# 附件3：

# 网络与信息中心攻击溯源审计系统

**配置要求：**

**1、数据接入**

具备基于HTTP、FTP接口的数据接入功能，单节点的接入性能可达1GB/s；

支持多种加载方式，包括HTTP协议加载、文件加载；

支持灵活通用的数据格式描述，包括CSV/AVRO，用户可按照统一数据描述规范进行数据组织；

支持多种字段类型，包含整形、字符型、浮点型等；

集群不存在单点故障，数据支持双副本或三副本存储；

提供了基于HTTPS的安全数据接入功能；

数据从输入到订阅者能够订阅到时延不高于5秒；

在万兆网络的环境下，单台客户端支持的数据加载速度不低于100MB/s，可以线性扩展。

**2、数据存储**

提供HDFS分布式文件系统。提供KV存储能力，支持按主键更新、字段扩展等功能， 支持Parquet，RcFile等常见存储格式；

支持对支持数据的压缩，支持snappy，gzip等常见压缩算法。 支持Parquet，RcFile等常见存储格式；

数据支持3副本存储，副本支持不在同一列机架存储。支持对本地文件系统的管理，支持lucene文件存储；

支持在线和离线两级的分级存储，可根据用户需求，设置数据的迁移策略，并自动迁移；

对于RcFile、Parquet文件，单节点的数据接收速度不低于60MB/s；对于lucene文件，单节点的数据接收速度不低于20MB/s，可以线性扩展；

对于RcFile、Parquet文件，压缩率不低于60%；

数据存储管理集群规模可达200台以上，单表数据规模可达万亿规模，条件检索性能为秒级响应。

**3、数据查询**

统一的对外接口，系统对外提供统一的接入接口，支持命令行、交互式shell、ODBC、JDBC等数据访问方式，为上层应用程序提供多种选择；

支持扩展SQL接口，可以将全文检索作为SQL的一种过滤条件，接口满足数据中心接口标准。支持中、英、德、法等多语言的智能分词，支持常见分词器，如IKAnalyzer。支持分词器的扩展，提供对URL数据的分词器；

支持整型、字符型、时间类型、文本类型、IPV4、IPV6等多种数据类型；

提供索引机制，如hash索引、位图索引等，对不同类型的数据提供定制的加速检索技术；

索引构建效率：集群单数据节点不小于20MB/S；

对10亿条数据，5个关键词以下的各类检索，返回前100条结果秒级响应；

支持用户并发数不少于50；

支持的最大数据规模万亿级；

查询效率：基本条件精确检索的响应时间为秒级；

单节点条件过滤类、聚合类等实时计算操作性能可达到400MB/s以上，性能可通过增加节点而近线性提升；

支持基于SQL的全文检索功能，支持条件组合、模糊检索、词距检索、相关度检索等多种检索功能。

**4、数据分析**

日处理日志容量大于2.5T

支持标准SQL接口，支持JDBC，ODBC驱动；

对于10亿级进行计数统计，完成时间小于60秒。对于10亿级数据进行分组排序，完成时间分钟级；

对于10亿级数据进行分组排序，完成时间分钟级；

百万条记录表与百亿条记录表等值关联查询分钟级完成；

批量导出数据，万兆网环境下，单节点速度大于100MB/秒；

对于10亿级数据的同源分析，完成时间分钟级；

支持跨数据中心查询业务，数据中心元数据变化同步秒级；支持数据中心个数不小于100个； 支持的用户并发数不少于10；

输入输出需要支持常见的字符集，包括UTF和GBK等。支持英文、中文、维语、藏语等少数民族语言内容的存储和查询；

须和主流品牌产品如：防火墙、路由器等进行日志数据对接。

对全网的sesion及flow信息进行存储，对全网dns，url等关键信息进行存储并进行溯源，归一化查询及多维度的计算。

**服务要求：**

1. 技术培训：提供原厂研发级培训（培训地点为产品研发中心）（提供原厂承诺原件）
2. 提供3年原厂服务质保、须根据用户网络条件的改变完成定制开发，如不符合承诺，将追究中标方责任；
3. 提供3年免费软件版本升级，免费更新版本中新增加功能，包含大版本及小版本。（提供原厂承诺原件）；
4. 产品巡检服务：通过上门服务等方式了解产品运行情况，一年不少于4次，提供最新的产品信息给客户并指导客户正确使用产品（提供原厂承诺原件）；
5. 安全通告服务:安全通告服务，及时提供符合客户实际情况的安全信息，包括最新的安全事件和相应的处理意见；服务期内不限次数（提供原厂承诺原件）；
6. 厂商在中标后一周内提供投标系统，并进行所承诺的所有功能测试，提供测试报告，如不满足功能要求，将不授予合同，一切后果由厂商承担。