警之后固定时间段内不再发送告警信息。

（2）实现告警的合并。

三、总体要求

本次日志分析管理系统建设项目中标方需严格按照招标方要求如期完成以下工作：

（一）项目规划及实施

1、负责编制实施方案；

2、负责统筹项目实施；

3、负责项目调优，配合安全合规性检查及整改。

（二）工作规范要求

中标方在开展测试服务工作期间，须严格遵守以下工作规范要求：

1、遵守国家法律和政府的有关条例、规定和办法，以及招标方相关管理规定开展工作；

2、执行有关项目建设的法律、法规、规范、标准和制度，履行测试服务规定的义务和职责；

3、中标方在签署技术协议时，须同步签订《安全协议》及《保密承诺书》并严格履行协议和承诺书条款。不泄漏所测试系统各方认为需要保密的事项。

（三）项目管理

1、负责项目统筹及管理；

2、负责各类文档收集、整理，协助甲方完成归档；

3、负责项目相关培训；

4、负责项目维保服务。

（四）项目交付及验收

1、中标方必须在合同规定时间内，完成本项目的实施。将招标范围内所界定的工作完成。在通过试运行验收后，中标方需将所有项目成果交付给招标方。

2、项目交付物包括但不限于《系统概要设计说明书》、《系统详细设计说明书》、《系统数据库设计说明书》、《实施方案及配置手册》、《运维手册》、《培训手册》、《常见问题及应对措施-应急预案》等文件。

四、项目建设要求

1、本项目所涉及的产品技术服务须由原产品厂商专家技术团队完成。其中方案设计、系统部署调试等重要工作须由产品厂商总体负责，需全程参与方案设计工作，负责项目管理工作，如系统部署、项目归档、验收等工作。项目的具体实施方式由招标方根据项目建设需要动态调整。

2、原产品厂商项目服务团队及人员资质能力要求

项目总负责人：本科以上学历，具备6年及以上日志运维系统项目建设及管理经验。

拟派实施工程师：具有3年及以上日志运维系统建设实施经验，且近3年参与3个以上金融行业日志运维系统建设项目实施。

3、中标方须做好严格的项目管理流程，做好项目的跟踪和管理，并提供招标方认可的高质量的项目管理文档等。

4、中标方的项目成员须根据招标方的计划安排全职参与项目的建设，在建设过程中，若中标方项目组成员未能达到招标方要求，招标方有权要求中标方更换项目人员，由此造成的项目延误由中标方承担责任；通过招标方认可的中标方项目人员，未经与招标方协商同意，中标方不得随意裁撤。

5、参与实施的中标方及原产品厂商项目组成员，须严格遵守保密承诺，为招标方的IT基础架构及信息数据保密，避免外泄任何招标人数据资产。

五、交付及验收要求

1、根据招标方日志分析管理系统项目建设安排限时完成系统安装、调试、系统适配、采集纳管等工作；

2、项目交付物包括但不限于项目实施计划、人员安排、设计方案、实施方案、详细配置、相关制度、操作手册、运维手册、培训文档、资产清单等文件。

3、中标方事前需充分评估实施风险,实施日志采集纳管后不能影响现有业务正常运行。

4、中标方提供的软件产品需满足行内每天30TB的日志吞吐量。

六、售后服务要求

中标方须提供原产品厂商一年维保服务，维保时间自《货物安装运行验收报告（二阶段）》签署之日起计算，为保证设备的可靠性服务，要求提供原厂针对本项目的授权原件及售后服务承诺书原件，并在维保期内提供规范化、高质量的维保服务，需提供以下售后服务：

1．驻场维保服务支持。为确保项目建设质量和推广效果，中标人应提供至少原产品厂商1人年的驻场维保服务。协助招标方处理和优化日志分析管理系统在扩容和推广过程中需要解决的业务、流程和技术问题。增强现场问题收集、沟通和处置的时效性。

2．定期维护技术支持：每年进行至少两次例行巡检，出具巡检报告并加盖公章，对巡检过程中出现的问题，中标人需配合整改优化；

3.技术服务支持：当集群架构有所调整时原产品厂商需提供技术服务支持。必要时，原厂技术工程师须提前1天内到达现场，配合招标人做好规划实施；

4.重保服务支持：遇国家重大节假日、双十一、重要业务时点、系统迁移期间等，中标人需向招标人提供重保方案，并提供7\*24小时的响应处理支持，若需要，中标人需派遣工程师到现场进行技术支持；

5.升级服务：在原厂商提供升级与更新服务基础上，中标人还需免费提供系统版本更新、系统缺陷修复、必要的补丁更新等技术支持服务；

6.快速响应服务：系统出现故障不能正常工作时，招标人通过电话、邮件等方式通知后，中标人需在30分钟内通过远程诊断解决问题，如果通过电话、远程协助等方式无法使系统恢复正常，需在4小时内安排原厂技术工程师到现场进行故障定位及处置；

7.系统运行事故维护：维保系统出现故障导致单节点或整个集群故障时，具备快速重新搭建系统的能力，重新搭建时间需保证在一小时之内，如因系统版本缺陷问题导致，需及时提供系统补丁包，有必要时需提供其他稳定版本部署。

8.技术培训服务：为了更好的保障招标人系统安全稳定运行，维保服务期内中标人需定期安排高级技术专家进行技术支持及培训交流工作。

9.扩容服务：未来如因业务发展需求，招标方需要进行扩容采购时，应按照不高于本次报价的明细价格进行采购。