ALEIYE

让 | 大 | 数 | 据 | 更 | 简 | 单

ALEIYE 证券大数据解决方案

北京数介科技有限公司

目 录

1. 证券业务现状与挑战

证券行业的网络与业务信息系统建设已经十分复杂，各类相关的日志信息分散在 IT 架构的各个位置，如何有效的对这些日志进行统一的监控审计成为了一大难题。与此同时，网络中的各种网络设备、安全设备、主机、应用和业务系统在工作中都产生了大量的安全事件和日志，却没有统一的进行管理，使得各个系统之间缺乏协同，整体安全无法得到保障。

对于证券公司而言，解决审计问题成为当前紧迫的形势。证券行业一个很重要的特点就是网络与业务连续性第一，系统日志量大，日志审计系统要尽可能地降低对现有网络与业务系统运作的影响。

1) 众多系统之间相互独立存在，无法进行协同关联：证券行业常见网络基础设施的日志采集，例如Cisco的网络设备、防火墙、IBM IDS入侵防御系统、F5负载均衡设备，以及网上交易系统如同花顺、通达信和手机炒股软件的留痕日志；

2) 各系统异常检测排查耗时费力，无法快速定位：对于证券行业客户而言，设备多、每小时产生的日志量巨大，如果性能跟不上，就无法实现日志的有效采集，后续分析和审计就失去了意义，内控的目标也就无法达成；

3) 现有网络与业务系统的影响性：包括日志采集的网络带宽占用情况，对被审计设备和系统的CPU、内存占用的情况和系统稳定性的影响；

4) 证券系统访问行为审计困难，无法跟踪交易用户行为；

5) 证券移动端应用的业务分析、用户分析无法开展；

2. 传统解决方案的局限性

传统的证券行业解决方案通常都会包括 IT 运维、网络安全、数据审计业务数据分析等内容，虽然能应对证券企业的大部分需要，但仍有些不足之处。

- IT 运维

1) 传统的网管软件有较好的采集能力，可采集粒度最小 5 分钟，实时性不强。对各设备告警信息。但误报率高；
2) 设备类型多，监管系统同样也多，管理不便；
3) 出现设备故障现象，需逐一排查，耗时费力。

- 网络安全

1) 针对不同设备会有不同安全设备，如防火墙 IPS、IDS、WAF 等，安全事件独立存放。

- 数据审计

1) 人工将各业务系统、网络日志数据导出，手动统一格式，提取关键业务数据信息；
2) 耗时费力：需要花费几天，甚至两、三周时间，动用几乎员工全体。

- 业务数据分析

1) 呼叫中心、网络交易系统等各系统都有独立的客户管理；
2) 当想查看客户全面画像时，需要将所有系统结合展示。

可见，传统的解决方案已经无法满足证券业务的实际需求。为了更好的满足不同岗位的业务分析要求，为了提高 IT 综合运维能力，证券企业急需一套具备强大数据处理能力和针对性的高效、完整、可行解决方案。

3. Aleiye 大数据平台解决方案

对大数据进行挖掘与分析，一是要能够廉价处理海量的数据，例如一次性可处理 100GB 甚至更高的数据量;二是要能够敏捷处理非结构化的海量数据，例如可以从海量的客户电话投诉记录中挖掘出有价值的营销机会点。

(一) 可扩展的开放架构

大数据量必然要求金融企业 IT 基础设施更易于数据的整合与集中、扩展与伸缩，以及管理与维护，同时还必须具备良好的可靠性、可控性、安全性。在稳定性、可用性及服务性也足以胜任海量数据对基础架构能力的要求，因此，具备高扩展性的开放架构正逐步成为金融行业应对大数据的优选方案。

1) 海量数据存储：Aleiye 大数据平台采用了分布式文件系统、分布式存储、高性能的索引机制，保障银行数据存储性能以及可靠性的要求。
2) 可弹性扩展系统：面对银行数据规模和复杂度持续增加，Aleiye 实现了存储系统的高可扩展性，支持随时硬件扩展。
3) 分布式数据索引：将全部索引数据水平切分后存储到多个节点上。这样可解决单个节点无法存储庞大的索引数据和单个节点构建索引的效率瓶颈。

（二）多源异构数据标准化

大数据可提供一个海量数据统一存储处理平台，通过多样的采集方式将多个数据来源汇总到一起，再利用强大的预处理技术将异构数据整合划一，为接下来的数据分析作好准备。

1) 通过数据采集器、协议采集等方式完成多数据源、多类型的数据实时汇总，解决不同系统下的数据相互关联的前提。

2) Aleiye预处理功能可以解决数据重复、无标签等问题，可以按用户要求在数据存储前完成提前处理使数据在Aleiye处理效率大大提高。

（三）智能化数据审计

大数据解决思路是将同源异构数据按照审计的标准变为了同构数据。将不同厂家的系统访问日志预处理，按照证监会要求提取所需信息完成审计智能化。

1) 按审计要求自动提取业务字段，快速完成业务报表与审计报表，并提供下载功能。

2) Aleiye数据引擎提供数据实时检索，可以按数据逻辑、条件检索，如在不同时间范围内按不同用户ID或用户操作类型过滤出相关事件。

（四）高可用的移动应用分析

移动统计基于 Aleiye 大数据平台，并结合移动应用实现的业务分析应用，支持 Android 和 IOS 两个平台，通过五大分析模块帮助移动用户进行统计和分析流量、应用版本、用户访问路径和地域分布等指标，从而帮助开发商通过数据进行产品的运营、推广等策略的决策。

1) 分析证券移动应用运营情况，按应用版本等指标对数据进行分析。

2) 精准定位，更了解用户。精准定位访问地址及路径，通过用户的行为特征，帮客户更加了解用户。