ALEIYE

让 | 大 | 数 | 据 | 更 | 简 | 单

银行大数据解决方案

北京数介科技有限公司

目　录

地址：北京市西城区新街口外大街 28 号普天德胜科技园 A 座 405　电话：010-82053991　|　让大数据更简单

1. 银行业务现状与挑战

随着银行业务不断发展，各种各样业务系统以及支撑运行的 IT 架构变得越来越多。目前银行业务主要出现的问题和挑战包括以下几点。

(一)运维内容庞杂，管理难度大

目前中型银行的系统有几百个应用，几千台 IT 设备；其中网络设备又包括核心交换机、接入交换机、路由器等几十个。当某个设备出现故障时，各系统之间无法进行协调配合。运维人员由于缺乏全面的业务知识，排查故障往往需要先弄清网络路径，再进行逐一排查，导致故障处理周期长，效率低下，无法满足监管机构、银行客户的效率需求。存在问题如下：

1) 各运维管理工具相互独立，无法快速进行信息关联；
2) 处理问题时以人工解决为主，处理效率低，并且员工素质影响工作质量；
3) 运维以治为主，被动接受，无法更好地优化 IT 架构并且资源浪费。

(二)安全分析综合性差

银行行业在保护客户银行信息、满足内部要求和法规要求的严峻挑战。安全员工需要将安全工作做到以监测为主，事后做好分析工作。存在问题如下：

1) 无法实时查看系统健康情况；
2) 难于对恶意网络攻击源进行定位分析；
3) 难于对高风险设备进行评级分析。

(三)应对监管与合规要求成本高

银监会的监管和合规要求对银行提出了更高、更精细化的要求。由于银行审计部门通常情况下员工较少，并且工作范围较大，快速响应审计、合规对员工提出更高的要求。存在问题如下：

1) 无法快速准确的将审计所需关键业务数据整理出来，如业务系统访问日志、操作系统日志、AD 日志等；

2) 无法将数据快速导入并归档，提供给审计监管部门。

（四）业务数据关联分析复杂

银行企业都希望能充分利用各业务系统中的业务数据，进行相互关联、交叉关联，完成对业务线的完整分析以及客户全生命周期管理。但由于各种业务系统相互独立存在，数据结构大相径庭，实现客户推荐、多维度指标分析需要耗时非常大的人力和时间成本：

1) 无法定制用户画像，分析客户喜好；
2) 行为风险分析没有完整的、多维度的数据报告。

2. 传统解决方案的局限性

传统的业务解决方案一般包括，IT 运维、网络安全、数据审计业务数据分析等环节。这里对每个环节进行分析。

- 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。

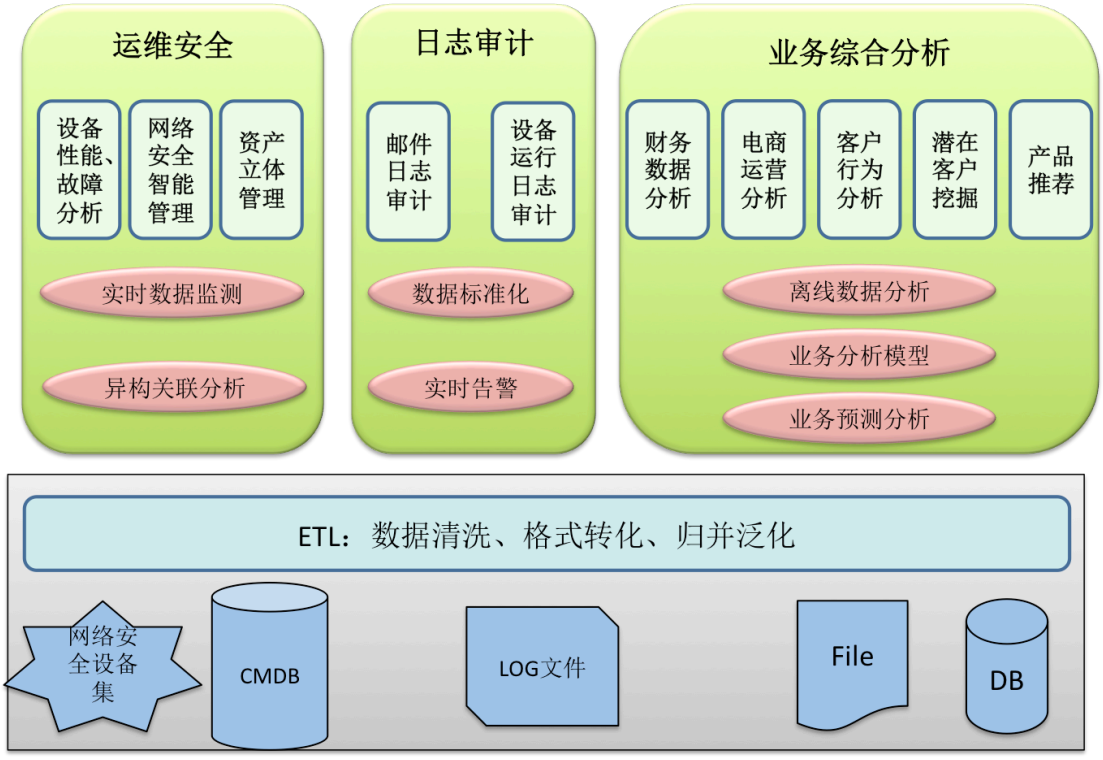
- 业务数据分析

1) 呼叫中心、网银系统、信贷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银行业务的实际需求。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，银行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

Aleiye 大数据平台解决方案具有大数据处理引擎、银行安全应用系统，为银行目前存在的问题能够较好地解决，不仅为运维安全人员、业务分析人员提供实时、综合的数据分析，并且对决策人员提供综合型的多维度报表。



（一）可扩展的开放数据处理平台

大数据量必然要求银行企业 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银行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 大数据平台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，为银行审计提供数据结果。

1) 数据采集：在整个企业架构各系统中设备种类、数量众多，每天产生大量的日志，且分散在各地网络与信息系统中。 Aleiye 大数据平台支持采集器、FTP 协议传输、文件上传、syslog、snmp、snmp trap、数据库接入等多种数据采集方式。
2) 数据预处理：面对海量不同源、不同结构的数据，Aleiye 大数据平台提供过滤、补全、合并、标记、关联等数据处理方式，对数据进行统一格式转换。

(三) 综合企业运维安全

1) 安全分析：对各层安全设备的入侵检测、入侵防护、应用防护、恶意行为防护日志进行实时检测和关联分析，并以可视化的形式展现。
2) 线路质量监控：线路质量量化统计和实时、关联性分析。实时对各条线路的使用情况根据总次数、运营商、外联单位等不同维度进行量化统计，从而评判该运营商的服务质量，关联分析外联单位所受的影响。
3) 负载分析及预测：实时监控各条线路的流量和流量占比等指标；根据流量数据建模进行流量预测。制定合理的流量使用区间，对超载情况

实时告警。

4) 系统健康分析：通过对系统中各台设备的性能、流量、安全事件等指标进行单点以及关联分析，以可视化的形式实时展现系统的健康状况。

5) 设备故障定位及关联分析：通过对该设备的性能、流量、漏洞等指标进行单点分析以及关联分析，进而对故障快速定位。

(四)挖掘隐藏价值进行业务创新

Aleiye 大数据平台通过高效的大数据分析挖掘能力，可以很好地支持服务创新，并通过对对客户访问、客户操作、客户信息的分析，实现了客户全方位分析。并且通过对客户消费行为模式进行分析(比如事件关联性分析)，提高客户转化率，开发出不同的产品以满足不同客户的市场需求，实现差异化竞争。

1) 分析挖掘：基于 Aleiye 大数据平台强大的数据整合和分析能力，可将企业不同类型的设备日志、不同业务系统的数据以及不同地域的数据通过分类、聚类、交叉关联等算法进行多维度数据分析。

Aleiye 大数据平台可以直接解决业务非结构化数据无法有效利用的问题，通过构筑新一代动态数据中心，使银行依托大数据处理分析技术的建立成智能银行。因为，项目需要一个为异构且多样化的数据提供了存储和分析的平台。为 IT 设备集中监控、提高应急处置、协作能力提供支持，并具备低成本、好的系统扩展性（存储容量无限）、高可靠性、分布式分析等优势。

通过使用 Aleiye 大数据平台，银行企业对资源的利用更加高效，管理手段更加灵活，IT 运维安全更加智能和强壮，为银行企业降低了运维成本，带来了投资收益率的最大化。