THE FORELAND OF
TRADING TECHNOLOGY

内部资料 免费交流
《准印证》编号沪（K）0671

交易技术前沿

2022年 第四期 总第51期

本期主题

交易系统

No.4

内部资料 2022 年第四期（总第 51 期）
准印证号：沪（K）0671

NO.4

主管：上海证券交易所
主办：上海证券交易所
总编：邱勇、蔡建春
副总编：王泊
执行总编：唐忆
责任编辑：徐广斌、徐丹、陆伟、王昕、黄淦

上海市杨高南路 388 号
邮编：200127
电话：021-68607129，021-68607131
传真：021-68813188
投稿邮箱：ftt.editor@sse.com.cn

篇首语

资本市场在现代经济活动的重要作用日益凸显，交易系统作为资本市场运作和发展的直接承载体，对于维护市场安全稳定高效运行发挥着至关重要的作用。开展交易系统核心技术研究，有利于行业机构改良自身技术、降低运行风险，亦有利于促进我国资本市场国际竞争力和影响力的提升。本期《交易技术前沿》以“交易系统”为主题，收录行业交易系统研究及前沿技术探索等方面的优秀文章，其中。

《异构交易系统介绍》展现了中金所自主研发异构交易平台的系统架构和技术亮点，该平台借鉴了航空航天业在软件可靠性上的最佳实践，旨在降低交易系统故障率、提高容灾容错性。

《可复用数据处理框架在证券数据处理中的探索和实践》在主流的数据处理框架基础上，开发了批处理系统的处理框架和元数据管理模式，在提高数据维护质量的同时降低数据血缘关系维护难度。目前该开发模式已运用在创新业务和交易系统的实际研发中。

《海通证券兼容多基础平台的新一代核心交易系统运营管理平台设计与实现》采用全面自主可控的链路技术，实现智能路由识别、统一路由管理，在保证平台兼容性的前提下，有效提升核心交易系统运营管理效率并降低运营管理成本。

《机构交易接入中台建设实践》聚焦于屏蔽核心交易系统差异性的自主可控交易接入中台，为各类交易终端接入 OST 极速交易系统、第三方快速交易系统等打下基础。

《基于证通云的数据跨境流动管理方案的研究与实现》旨在通过综合运用数据加密、权限控制、操作留痕等技术手段，在现有政策环境下，提出一种基于“证通云”的数据跨境流动管理解决方案。

《交易技术前沿》编辑部

2023 年 3 月 23 日

目录 Contents

本期热点

探索与应用

信息资讯采撷

本期热点

1 异构交易系统介绍
2 海通证券兼容多基础平台的新一代核心交易系统运营管理平台设计与实现
3 机构交易接入中台建设实践
4 可复用数据处理框架在证券数据处理中的探索和实践
5 基于 oneAPI 的金融衍生品定价加速

异构交易系统介绍

应国力、仇沂、李雯、王维 / 上海金融期货信息技术有限公司 交易系统部 上海 200127
E-mail：yinggl@cffex.com.cn

近年来，在全球经济复苏疲软叠加疫情冲击的背景下，全球交易所核心系统稳定性面临较大考验，软件故障频发。针对软件缺陷类故障无有效应对方式的现状，中国金融期货交易所（以下简称为“中金所”）自主设计研发打造了异构交易系统，该系统是一套软件架构与主交易相异的容错备系统，通过多版本容错技术、维护多个异构交易系统来降低服务的整体故障率，在主交易系统发生严重软件缺陷、且已有的应急保障措施均失效的情况下，可尝试快速接管，持续为市场提供基本的交易及行情服务。

1、关键技术问题

如何提升软件可靠性：软件可靠性是软件质量体系中最重要的衡量指标之一，根据软件可靠性理论，缺陷是无法完全穷举罗列的，无法完全避免。中金所已具备完备的硬件故障恢复体系，应对软件故障也有较丰富的应对手段，如图 1 所示，但面对其他软件逻辑缺陷或架构级别严重缺

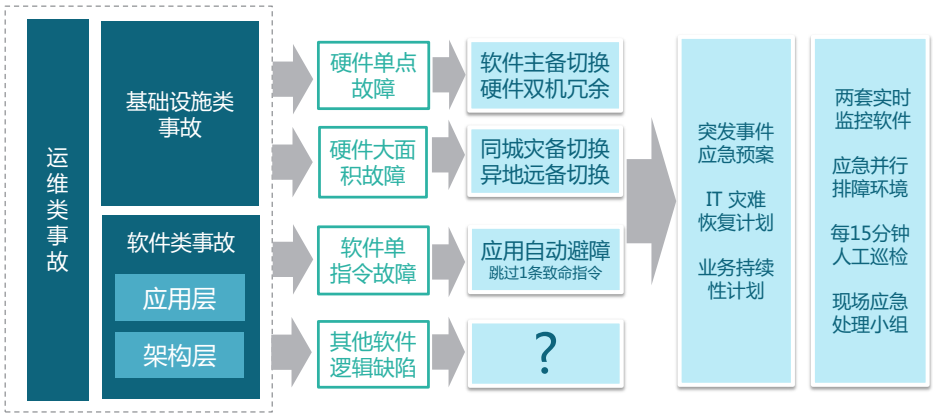

图 1：核心系统事故应急方案

陷类故障仍缺乏解决方案。

极简架构下的高性能：交易核心系统对性能容量有着极致的要求。建设一套全新的系统需要较大资源投入，一是研发阶段的成本投入，需要实现所有线上业务功能；二是运维阶段的成本投入，需要同时维护两套线上系统。因此，在资源极简的前提下，如何实现高性能目标也是难点之一。

切换影响最小化：当主系统发生软件故障切换到异构交易系统时，需要尽可能降低内外部影响。一方面是切换效率要高，对市场无影响，会员端需要做到无感切换；另一方面是对交易所内部上下游系统无影响，需要做到切换后周边各业务系统持续平稳运行。

数据一致性：异构系统与主系统架构不一致，存在业务不一致的风险，如何保证异构系统接管后仍能正确运行不出错，也是关键之一。

“卡脖子”问题仍需攻关：面对严峻多变的国际形势，提升交易所技术的安全自主可控性更是迫在眉睫。打造核心技术的安全自主可控体系、探索交易所核心系统在自主可控环境落地，才能在面对不同局势时从容不迫。

2、异构交易系统架构介绍

异构交易系统内部异构于主交易系统，采用了以高性能通信组件为连接件、多级交易流水线为中心、内置查询业务和行情生成的架构，外部复用了主系统前置和外围系统。异构交易系统总体架构如图 2 所示。

高性能通信组件是中金所在多年来交易系统研发的基础上，对底层开发框架及通用功能组件进行分离封装，形成的一套功能丰富的开发框架。开发框架由 C++ 实现，包含了事件处理框架、高性能通信、可靠多播、高级容错组件等。

多级流水线模型是异构交易系统的消息处理架构，异构于主交易的业务单线程处理，后续章节中将详细介绍。

内置查询业务和行情生成是考虑到查询模块和行情生成模块的轻量性及其与交易行为的耦合，将这两个模块纳入异构交易系统核心进程中，可降低异构系统运维的复杂度。

复用主交易前置和外围接口模块可以保证在切换时省去反演恢复数据的时间，提高切换效率，并且可维持切换后对外服务地址不变，降低切换

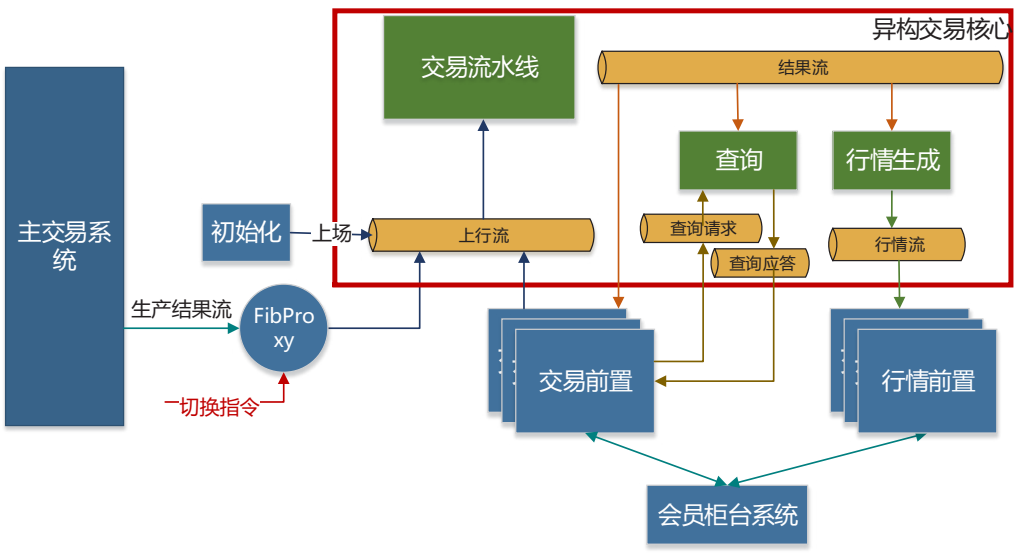

图 2：异构交易系统架构

对会员端及交易所内部上下游系统的影响。

从运行方式与数据流向上来看，异构交易系统日常作备并行运行，实时订阅主系统撮合结果流水，实时恢复最小完整状态集。当主交易系统出现故障切换至异构交易系统时，开始订阅外部前置及上场消息继续进行交易业务。

3、系统关键技术

3.1 运行模式及流水复制恢复技术

异构交易系统支持两种运行模式：撮合模式和恢复模式。运行模式属于架构层的概念，它决定了系统的订阅关系、流持久化逻辑等。详细介绍如下：

撮合模式：异构交易系统做主系统运行，从上场模块进行初始化，从交易前置接收外部指令（如报单、报价等）。业务层进行撮合操作，撮合结果直接写入结果流。此模式下与主系统运行模式无异，当主系统故障切换至异构系统时，异构系统以此模式运行。

恢复模式：异构交易系统作为备系统运行，此时作为主系统的并行系统，将订阅主中心发来的全量流。此模式下应用了流水复制恢复技术，只处理结果消息，用来复制主中心的撮合结果，恢复构建对应业务域状态、内存表以及相关变量的状态，如资金占用、仓位统计、活跃订单簿等，保证异构一致性。收到切换指令后，异构交易系统会切换为主中心，发生订阅关系和业务层操作模式的变化：取消订阅主中心结果流，转向订阅上场模块消息，开始接收前置的外部消息，业务层操作由流水复制恢复切换为撮合。线上运行默认为此模式。

3.2 基于聚合根的多层领域模型

通过抽取基于交易参与者 + 合约的最细粒度数据聚合根，将不同业务域数据按层级进行挂载，实现数据访问的简化和高效率，对原主交易系统的业务模型进行了完全的重构，通过异构避免严重故障，提升了软件可靠性。

全新的领域服务校验模型内部通过业务功能、领域模型、内存数据三层进行划分，配合数据聚合根，业务逻辑不再关心数据存取访问，模型抽象程度更高。同时，领域服务不依赖外部系统、不保存状态，所以更容易进行单元测试，这对于提高系统的质量是非常有帮助的。

3.3 高性能多级流水线模型

异构交易系统的消息传递采用多级流水线模型，将业务数据处理流程在逻辑上划分成相互独立的若干部分，每个部分由一个线程驱动，线程之间共享消息队列。

从总体业务模型的角度上来看，如图 3 所示，相比于主交易系统的订阅 -> 单线程撮合 -> 发布的结构，异构交易系统将撮合线程按延时占比拆分为撮合前、撮合、撮合后三部分异步处理消息。

在同一测试环境进行测试，多级流水线性能提升显著，具体如表 1 所示。引入撮合流水线后，系统吞吐能力显著提升。由于架构上进行了本地持久化的原因，延时略微增加，但仍在合理范围以内。

从技术模型实现来看，异构交易系统的业务处理部分由四个线程驱动，分别为订阅消息加工

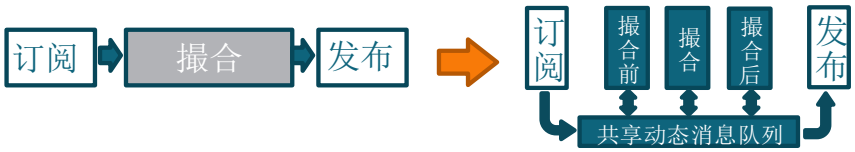

图 3：交易系统多级流水线业务模型

表 1：异构交易性能比对表

系统	处理延时	吞吐能力
主交易系统	98us	7.1 万笔/秒
异构交易系统	110us	16.5 万笔/秒

线程、撮合前检查线程、撮合及撮合后处理线程、发布消息处理线程，与图 4 中线程一一对应。其中，订阅消息加工线程将异构交易上行的消息包进行解包，生成消息队列的包头以及流水线的第零级消息，消息队列包头是多个线程访问消息队列的关键，控制着线程对同一个消息的读写权限，第零级消息通常是上行数据包的原始数据，也就是输入的请求包；撮合前检查线程消费消息队列包头和第零级流水线的消息，同时生成第一级流水线的消息；撮合及撮合后处理线程消费消息队列包头和第零、一级流水线的消息，同时生成第二级流水线的消息；发布消息处理线程消费消息队列包头和第零、一、二级流水线的消息，并将消息打包，提供给其他模块消费。消息队列保存了每一级流水生成的消息，并维护了消息之间的对应关系。

其中，动态消息队列是为了适配多级流水线模型而设计的组件，它的生产消费模式与多级流水线模型是紧耦合的。对于消息队列而言，订阅消息加工线程是生产者，发布消息处理线程是消费者，撮合前检查线程和撮合及撮合后处理线程既是生产者又是消费者。

在动态消息队列中，消息头的结构至关重要，对于一个原始请求消息及其在各级流水线中生成的衍生消息，消息头记录了流水线的处理结果和上一级处理该消息的流水线序号，各级流水线通过消息头判断消息是否可读。动态消息队列内部实现大致如图 5 所示。

3.4 架构极简及业务极简

在技术架构方面，异构交易系统主要用于应急场景，因此在架构上剥离了分布式容错撮合集群，仅保留订单、行情关键路径模块，构成最小完整状态集，使得架构层代码减少 20%。

在业务架构方面，基于全新的抽象程度更高、基于聚合根的领域服务业务模型，剥离了非必须业务，仅保留交易业务最小集，去除了为扩展性预留的以及未开启的业务功能，在确保业务延续性的同时，保证了业务应用层的简化，精简了核心计算逻辑。以不同的实现方式重构之后，实现了相同的业务功能，业务代码行数减少 55%，减少了开发成本。

在模块架构方面，对比主交易系统，考虑到查询模块和行情生成模块的轻量性及其与交易行

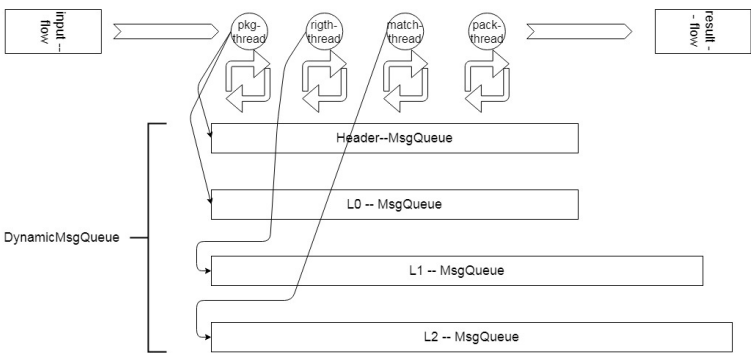

图 4：异构交易系统多级流水线运行架构

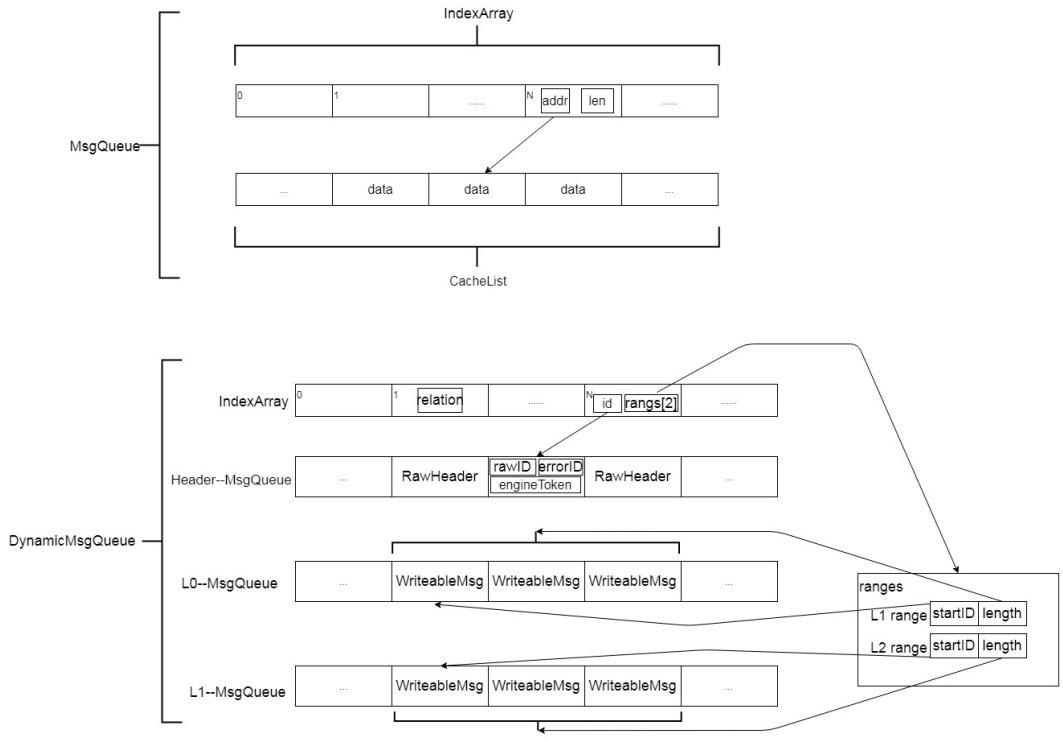

图 5：动态消息队列实现结构

为的耦合，将这两个模块纳入异构交易系统核心进程中。除了复用的主交易前置及外围模块，异构交易系统仅有一个进程，保证了异构交易系统的轻量级和灵活性。

3.5 运维视图及故障根因分析系统

为了实现故障的快速发现和定位，在开发异构交易系统的同时，交付了一套基于大数据、集成了运维视图及故障根因分析系统的智能运维平台，实时跟踪主交易系统及异构交易系统运行状态。

根因分析系统融合了 Logging+Tracing+Metrics 的监控设计理念，定义了异构交易系统健康运行五大黄金指标：通讯量、错误率、资源饱和度、进程状态、同步数据落差，通过数十个监控子指标监控系统运行状况，运用 Splunk 搭建了运维指标视图，所有指标均支持分钟粒度告警和回溯，实现了事前监控、事中定位、事后回溯的全时段功能。

指标监控报错监测到故障时，可通过根因自动分析系统（图 6）查看故障根因，也可通过日志全链路追踪，进行主系统的故障发现及定位，大幅减少根因定位时间，快速为切换异构交易系统决策提供辅助依据。同时，智能运维平台也支持一键切换，切换至异构交易系统后同样可持续监控异构系统作为主系统运行时的各项指标。

智能运维平台针对日常运维和特殊排障场景提供了全面的运维方案和体系，减少了异构交易系统的运维成本。

3.6 平滑切换

接口一致性：异构交易系统在设计开发中维持对外 API 及对内上下游系统接口不变，使得切换时会员端系统、所内上下游系统可持续平稳运行。在故障切换时，对外会员无需任何操作，做到会员端无感知。对内支持断点续传，保证了数据一致性与完整性。在业务层面保证了平滑切换，切换后的所支持的业务也维持不变。

业务一致性：异构交易系统以备模式运行时，

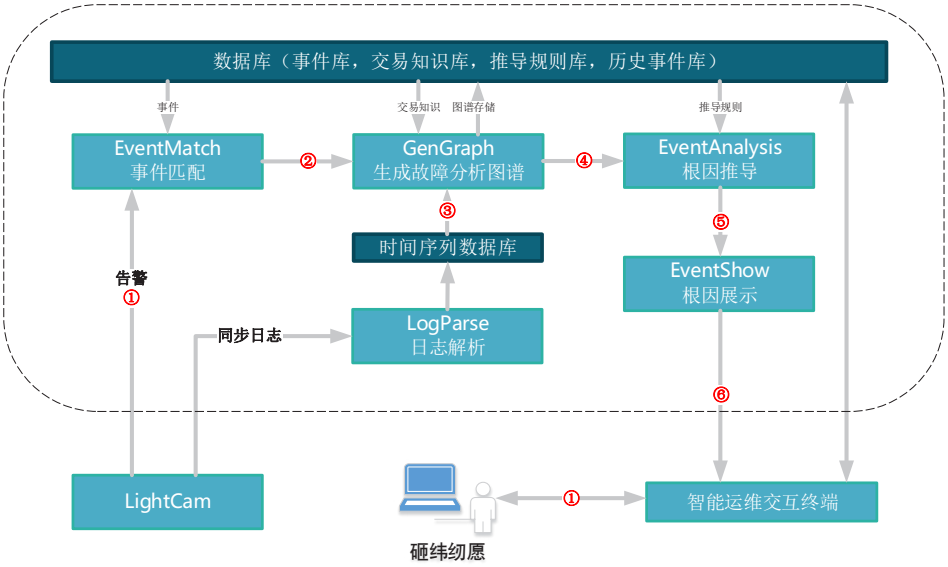

图 6：根因自动分析系统

实时接收来自主系统的数据，并将数据进行重构，使得异构交易系统的数据及状态与主系统保持一致。以主模式运行时，为了保证重构结果的一致性，通过近年的交易流水反演比对和同步一致性比对，验证了异构交易系统在主模式下与主系统业务功能结果完全一致。业务一致性保证了切换后异构交易系统可平滑接管业务。

为了保证异构交易系统与主交易系统的业务、行情的一致性，采用了两套同步一致性比对方案：

一是实时接收主交易系统和异构交易系统恢复模式下的撮合结果及行情流水，进行交易结果数据、行情发布数据的业务比对稽核，确保在恢复模式下主系统与异构系统的数据一致性；

二是在并行环境上部署了一套以撮合模式运行的异构交易系统，实时接收主中心的请求消息并进行撮合，将撮合及行情结果与主中心进行比对。此系统仅用作撮合模式的结果比对，验证异构系统撮合模式的正确性，不参与应急切换。

极速切换：异构交易系统复用主交易的交易前置和行情前置，切换后核心与前置均无需进行反演就可直接进行交易，除去停止主交易核心进程和决策的时间，可以做到秒级切换，最大程度保证业务连续性。

3.7 国产化自主可控

异构交易系统在设计阶段充分考虑跨平台运行需求，在组件开发阶段严格在自主可控环境进行测试验证，确保自主可控环境的可用性。在基于 X86_64 架构、浪潮服务器、麒麟操作系统、海光 CPU 的自主可控环境上，异构交易系统的各项功能平稳运行、延时及吞吐的性能指标达标，并在自主可控环境成功上线，平稳运行至今。

在功能方面，异构交易系统在自主可控环境上累计执行回归测试用例 14 余万条，并通过了近两年的生产流水反演比对测试；在性能方面，对环境特性及参数进行了分析和调优，使得性能提升了 8%，异构交易系统在自主可控环境中的报单吞吐量为 9 万笔 / 秒，报单延时约为 150 微秒。

4、系统建设成效

提高交易所业务连续性保障能力。交易系统是交易所核心竞争力的重要体现，是金融市场中

最为核心的交易基础设施。异构交易系统上线后，可提高核心系统的整体可用性。在主系统可用性为 99.999% 的情况下，主系统每年的宕机时间为 36 秒以下，而加入了异构交易系统后，在异构系统本身可用性为 99%、异构率为 50% 的情况下，根据计算，整体系统每年的宕机时间将下降为 18 秒，且随着异构率的上升，宕机时间还将继续减少。异构交易系统的上线，有效提高了交易所的业务连续性保障能力，降低了技术故障对市场的冲击，在保障金融市场安全稳定运行方面起到重要作用。

探索实践下一代核心系统。异构交易系统作为具备主交易系统完备业务功能的异构系统和下一代交易系统的原型，在简化了部分可靠性保障机制的情况下，比照全面建设一套新系统再上线的时间周期，异构交易系统在上线周期上大约可缩短 60%。其在生产环境上的运行，绝大部分时间在作备的场景下运行，既能作为主系统软件故障时的应急补充，又能使其经历生产环境真实场景的考验逐步迭代完善，大大降低了下一代系统验证的成本。此外，异构交易系统中投入使用的更先进的框架、组件、模型等不但可作为下一代核心系统的技术底座，还可以在其他项目组中被复用，也可为公司节省下一定软件研发费用，并缩短研发周期。

核心系统自主可控环境落地。异构交易系统在设计阶段充分考虑跨平台运行需求，在开发阶段严格在自主可控环境进行测试验证，确保系统在自主可控环境的可用性。在基于国产海光服务器、麒麟操作系统的自主可控环境，异构交易系统运行平稳、各项功能正常、延时及吞吐等性能指标达标。异构交易系统在自主可控环境的成功落地，实现了软件层硬件层双异构，提升了核心系统在基础设施层的自主可控性。

5、总结与展望

本文对异构交易系统的技术难点、架构、关键技术分别进行了介绍和阐述。异构交易系统在大规模数据量、极低时延要求的应用场景下，可实时接替主系统提供全量交易服务，大幅提升核心系统的可靠性，降低由于软件故障导致系统性风险发生的可能性。同时在自主可控环境中，维持内部延时基本不变的前提下，相比非自主可控环境撮合吞吐仍可提升 135%。

目前，异构交易系统已在生产环境顺利上线，成功主备并行运行至今。同时，在测试演练方面，先后组织了多次自主可控生产环境的会员切换演练，在会员接入的情况下，成功从非自主可控主核心系统切换至自主可控异构交易系统，业务持续平稳运行。

未来随着中国金融市场的发展，各家交易所的系统复杂性必然会不断上升，外部环境也趋更加变幻莫测，“交易不断，数据不乱”的目标仍会是重中之重，如何在软件层面建立完备的容错机制就显得更加重要。异构交易系统将结合各家交易所先进经验，持续探索优化，为金融市场稳定运行作出贡献。

海通证券兼容多基础平台的新一代核心交易系统运营管理平台设计与实现

霍轶伦、周尤珠、陆颂华、王东、袁康 / 海通证券股份有限公司
E-mail：hyl13866@haitong.com

随着客户数量的增加，业务功能的完善，以及多节点的扩展需求，海通证券新一代核心交易系统运营管理平台的统一路由模式应运而生。海通证券新一代核心交易系统的运营管理平台链路技术创新，全面自主可控，适配多种基础平台及中间件。其采用了智能路由识别、统一路由管理机制，并支持全节点汇总数据查询，具有高可扩展性、安全性、灵活性的特征。

1、引言

在证券行业快速发展、金融科技广泛应用的背景下，分布式系统逐渐成为了证券行业核心交易业务的发展趋势，全球许多证券交易所和投行机构都在使用分布式的平台和架构用以提高交易系统的处理能力，降低交易系统响应时间。海通证券新一代核心交易系统拥有上海和深圳两个交易中心，多个分布式交易节点，因此其对于使用一套运营管理平台运营维护多个分布式交易节点也提出了更高的技术要求。此外，全面自主可控的链路技术也是保障数据安全与网络安全的关键。在这种情形下，海通证券新一代核心交易系统急需一个统一的运营管理平台，实现用一套运营管理平台统一路由分发，进行全节点客户交易与运营管理，并对多个交易节点数据汇总查询的功能。有效提升运营管理效率、降低运营管理成本，满足统一平台运营管理多节点的市场需求。并需要开发适配各种创新可控的应用服务器与中间件，兼容多种创新浏览器及版本，高度保障网

络安全、数据安全。

2、多技术平台兼容适配

目前证券公司交易系统的核心部件大多依赖于外部供应厂商，自主选择余地较小。同时关键领域的自主可控能力已经逐渐发展为行业可持续发展的核心竞争力。海通证券的新一代核心交易系统研发出一套自主可控、应用技术创新的核心交易系统运营管理平台并成功投产运行。

2.1 采用海通统一研发平台

海通证券新一代核心交易系统的统一运营管理平台采用海通证券统一的研发管理平台技术，在开源框架 GUNSV6.0 的基础上开发集成，并整合了海通管理类框架的技术优势。其基于主流的前后端开发技术 Vue+SpringBoot，并拥有丰富的 UI 组件体系。研发平台提供统一的技术标准与脚手架，封装通用技术能力，有效提高研发效率和质量。

新一代核心交易系统的运营管理平台除支持例如微服务框架、安全机制、链路监控、配置中心等核心模块外，还拥有丰富的插件化架构体系，使得在平台建设过程中可以自由组合各模块，实现不同功能的结合与分离，从而更加便捷高效地搭建可扩展的业务系统。整个运营管理平台采用“基座 + 插件”的架构模式，“基座”保证整体框架的稳定性、兼容性、连续性。“插件”用于扩展整体框架的适配性，提高连通性、安全性，用以快速响应客户需求。

整体运营管理平台架构规范、完善，并具有较高的研发效率和研发质量，拥有更高的设计和源码掌控能力。

2.2 兼容多个应用技术创新平台

海通证券新一代核心交易系统的统一运营管理平台采用 B/S 架构，开放兼容多个应用技术创新平台，并可以灵活进行平台之间的迁移。高度保障网络安全、数据安全，搭建了稳固的自有生态。

如图 2 所示，对于浏览器，其可兼容多种应用技术创新浏览器，如 360 浏览器、奇安信可信浏览器等，并适配支持浏览器的多个版本，保障用户无感迁移使用。对于各种浏览器均能保证页面显示兼容性、插件兼容性与代码兼容性。对于应用中间件、Nginx 及缓存服务，其兼容东方通的 tongWeb、tongRDS，及保兰德的 BES 等。对于数据库，其适配 Oracle、达梦数据库、巨杉数据库等数据独立存储的关系型数据库，也适配 MYSQL、GOLDENDB、TiDB 等分布式数据库。对于操作系统，可适配诸如麒麟操作系统（基于 Hygon 芯片）、欧拉操作系统等面向企业级的通

图 1：运营管理平台技术框架图

图 2：兼容多应用技术创新平台

用服务器架构平台。

3、统一路由应用层设计与实现

随着我国证券交易市场的发展与完善，证券交易业务愈发多样化、复杂化。为提升证券交易这一核心业务的低时延、高可用、高扩展能力，满足不同业务场景需要，海通证券新一代核心交易系统采用了基于开放平台和消息总线的分布式架构，支持各分布式节点灵活部署与水平扩展。海通证券新一代核心交易系统拥有上海和深圳两个交易中心，多个分布式交易节点，其对于统一运营管理也提出了更高的技术要求。因此为了运营维护多个分布式交易节点并支持后续节点高效扩展的需求，海通证券新一代核心交易系统采用了统一路由的策略进行路由识别与转发，实现一个运营管理平台对多个分布式节点的运营管理。

3.1 运营管理平台统一路由功能实现

3.1.1 统一路由链路设计

如图 3 所示，运营管理平台由 WEB 服务、统一路由微服务、公司级企业服务总线有机组成。柜员从浏览器端发起访问请求，各个访问请求通过 Nginx 反向代理发送至运营管理平台的统一路由微服务，并根据系统节点、客户节点及指令节点增加节点信息字段，将此信息发送至公司级企业服务总线，并在此进行路由分发，各节点的数据库变更内容实时采集同步至汇总数据库，用于汇总数据查询。

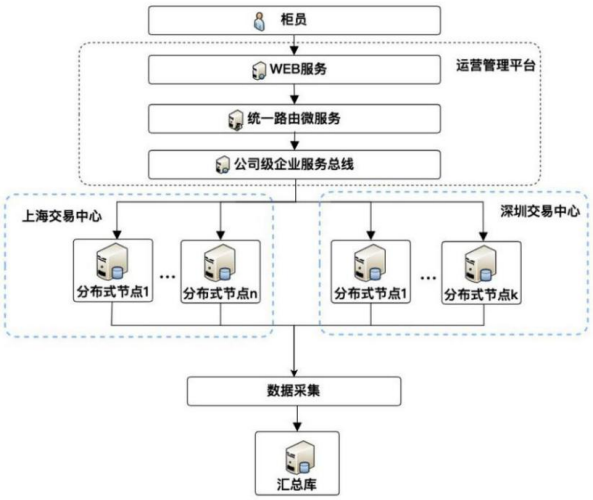

图 3：运营管理平台链路

1）WEB 服务采用 Nginx 反向代理负载均衡

为提高系统并发处理能力，解决系统同一时间段接受到大量客户端请求的问题，采用 Nginx 反向代理模式，将请求信息根据 Nginx 配置的服务器地址随机分发到负载均衡的微服务中进行处理，以保证更快的响应和更好的用户体验。

2）统一路由微服务解析客户端信息

统一路由微服务是解析处理客户端请求并连接公司级企业服务总线的信息转换器，其根据浏览器请求中携带的系统节点、客户节点、指令节点在消息的报头中添加代表节点信息的字段，并

将此信息发送至公司级企业服务总线。

3）公司级企业服务总线分发多个分布式节点

公司级企业服务总线也称 ESB（Enterprise Service Bus），主要负责对于消息进行路由节点分发。根据沪深两个交易中心，ESB 设置了两个安全集成平台（也称 DataPower），并为每一个交易节点配置一个协议转换平台（也称 CpackPower）进行消息分发。DataPower 根据请求中携带的节点信息发至不同的 CpackPower，并将 HTTP 协议转换为加密后的安全协议。

3.1.2 统一路由分发机制

如何正确反映客户端请求与各节点后台组件之间的映射关系从而让请求发送至对应的系统节点是成功实现多节点路由分发的关键，简洁可靠的路由分发机制可以保障运营管理平台的路由安全性与路由准确性。

1）节点信息映射

每一个节点的后台组件都有相应的系统编号，在数据库中存在一个系统路由映射表，其唯一确认并代表着网页端选择的系统节点和后台组件系统编号的映射关系，根据此映射表，可以准确获取前后台节点之间的对应关系。统一路由微服务根据前台界面中选择的节点号在系统路由映射表中获得此请求对应的后台组件节点号，并为此 WEB 前端请求补充了代表后台节点信息的 route 字段。

2）路由分发中心

DataPower 作为公司级企业服务总线的关键组成部分，其也是运营管理平台的节点路由分发中心。节点路由分发中心的各子元素的节点名称为统一路由微服务中的 route 字段值，子元素的值则为对应节点适配器的负载均衡地址，该地址指定请求所发往的后台组件系统，从而进行安全可靠的路由分发。

3.2 统一路由技术亮点

3.2.1 动态扩展路由

新一代核心交易系统的运营管理平台支持在系统路由界面动态扩展系统路由并实时生效，该动态路由策略具备很好的可靠性和灵活性，为系统灵活扩展的需求提供了有效的技术途径。

1）扩展可靠性

支持配置某个节点作为默认的系统路由，当操作人员在界面既不选择操作的节点，也不选择相应的客户号时，则选取此运营管理平台配置的默认节点作为其发送的系统节点，进行请求数据的分发，保证系统的可靠性。

2）配置灵活性

当需要新增或者减少系统节点时，仅需在系统路由界面针对相应的节点配置或删除对应的系统名称、系统编码、企业服务总线地址即可，支持横向扩展配置，没有流量限制，可以任意配置多个节点且能够及时生效，增强系统的灵活扩展性。

3.2.2 路由策略控制

新一代核心交易系统的路由策略主要可分为节点级、客户级、指令级三个控制力度，分级可控。

1）节点级：对于每个系统节点可以在系统路由中进行节点配置，选择是否为运营管理平台的默认系统路由，同时也可以直接选择访问节点，实现节点级别的路由控制。

2）客户级：根据客户号获取客户所属交易节点，自动进行对应节点的请求发送，简化操作人员的操作复杂度，无需进行节点的选择即可自动控制路由配置进行请求的发送。

3）指令级：针对每一个不同的业务和交易，运营管理平台都为其分配有对应的交易编码指令号，对于每一个交易编码系统都支持配置其可发送的路由节点，实现控制每条操作指令对应的系统路由。

3.3 统一路由业务亮点

3.3.1 适配多种统一路由业务场景

新一代核心交易系统运营管理平台的统一路由适配的业务场景主要分为以下几类，涵盖了全

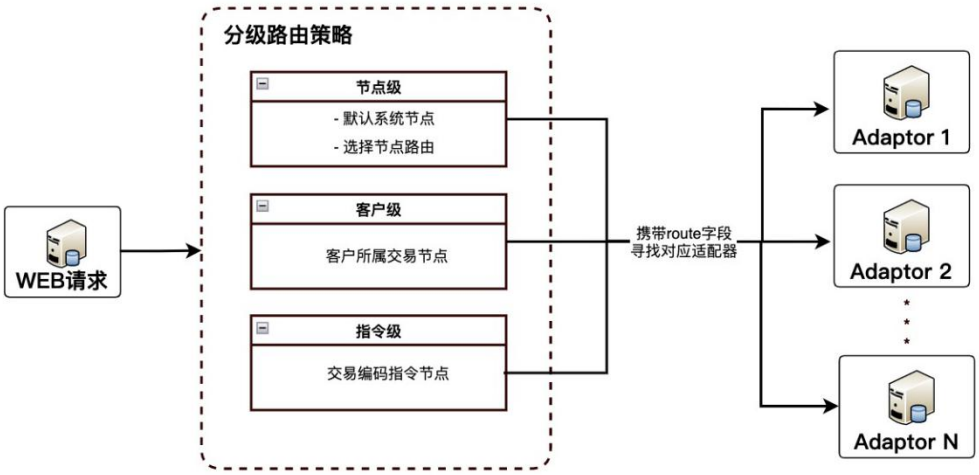

图 4：分级路由策略

部业务人员使用需求：

1）参数设置类：操作人员使用同一客户端即可对于证券基本信息等参数设置业务指定需要同时修改的相应节点，进行一次设置多节点分发的参数设置模式。

2）查询类：查询类路由场景可分为客户类查询和节点类查询。对于客户类查询，即操作人员输入客户号后由系统自动识别客户所在节点，并将查询请求发送至此客户所在节点进行针对此客户的数据查询。节点类查询即操作人员指定系统节点，对于此节点内的全部有权限数据进行查询。

3）交易类：操作人员输入客户号后系统即可自动识别客户所在系统节点，并将此下单信息发送至客户对应节点的后台组件进行交易类功能。

4）清算管理类：运维人员在清算管理全流程中灵活配置，对于多个节点统一管理，并清晰记录操作日志，使得运维人员在一个清算管理模块即可清晰直观地统一维护多节点清算管理步骤。

3.3.2 降低运营管理复杂度，简化运维升级流程

对于运营部门的参数管理岗位人员，其需要对于全部分布式节点中的权限数据、基本信息等参数进行维护。采用统一路由机制的运营管理平台可以使得运营人员仅在一个平台进行设置即可实时同步至多个交易节点后台，提升参数管理维护的效率，及参数维护的安全性、一致性。

对于运维升级人员，原有的一套运营管理平台对应一套分布式交易节点后台的模式需要对于多个运营管理平台进行升级维护，耗时较大，维护成本较高。统一路由的运营管理平台解决了此运维痛点，同时其简化了整个运维升级流程，采用配置中心模式，极大的缩减了运维升级时间，提高了运维升级效率。

4、分布式节点数据汇总

分布式架构逐渐成为证券行业核心交易系统的技术发展必然趋势，随着客户量的增加，业务复杂度的增长，分布式节点也在快速水平扩展。各节点的数据信息分散在各自节点的数据库中，对于需要同时获取多节点信息的场景，在节点路由分发的过程中，考虑到数据请求的全面性、实时性，以及对于多交易节点请求的复杂度，其不再适用各节点分别分发请求并对返回数据汇总的方式。因此如何能够在同一套运营管理平台对于全节点的客户数据、交易信息进行汇总查询是适

应分布式节点扩展的关键。为了解决此问题，海通证券新一代核心交易系统的运营管理平台采用了将各自节点数据实时同步更新至汇总数据库的机制，有效提升汇总查询效率，保障查询的实时性、全面性。

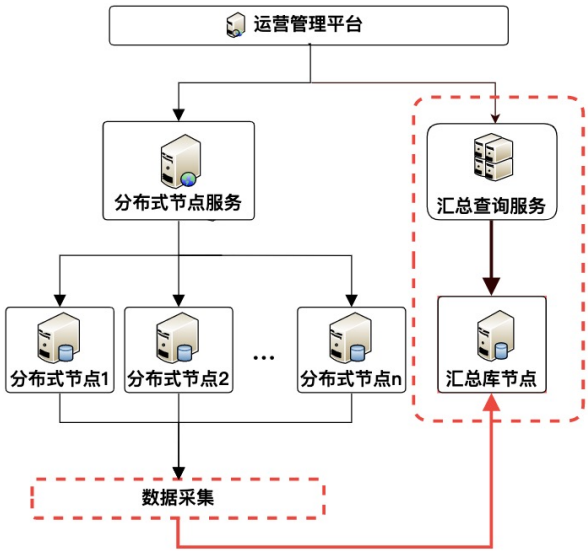

图 5：汇总数据库

4.1 节点备数据库的实时同步

每个分布式节点的数据库都有主备机制，为不影响主库的正常使用，使用备数据库进行数据同步至汇总数据库节点。保证对于生产系统和网络影响最小化，同时在秒级水平进行数据同步，保证数据的实时性和一致性。

汇总数据库不仅支持本地局域网数据同步，还支持跨广域网数据同步。同时其还支持增量同步，数据压缩传输，减少网络带宽。

4.2 视图形式汇总数据

汇总数据库除了包含各个节点备数据库同步过来的节点数据库对象集合，还有一个以各个数据库对象集合汇总构建的视图，根据不同数据表结构和业务含义将不同的表进行去重排序。采用视图的形式使得基表中的数据安全性得以保障，同时可以聚焦于特定的数据集合，增强逻辑数据的独立性。

4.3 汇总数据查询服务、盯市服务

汇总数据查询服务部署于汇总数据库的服务器上，其作为一个特殊节点的后台组件，用以查询汇总库中的数据。对于汇总类公共数据，操作人员选择节点为汇总节点，即可将请求通过统一路由微服务及企业级消息总线发送至汇总节点的汇总数据查询服务，对于此汇总数据库内的全部有权限数据进行查询。

盯市服务作为对于融资融券客户进行维保比例监控的重要组件，其通过数据同步机制将汇总数据库的数据实时同步至服务内的内存数据库中进行实时计算并盯市监控，通过汇总数据库模式，其可同时对于全部分布式节点的客户数据进行汇总监控，更加高效便捷。

5、总结

本文首先介绍了基于分布式架构的海通证券新一代核心交易系统运营管理平台建设的客观背景，随后介绍了应用技术创新、多技术平台兼容机制，统一路由的设计方案与具体实现，及分布式节点数据汇总模式。运营管理平台采用了海通统一的研发平台，并兼容多个应用技术创新平台，整个链路技术创新，全面自主可控，保障数据与网络安全。海通证券新一代核心交易系统采用分布式架构，有效提高交易系统的处理能力，降低交易系统响应时间。为适应多分布式节点的发展需要，运营管理平台采用了统一路由分发模式，其具有节点策略多样性、动态灵活扩展的特点，同时符合业务功能使用的全部场景，降低了系统运营维护成本。分布式节点的数据汇总模式有效提升了系统的实时性、全面性，有效解决了多节点统一查询汇总问题。以上是海通证券兼容多基础平台的新一代核心交易系统运营管理平台建设过程中的实践总结，希望能给业内同行提供一点参考与借鉴。

机构交易接入中台建设实践

胡长春、单兴邦、高春蕾、李沁、黄赛、何少锋 / 东方证券股份有限公司 系统运行总部 上海 200010
E-mail：huchangchun@orientsec.com.cn

随着东方证券机构交易服务的深入发展和东方雨燕极速交易系统的日趋完善，为支持各类机构交易终端以非极速的方式接入到东方雨燕极速交易系统、集中交易系统、新一代业务核心系统、及其他第三方快速交易系统，并支持客户在不同交易系统中切换，以及为构建机构交易生态圈打好基础，需要建设屏蔽核心交易系统差异性的自主可控的机构交易接入中台。本文将重点介绍东方证券机构交易接入中台系统建设方案和实践经验。

1、引言

由东方证券和东证期货联合自主研发的东方雨燕 OST 极速交易系统上线平稳运行，大量对交易速度有极致要求的量化私募、量化策略及做市交易型客户、量化社区客户、银行 / 保险 / 公募 / 期货等持牌机构量化业务客户通过类 CTP 的 API 接口对接进行证券交易，日均交易量百亿规模。随着东方证券机构交易生态圈逐渐完善以及 OST 极速交易系统在量化客户中口碑稳步提升，除极速量化客户外，越来越多高净值客户及活跃交易型客户均希望通过原有机构交易终端在 OST 极速交易系统中进行交易。其次为夯实财富管理业务基石，快速响应公司财富管理业务转型发展需要，提升公司核心业务系统的连续服务能力，保障安全稳定，东方证券开始构建统一技术架构的新一

代核心业务系统逐步替换原有集中交易系统。另外为进一步落实以量化交易为重点的机构经纪业务的定位，为客户提供从策略生成到交易执行、软硬件配置等一系列优化支持服务，在量化交易领域中的保持领先优势，满足特定客户需求可能会进一步引入 FPGA 极速交易系统。

为支持机构交易终端接入 OST 极速交易系统、集中交易系统、新一代核心业务系统、以及可能后续可能引入的 FPGA 极速交易系统等第三方快速交易系统，机构交易接入中台兼容不同交易系统接口协议，为机构交易终端提供统一接入，屏蔽后台复杂性和差异性。机构交易终端对接中台后，客户在不同交易系统切换，机构交易终端系统无需重新对接开发，通过验收测试后即可投入生产，极大提高机构交易终端接入效率。

2、背景

2.1 交易系统

2.1.1 普通交易系统

普通交易系统即集中交易系统为证券公司的核心业务系统，定位于面向所有普通客户进行全部场内和部分场外交易。系统实现的目标是稳定、容量大并支持全业务，技术上主要基于传统的关系型数据库模式，交易延时较高，并发有一定限制。

2.1.2 快速交易系统

快速交易系统目标客户为有快速交易需求的量化客户；系统通常追求高性能、高可靠性、容量可扩展，并支持场内大部分业务；技术上主要采用内存交易技术，部分采用硬件加速机制。为满足客户上海深圳报盘极致速度的要求，通常支持灵活的双节点，在上海和深圳分别部署，支持同一投资者的两个证券账户两地就近报盘。

2.2 客户交易渠道

2.2.1 普通散户

客户通过互联网使用手机 APP、网上交易 PC 终端如同花顺、通达信等接入普通交易系统进行场内和场外交易。客户对交易速度不敏感，由于通过纯手工操作，对百毫秒级别的延迟感知不明显。

2.2.2 极速量化客户

极速量化客户通常托管系统对接快速交易系统进行场内竞价交易。托管系统主要指极速量化客户自建的一套系统，该系统通过 API 对接证券公司快速交易系统，并由证券公司向客户购买后部署在证券公司机房，仅提供给该客户使用。客户对交易速度非常敏感，毫秒级延迟可能影响程序化交易的收益，通常追求微秒级延迟。客户除主要通过托管系统进行交易外，通常还需要一套备用机构交易终端，满足客户除托管系统交易外的全业务交易需求。

2.2.3 机构交易终端客户

机构交易终端客户指通过机构交易终端进行交易的客户，主要包括使用 PB 交易终端，如迅投 PB、恒生 PB 客户、卡方、宇量策略平台，和机构 PC 交易终端，如同花顺机构版、通达信机构版、日内快速交易终端等的客户。机构交易终端客户中的交易型客户通常对交易速度较敏感，通常追求毫秒级延迟，将客户从普通交易系统迁移至快速交易系统，能提升客户交易体验。

3、方案

3.1 总体方案

机构交易接入中台核心需求为提供成熟的、符合竞价交易速度、稳定性、连续性要求的统一入口，承载机构交易统一协议，实现路由控制、负载均衡、安全控制、流量控制、访问控制、运维支持等功能。

中台基于多套交易系统提供的接口协议定义机构交易统一协议，实现 C++、Java、Python 语言的 API 封装机构交易统一协议；基于开源 Netty 开发实现 API 网关支持机构交易终端系统

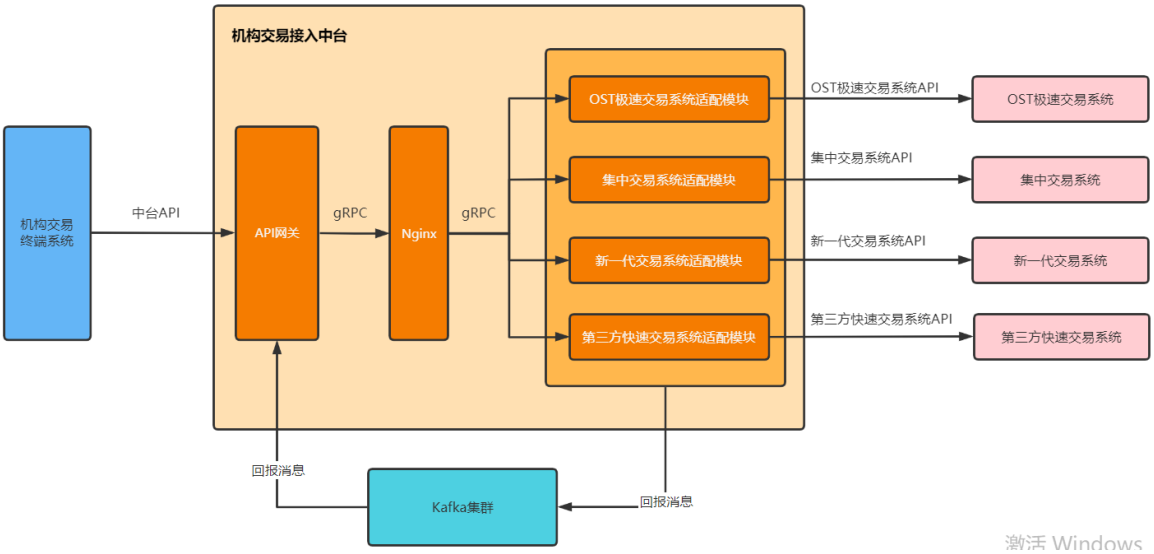

图 1：机构交易接入中台总体架构图

接入，通过会话管控保证安全和访问控制并通过 gRPC 协议实现 API 网关与交易系统适配模块之间内部通讯；并基于微服务 gRPC 框架实现交易系统适配模块，负责将机构交易统一协议适配转换为各种交易系统的接口协议。另外为简化系统复杂度并提高系统可用性，引入开源 Nginx 服务器提供具体路由控制、负载均衡、流量控制能力；为支持主推送方式接入，引入开源 Kafka 消息中间件存储回报消息，由 API 网关通过订阅 Kafka 获取和缓存回报消息并通过 TCP 协议推送至机构交易终端。

3.2 API 与 gRPC 选择

关于机构交易终端系统接入方式，支持类 CTP API 方式还是采用公司业务中台广泛推广的 gRPC 接口，在比较 API 方式和 gRPC 接口的特点后，考虑到主流 PB 交易终端系统的对接习惯，以及 gRPC 接口在支持互联网接入情况下可能遭遇非法终端接入的风险，最终选择支持 API 方式。

3.3 API 网关请求处理过程

为减少中心节点 API 网关的复杂度，提高系统稳定性，API 网关采用基于机构交易统一协议

表 1：API 方式与 gRPC 接口对比

	API 方式	gRPC 接口
对接模式	主查询模式、主推送模式	主查询模式、主推送模式
支持语言	C++、Java、Python	Java、C++、Python、C#、Go、Kotlin、Node、PHP、Ruby
支持平台	Linux、Windows	Linux、Windows、Mac
API 开发	需定制开发	无需 API 开发，仅提供接口文档，可通过工具自动生成客户端 API
通讯特点	通过 TCP 长连接通讯，委托、回报时延低	采用 HTTP2 通讯，gRPC 协议相对 TCP 协议复杂，委托、回报时延相对较高
适用场景	符合主流 PB 交易终端系统对接习惯	微服务架构，无需维护连接，无会话状态，容易横向扩展

的 gRPC 接口调用交易系统适配模块，机构交易统一协议和交易系统接口协议的适配转换由交易系统适配模块完成，API 网关负责解析通讯报文、校验报文入参、校验会话、并根据业务功能、客户、请求参数确定路由信息，转发请求和处理响应。

3.4 API 网关设计

API 网关主要内容包括 API 消息协议、API 网关初始化、会话管理、路由管理、订阅推送等功能。

API 消息协议 TCP 报文内容结构包括消息头、消息体、校验位三部分。消息头包括请求类型、请求编号、业务消息长度、压缩标志、最后报文标志、API 版本等内容；消息体包括业务消息；校验位为检查报文内容有效性。

API 网关启动初始化过程中，从管理数据库获取资金账户白名单、以及关联的 IP、MAC 信息，并通过调用交易系统适配模块 gRPC 服务获取各交易系统节点支持的资金账户和市场。

机构交易终端在与 API 网关建立 TCP 连接后，调用登录接口认证建立会话。建立会话过程主要包括资金账户白名单、终端 IP、MAC 信息校验，以及交易密码校验，校验通过后建立会话。API 网关管理会话相关的 TCP 连接、资金账户、消息订阅状态、终端信息等信息。在 TCP 连接断开时，API 网关注销会话并清理会话相关内容。

API 网关根据请求资金账户和市场代码，确定客户竞价交易相关请求对应的交易系统节点。针对

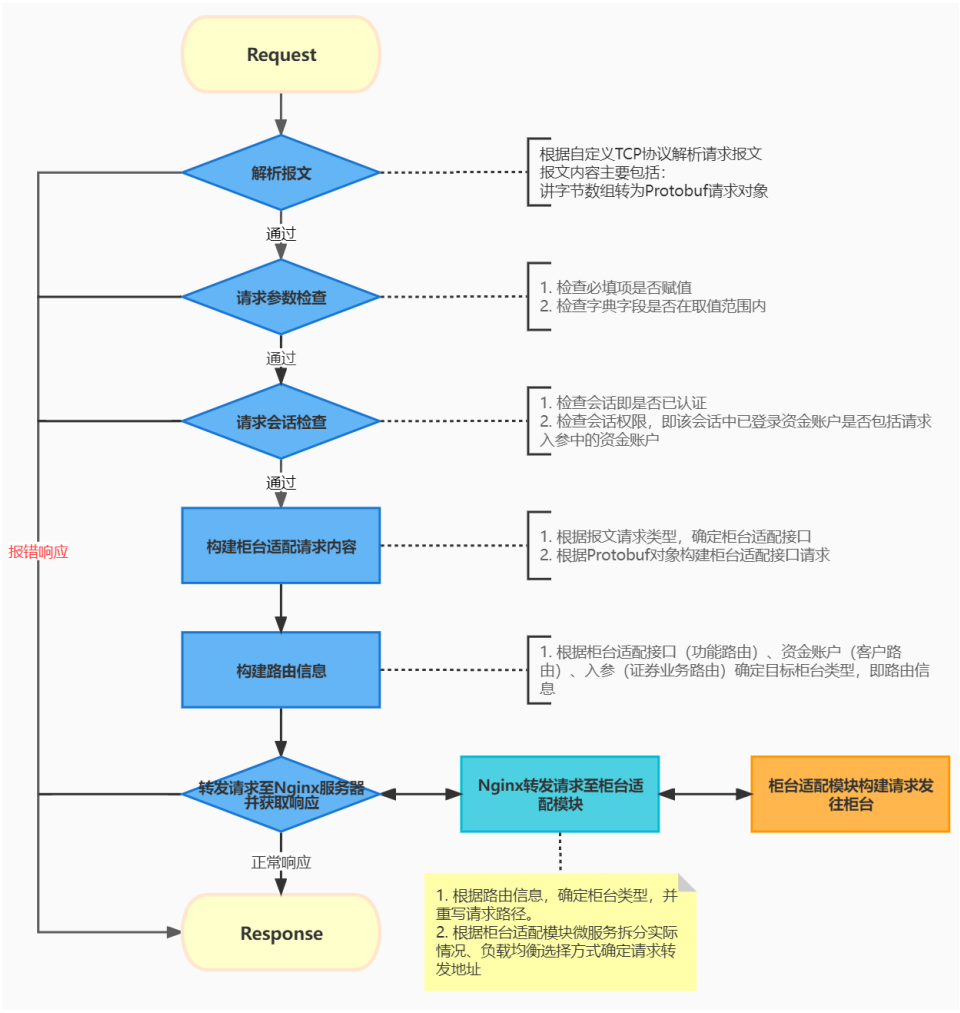

图 2：API 网关请求处理过程

快速交易系统不支持的业务，确定客户对应的普通交易系统。通过在发往 Nginx 服务器的 gRPC 请求元数据中加入交易系统类型信息，由 Nginx 服务器将请求转发至对应交易系统适配模块。

3.5 交易系统适配模块

东方证券制定了企业技术架构向以微服务为核心的现代化架构转型并选择了具有跨语言特性的 gRPC 为核心框架，并在其基础之上新增服务治理特性和星辰服务治理平台，优化改进服务质量。综合考虑 gRPC 协议多路复用、高效编解码方式、框架成熟度以及复用公司服务治理平台提供的监控和告警等功能，交易系统适配模块采用 gRPC 接口方式实现机构交易统一协议，供 API 网关内部调用。基于机构交易统一协议，快速交易系统适配模块提供给其支持的竞价交易相关的接口，普通交易系统适配模块基本涵盖机构交易统一协议定义的全部接口。

在引入新交易系统的情况下，通过新增交易系统适配模块，并在 API 网关和 Nginx 调整路由配置，即可支持原有机构交易终端接入新的交易系统。

4、实践

4.1 统一协议

不同系统对于新股申购、ETF 申赎等业务功能接口提供方式，资金账户、市场代码等业务字段命名，委托市价、信用交易相关参数的组成，市场代码、委托状态字段取值均可能不同。

机构交易统一协议主要以快速交易系统提供的接口为基础，补充机构交易终端支持客户全业务交易时所需证券交易接口。其中针对普通账户，支持普通买卖、ETF 申赎、国债逆回购、新股申购、配股配债、转股回售、港股通业务；针对信用账户，提供担保品买卖、信用交易、非交易委托、新股申购业务；针对股票期权账户，提供买入开仓、卖出平仓、卖出开仓、买入平仓、备兑开仓、备兑平仓等业务。

机构交易统一协议主要包括接口清单、接口出入参字段、字典字段取值三部分内容。机构交易统一协议接口 73 个，其中同时支持普通账户、信用账户、期权账户的接口 27 个；同时支持普通账户、信用账户的接口 37 个；接口出入参字段 413 个，其中浮点型字段 170 个，字符类型 114 个，整型字段 76 个，长整型字段 53 个，入参字段 131 个；字典字段 41 个，包括委托状态、委托方式、委托属性、市场代码等。

4.2 全业务支持

由于快速交易系统主要支持竞价交易业务如普通买卖、ETF 申赎、国债逆回购、信用交易、股票期权交易等，而对速度要求不高的业务如新股申购、配股配债、转股回售、港股通业务由普通交易系统支持。统一协议中将委托接口主要拆分为竞价委托和普通交易系统委托。

关于竞价委托，API 网关根据客户竞价交易所在的交易系统，将请求转发至对应的交易系统适配模块。而针对有的交易系统的竞价委托业务，如市价委托、限价委托、ETF 申购、ETF 赎回，由不同的接口支持，交易系统适配模块根据统一协议确定请求具体业务类型，完成接口字段和字典字段的适配，调用交易系统对应的 API。

关于普通交易系统委托，由于部分快速交易系统也支持如新股申购、配股配债、转股等业务，API 网关根据统一协议中普通交易系统委托的委托属性判断业务类型，并根据客户该业务所在的交易系统，将请求转发至对应的交易系统适配模块。

4.3 双节点客户支持

对于沪市深市证券账户分别在上海和深圳快速交易系统节点的客户，称为双节点客户。通常为追求报盘极致速度，这类客户通过托管系统进行交易。部分交易型的机构交易终端客户也为双

节点客户。针对双节点客户交易、资金、持仓、委托流水、成交流水在不同交易系统节点的情况，传统的方案是机构交易终端系统连接两个不同交易系统地址，分别进行对应市场的交易，客户需选择对应的地址或账号进行登录。

中台通过 API 网关路由和对查询结果进行合并汇总，实现单点接入的方式支持双节点客户。对于客户的资金、持仓、委托流水、成交流水在不同节点的情况，API 网关分别将请求转发至对应交易系统节点，并将查询结果进行合并汇总。对于交易类请求，API 网关根据入参中市场代码，将请求转发该市场对应交易系统节点。为兼容传统方案，API 网关通过侦听不同的端口分别表示对应上海、深圳、全市场交易系统节点。如果终端系统连接上海或深圳交易系统节点对应的端口，则 API 网关则将请求转发至对应交易系统节点，不进行双节点消息的合并汇总处理。

4.4 消息订阅

为支持主推送模式接入，避免机构交易终端定时查询的消息延迟，中台支持消息订阅，当委托状态发生变化或有成交产生时，主动推送消息到机构交易终端。通常机构交易终端系统启动时以“从本交易日开始重传消息”的订阅模式接收全量消息，在发生网络异常情况下以“从上次收到点续传消息”的订阅模式接收后续消息，部分不需要全量消息的机构交易终端，以“只传送订阅后的消息”的订阅模式接收当时间节点后产生的消息。

交易系统适配模块根据各自交易系统对于委托状态和成交回报推送的方案，获取当日推送消息并转换为机构交易统一协议定义的委托状态和成交回报消息，存储到 Kafka 消息中间件。对于不支持消息推送的交易系统，交易系统适配模块定时增量查询获取并存储数据。

API 网关从 Kafka 消息中间件订阅数据进行必要转换后在内存中按照客户缓存消息队列，并维护会话中客户消息订阅请求和当前推送序号等状态，在有后续消息达到内存消息队列时通过会话的通讯通道主动推送消息到机构交易终端系统。

4.5 基于订阅消息提供查询

由于快速交易系统通过基于内存交易技术，大量查询请求可能影响快速交易系统交易性能。中台基于缓存的消息队列，提供委托查询和成交查询，避免委托查询和成交查询请求透传至快速交易系统。

对于成交查询，成交回报消息即为成交明细消息。API 网关维护客户、消息定位串到成交回报消息的映射关系，其中消息定位串以跳表的数据结构组织，支持基于消息定位串入参的增量查询。

对于委托查询，每笔委托的最新委托状态消息即为该笔委托的查询结果。API 网关维护客户、消息定位串到委托状态消息的映射关系，并在委托的最新消息到达时，更新映射关系。

基于缓存消息提供的查询接口，在查询性能和并发支持方面有数量级提升。

4.6 委托引用

机构交易终端收到委托状态消息时，通常使用委托状态消息的委托引用关联原委托。由于部分交易系统对委托引用取值规则进行限定或者定义类型不一致，不能返回机构交易终端委托的委托引用。中台将委托引用定义为长整型字段，对于支持长整型委托引用的交易系统，中台采取透传方式；对于不支持长整型委托引用的交易系统，中台维护委托引用和委托的关系，并在委托查询结果和委托状态消息推送中补充委托引用字段。

中台在向交易系统转发委托请求前，在内存维护委托引用和委托的关系，并通过 Kafka 消息中间件存储和共享全量映射关系。在查询委托消息或收到交易系统委托状态消息推送时，中台根据映射关系填充委托引用字段。由于部分映射关系是通过 Kafka 共享，极端情况可能发生存在先

表 2：单笔查询平均耗时比较

记录条数 / 查询方式	1	100	1w	10w	100w
透传至交易系统	7.52ms	43.21ms	1.58s	12.08s	不支持
基于缓存消息查询	1.29ms	4.46ms	110ms	737ms	6.94s

收到委托状态消息而后获取映射关系的情况，为保障推送客户消息的顺序性以及委托引用原值返回，中台采用更新委托引用和回填委托引用两部分。在更新委托引用阶段，如果未获取委托引用，则等待若干毫秒后重试，直至超过允许处理的时间，在该阶段该委托所属客户的其他消息也均暂时阻塞，以保证消息的顺序性。回填阶段是指在允许处理的时间内，未更新委托引用的消息，被会记录并定时检查根据获取的映射关系进行回填。

4.7 算法交易

中台提供算法交易接口支持机构交易终端算法交易，机构交易终端系统登录中台后其算法单的母单子单处理流程如图，机构交易终端系统通过子单的委托引用与母单委托编号一致匹配母单字单。

5、总结与展望

目前机构交易接入中台已投入生产使用，已支持一套 PC 交易终端直接从互联网访问和一套 PB 交易终端，日均交易量约数千万。中台在测试环境已支持 3 套交易系统的沪深 A 股普通交易、沪深 A 股两融交易、港股通、ETF 申赎、期权业务接入，并完成多家 PB 交易终端接入的联调测试工作，随着联调测试继续推进，机构交易接入中台将进一步完善。预计在东方证券完成新一代核心业务系统切换时，机构交易终端系统均通过中台接入交易系统，日均交易量约为数十亿。

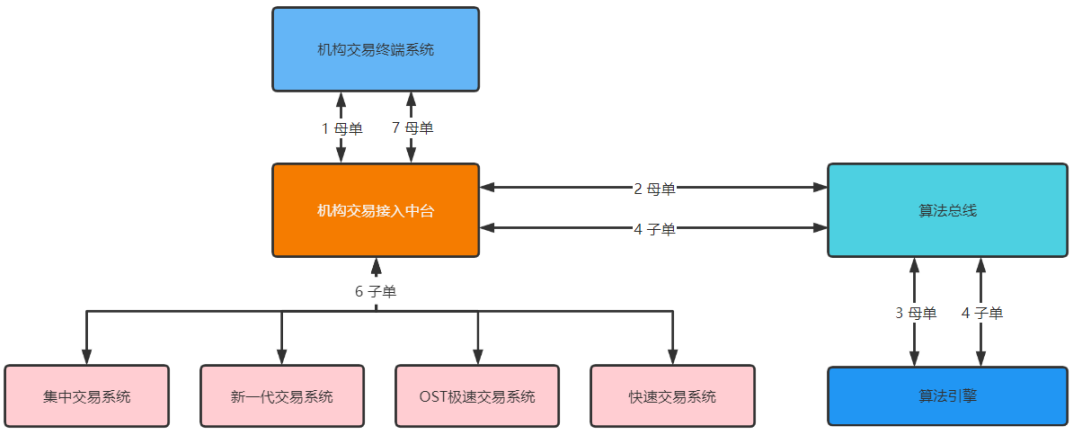

图 3：算法交易处理流程

参考文献：

[1] 微服务框架 gRPC 交易接入网关实践 https://mp.weixin.qq.com/s/-PK26QNJy2t9p4TCTf2dEw
[2] 东方证券服务治理建设实践 https://mp.weixin.qq.com/s/igX11UL_cbLh-UrpjK-BQg
[3] 新一代证券交易系统应用架构的研究 https://mp.weixin.qq.com/s/SAvXEkaF0ck7XXApGYgk2A
[4] 企业级证券业务中台探索与实践 https://mp.weixin.qq.com/s/1RL6iSHU7t8R-COk1i7kJQ

可复用数据处理框架在证券数据处理中的探索和实践

蔡文博、张舒、鲍倩倩、杜小静、胡红星 / 上交所技术有限责任公司 技术开发总部 上海 200120
E-mail：wbcai@sse.com.cn

随着上交所批处理系统承接的业务越来越多，为了应对业务响应及时性、数据维护质量和系统运行效率等方面的挑战，上交所技术在借鉴主流数据处理框架优秀设计的基础上，结合自身系统特性，以提高代码复用度为目标，开发了一套轻量级的 C++ 数据处理框架，并且结合元数据管理，在提高数据维护质量的同时降低了数据血缘关系维护难度。本文从批处理系统面临的实际挑战出发，通过分析 Spark 等系统的优势以及自身需求，设计和开发了批处理系统的数据处理框架和元数据管理模式。目前，新开发模式已投入在创新业务及交易系统升级建设的研发工作中。

1、背景和挑战

上交所批处理系统作为核心交易系统数据加工及处理的重要模块，主要承担着交易后清结算处理和基础数据维护两大功能。随着创新业务不断发展及交易系统技术持续升级，对批处理系统在业务响应及时性、数据维护质量、系统运行高效等方面提出了更高的要求。现有的批处理系统已表现出诸多不足，主要问题有：一是研发效率不高，虽然使用了相对高效易用的基础库，但业务应用抽象程度低，代码复用程度低，进而导致创新业务需求响应能力差；二是缺乏统一的数据标准，目前各接口独立定义字段，导致定义工作重复、同一字段在不同接口命名不一致，增加系统维护成本，降低数据整体质量；三是数据血缘关系维护难度大，随着批处理系统承载的业务越

来越多，数据处理流程越来越复杂，准确全面维护血缘关系的难度也越来越大。

近年来，上交所持续推进数字化转型，积极助力科技赋能，批处理系统技术服务能力和数据管理水平亟待升级。为解决以上问题，批处理系统启动研发轻量级数据处理框架，既易于与现有技术体系融合，又便于数据血缘关系的提取。首先考察主流的数据处理框架，如 Spark，Flink 等，在借鉴其关于数据算子抽象的基础上，设计开发 C++ 语言的数据处理框架。通过对业务逻辑的抽象与封装，形成可复用的功能组件，沉淀技术共享能力，进一步提高研发效率。此外，结合数据标准及元数据管理，设计了包含数据元、字段、模型、物理表 / 文件等四层结构的维护模式，确保字段在所有模型中均有一致的定义，有助于提高数据质量。

2、数据处理框架

2.1 整体架构

上交所批处理系统的数据处理框架整体可分为组件层和存储抽象层。组件层包含基础组件层和功能组件层，其中基础组件提供原始的数据处理语义，如过滤、联合、映射、分组等；功能组件是对基础组件的组合，实现一个完整的数据转换功能，如表 A 数据关联更新表 B 数据、表数据格式转换后导入文件等。存储抽象层则定义了统一的数据访问接口，如读取、写入、查找、更新等，使组件层可以无差别的处理文件、数据库表、共享内存库、Map 等多种存储形式中的数据。

应用层的业务逻辑通常使用预定义的功能组件实现，特殊情况下可直接组合基础组件实现。存储抽象层屏蔽了存储介质的差异，使框架易于

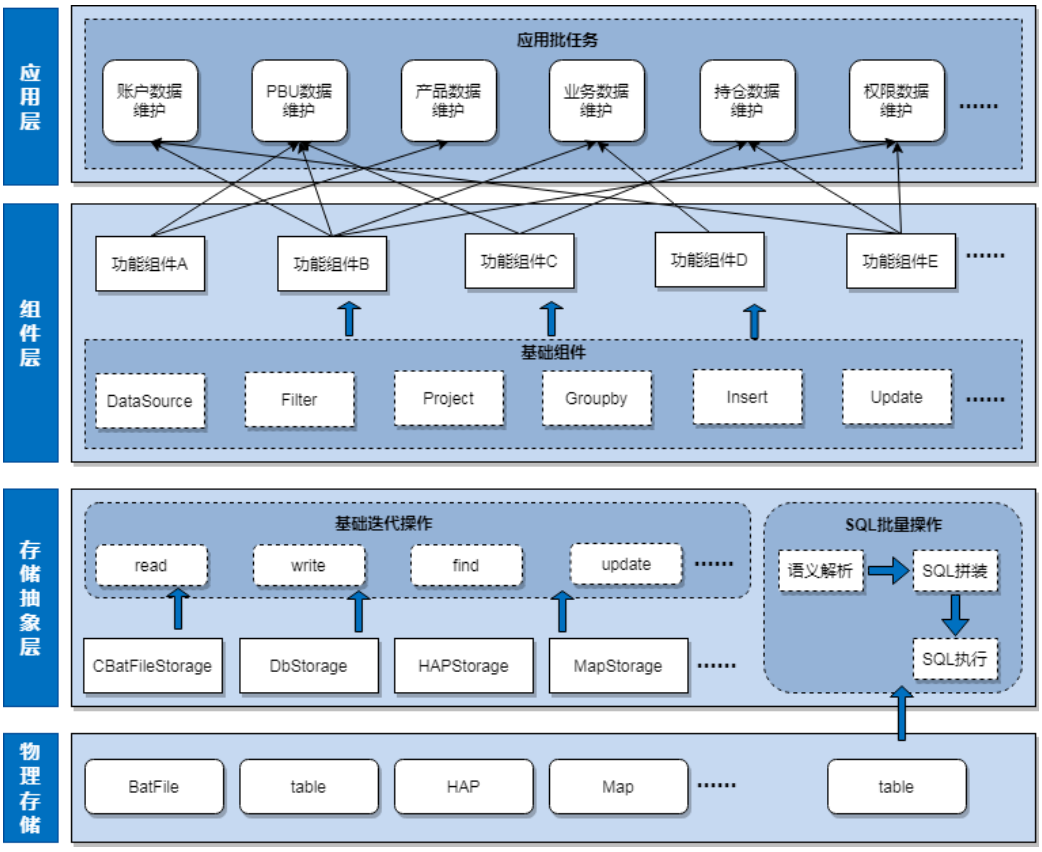

图 2.1：数据处理框架整体架构图

融入现有的技术体系；组件层则主要体现了业务逻辑的抽象与复用，加强代码可复用能力，降低开发及测试成本。框架的整体层次如图 2.1 所示。

2.2 存储抽象层

存储抽象层为不同存储介质（如文件、数据表、Map 容器等）中的数据提供统一的访问接口。对数据处理框架而言，一方面屏蔽了存储介质特性，使组件层可以无差别地处理各种存储形式的数据；另一方面应用层无需关心存储特性，提高了应用批业务表达的清晰度。

技术实现上，不同的存储类均实现 Storage 接口，类层级关系如图 2.2 所示。根据存储介质的特性，并非所有接口都要实现，比如文件存储类（CBatFileStorage）无需实现查找和更新接口。

2.3 组件层

2.3.1 基础组件

基础组件是对常见批量数据处理动作的提炼，描述了一次数据集的转换。基础组件类似 Spark 和数据库中的算子（Operator）概念。

主要基础组件及其功能如下表 2.1 所示。

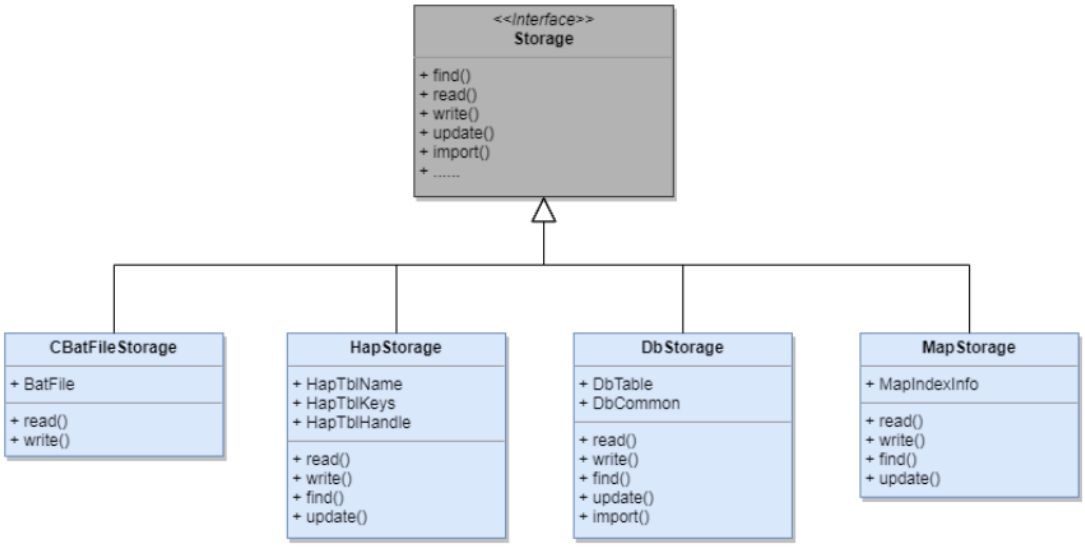

图 2.2：类层级关系

表 2.1：基础组件及其功能

基础组件	功能简介
Aggregate	支持数据聚合操作
DataSource	用于指定源数据集
CreateView	创建数据库视图
Expand	支持数据扩展操作
Filter	根据某一条件过滤数据集
Groupby	将数据集按某一条件分组，并执行后续操作
Import	支持批量导入数据
Insert	支持数据插入
Join	支持数据集联合
Orderby	支持数据集排序
Update	用于数据更新
Upsert	存在即更新，不存在即插入
Validate	支持数据校验

基础组件具备以下三个特征：

• 可组合性。基础组件输入输出接口的一致性保证了其可组合性，基础组件的可组合性是实现复杂数据处理逻辑的基础。

• 可复用性。单个基础组件是对一类数据操作的抽象和提炼，实际使用时根据具体场景对其实例化。

• 可扩展性。新的数据处理模式可以通过开发新的基础组件来支持，且由于组件的可组合性，新组件可获得更广的应用范围。

2.3.2 功能组件

功能组件以具体的数据转换模式为基础，统一代码模式，内化实现细节，仅表达数据转换关键信息，清晰地表达数据的变更方向和变更方式，使代码的业务表达能力更精练。组件的标准化和可复用性有效提高了代码的利用率，减少了应用代码的冗余度，对提高开发效率具有积极意义。

功能组件一般描述了数据从一个载体到另一个载体的转换过程。组件并不关心载体具体是什么，重点是转换过程。比如同一个组件既可以处理文件数据经过过滤后导入 Map 的过程，又可以处理表数据经过过滤后导入文件的过程。如前所述，功能组件都是由一系列基础组件组合而成。图 2.3 展例了两个功能组件实现。

• 功能组件 1：适用于需要过滤源头数据集

```
// 功能组件1：根据某条件过滤源数据集，插入目标数据集
template <typename FT, typename OT>
void IterateExecute(FROM<FT> from, FILTER filter, INSERT<OT> dest) {
    auto ds = from.ds.filter(filter.condition)
        .template project<OT>(dest.assigns)
        .insert(dest.ds)
        .save();
}

// 功能组件2：源数据集和输入数据集联合，插入目标数据集
template <typename FT1, typename FT2, typename OT>
void IterateExecute(FROM<FT1> from, JOIN<FT2> join, INSERT<OT> dest) {
    auto ds = from.ds.join(join.ds, join.ons, join.type)
        .template project<OT>(dest.assigns)
        .insert(dest.ds)
        .save();
}
```

图 2.3：功能组件示例

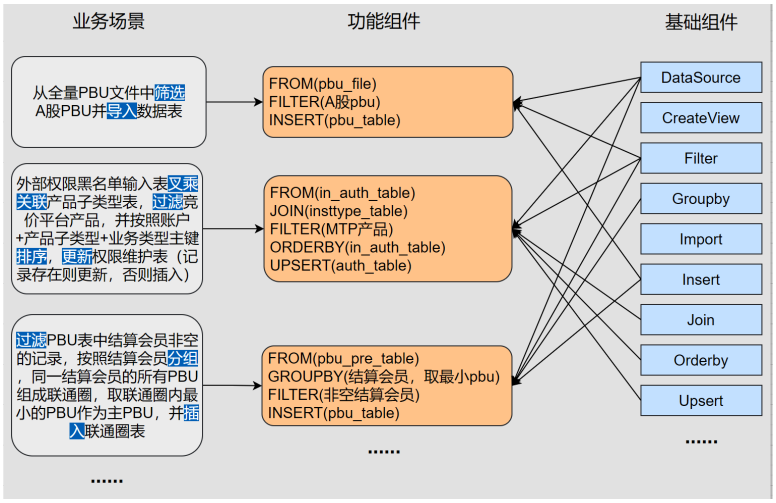

图 2.4：业务场景与组件关系

的场景。如筛选出输入产品全量数据中的所有股票产品并插入数据库表。

• 功能组件 2：适用于目标数据集为源数据集和中间数据集联合的场景。如在展开账户对所有产品子类型的权限并插入到进程 map 的需求中，使用 cross join 操作。

根据实际业务场景，选择合适的功能组件是实现应用业务处理的关键点。当功能组件不满足业务场景时，可通过组合基础组件开发新的功能组件。以具体业务场景为示例，图 2.4 展示了具体的业务场景衍生出的功能组件和基础组件的关系。

功能组件根据执行模式可分为两种。一种是在内存中迭代执行，另一种是转换成 SQL 后在数据库内执行。下面分别介绍两种执行模式的执行步骤。

一、迭代执行模式

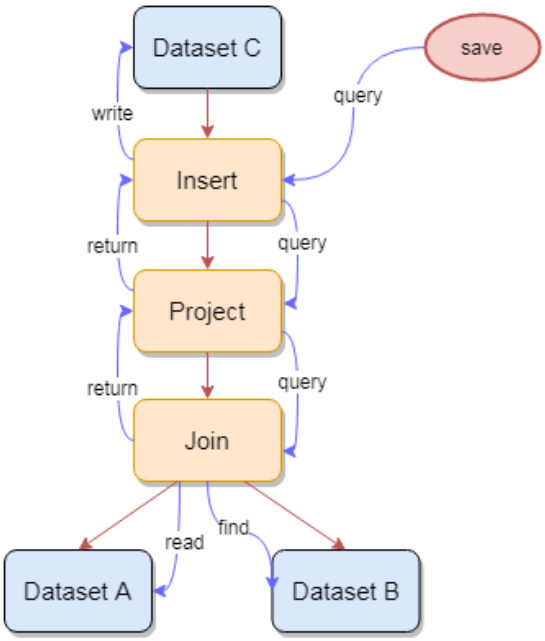

图 2.5：迭代执行模式

红线表示节点引用关系，箭头表示下游节点对上游节点的引用；蓝线是函数调用执行的顺序

迭代执行的组件都重载 IterateExecute 函数（如图 2.3），且都由 save() 接口触发。执行规则是下游节点递归的向上游节点请求数据（query），直到最上游的算子节点直接从源数据集中取到数据，然后数据经过各级节点处理后返回（return）最下游的算子节点。为避免对内存过多的占用，数据以分批的形式在各节点间传递。同时，为避免数据在各节点间过多拷贝，节点间传递的是数据指针，且多数节点不缓存数据。例外的是映射节点（project），因为涉及到数据结构的变动，映射节点将缓存新结构的数据，并向下游传递新数据的指针。

二、数据库执行模式

与迭代执行不同，数据库执行的组件都重载 DbExecute，且都由 doDbExecute 触发，如组件 3 所示（图 2.6）。

图 2.7 展示数据库执行的机制。

数据库执行组件先将数据处理流程编译成 SQL 语句，然后在数据库中执行对应 SQL。SQL 的编译过程借鉴 SQLAchemy 项目的思路，主要应用了 Visitor 设计模式。每个算子节点可接收一个 Visitor 对象，并把其参数传给 Visitor 对象。在上图的例子中，Insert 算子通过 visit_insert 接口把目的表信息传递给 SqlVisitor；Project 算子把字段映射关系通过 visit_project 接口传递给 SqlVisitor；Join 算子把关联的左表和右表以及关联条件传递给 SqlVisitor。通过遍历整个数据流中的节点，SqlVisitor 收集到所有的表操作要素并放在其内部的 SqlBuilder 中，最后由 SqlBuilder 将表操作要素编译成 SQL 语句。

2.4 应用示例

对于实际的盘后批处理应用，可将一个批（Job）的业务功能拆分成多个步骤的数据集转换（Stage），每个 Stage 由单个功能组件实现，完成一次数据集的转换。多个 Stage 顺序执行最终完成目的数据集的生成。

Step1：为 DatasetContext 对象提供上下文参数，构造初始数据集对象（Dataset）。构造 Dataset 时需指定其存储类型、存储资源 ID、数据结构（C-Struct）等信息。这些数据集既包含

```
// 功能组件3：两个源数据库表联合后，插入目标数据库表
template <typename FT1, typename FT2, typename OT>
void DbExecute(FROM<FT1> from, JOIN<FT2> join, INSERT<OT> dest) {
    auto ds = from.ds.join(join.ds, join.ons, join.type)
        .template project<OT>(dest.assigns)
        .insert(dest.ds);
    doDbExecute(ds);
}
```

图 2.6：数据库功能组件

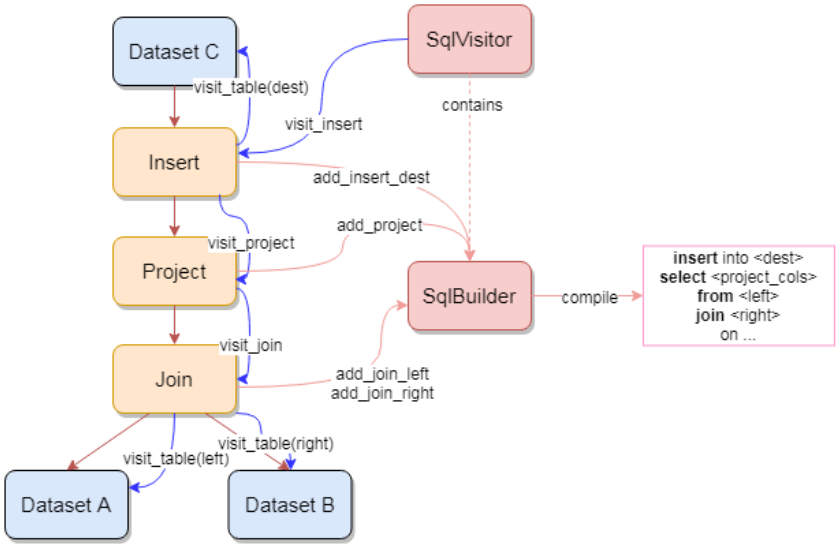

图 2.7：数据库执行模式

红线表示节点引用关系，箭头表示下游节点对上游节点的引用；蓝线是函数调用执行的顺序

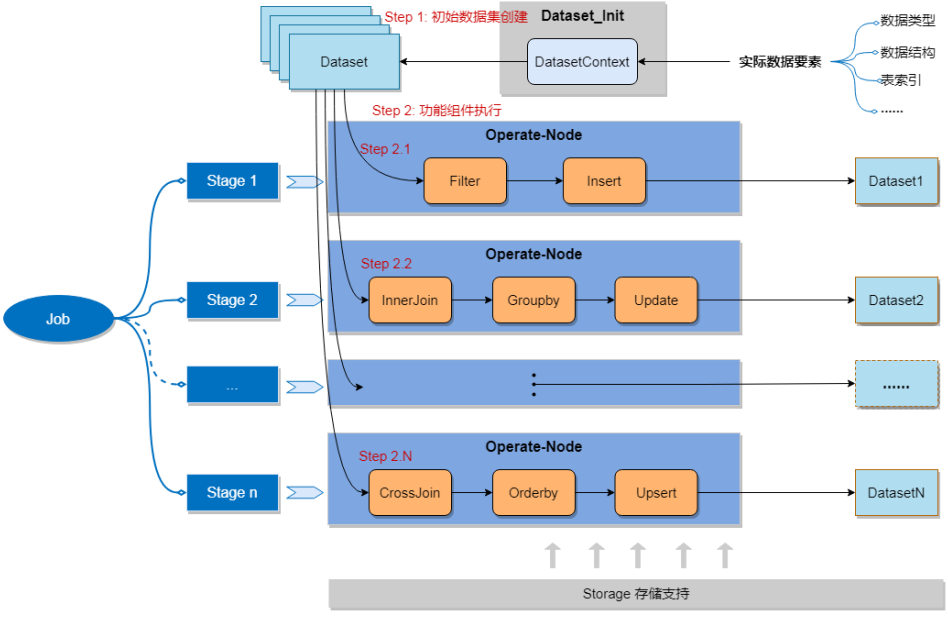

图 2.8：应用示例解析

输入数据集也包含输出数据集。

Step2：按顺序执行每个 Stage 的功能组件。每个功能组件完成一个目标数据集数据的生成。前面 Stage 的目标数据集可作为后续 Stage 的源数据集。数据集的读写均通过 Storage 接口统一完成。

2.5 代码生成

由于批任务代码基于预定义的组件，且代码结构有较强的规律性，我们在此基础上设计了一套 Yaml 配置规则，并开发了配套的代码生成程序，支持将 Yaml 配置翻译成批任务代码。其收益包括：一方面进一步提高了业务开发人员的编码效率；另一方面在于将业务逻辑结构化处理，支持后续对业务逻辑的进一步解析与应用，生成数据的血缘关系。如图 2.9 所示，左边为 Yaml 配置，右边为生成的批任务代码。

3、元数据管理

3.1 数据模型构建

批处理系统承载交易系统文件聚合、转发等业务功能，具有数据量大、数据结构复杂等特点。批处理系统强化数据标准体系建设工作，在业务层面，有助于明确业务含义，明确业务与业务间、业务与技术间统一口径与认识；在技术层面，有助于构建规范的物理数据模型，提供对数据元的格式规范，进而提高数据质量水平；此外，有助于配合与对接所级别数据标准的建设。

目前，批处理中心使用数据元定义、字段定义、模型定义、文件 / 数据表定义的递进引用结构（如图 3.1），对系统所使用的元数据进行管理与维护。

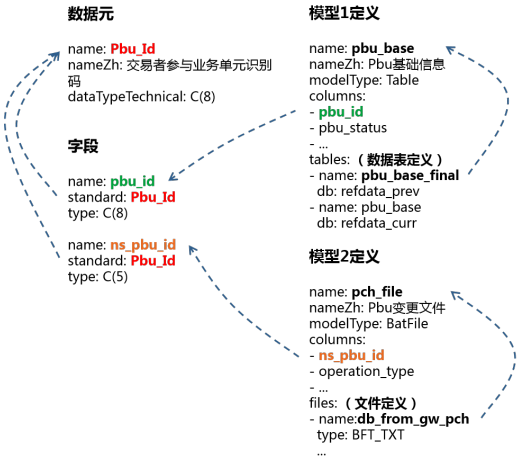

图 3.1：递进引用结构

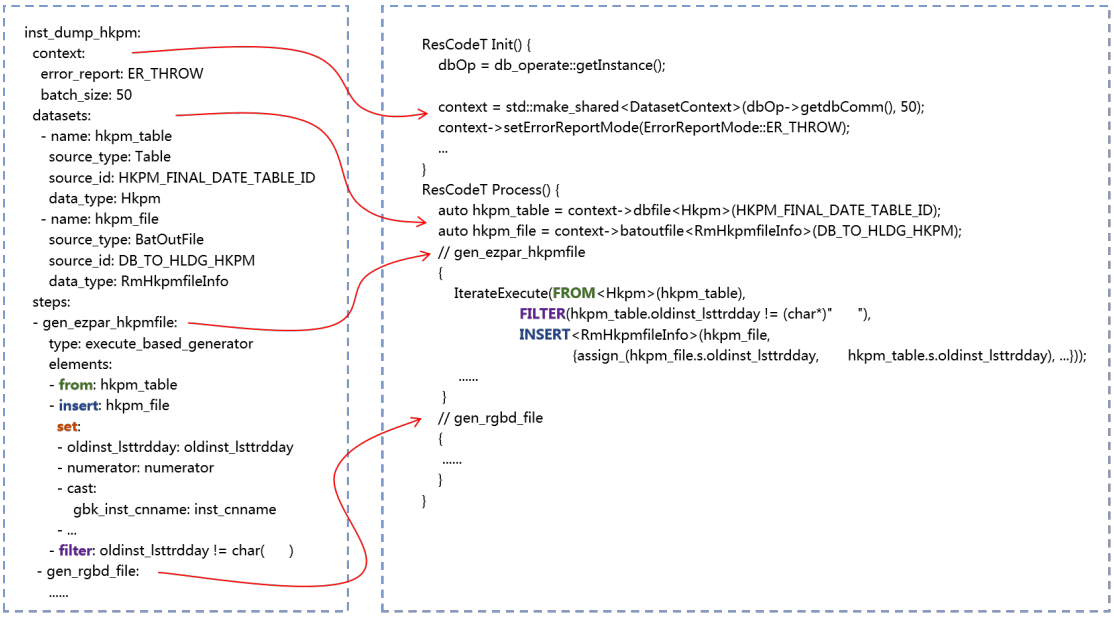

图 2.9：业务配置与代码生成

其中，数据元是数据标准定义的基本单位。以标准数据类型为基准，建立数据标准体系。数据元按照主题大类、主题子类划分类别（详见表 3.1）。

字段在数据元基础上进行定义，同一个数据元可拥有多个字段，多个字段可指向同一数据元。同一数据元仅有一个标准格式字段；可拥有多个扩展格式字段；其中，在模型设计规范中定义：批处理系统内部维护的字段均为标准格式字段。若输入接口中的字段非标准格式，其进入系统内部模型前需转换为标准格式；若输出接口中的字段为非标准格式，需将内部模型中的标准格式字段转换为输出接口要求的格式。

模型是由字段组合形成的逻辑概念；文件、数据表在逻辑模型的基础上定义，增加落地的物理属性。同一个模型可被定义为多个文件 / 数据表实体。

3.2 配置自动生成

数据元配置可自动化生成文件 / 数据表等模型的接口文件。目前支持生成文件结构接口、数据表结构接口、SQL 建表语句等。既减轻了开发人员的工作量，另一方面保证了元数据与代码结构的同源性，提升研发效率的同时有效提高数据维护质量。配置自动生成说明如表 3.2 所示。

在后续工作中，批处理系统将持续加强对元数据组织方式、标准及规范定义、评审流程等工作的完善，形成高效可控的管理机制。

4、血缘关系提取

上交所批处理系统涉及的证券数据，主要有以下特征：一、业务繁多，几乎所有业务均包含盘后处理；二、相关方多，上下游交互系统较多，主要包含外部对等机构、所内业务系统、市场这三大类；三、业务规则变更、所内外接口变更较频繁，影响评估工作量大；四、盘后批处理应急场景多，亟需高效的影响评估手段。

基于以上交易系统盘后批处理数据及业务特征，通过维护数据血缘关系，可有效提高数据变更影响评估的效率和准确度；生产应急情况下，应急时间窗口紧张，短时间内人工评估数据影响容易错漏，提供自动化手段可提高运维效率；方

表 3.1：数据模型分级试图

逻辑主题	主题大类	主题子类
市场参与者	账户信息	账户基础信息
		账户指定关系
		账户权限
	持有	账户持仓
机构	机构信息	机构基础信息
	PBU 信息	PBU 基础信息
		PBU 产品业务权限
产品	产品信息	基础信息
	产品业务信息	产品业务交易参数
		产品业务平台对应关系
业务	业务信息	业务基础信息
		业务时间表
市场	市场信息	交易日历
		全局交易时间表

表 3.2：配置自动生成说明

使用场景	生成物名称	生成物用途
数据库表注册信息	table_info_list.cpp	数据表与结构体对应关系
	refdata_table_list.cpp	数据表分类情况
	table_id_enum.hpp	数据表 ID 注册
	table_flag_index.h	数据表 flag 文件注册
数据库表、视图接口	db_interface_<tablename>.hpp	数据库表结构&建表语句定义
	<tablename>.h	数据库表就绪通知文件
文件接口	ifm_<filename>.h	文件结构定义
	from/to_<filename>.h	文件路径等属性定义
模型文档	tables.xls	数据表接口文档
	files.xls	文件接口文档

便业务理解，提高需求分析、运维工作效率和工作质量。

4.1 提取方式

常见的数据血缘关系提取主要以解析 SQL 为主。通过遍历 SQL 的抽象语法树（AST）分析数据血缘关系。但是批处理系统除了有基于数据库的数据处理，还有基于文件和内存的处理过程，这些处理过程无法用 SQL 体现。因此通过解析体现业务逻辑的 Yaml 配置可以获得更为完整的数据血缘关系。

与代码生成逻辑类似，通过解析每个数据处理流程的 From、Join、Insert、Update 等节点的数据集信息可以获取文件和表级别的血缘关系（粗粒度）。进一步解析 Insert 和 Update 等节点的字段赋值关系可以收集字段级别的血缘关系（细粒度）。

一、文件 / 表级别

任务包含多个输入和输出，通过建立文件 / 数据表的血缘关系，便于分析数据流向，了解数据的重要程度，为相关业务决策提供参考基础。特别对于上下游系统交互较多的多任务处理系统，当生产环境上游文件未及时到达，能迅速进行影响分析，为应急处置提供帮助。目前我们已经完成粗粒度血缘关系提取工具的开发，并将血缘关系导入到了 Apache Atlas 平台。下图 4.1 展示了港股通限制产品导出功能的文件、表与批任务的血缘关系。

二、字段级别

交易系统基于数据处理，海量交易数据分散在多个系统，实际场景中经常会遇到分析字段变更的影响范围、字段来源于哪里等问题。因此，分析字段间的血缘关系变得尤为重要。通过分析批业务配置中文件或表字段赋值的关系，可以生成细粒度 column 级别的字段流向树。图 4.2 为 mem_code（会员代码）字段的血缘图谱分析结果。后续将开发字段级别血缘关系的自动化的提取工具，完善细粒度血缘关系的展示。

血缘关系的维护对后续构建交易系统业务画像、优化系统业务架构和性能、分析数据变更对系统造成的影响评估等方面起到更大应用。

5、总结与展望

在借鉴主流数据处理框架优秀设计的基础上，结合上交所批处理系统特性自研了一套数据处理框架。一方面可以与批处理系统现有的技术更好的融合；另一方面无需独立的运行时环境，避免额外的运维负担；数据处理框架同时支持内存迭代执行和数据库 SQL 执行两种模式，统一了数据库外和数据库内两种数据处理模式的表达方式。最后，元数据管理不但统一了字段的业务含

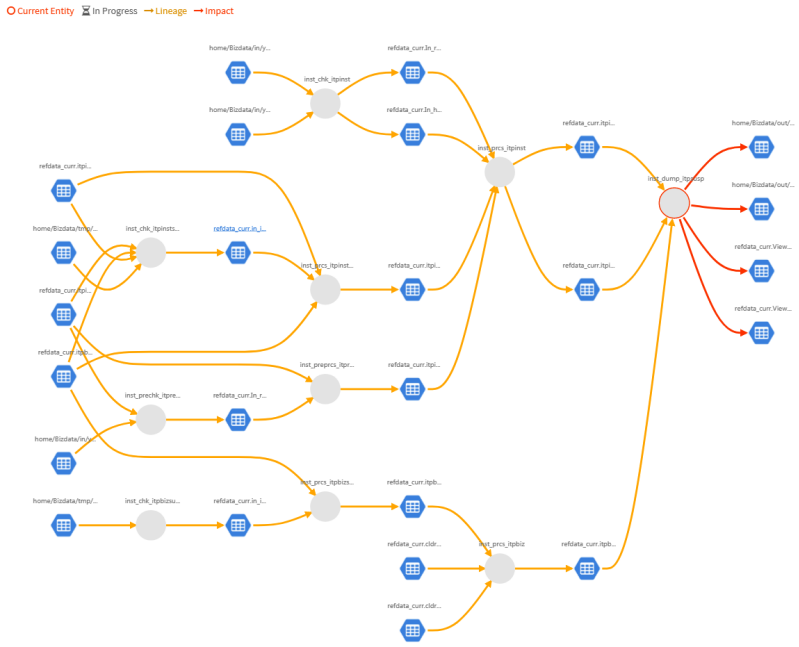

图 4.1：文件级别血缘关系提取

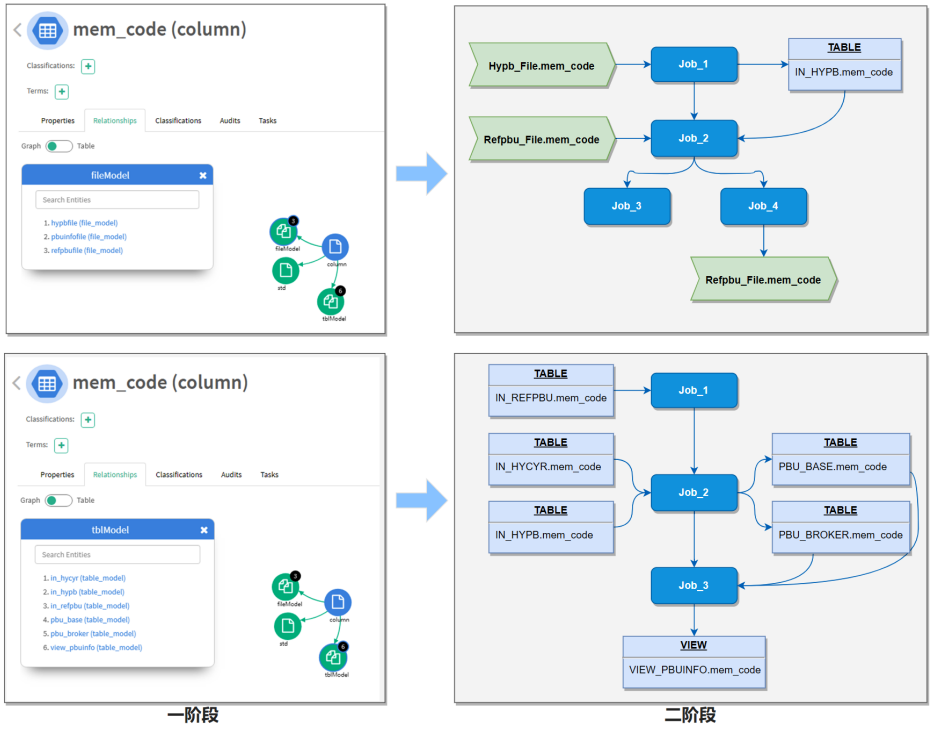

图 4.2：字段级别血缘关系提取

义和技术定义，也使接口代码可自动化生成，提高了开发效率和准确度。

目前批处理系统已经使用新的开发模式投入创新业务及交易系统升级建设的研发工作中，基本实现代码复用、自动化的血缘关系提取以及提高数据维护质量的目标。将在后续业务支持过程中持续完善数据处理功能，并探索把数据处理框架的应用范围扩展到其他处理场景。

基于oneAPI的金融衍生品定价加速

马辉[1]、邹经纬[1]、白君洁[1]、钟浪辉[2]、韩大伟[2]、黄琦[3]、余洋洋[3]、李彪[3]/[1]国泰君安证券股份有限公司 上海 [2]上交所技术有限责任公司 上海 [3]英特尔移动通信技术（上海）有限公司 上海
E-mail :baijunjie026611@gtjas.com

目前，沪深市场上的普通期权产品以及国泰君安的场外期权产品的定价方式均是采用基于蒙特卡罗模拟，通过软件计算来实现。由于蒙特卡罗模拟往往需要模拟十万条以上的路径，传统的期权定价方法面临着处理时间过长，计算效率过低等问题。本文基于此类问题，提出并通过 oneAPI 实现了一种基于 FPGA 的并行流水线期权价格计算方案，能够完成对欧式香草期权与雪球期权的定价。经过对比与测试，相比于 CPU 通过 C++ 软件实现的方式，通过 oneAPI 设计，并通过 FPGA 来实现的定价方式在性能上有显著的提升。

引言

期权作为最基础的金融衍生产品之一，为其定价一直是金融工程的重要研究领域，主要使用的定价方法有偏微分方程法、鞅方法和数值方法。而数值方法又包括了二叉树方法、有限差分法和蒙特卡罗模拟方法。蒙特卡罗模拟方法的理论基础是概率论和数理统计，其实质是通过模拟标的资产价格路径预测期权的平均回报并得到期权价格估计值。

蒙特卡罗方法的最大优势是误差收敛率不依赖于问题的维数，从而非常适宜为高维期权定价。当期权定价模型维数增大时，如多资产的期权模型，无论是理论还是实际中，不会采用确定性方法。因此，业内最普遍采用的方法还是蒙特卡罗方法，特别是对 Path-Dependent（路径依赖）的各类奇异期权以及 Multi-Asset（多资产）期权模型，蒙特卡罗方法直观有效。理论上，随机模拟方法效率和精度很低，但蒙特卡罗算法的模拟路径部分相互独立，可以并行计算。但是，蒙特卡罗模拟的缺点就是速率很慢，数值解误差与随机次数开根号分之一同阶，也就是说，若数值解要精确到小数点后面 1 位，需要试验 100 次；要精确到小数点后面 2 位，则需要试验 10000 次；要精确到小数点后面 3 位，需要试验 10 的 6 次方次。

使用 CPU 通过软件计算的传统期权定价会相当耗时，相比，FPGA（Field Programmable Gate Array，现场可编程门阵列）具有良好的并行计算特性，使用 FPGA 通过蒙特卡罗模拟进行期权定价能获得很好的性能提升。本文使用 Intel 公司的 oneAPI 开发工具，通过 DPC++(Data Parallel C++，数据并行 C++) 语言设计了各类型期权定价算法，并完成综合实现，在 FPGA 加速

板卡上进行了功能验证与性能对比。

1、期权定价原理

欧式和美式看涨看跌期权等衍生品被称为普通期权（也称为香草期权），其具有定义良好的标准属性与广大的交易占比。国内市场上常见的50ETF 期权、沪市 300ETF 期权、深市 300ETF 期权、沪深 300 股指期权均为欧式期权。

场外衍生品属于非标准产品，场外期权也被称为奇异期权，尽管它们通常只占投资组合中相对较小的一部分，但对于衍生品交易商来说，外来产品是非常重要的，因此它们通常比普通衍生品的利润更高。

国泰君安在普通期权与场外奇异期权的定价都有深入的研究，本文以欧式香草期权与场外期权中的雪球期权为例进行分析。

1.1 欧式期权定价

欧式期权可分为看涨和看跌期权，是指在将来的某个特定的时间（到期日），期权的持有者有权力以事先约定的汇率（敲定价）向期权出售者购买 / 出卖约定数量的货币，并支付购买该项权力的权力金。欧式期权风险中性定价通过 Black-Scholes(BS) 模型实现，其随机微分方程（SDE）由下面公式给出：

$$dS(t) = \mu S(t)dt + \sigma S(t)dB(t) \quad (1)$$

其中，S 为资产价格，μ 为股票的漂移量（瞬时期望收益率），σ 为股票的波动率，B 为布朗运行（维纳过程）。

可以认为 dB 是一个均值为 0，方差为 dt 的正态分布随机变量，使用欧式香草期权的价格作为最终现货价格的期权收益的贴现期望，到期时间为 T：

$$e^{-rT}E\left(f(S(T))\right) \quad (2)$$

这个期望是在适当的风险中性度量下得到的，该度量使漂移量 μ 等于无风险利率 r，可得到：

$$dS(t) = rS(t)dt + \sigma S(t)dB(t) \quad (3)$$

通过伊藤引理得到：

$$d\log S(t) = \left(r - \frac{1}{2}\sigma^2\right)dt + \sigma dB(t) \quad (4)$$

这是一个常系数随机微分方程，可由下式解出：

$$\log S(t) = \log S(0) + \left(r - \frac{1}{2}\sigma^2\right)T + \sigma\sqrt{T}N(0,1) \quad (5)$$

这里由于 B(t) 为布朗运动，因此满足均值为 0，方差为 T 的正态分布，可以改写为：$B(t) = \sqrt{T}N(0,1)$。

将上式使用 S(t) 的指数形式改写为：

$$S(t) = S(0)e^{\left(r-\frac{1}{2}\sigma^2\right)T+\sigma\sqrt{T}N(0,1)} \quad (6)$$

使用风险中性定价方法可以得到期权价格的表达式如下：

$$e^{-rT}E\left(f\left(S(0)e^{\left(r-\frac{1}{2}\sigma^2\right)T+\sigma\sqrt{T}N(0,1)}\right)\right) \quad (7)$$

在这种情况下，f 的值是看涨期权或看跌期权的收益。通过对这些收益的总和取平均值，然后取无风险折现，我们得到了期权的近似价格。

2.2 雪球期权定价

雪球期权属于路径依赖型奇异期权，其结构相对复杂，本质是一种带障碍的看跌期权，自 2019 年开始，雪球这种非保本型收益凭证受到市场上越来越多的关注，各类金融机构纷纷以不同角色参与其中。以表 1 所示案例为例。

其年化收益率与挂钩标的价格变化的关系如图 1 所示。

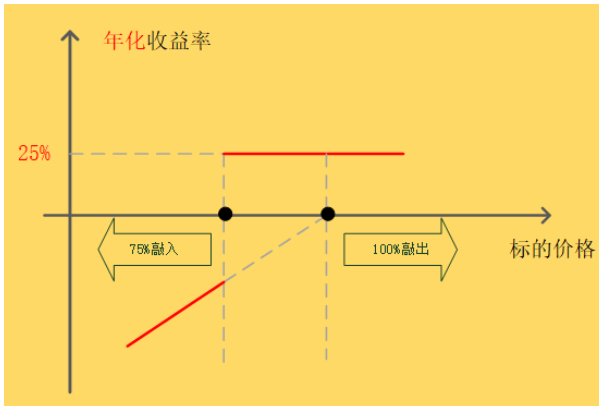

图 1：雪球期权与标的价格关系

雪球期权最主要的特点是具有敲出水平和与

表 1：雪球期权相关要素

雪球期权	
挂钩标的	股票/指数
标的初始价格	100 元
期限	6 个月
敲出水平	100%
敲入水平	75%
票息	年化 25%

敲入水平两个门限，敲出水平每月观测一次，敲入水平每日观测一次，如果发生敲出事件，产品终止并兑付收益；如果发生敲入事件，保护失效，若期末未敲出，则相当于持有该股票。因此截止期末可分为三种情况：第一种情况为敲出，可获得票息为：年化票息 × 名义本金 × 存续月数 /12，如图 2 所示，第二个月虽然发生了敲入事件，但第三个月底敲出观察日时发生了敲出事件，因此可本金无损外加 3 个月的票息收益。

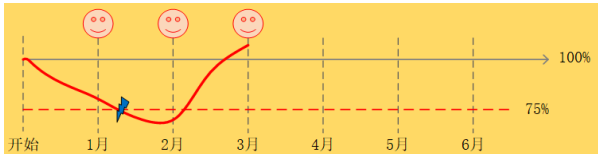

图 2：敲出

第二种情况为敲入未敲出，结算金额为：名义本金 ×MAX（0，期初价格 - 期末价格）/ 期初价格，如图 3 所示，在第三个月发生了敲入事

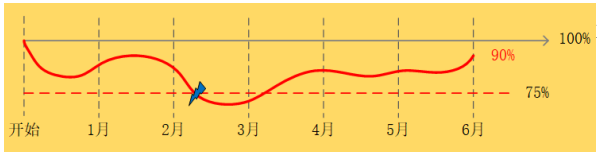

图 3：敲入未敲出

第三种情况为未敲入未敲出，可获得票息为：年化票息 × 名义本金 × 存续月数 /12，如图 4 所示，存续期间期间未发生敲入事件与敲出事件，可获得满期 6 个月的票息收益。

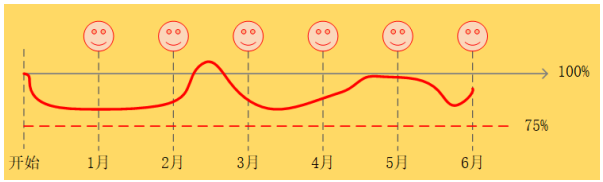

图 4：未敲入未敲出

2、FPGA 与 oneAPI 的优势

CPU（Central Processing Unit，中央处理器）的摩尔定律已入暮年，在高性能计算领域，CPU 的表现已经渐渐被 GPU（Graphics Processing Unit，图形处理器）、ASIC（Application Specific Integrated Circuit，专用集成电路）和 FPGA 等硬件超越。FPGA 常年来被用于 ASIC 的小批量替代品，以同时提供强大的计算能力和足够的灵活性，如图 5 所示。

CPU、GPU 都属于冯 · 诺依曼结构，指令译码执行、共享内存。FPGA 之所以比 CPU 甚至 GPU 能效高，本质上是无指令、无需共享内存的体系结构带来的福利。冯氏结构中，由于执行单元（如 CPU 核）可能执行任意指令，就需要有指令存储器、译码器、各种指令的运算器、分支跳转处理逻辑。由于指令流的控制逻辑复杂，不可能有太多条独立的指令流，因此 GPU 使用 SIMD（Single Instruction Multiple Data），单指令流多数据流）来让多个执行单元以同样的步调处理不同的数据，CPU 也支持 SIMD 指令。而 FPGA 每个逻辑单元的功能在重编程（烧写）时就已经确定，不需要指令。冯氏结构中使用内存有两种作用。一是保存状态，二是在执行单元间通信。由于内存是共享的，就需要做访问仲裁；为了利用访问局部性，每个执行单元有一个私有的缓存，这就要维持执行部件间缓存的一致性。对于保存状态的需求，FPGA 中的寄存器和 BRAM（Block RAM，片上内存）是属于各自的控制逻辑的，无需不必

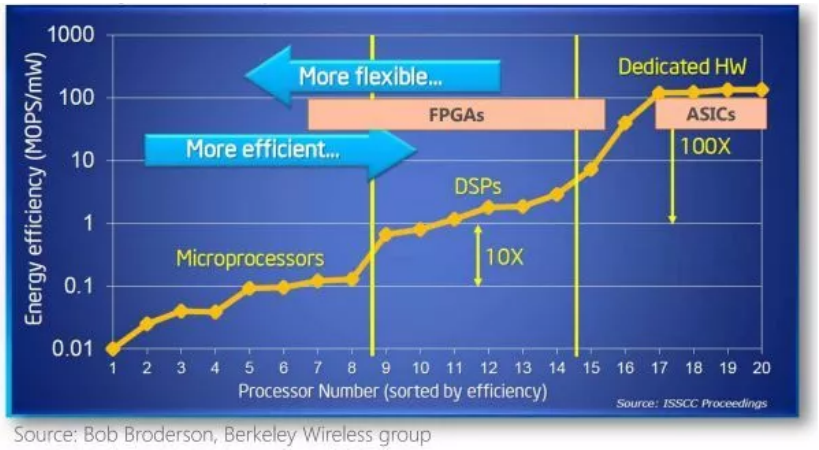

图 5：不同体系结构性能和灵活性的比较

要的仲裁和缓存。对于通信的需求，FPGA 每个逻辑单元与周围逻辑单元的连接在重编程（烧写）时就已经确定，并不需要通过共享内存来通信。

FPGA 同时拥有流水线并行和数据并行，而 GPU 几乎只有数据并行（流水线深度受限）。

例如处理一个数据包有 10 个步骤，FPGA 可以搭建一个 10 级流水线，流水线的不同级在处理不同的数据包，每个数据包流经 10 级之后处理完成，每处理完成一个数据包，就能马上输出；而 GPU 的数据并行方法是做 10 个计算单元，每个计算单元也在处理不同的数据包，然而所有的计算单元必须按照统一的步调，做相同的事情，这就要求 10 个数据包必须一起输入、一起输出，输入输出的延迟增加了。

当任务是逐个而非成批到达的时候，流水线并行比数据并行可实现更低的延迟。因此对流式计算的任务，FPGA 比 GPU 天生有延迟方面的优势，如图 6 所示。

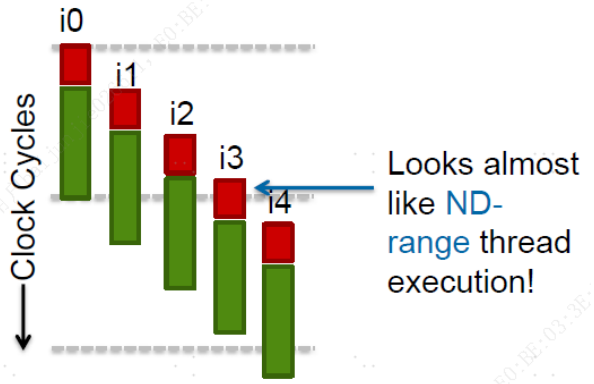

图 6：并行流水线

各体系架构性能数量级比较（以 16 位整数乘法为例）如表 2 所示。

期权计算不可能有闭合形式的解，而是通过用蒙特卡罗方法模拟了许多可能的路径，最终得到了一个预期的收益值。使用蒙特卡罗模拟需要生成高质量的随机数，并进行上千万点的模拟，传统的使用 CPU 来进行计算，耗时非常巨大，

表 2：各体系架构性能数量级比较

体系架构	吞吐量	延迟	功耗	灵活性
CPU	~1T	N/A	~100W	很高
GPU	~10T	~1ms	~300W	高
FPGA(Stratix 10)	~10T	~1us	~30W	高
ASIC	~10T	~1us	~30W	低

而 FPGA 通过使用通道以及循环流水线的排布，能够有效提升性能，减小计算延迟。

而传统的 FPGA 开发一般选择硬件描述语言（如 VHDL/Verilog HDL），开发周期长、难度大，对于使用高级语言进行开发的软件工程师而言，进入的门槛非常高。在开发 FPGA 时，需要硬件理解深刻，重点是需要非常详细的设计工作，合理规划硬件资源进行任务并行和数据并行的处理业务，包括处理的时序、RAM 的分配，还要经过一系列的仿真、综合等。

Intel FPGA SDK 提供了高效的使用高级语言开发 FPGA 的方式，通过 OpenCL 或 oneAPI 工具来进行 FPGA 开发。相比于 OpenCL，作为升级版，oneAPI 真正意义上实现了天下大同。oneAPI 编程模型简化了 CPU 和加速器的编程，基于 C++ 特性与 SYCL 并行性的标准跨体系结构语言 DPC++。DPC++ 支持主机和加速器的代码复用，使用单一的源语言，执行和内存依赖清晰地沟通。DPC++ 代码内的映射可用于将应用程序转换为在硬件（或一组硬件）上运行，从而最大程度地加速工作负载。主机可以简化设备代码的开发和调试，甚至在没有加速器的平台上也是如此。

图 7 所示为一个通过 DPC++ 语言开发的 oneAPI 简单应用，用来将数组的每个元素设置为其下标的值。可以看出，主机代码和加速器代码都组合在一个源文件中，使用的语法是标准的 C++，并通过 C++ 类来实现并行性。该示例的逻辑为：第 8 行和第 9 行创建了一个包含 16 个 int 元素的 buffer，第 11 行构造一个队列来表示主机到加速器之间的连接。创建队列后，调用形参为 lambda 函数的 submit() 成员函数向加速器提交工作，它在第 12 行创建一个访问器，使得可以在 buffer 中写入元素，在第 13 行调用 parallel_for() 函数来执行加速器上的代码。调用的 parallel_for() 函数有两个参数，一个参数是 lambda 函数，另一个是表示 buffer 中元素数量的范围对象“r”，lambda 在加速器上被该范围内的每个索引调用一次，通过使用在第 12 行创建的 out 访问器将一个值赋给 buffer。在调用 parallel_for() 之后，代码的主机部分将继续运行，而无需等待加速器上的工作完成，并在第 18 行创建一个构造函数 host_accessor 来读取 buffer 中的元素，这里 buffer 中的元素是由加速器写入的，所以在 parallel_for() 的数据传递完成之前，host_accessor 将被阻塞，加速器工作完成后，主机开始执行第 18 行之后的代码。

```
1.  #include <CL/sycl.hpp>
2.  #include <iostream>
3.
4.  constexpr int num=16;
5.  using namespace sycl;
6.
7.  int main() {
8.      auto r = range{num};
9.      buffer<int> a{r};
10.
11.     queue{}.submit([&](handler& h) {
12.         accessor out{a, h};
13.         h.parallel_for(r, [=](item<1> idx) {
14.             out[idx] = idx;
15.         });
16.     });
17.
18.     host_accessor result{a};
19.     for (int i=0; i<num; ++i)
20.         std::cout << result[i] << "\n";
21. }
```

图 7：oneAPI 开发示例

此外，oneAPI 编程模型提供了可以跨硬件目标使用的全面统一的开发人员工具组合，包括跨越多个工作负载域的一系列性能库。这些库包括为每个目标体系结构定制编码的函数，因此相同的函数调用可以在受支持的体系结构之间提供优化的性能，如图 8 所示，利用 oneAPI 编程模型的应用程序可以在从 CPU 到 FPGA 的多个目标硬件平台上运行。

与此同时，Intel 也在大力投入对 oneAPI 的研发，使其开发效率，编译性能，以及运算性能都在不断提高，oneAPI 的某些运算引擎甚至超过了硬件语言描述 DPS 的性能。使用 oneAPI 来通

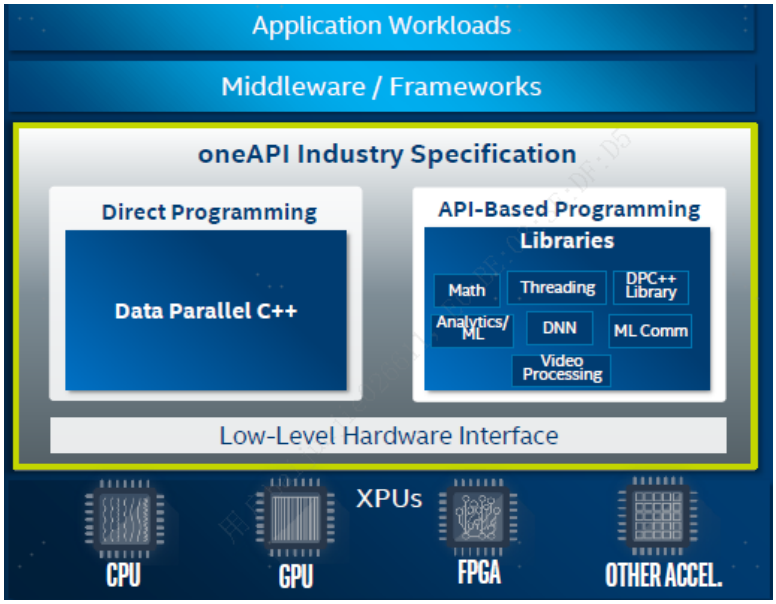

图 8：oneAPI 跨工作域

过 FPGA 进行期权定价加速，无论从效率还是性能上讲都是不二之选。

3、基于 oneAPI 期权定价设计

期权计算的流程主要可分为随机数生成与期权数值计算两部分，随机数部分又可分解为随机数初始化和随机数生成，数值计算部分可分解为定价和求和。使用 oneAPI 进行设计，每部分都可通过 Channel 利用 FIFO 队列将各 kernel 模块连接起来，达到流水线并行的效果，流程如图 9 所示。MT Initial 选择一个随机数种子，计算出梅森旋转链，放入 Channel 0；MT Generation 从 Channel 0 中取出梅森旋转链数据，计算出伪随机数，输入 Channel 1；Stock price Motion 从 Channel 1 中取出生成的随机数，利用定价模型计算出的结果输入 Channel 2；累加器 Partial Accumulate 从 Channel 2 中取出计算结果，累加求和，输出结果。

Mersenne Twister 初始化时，需要一个初始化种子，然后生成长度为 624 的梅森旋转链。因为旋转链上的后一个数据需要对前一个数据进行计算才能得到，所以旋转链的生成无法数据并行，可以选择流水线的方式进行优化。MT Initial 和 MT Generation 之间通过 Channel 0 传输梅森旋转链数据。一般在选择 Channel 数据大小和深度时，选择 2 的整数次幂。MT Initial 生成的旋转链长度为 624，可以选择每次传输旋转链中的 64 个或 128 个数据给 MT Generation。

MT Generation 的计算逻辑是：取出初始化的 624 长度的初始化旋转链，然后执行旋转算法（针对整个链），以后以 624 为周期，用梅森状态链每生成 624 个随机数，旋转一次，随后生成下一组 624 个随机数。同样，将生成的随机数通过大小为 64 或 128 的 Channel 1 传入到下一个 kernel 进行计算。欧式期权和雪球期权随机数生

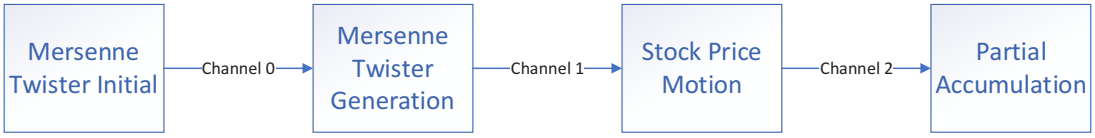

图 9：期权定价流水线并行

成的方法是一样的。

Stock Price Motion部分为最主要的计算部分。与上面逻辑相同，通过 Channel 进行数据读写，首先将 MT Generation 传入的随机数值域限定在0~1 之间，此时满足（0，1）上的均匀分布，随后通过 Box-Muller 算法将（0，1）上的均匀分布转化为标准正态分布，进行下面的计算。对于欧式期权，可直接使用 BS 公式进行定价，将结果写入 Channel 2 中，由于运算逻辑简单，可使用 NDRange 提升计算性能，每次下发 8192 个计算任务，充分使用流水线计算。对于雪球期权，在 BS 公式的基础上，还需要进行复杂的向量运算，来模拟三种不同的情景，所以每次展开一条蒙特卡罗路径进行模拟，将每条路径的模拟价格写入 Channel 2 中，每条路径内部的 for 循环可以使用数据并行来提高计算性能。

最后 Partial Accumulation 部分为累加求和，从 Channel 2 中读取出期权价格之和，写回 Buffer 中。对于欧式期权，每次发送 8192 个线程，所以需要读取完 8192 个数据；对于雪球期权，进行了 mc 条蒙特卡罗路径的模拟，所以需要读取完 mc 个数据。将和写回主机的 Result Buffer 中求取平均值完成最终的期权定价。

4、结果验证与分析

CPU 和 FPGA 在期权定价流程中有各自擅长的模块，本次验证对欧式期权和雪球期权定价最终性能在 CPU 和 FPGA 上进行综合对比。

测试验证对比环境：

CPU: Intel core i7 10700 @2.9GHz 8 cores

FPGA: Intel PAC D5005 with Stratix 10 GX FPGA

4.1 欧式期权性能分析

在相同参数与相同蒙特卡罗模拟次数情况下 CPU 与 FPGA 的对欧式期权的定价结果如图 10 与图 11 所示。

改变蒙特卡罗模拟次数，对定价性能进行比较，如图 12 所示，可以看到，模拟次数越多，FPGA 能够更大程度地释放性能。

FPGA 资源使用情况如图 13 所示。

4.2 雪球期权性能分析

同样，在相同参数与相同蒙特卡罗模拟次数情况下 CPU 与 FPGA 对雪球期权的定价结果如图 14 与图 15 所示。

改变蒙特卡罗模拟次数，对定价性能进行比较，如图 16 所示，同样，随着模拟次数的增加，FPGA 性能提升更加明显。

FPGA 资源使用情况如图 17 所示。

图 18 与图 19 分别为雪球期权价格与波动率 sigma 以及票息 coupon 关系的线性回归，计算符合预期效果。

```
Starting Computations
call = 0 ,DEVICE 0: r=0.08 sigma=0.21 T=0.2 S0=2.5110 K=2.6000 : Resulting Price is 0.087101
1 Devices ran a total of 1.67772e+07 Simulations
Throughput = 5.68 Million Simulations / second
```

图 10：欧式期权 CPU 定价结果

```
[root@localhost src]# ./eo262144.fpga
Starting Computations
call = 0 ,DEVICE 0: r=0.08 sigma=0.2064 T=0.2500 S0=2.5110 K=2.6000 : Resulting Price is 0.087101
1 Devices ran a total of 1.67772e+07 Simulations
Throughput = 33.71 Million Simulations / second
```

图 11：欧式期权 FPGA 定价结果

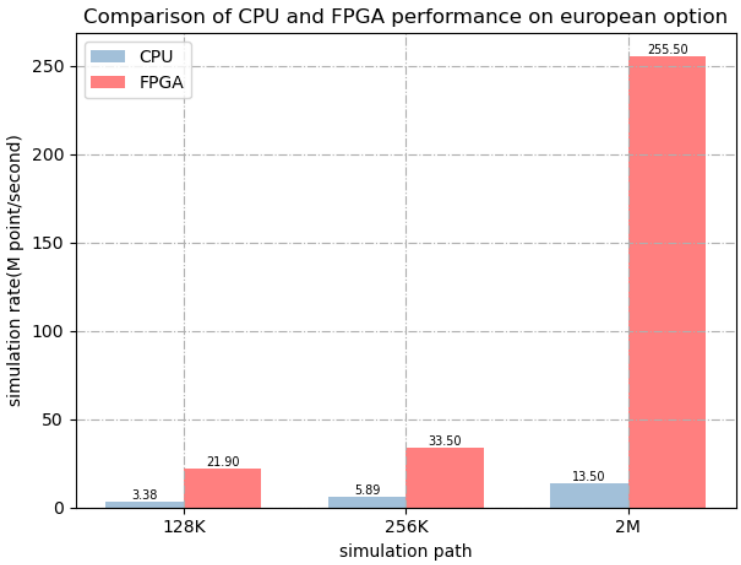

图 12：欧式期权性能对比

	ALUTs	FFs	RAMs	MLABs	DSPs
Static Partition	594280 (32%)	1182640 (32%)	3737 (32%)	0 (0%)	1779 (31%)
Board interface	594280	1182640	3737	0	1779
Kernel System	439225 (24%)	565715 (15%)	696 (6%)	2904 (3%)	1137.5 (20%)
Global interconnect	1289	11421	26	0	0
System description ROM	2	71	2	0	0
Pipe resources	99 (0%)	12534 (0%)	0 (0%)	212 (0%)	0 (0%)
black_scholes_kernel	357548 (19%)	436996 (12%)	533 (5%)	2546 (3%)	1136 (20%)
mersenne_twister_init_kernel	5861 (0%)	20224 (1%)	53 (0%)	6 (0%)	1.5 (0%)
mersenne_twister_generate_kernel	70877 (4%)	79652 (2%)	57 (0%)	134 (0%)	0 (0%)
accumulate_partial_results_kernel	3549 (0%)	4817 (0%)	25 (0%)	6 (0%)	0 (0%)

图 13：欧式期权 FPGA 资源使用情况

```
[root@localhost src]# ./snowball11011625.fpga
Starting Computations
DEVICE 0: r=0.036 sigma=0.130 T=0.50 S0=100.000 coupon=0.25 : The SnowBall Option Resulting Price is 0.04
1 Devices ran a total of 262144 Simulations
Throughput = 515508.80  Simulations / second
```

图 14：雪球期权 CPU 定价结果

```
Starting Computations
DEVICE 0: r=0.036 sigma=0.130 T=0.50 S0=100.000 coupon=0.250 : The SnowBall Option Resulting Price is 0.044858
1 Devices ran a total of 262144 Simulations
Throughput = 22533.20  Simulations / second
```

图 15：雪球期权 FPGA 定价结果

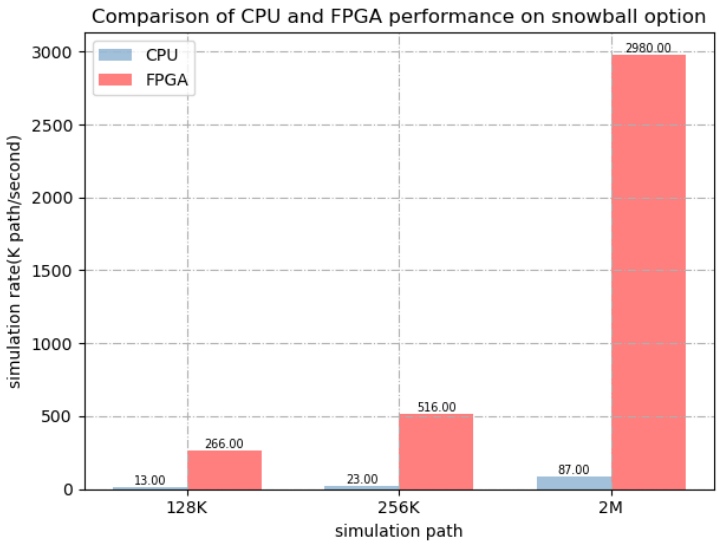

图 16：雪球期权性能对比

	ALUTs	FFs	RAMs	MLABs	DSPs
Static Partition	594280 (32%)	1182640 (32%)	3737 (32%)	0 (0%)	1779 (31%)
Board interface	594280	1182640	3737	0	1779
Kernel System	707696 (38%)	938406 (25%)	2523 (22%)	3460 (4%)	2408.497 (42%)
Global interconnect	1289	11421	26	0	0
System description ROM	2	71	2	0	0
Pipe resources	187 (0%)	24870 (1%)	52 (0%)	316 (0%)	0 (0%)
mersenne_twister_init_kernel	9846 (1%)	38669 (1%)	104 (1%)	6 (0%)	1.5 (0%)
mersenne_twister_generate_kernel	142498 (8%)	140446 (4%)	109 (1%)	134 (0%)	0 (0%)
accumulate_partial_results_kernel	3550 (0%)	4821 (0%)	25 (0%)	6 (0%)	0 (0%)
pv_kernel	550324 (29%)	718108 (19%)	2205 (19%)	2998 (3%)	2406.997 (42%)

图 17：雪球期权 FPGA 资源使用情况

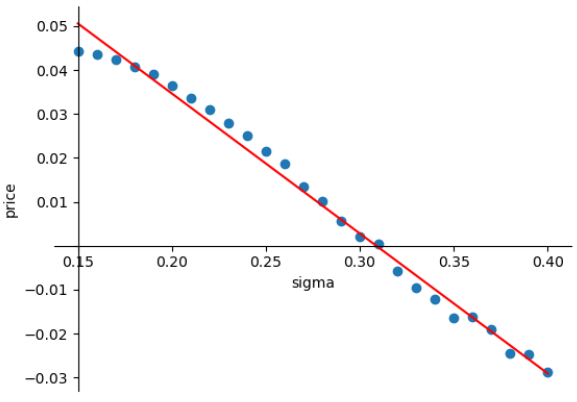

图 18：雪球期权价格与 sigma 的线性回归

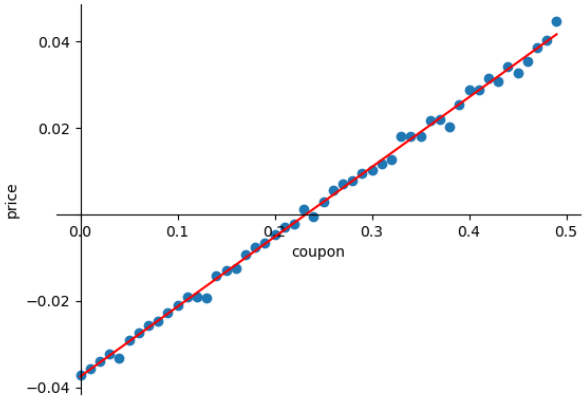

图 19：雪球期权价格与 coupon 的线性回归

结论

本研究作为使用 oneAPI 在金融领域进行加速的初步探索，使用 DPC++ 语言，采用流水线并行与数据并行方式，设计出多种期权定价模型，并分别通过对欧式期权定价与雪球期权定价的对比分析，相比于传统软件处理方式，使用 FPGA 处理的综合性能均可获得较大的提升，并且随着模拟次数的增加，获得更加精确的期权定价结果的同时，FPGA 能够更大程度地释放性能，在模拟 2M（2*1024*1024）条蒙特卡罗路径时，分别可获得 20 倍左右与 30 倍左右的性能提升。国泰君安在金融硬件加速领域深耕多年，后续将继续精进，使用 oneAPI 与 FPGA 在金融硬件加速领域进行更多的研究与探索，为业内持续输出经验。

探索与应用

证券运维系统自动化代理平台建设实践

肖钢、徐志彬、柴晨、王军、喻文强、张皓凌 / 中信建投证券股份有限公司
E-mail：chaichen@csc.com.cn

在全球数字化经济的大浪潮下，人工智能、区块链、云计算和大数据等技术的发展不断冲击着证券行业的运维模式。随着运维体系的复杂化和服务器的差异化加剧，运维成本不断增长，运维人员的技术要求更加苛刻，因此，智能化、高可靠、统一的自动化代理平台成为证券运维体系的一项重点工作。

中信建投证券自动化代理平台通过构建统一的运维服务入口，将运维系统有机结合在一起。近年来，微服务架构与异步通信技术快速发展，并逐渐成为系统建设的主流技术，微服务架构与异步通信技术能够有效提高系统稳定性与可扩展性，为自动化代理平台建设提供了成熟的解决方案。本文通过介绍自动化代理平台的探索和实践，针对运维体系数字化转型中遇到的外部数据规范不统一、服务器差异化、运维系统复杂化等问题，分享解决方案和实践经验，助力证券行业数字化发展。

1、概述

在智能运维时代，自动化代理平台是必不可少的网络运维系统。面对众多运维子系统，系统基本是“相互孤立、独自运行”的，并没有统一的代理平台对接庞杂的服务器，各个运维子系统在执行业务操作的时候，往往自研一套服务器交互系统独自进行，既造成了公司内部研发资源的浪费，同时这些交互系统无论是系统架构可用性还是稳定性，可扩展性上都差强人意。甚至有些

业务场景下，还需要运维人员人为干预，手动的在服务器上执行运维指令，无形增加了运维人员的工作难度，加大了运维成本。

自动化代理平台将运维子系统和服务器有机的连接在一起，通过自动化代理平台统一对服务器进行动态管理，同时使用高效的异步接口为运维子系统提供服务。自动化代理平台作为外部系统和内部服务器之间通信的桥梁，我们设计了文件传输、命令调用等基础功能，在此基础上，又将扩展出信息采集、数据备份、应用部署和代理节点状态监控等一系列功能。为了系统的稳定运行，需要对代理的稳定性、安全性进行有效地把握，所以对代理的性能的并发量、吞吐量、安全性又有一定的要求。此外，还需要对代理的各个客户端进行统一管理，实现代理状态监控和自动修复。

目前，运维系统逐渐走向智能化、标准化，自动化代理平台可节省大量人力运维成本，并且可提供高效、稳定的运维服务。如何利用云计算技术与微服务架构，构建高可用、可扩展的自动化代理平台，成为证券公司亟需解决的问题。本文将介绍中信建投证券对于自动化代理平台的架构探索，并阐述架构探索中的实践与经验。

2、自动化代理平台架构

2.1 总体设计

自动化代理平台采用微服务架构，系统中的各个微服务可被独立部署，各个微服务之间是松耦合的。每个微服务仅关注某项独立的功能模块。整体架构具有快速部署、高扩展性、高容错性和去集中化等特点，主要由六个层级构成：

（1）用户层

用户层是自动化代理平台的操作入口，用户可以通过将运维管理系统与自动化代理平台对接来处理自身业务诉求，也可以通过访问自动化代理平台的 Web 页面进行人机交互。为了便于用户系统对接用户层，我们提供了可直接集成的自动化代理平台工具包，用户通过 API 指令调用自动化代理平台工具包，并由自动化代理平台工具包来完成与自动化代理平台系统的交互。

（2）网关层

网关层可以对外暴露聚合 API，屏蔽内部微服务的微小变动，保持整个系统的稳定性。

在运维体系中，通常会有众多终端服务器，他们提供不同类型的服务，且通常分布在不同的物理机房中。想要从用户层精准的操作某一个机

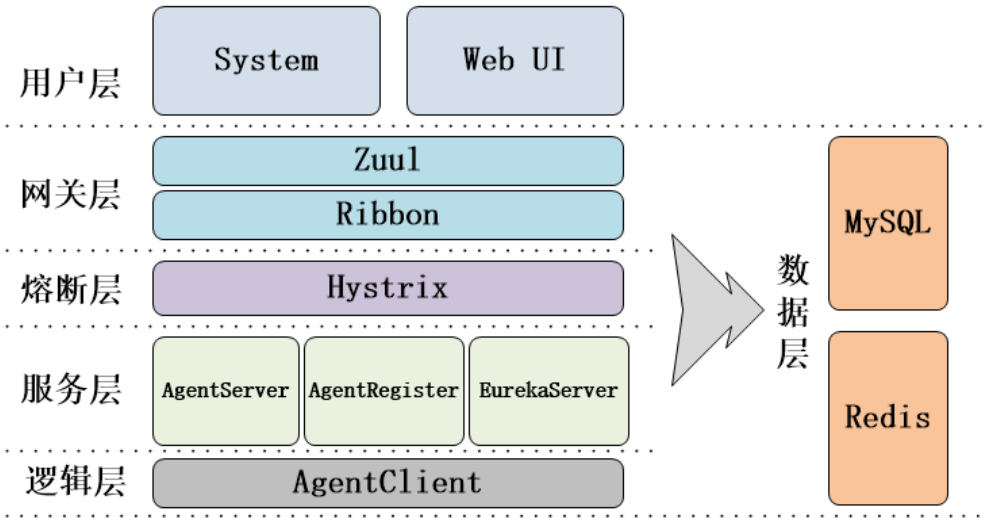

图 1：自动化代理平台层级结构图

房的某一台服务器通常是很困难和繁琐的。自动化代理平台采用了二级代理和动态路由的方案解决了这个痛点问题，通过在物理机房部署二级代理，将机房内的服务器使用 Netty 连接在一起，再通过动态路由的方式将用户请求路由到各二级代理，最终通过 Netty 完成指定服务器的业务操作。

当然这只是网关层众多功能中的一部分，它还可以做负载均衡，统一鉴权，协议转换，监控监测等一系列功能。

（3）熔断层

分布式系统环境下，服务间依赖非常常见，一个业务调用通常依赖多个基础服务。对于同步调用，当某服务不可用时，会导致上级服务的请求线程被阻塞，当有大批量上级服务请求时，最终可能导致整个系统资源耗尽，无法继续对外提供服务。并且这种不可用可能沿请求调用链向上传递，导致雪崩效应。因此，为了构建稳定、可靠的分布式系统，熔断层必不可少，熔断层能够对对来自依赖的故障进行隔离，当依赖服务不可用时，当前服务启动自我保护功能，从而避免发生雪崩效应。

（4）服务层

服务层负责提供可复用的服务，通过集群方式实现高可用，用户层通过分布式服务调用框架访问到服务层，分布式服务调用框架会在网关层实现软件负载均衡，并通过服务注册中心服务 EurekaServer 对提供服务的服务器进行心跳检测，发现有服务不可用，立即通知客户端程序修改服务访问列表，剔除不可用的服务器。

AgentServer 在架构上充当了二级代理的角色，通过 AgentServer 将用户层和逻辑层连接在一起，AgentServer 在功能上是自动化代理平台的核心服务，通过 Netty 服务端的形式与逻辑层的服务器中的 Netty 客户端进行连接，将用户层请求处理过后交由逻辑层进行执行。

AgentRegister 主要有两个作用，一是作为 Netty 客户端的注册中心，对 Netty 连接状态进行监控管理，二是为网关层提供动态的 Netty 连接信息，是实现动态路由的关键。

（5）逻辑层

逻辑层包含特定于业务领域的逻辑，是最终进行业务操作的环节。各服务器通过 Netty 客户端与服务层建立连接，接收服务层请求并完成相应业务逻辑，对于耗费资源类操作部分通过服务层运算完成后再交由逻辑层进一步处理，避免服务器负载过高影响其他交易系统的操作。

（6）数据层

数据层是操作数据（数据库或者文本文件等）的操作层，为业务逻辑层或控制层提供数据服务。对于使用频率较低，数据量庞大的数据，例如审计信息、历史数据等，使用关系型数据库 MySQL 进行管理，对于使用频率较高，同时对使用场景的响应时间要求较为严格的关键数据，在存储 MySQL 的同时还运用到了缓存数据库 Redis，一来提升数据查询的响应速度，二来对 MySQL 进一步保护，避免出现缓存击穿和雪崩，三来提供分布式锁，避免集群场景下的服务间状态不感知导致的业务故障。

2.2 技术框架

自动化代理平台技术选型为 Spring Cloud 微服务架构和 Netty 框架。

Spring Cloud 是一系列框架的有序集合。它利用 Spring Boot 的开发便利性巧妙地简化了分布式系统基础设施的开发，如服务发现注册、配置中心、消息总线、负载均衡、断路器、数据监控等。Spring Cloud 作为一套成熟的分布式服务治理的框架，已得到了广泛的应用。

Netty 是一款用于开发高性能网络系统的 Java 框架，它封装了网络编程的复杂性，使得网络编程更容易的实现，同时 Netty 作为高度可伸缩的、异步的、事件驱动的网络编程框架，完美契合了自动化代理平台对多服务器管理、快速响应、异步调用的场景需要。

自动化代理平台采用网关加二级代理的通信方式，用户侧请求进入网关后动态路由到对应物理机房的二级代理，再通过二级代理与服务器之间的 Netty 连接进行进一步业务操作。同时 Netty 的连接信息通过注册中心进行管理，并动态刷新到网关，使得网关能将用户请求正确路由到对应二级代理。如图 2 所示。

二级代理的方式解决不同物理机房间服务器网络不互通的安全需求，机房中使用 Netty 架构构建二级代理和服务器的连接。基于 Netty 无连接数据报套接字支持和相较 Java 核心 API 更高的吞吐量以及更低的延迟，使得二级代理能同时处理成千上万的并发客户端。客户端创建消息处理的入站处理器流和出站处理器流，并向服务端发起建联请求。二级代理作为服务端创建消息处理的入站处理器流和出站处理器流，并通过 Channel 完成与客户端的对接。在业务处理时，二级代理通过目标索引获取到对应服务器的 Channel，使用事件对服务器进行业务指令下发。

注册中心用于统筹全局的服务器信息，作为特殊的 Netty 客户端与各物理机房的二级代理服务端建连，实时同步服务器信息并将数据写入本地数据库中。同时将二级代理与服务器之间的基本信息存入缓存数据库，并将该缓存数据与网关实时共享。

自动化代理平台为用户提供 Restful 和 API 两种类型的调用接口，Restful 接口主要用于操作指令，如服务升级、信息采集等，API 接口提供文件的上传下载。Restful 接口进入网关后，网关根据指令的服务器信息从缓存中匹配对应的二级代理，并负载均衡的将请求路由到指定二级代理。API 接口需要用户系统导入自动化代理平台为用

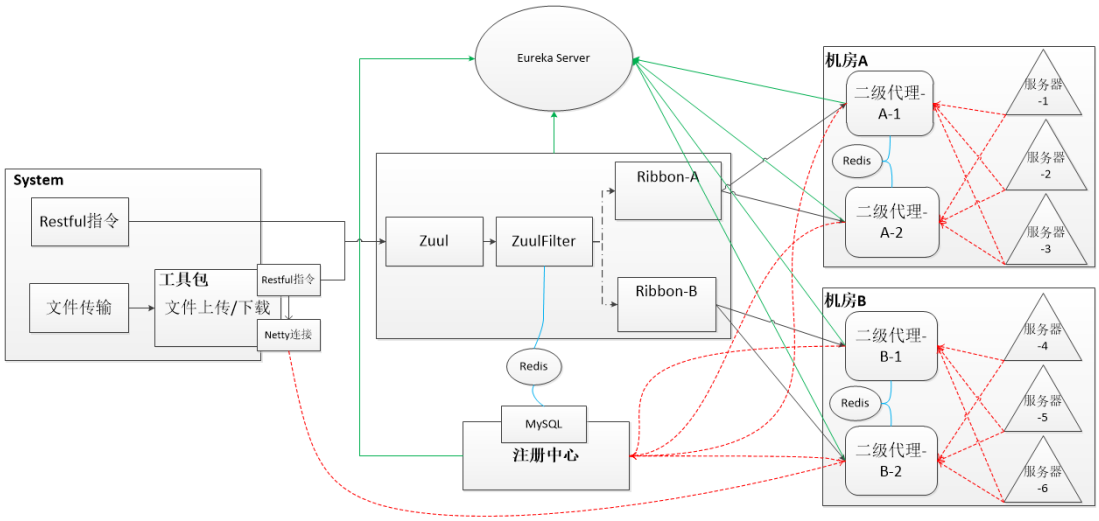

图 2：自动化代理平台架构图

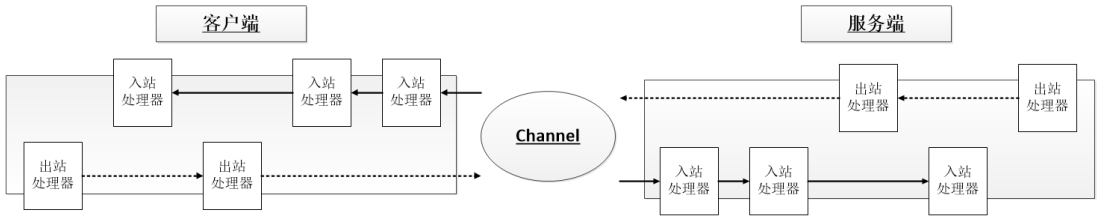

图 3：自动化代理平台消息流转图

户系统开发的工具包，该工具包首先通过 Restful 请求从网关处获取到服务器所对应的二级代理信息，然后创建 Netty 客户端与二级代理建立连接，二级代理客户端采用零拷贝的方式作为用户端和服务器间的桥梁将文件进行分片传输。其中零拷贝是一种使用在 NIO 和 Epoll 传输时使用的特性，它可以快速高效的将数据从文件系统移动到网络接口，而不是将其从内核空间复制到用户空间。

2.3 部署方式

自动化代理平台作为运维系统的操作处理平台，对接了多个运维子系统并且面临大量的 QPS，同时还管理着近万台服务器，因此高可靠、高可用的部署方案是不可或缺的。

自动化代理平台的微服务均采用集群方式部署，其中网关层使用 Nginx 和 Zuul 集群组合的方式对外提供稳定的网络服务。利用 Eureka 搭建微服务集群的注册中心，EurekaServer 提供服务注册和发现，这使得系统中的微服务可以方便的进行动态扩缩容，当业务量增加导致微服务出现性能瓶颈时，通过新实例的上线便可被 EurekaServer 自动将其扩容到服务列表中并将节点信息实时同步到网关层，网关层将新增节点加入到负载均衡循环列表中路由网络请求。对于不同物理机房的二级代理服务，虽然从业务和开发角度属于相同的服务，但在自动化代理平台中我们将其划分为不同的微服务，网关层对不同的微服务创建不同的 Ribbon（一个基于 HTTP 和 TCP 的客户端负载均衡工具），对指定的微服务集群使用 Ribbon 进行负载均衡的路由分发。

二级代理场景中服务器和二级代理通过 Netty 进行长连接，由于二级代理属于集群化的可动态变化的微服务，因此服务器需要动态的感知二级代理的实例，并分别与其建立 Netty 长连接。二级代理各实例通过共享的数据库中同步比对服务器的连接状态，保证所有实例与服务器的连接状态是一致的。在文件传输场景，用户端创建 Netty 客户端与二级代理建立连接，在完成文件传输时断开连接，释放冗余的资源占用。

缓存数据库是维持自动化代理平台工作的重要环节，采用“一主二从三哨兵”高可用解决方案，其部署架构主要包括两部分：Redis 哨兵集群和 Redis 数据集群。如果主实例宕机，哨兵主动将一台从机升级为主机继续对外提供数据服务。在业务层面，缓存数据库除了提供二级代理场景下的实例间数据共享外，还提供了实例间的分布式锁，保证 Netty 连接数据的最终一致性。

3、系统分析与实践建议

3.1 系统分析

中信建投证券在自动化代理平台持续探索，在系统架构和功能模块上不断演进与扩展，取得了一定的成效。目前的自动化代理平台能够大大降低运维系统的使用难度，释放运维人员的繁琐劳动，从架构设计上能够有效改善系统的运行效率与稳定性，具体体现在以下几个方面。

（1）安全性

自动化代理平台运行在系统的内网环境，只有网关层提供内网其他系统的访问，避免了业务服务被直接访问攻击的风险。网关层采用用户认证以及 token 校验，对恶意访问的用户或 ip 地址进行黑名单处理并上报告警。

（2）可靠性

采用无状态化的集群部署方式，保障系统有效的利用服务器资源，多实例的服务模式以及主备容灾的数据模式有效分担了系统的计算压力，避免出现 CPU 或内存资源出现满负荷的状况。微服务在微服务注册中心注册后由网关进行服务转发，并且具有降级、熔断和限流等功能保障系统持续提供服务。高可用的数据库与中间件提供完善的数据备份和可靠机制，系统可靠性增强显著。

（3）稳定性

对外网关采用 Zuul 集群的形式，有效提升外部的访问吞吐量，系统内使用负载均衡的消息分发策略，将计算压力分流到多实例服务中。将热点数据存贮到缓存数据库中，降低了外部访问对系统的压力，提升了请求相应速度。微服务的功能单一、业务独立使得整个系统耦合性极低，模块间调用关系更清晰，并可进行链路跟踪与分析，显著提高开发效率与系统运行监控能力。

（4）易用性

统一的对外网关，有效了屏蔽了用户层和服务层直接的状态感知，用户只需关注自身的业务请求指令，无需关注服务器的物理位置，网关层会通过自定义过滤器功能将业务请求指令路由到对应的服务层。为了便于用户系统对接，我们提供了封装完善的工具包，用户系统可以很容易的集成，并直接通过 API 指令完成自动化代理平台提供的业务功能。

3.2 实践建议

自动化代理平台作为运维系统的核心服务之一，是简化运维复杂度、降低人工干预风险、提升运维人员工作效率的重要环节。如何更切实的完成这些目标是我们努力探索的方向，在实践过程中总结了几点建议，并规划进一步完善自动化代理平台。

（1）数据可视化

可视化数据报表比传统的数据报表更有表现力，借助 Web UI 的窗口将系统中的服务器关系以及运行状态转换成视觉或表格的格式，以便可以分析数据和数据项或属性之间的关系与特性，方便用户直观分析大量视觉信息，检测一般规律和趋势。

（2）异地容灾

自动化代理平台拥有大量的运维系统对接，对自身的容灾要求更为严格，通过异地容灾的部署方式将主备两个物理站点隔离开来，预防自然灾害等造成的系统瘫痪。将自动化代理平台分别部署在不同站点，主站点对外提供服务，备站点定时从主站点同步数据备份，在主站点心跳停止后自动升级为主站点并向运维系统发送主备倒换通知，进而接管自动化代理平台业务。

（3）智能化改造

随着业务量的不断增加，运维人员的操作请求也会不断增加，系统智能化是提升业务精准度和降低人力成本的有效途径。使用自动化任务流，对于异常任务进行智能化回滚或重试，探索智能机器人与人工的协同工作模式，以最大化用户满意度，同时提高处理效率。

4、总结与展望

为提升用户的满意度，应对快速增长的业务请求，中信建投证券以自动化为导向，微服务架构为标准，针对自动化代理平台不断探索。本文针对中信建投证券在自动化代理平台的探索与实践进行阐述，对系统架构演变进行详细介绍。此外，本文还介绍了自动化代理平台建设的成果，从系统功能设计角度阐述系统的模块设计与架构调优。最后，本文分析了自动化代理平台所带来的成效，并介绍了系统建设的实践经验。

未来自动化代理平台还有广阔的探索空间，一方面随着人工智能技术在证券行业的应用逐步深化，运维系统将逐步向智能化、自动化方向演进。另一方面，随着证券业务越来越多，系统间交互越来越复杂，搭建完善的自动化代理平台的诉求将更加强烈，自动化代理平台作为很好的切入点，在提升用户服务体验以及构建开放生态上，将发挥出更大的价值。未来自动化代理平台将以云原生和智能化为方向持续改进优化，以为用户提供高质量服务为最终目标不断努力。

基于上证云的数据跨境流动管理方案研究与实现

操浩东[1]、刘政言[1]、何雷[2]/[1]上交所技术有限责任公司 云基础设施运营部 上海 200120
[2]中金所数据有限公司 数据研发部 上海 200120
E-mail：hdcao@sse.com.cn

随着金融领域不断对外开放，我国已全面取消外资持有境内证券、基金公司股权比例限制，外资金融机构正加速进入中国市场，随之而来的数据跨境流动问题也日益凸显。因此，如何安全、合规地进行数据跨境流动已成为外资金融机构以及监管部门关注的核心问题。本文在研究数据跨境流动国内外政策以及现状的基础上，探索一种基于“上证云”的数据跨境流动管理解决方案——虚拟数据室，即通过数据加密、权限控制、操作留痕、关键字检索等技术手段，解决外资金融机构日常数据跨境流动涉及的相关问题，同时利用统一日志、数据接口等技术手段便利监管与审计。

1、概述

随着数字经济及全球化的深入发展，数据已成为全球经济的基础性生产要素，同时也是国家重要的战略性资产。在数字化时代，数据作为新的关键生产要素，只有实现在更大范围的流动共享，才能更好地发挥对经济增长、社会发展、全球化进程的推动作用。

我国自 2020 年取消境外金融机构持股比例限制后，境外金融机构在境内控股证券、基金管理公司逐渐增多，客观上有基于并表管理、业务协同、统一风险控制等目的开展数据跨境流动及信息系统跨境部署（以下简称“双跨”）需要，也需要通过“双跨”落实对外开放的目标。同时，伴随着全球普遍加强网络数据安全、个人隐私保护以及我国陆续发布数据安全有关法律法规，对

如何在安全、合规前提下支持外资机构数据跨境流动需求提出了更高要求。

1.1 国内外相关政策

目前，全球正积极推进网络空间主权、数据安全、个人隐私保护等相关立法进程，但各国立法纷繁复杂，针对数据跨境流动也尚未形成统一、对等的监管协作机制。

2018 年，美国发布《澄清域外合法使用数据法》（CLOUD Act，以下简称《云幕法案》），赋予美国政府调取存储于他国境内数据的法律权限，无论数据是否存储在美国境内，服务提供者需依法进行信息披露。他国政府想调取存储在美国的数据，须通过美国“合格外国政府”的审查（大部分国家都不满足审查标准）。

2018 年 5 月，欧盟发布《通用数据保护条例》（GDPR），对通过“充分性认定”国家（大部分为欧盟成员国）的数据跨境流动实行统一、对等的监管要求，减少或取消成员国内对数据流动的地域限制，从而推动欧盟范围内数据的自由共享。对于未通过“充分性认定”的国家，在数据共享过程中则需满足欧盟颁布的标准合条款（SCC）、集团企业规则（BCR）等诸多法律法规限制。

俄罗斯等国家基于维护国家安全的历史传统和现实中的网络数据安全威胁，明确提出公民数据的存储和处理必须在俄罗斯境内进行。

我国基于“维护国家安全及公众利益、保护个人隐私”等目的，在服务对外开放大局的前提下，高度关注与国外监管机构划分合理监管边界，防范“长臂管辖”。在现行的法律中，《网络安全法》将“网络空间主权”置于国家安全同等重要的地位，同时提出了重要数据本地化存储等有关要求，通过强化地域管辖实现对数据主权的保护；本次修订的《证券法》，提出了数据出境需经国务院有关机构或部门同意等要求；《反洗钱法》提出了非依法律规定，不得向任何单位和个人提供反洗钱相关客户身份和交易信息等有关要求；《个人信息保护法》进一步明确了个人信息、重要数据的定义以及数据出境需经严格的评估等要求；《数据安全法》，提出了数据分类分级管理、数据出境评估、加强国际合作等一系列要求，保障数据依法有序自由流动；新出台的《数据出境安全评估办法》提出了数据出境安全评估的具体要求，规定数据处理者在申报数据出境安全评估前应当开展数据出境风险自评估等一系列要求。

1.2 数据跨境流动需求

无论是境内外资机构基于发挥境外集团在全球范围内的资产配置作用、复用集团先进系统及经验等目的，还是境外集团借助境内外资机构更好的了解中国市场，发掘中国市场蕴含的潜在机会等需求，双方均有较大的数据流动需求。目前，金融机构跨境流动的数据主要可以分为以下几类：一是基于业务协同需要，以满足集团化运营管理为目的的业务数据和管理数据，如跨境并购时需与境外团队共享的概要性尽职调查信息、用于风险敞口计量的数据、证券自营业务交易数据、符合我国有关法律法规要求并取得员工同意的员工个人信息等。二是基于公司财务并表管理或流动性风险计量需要，需定期通报股东单位的结果类、汇总类信息。三是基于复用经验、提升项目质量的目的，供全球业务领域专家做专业研判的数据。四是基于满足境外监管要求需报送的数据，如出于满足反洗钱、反恐怖等司法目的的数据、为协助境外集团满足巴塞尔协议资本计量的要求，需报送风险损失等数据。

1.3 数据跨境流动存在的问题

1. 数据跨境传输手段落后。目前，金融机构主要使用邮箱、文件传输系统，或者直接通过数据接口等传统方式进行数据跨境传输。随着数据跨境流动场景的规模化和复杂化，此类方式缺乏足够的管控手段覆盖敏感、复杂数据的跨境流动风险，也无法满足防范数据泄露、传输留痕、配

合审计等合规需求。

2. 缺乏高效的审计方式。根据监管要求，金融机构应对跨境数据进行分类分级管理，建立完善的日志、记录等留痕管理及防篡改机制，并对相关内容定期开展审计。由于数据的类型、敏感度不同，金融机构往往采用多种数据传输方式，相关操作的留痕记录相对分散，且留痕标准参差不齐，导致审计成本较高，审计效率低下。

3. 缺乏有效的监管手段。在互联网以及其他技术手段的支持下，数据跨境流动更加便捷，但随着外资金融机构数据跨境流动场景日益增多，监管方面缺乏有效的技术管控手段及时感知全市场的数据跨境流动风险，导致监管效率低下，一旦发生风险，容易出现爆点多、燃点低的特征。

2、数据跨境流动管理探索

2.1 场景分析

在全球普遍加强网络空间主权、数据安全、个人隐私保护以及数据跨境流动场景日益复杂化、多样化等背景下，数据跨境流动管理应聚焦于在安全、合规的前提下保障外资机构的数据跨境流动需求，同时兼顾效率和成本。以下将从五个方面简要分析数据跨境流动管理场景需兼顾的几个问题：

1. 提供多种数据跨境流动方式，支持多种数据出境场景。外资金融机构应根据数据分类分级管理要求，使用与数据敏感性、重要性相匹配的传输方式。因此，解决方案应支持直接传输、模板传输、受限访问等多种跨境流动方式，且相关数据的操作权限均可灵活配置，实现数据分类分级管理以及多种数据跨境流动需求。

2. 降低合规成本，提升效率。在技术的赋能下，数据跨境流动及数据访问往往具有瞬时性，同时数据的规模化及复杂化已必将带来合规要求的推陈出新，而传统线下或半线下的合规方式难以及时、有效的识别风险。因此，解决方案在设计时应考虑在代码中嵌入合规及监管要求，真正实现“规则即代码”，对多种跨境流动方式提供统一的留痕标准，在便利监管和审计的同时有效降低成本。

3. 开放数据接口，便利监管机构。数据跨境流动表面属于技术问题，背后则涉及个人隐私保护、社会公众利益、国家安全等，监管机构需立足于整个行业进行数据跨境流动的监管。因此，解决方案需设计成开放接口，利于对接监管端集中平行监测平台，以便监管机构及时掌握金融机构的数据跨境流动情况，有效解决监管效率及成本问题。

4. 降低系统改造运维成本，提供安全、合规、可靠服务。随着数据跨境流动场景日益复杂化、多样化，外资金融机构加强对跨境数据流动的合规管控措施，对其信息系统的改造维护成本也随之提高。解决方案部署于行业云，符合行业标准与安全规范要求，用户资源可按需弹性扩展，提高升级运维效率和灵活性，能有效降低经营机构改造、使用、运维成本。

2.2 方案探索

由于外资金融机构存在开展业务多种多样，内部 IT 建设能力参差不齐，数据接口规格难以统一等特点，为外资机构提供数据跨境流动管理的解决方案初衷并不是提供一种大而全且满足所有机构需求的“万能服务”，而是要在满足监管合规前提下，降低外资机构接入与使用成本，并且作为服务提供方应具备一定行业中立属性，与服务使用方无商业利益往来或业务合作，以免影响该服务的公信力与监管中立性。

此外该方案应根据数据分类分级管理、最小必要原则、白名单管理制度、与风险特征相匹配的增强型管控措施等合规要求，结合外资金融机构展业特点，通过数据加密、权限控制、操作留痕、关键字检索等技术手段支持多场景下的数据跨境流动，并通过统一日志、数据接口等技术更

好地支持审计和监管。

对此，我们设想的外资金融机构数据跨境流动解决方案核心是基于上证云部署的“虚拟数据室”服务。该服务可根据相关法律法规要求，按照“事前可存、事中可控、事后可查”原则，对数据的采集、存储、流动等各环节进行加密、权限控制、操作留痕等管理，为机构提供安全、合规的一站式数据跨境流动管理服务。具体来说，境内外资机构将出境信息上传至上证云“虚拟数据室”服务端，境外用户通过客户端进行受限操作。同时，监管端可通过相关接口及时掌握数据跨境流动情况。“虚拟数据室”服务设想系统架构如图 1。

2.2.1 服务端

“虚拟数据室”主要为跨境数据提供脱敏、加密、存储、赋权和留痕等功能，覆盖跨境数据收集、存储、加工、使用等各个环节，主要功能包括：

数据分类分级。根据外资经营机构开展业务的类型、海外总部对其经营管理数据的需求以及我国跨境数据领域的法律法规行业标准，制定跨境数据的数据模板，对跨境数据传输的元数据、数据字典、数据标签等进行标准化规约，便于监测及数据分析；

跨境传送通道管控。提供云端文件交换模块和用户端数据交换前置模块，在核心的数据跨境传送通道上实现了精准管控；

跨境数据留痕。对于通过“虚拟数据室”完成的数据跨境活动，系统会对已经完成跨境动作的数据进行备份和标记，实现对应的审计留痕；

敏感信息扫描与出境监控告警。对数据跨境传输行为进行内容扫描，根据事先定义的规则确定是否存在敏感信息，并对风险事件及时发起监控告警；

数据脱敏。服务提供预定义或用户自定义的数据脱敏规则，在发起数据跨境传输行为前，用户可以选择执行脱敏动作，避免触发敏感信息扫描告警；

统一日志审计。服务对数据跨境行为进行跟踪，记录下跨境行为的发生时间、操作人员、数据类型、数据分级分类、原始数据等信息，并生成操作日志，以便监控层的日志审计模块进行查询、汇总和生成报告。

监控预警。监控模块可对用户数据操作的全流程监控，包括账号、源地址、路径、操作类型、时间、所属机构等每个环节进行日志留痕，提供完整的操作溯源能力，便于日志调取和合规审计；针对非法操作，监控模块通过设置告警规则、告警阈值，以短信、邮件等多种形式向用户发出告警，及时监测数据资产，确保安全可控。

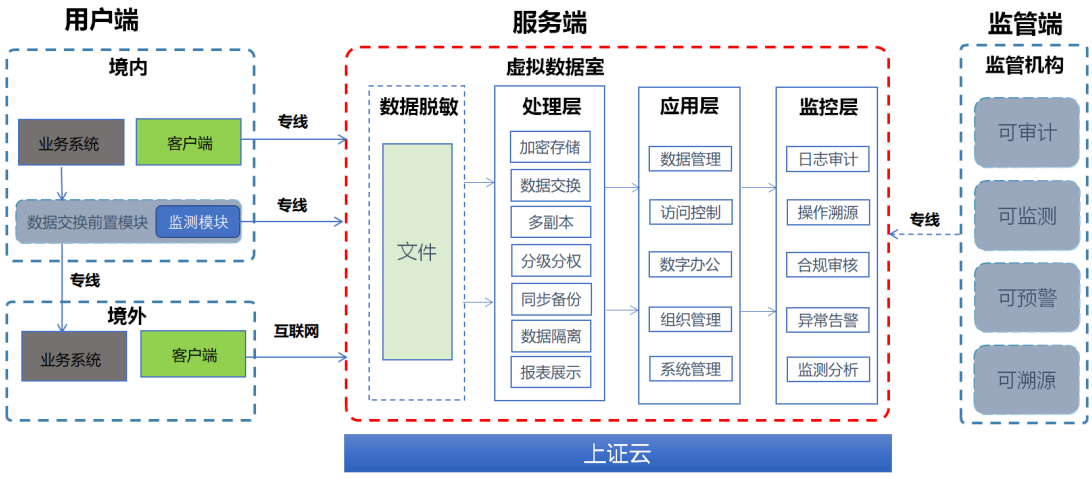

图 1：“虚拟数据室”系统架构图

2.2.2 用户端

境内外资机构可根据情况选择文件上传、录入、系统对接等多种方式数据传入方式，根据不同的信息类型、敏感程度选择直传、模板传输、受限访问等多种跨境流动方式，为境外用户分配受控的访问权限。在接入方式上，境内外资机构可通过专线（如证联网）、VPN、互联网等线路接入，境外用户则通过互联网接入，在保障数据传输安全前提下，满足不同接入需求。服务支持PC端、网页端和移动端访问，可提供数据交换模块前置于机构内部网络，该前置模块主要满足于机构内网信息系统与其海外总部间数据直传场景，可根据合规和监管要求进行监测、预警与备份。

2.2.3 监管端

“虚拟数据室”服务对跨境流动数据的存储、流动、使用等进行全方位、统一的留痕管理，可为审计、监管等提供直观查阅界面，并可提供API接口，进行满足特定规则的审计、监测、预警和溯源功能实现。虽然目前针对外资金融机构数据跨境监管的行业细则未出台，但长远来看，具备能够对全行业外资机构进行统一监管审查的平台仍具有参考意义，按照“事前可存、事中可控、事后可查”的设计原则，一套统一的、基于全行业的平行监测平台可及时感知机构的数据跨境流动情况，便于执法机构监管检查、有效降低执法成本，提高监管效率。

2.2.4 上证云

“虚拟数据室”服务底座基于上证云。上证云是上交所技术有限责任公司面向证券、基金等金融机构推出的云服务平台，其依托上交所技术T3+等级数据中心，使用两地三中心（上海和北京）高可用架构，拥有成熟稳定的云技术平台、完善的用户服务体系及丰富的安全运营管理经验，严格遵循国家相关部门监管政策，符合行业标准与行业安全规范要求，为金融机构提供技术领先、稳定可靠、安全合规的云计算服务。基于上证云可对“虚拟数据室”服务的整体容量、集群健康状态、网络带宽、iops、延迟、存储池、硬件服务器以及对象存储等服务状态进行监控和运维，确保服务健康与安全。

3、总结和展望

目前，外资金融机构数量及业务规模尚处于

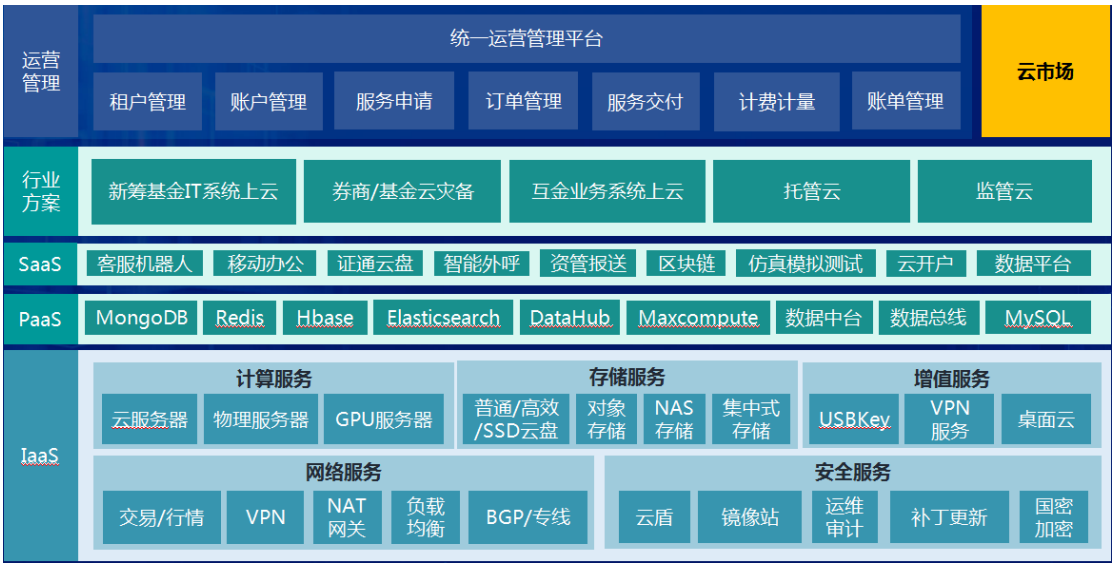

图2：上证云产品及服务能力

初始阶段，随着对外开放的深入，数据跨境流动场景日益复杂化、多元化，同时，内资金融机构在境外展业过程中也同样面临境外监管机构对数据收集、传输、使用等的各项监管要求。因此，“虚拟数据室”服务将进一步拓展使用场景，更好地支持金融机构在“走出去”和“引进来”过程中涉及的数据流动需求。未来将做好以下研究与准备工作：

积极探索境外信息技术系统或模块的运行模式，支持其本地化部署。外资金融机构出于自身需要及展业特点，有使用境外集团的信息系统或模块的现实需求，过程中往往涉及大量敏感的数据跨境流动。为此，我们将积极研究此类技术系统特性，为其境内部署提供安全、稳定的运行环境，将需要跨境流动的敏感性数据转变为敏感度较低的结果类、汇总类信息，在避免敏感数据的跨境流动的同时，极大提升境内系统与境外系统进行信息共享的便利性，有利于在符合现行法律法规相关要求的前提下更好的实现外资机构自身需求。

2、融合深化“虚拟数据室”服务，打通云上服务全流程管理。伴随行业机构云上服务需求愈发多样，上证云可根据行业机构需求，提供办公系统、邮件系统、风控系统、业务系统、资管数据报送系统、投行底稿管理系统以及其他业务系统云服务，全方位、多层次、大广度覆盖行业需求。研究将“虚拟数据室”服务组件化，根据需要嵌入机构用户的各类应用系统中，直接参与数据的全生命周期，打通云上产品服务全流程管理，全面参与外资金融机构信息系统能力建设，深入满足用户合规需求。

3、引入境外相关规则，适时开放数据接口，探索跨境监管协作技术实现方式。目前各国对数据跨境流动尚未形成统一、对等的监管协作机制，我们将加强对国内外相关政策以及各国对数据跨境流动监管方式的研究，将境外监管经验及数字空间治理规则融入“虚拟数据室”服务，适时开放相应的技术接口，为推动跨境监管协作做好技术准备。

4、加强前沿技术储备，满足不同应用场景。探索运用系统跨境部署、支付标记化（Payment Tokenization）、区块链、隐私保护集合求交（Private Set Intersection）、联邦学习等前沿技术，实现对个人、企业和监管三方数据隐私保护和数据应用之间的平衡，打造全行业通用解决方案，有效释放行业数据红利。

安信证券网络系统自动化运维平台建设实践

梁德汉、何洲星、武孟军 / 安信证券股份有限公司
E-mail：liangdh@essence.com.cn hezx@essence.com.cn wumj@essence.com.cn

本文介绍了安信证券建设网络自动化运维平台的实践经验，针对网络日常运维工作中涉及的重复性高、或涉及大批量操作对象的操作，进行了多种方式的自动化尝试和探索。经过几年长期坚持不懈的努力，一个可弹性扩展、功能完备的网络系统自动化运维平台初具雏形，不仅可以自动化处理流程类申请引发的各类网络日常操作变更，还可以协助网络管理员自动化处理各类人工难以完成的运维工作和批量操作。极大提升了工作效率，有效降低人工操作在网络日常运维中的各种潜在风险。

1、引言

作为 IT 系统运维的一部分，网络运维工作大致包括三部分内容：系统建设、系统监控和系统变更。其中，网络系统建设属于一次性的工作，而系统监控和变更则贯穿于网络系统的整个生命周期，也是网络日常运维工作的主要内容。

网络运维自动化，就是要实现网络系统的监控和日常变更自动化。相较于其他 IT 系统，得益于网络简单管理协议 SNMP 标准的制定和普及，网络监控自动化实现得最早也最成熟，各种基于 SNMP 协议的网络管理软件得到普遍应用，实现了整个网络系统的运行性能的自动化监控，基本上满足了网络系统日常监控需求。

然而，网络日常变更工作的自动化却是困难重重，虽然近年来出现了许多基于 Python 的自动

化运维工具，诸如 Ansible 或 SaltStack，但是和网络工程师们心目中所期望的“自动化运维”情景还是相差甚远。可以说，网络日常变更 90% 的工作，仍然需要网络工程师通过终端登录设备的命令行模式，逐行将命令输入的方式实施。

本文所涉及的网络运维自动化，即是指网络日常变更这部分工作的自动化实现。同时，作为监控系统的补充，也包括少部分属于监控系统未能实现的监控功能，例如特定设备性能指标的日常巡检。网络系统的建设、日常运行性能指标监控，不属于本文自动化运维讨论的范畴。

2、网络运维工作特点

网络日常运维工作种类繁多，涉及到的网络设备更是五花八门，有路由器、交换机、防火墙、负载均衡等等。有的运维操作重复频率高，几乎每天都有；有的操作涉及到的对象数量庞大，工作量大。从操作结果来看，有的操作变更了设备配置，有些操作仅仅是察看设备状态，不改变设备配置。

（一）流程类配置变更

此类网络变更通常由申请人通过各类管理流程发起，经过层层审批后，最终流转到网络运维人员，根据具体需求进行变更处理。典型的例子如防火墙访问权限开通，物理机上架时交换机端口 VLAN 划分等。

流程类配置变更的特点是，变更由流程触发；申请人需要提供一定的配置参数，比如源，目的地址，交换机端口等；涉及到的操作对象数量不多，但是同类的流程数量非常多，每天重复不断，配置操作琐碎繁杂，手工操作极易疲劳出错。

（二）查询类操作

有时候运维人员需要查询现有设备的配置情况，再决定后续的配置操作。比如，在一台防火墙上配置一条访问策略前，需要检查相同的策略配置是否已经存在；设备健康巡检时，需要输入察看类的指令，根据返回结果检查自己关注的文本信息。

查询类操作的特点是，不涉及设备配置比变更，但是需要检查大量的文本信息，并从文本信息中筛选出感兴趣的信息。在查询两台主机之间的访问关系时，需要处理的设备可能不止一台，需要将访问路径中每台设备的检查结果综合考虑后才能得出结论。对网络运维人员来说，这类操作是非常劳神费力的。

（三）定期执行的任务

需要定期执行，每天，或每周、每月都有可能。例如设备配置文件备份，通信线路性能巡检，设备健康检查，设备信息定期采集等工作。

定期执行类的操作不涉及配置变更，但是涉及的操作对象数量庞大，通常是几百甚至上千。人工操作需要耗费大量人力和时间，且容易出错和漏操作。

（四）批量设备操作

通常为执行某一特定任务而引发。例如密码到期更新设备密码，修改某一范围内的设备访问控制列表，增加特定路由条目等操作。

此类操作需要修改设备配置，同样涉及的操作对象数量庞大。更困难的是，不同的设备下发的配置脚本可能不同。手工操作，同样需要耗费大量人力和时间。

（五）其它

另外，有一些运维辅助类的操作，例如各种防火墙策略的管理操作，网络应急操作等。

总的来说，上面列举的运维操作，要么重复性强，要么涉及的操作对象数量庞大，如果能从传统的手工操作转化为自动化，不仅可以提高运维效率，减少错误，降低运行风险，而且可以节

省大量的人力和时间成本，获取最大化收益。

3、网络自动化运维平台

2019 年，迫于应用系统访问权限开通流程手工处理效率低下的压力，我司已经组织力量，自行开发了一套防火墙策略自动化开通的系统，成功将防火墙策略开通由传统手工模式转型为自动化处理，并在 2020 年第 3 期《技术交易前沿》作了题为《网络自动化运维系统自主研发的探索与实践》的分享。

有了以前的自动化系统开发经验，我们决定在现有的开发基础上，继续完善系统功能，打造一个网络系统自动化运维平台，除了已有防火墙策略自动化开通功能，计划实现下列功能：

（一）安全策略查询功能

在全网范围内，实现访问权限的任意查询功能。具体说来，假定 h1 和 h2 是两台主机，则可以查询：

① h1 能否访问 h2 的指定服务（例如 HTTP）？

② h1 可以访问 h2 的哪些服务？

③ h1/h2 能访问哪些主机的哪些服务？

④ h1/h2 的指定服务能被哪些主机访问？

⑤ h1/h2 能访问哪些主机的指定服务？

⑥ h1/h2 的哪些服务能被哪些主机访问？

策略查询功能可用于申请人在提起流程前确认访问策略是否已经开通，避免重复提流程；应用系统新增客户端时，往往需要查询已有的客户端已经开通了哪些访问权限作参考；还可用于访问故障排除，高危端口攻击链分析，查找潜在风险主机。

（二）防火墙策略管理

防火墙安全策略管理，主要实现下列功能：

① 根据指定条件，筛选出一台指定防火墙中符合条件的所有策略；

② 分析一台防火墙中策略之间的包含或相同关系，查找无用的地址对象和服务对象；

③ 批量策略迁移。根据指定条件，从防火墙 A 中筛选出符合条件的所有策略，进行指定的转换后，将筛选出的所有策略迁移到防火墙 B 中；

④ 垃圾策略的识别。防火墙中无用策略既视为垃圾策略。识别垃圾策略，是根据一定时间段内特定策略的命中匹配数确定。例如，如果 3 个月内，某条策略的命中数为 0，则可以认为该策略为垃圾策略，后续公示后可作删除处理。

（三）统一地址对象

统一地址对象功能，目的为了简化防火墙策略申请和部署。主要解决：

① 个人办公 / 交易终端的地址改变，导致原来申请的访问权限需要全部重新申请一遍。这样不仅增加了工作量，还会增加垃圾策略数量；

② 应用系统内，一组相同功能的主机，往往具有相同的访问策略。当需要增加组中成员时，往往需要先查询现有主机的访问权限，然后再申请新增成员的访问权限，费时费力；

③ 一组用于特定目的的主机 IP，数量多，需要在多台防火墙进行部署。如果需要增减组成员时，需要在多台设备上进行操作，非常麻烦。

统一地址对象功能，将上述主机定义为逻辑地址对象，申请人可以直接使用地址对象来申请访问权限。这样，当地址对象的成员变更，成员增减时，只需要操作地址对象即可，所有用到该地址对象的安全策略，跟随变更，极大地减少了工作量。

（四）交换机端口配置

该功能可以根据需要，在物理机上架时，对选定的交换机接口进行配置。可以将接口划分到指定 VLAN，或配置成 trunk 模式。

和防火墙策略配置功能类似，交换机接口

配置是基于申请人发起的物理主机上架流程进行的，属于重复性高的日常维护类操作。机房管理人员负责将需要的参数，如指定交换机管理 IP、交换机接口、vlan 号、接口要求速率等参数提交，系统在指定变更时间窗口内，统一读取，根据参数生成不同的配置脚本，然后下发到交换机设备。

（五）定期执行类任务

定期执行类的任务包括网络设备定期配置文件备份，重要核心设备接口日常运行参数检查（光衰，双工模式等），交换机端口工作状态采集等工作。

此类操作大多属于在设备上执行查看类命令，然后分析返回结果，获取关注的信息，再判断结果。由于需要执行的查看类命令各种各样，不同的设备命令格式，返回信息都不相同，因此实现的关键是要能够自行配置和定义执行任务所需的各种参数，这样才能满足当有新的任务需求时，能够快速部署实施。

（六）网络设备批量操作

网络设备批量操作，通常是指对大批量设备进行相同或类似的配置变更，典型的例子如数据中心所有网络设备的更新登录密码。自动化实现的思路和基本操作步骤如下：

① 在纳管的设备库中筛选出一批目标设备；

② 配置需要下发的指令序列。如果选中的设备使用的命令序列不一样，可以有多个命令序列；

③ 如果有多个命令序列，则需要配置设备选择命令序列的条件；

④ 命令序列中如果有变量，例如不同的网络中心可能密码不一样；增加路由时的命令中下一跳网关不一样等等，都可以通过定义变量来实现。每个变量，都需要对应定义一个取值条件，用来最终确定命令行的最终形式；

⑤ 根据上述配置，为每台设备生成特定格式下发命令脚本。命令脚本就是一个普通的文本文件，可以进行检查和手工修正；

⑥ 检查脚本无误后，下发到设备。

上面的操作场景，下发到设备的命令序列相对固定的。还有一种复杂场景，假设有一个批量操作需求：将所有交换机中运行状态为 down 的接口，配置为 shut down 状态。这种操作下发到设备的命令序列，就和单台设备中接口状态有关了。就是说，在产生命令序列前，需要从操作对象取回一些参数，这些参数作为生成命令序列的输入，再最终生成正确的命令序列。

除了上述主要功能外，系统还需要具备设备管理功能，即对纳管网络设备添加、删除、登录方式和密码的管理等；支持 IPv6，即能够处理 IPv6 安全策略的处理；应急操作的自动化，既执行事先定义好的应急操作脚本；与外部系统的接口，可接受其它系统发送过来的流程参数，对其它系统提供策略查询，网络接口状态查询的服务等等功能。

4、系统架构及主要模块流程

（一）系统架构

整个系统由操作界面、事务处理和数据库三部分组成。其中，操作界面实现系统管理和用户输入申请流程功能；数据库保存各种系统数据，包括系统自身使用的初始化配置信息，用户申请的流程信息等；事务处理则完成各种系统功能，它由一组互相独立运行的服务组成，每个服务完成不同的系统功能。事务处理的启动可以由定时器触发，也可以由操作界面的命令按钮触发。

图 1 所示为系统的逻辑架构图。

系统核心功能在业务处理模块中实现。各个业务模块相互独立，互不影响，单个功能模块可以随时启动和停止，提供了一种类似“微服务”的架构，各个模块通过数据库和文件服务器共享数据。这种架构的特点是灵活且容易扩展，只要

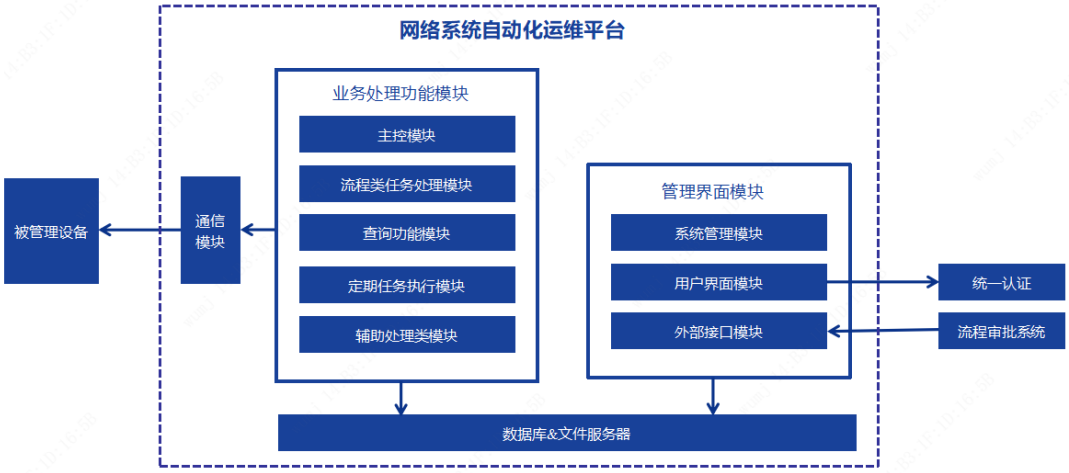

图 1：网络系统自动化运维系统逻辑架构图

由新的业务需求，只需开发新的功能模块并添加进去即可。

（二）访问权限申请处理流程

申请人通过流程审批系统入口，输入要求的参数并提交。其中，所有的参数被保存到自动化系统的流程数据库中，流程在流程审批系统中继续流转直至审批完毕，审批结果会传输到自动化系统。自动化系统中的每个提交的流程，根据不同的审批结果，有“待审批”、“审批通过”、“审批未通过”等几个状态。

凡是审批通过的流程，自动化系统在每天指定的变更时间窗口内，间隔一定的时间，读取状态为“审批通过”的流程，按照图 2 所示步骤进行处理：

（三）交换机端口配置

交换机端口配置完成物理主机上架时接入

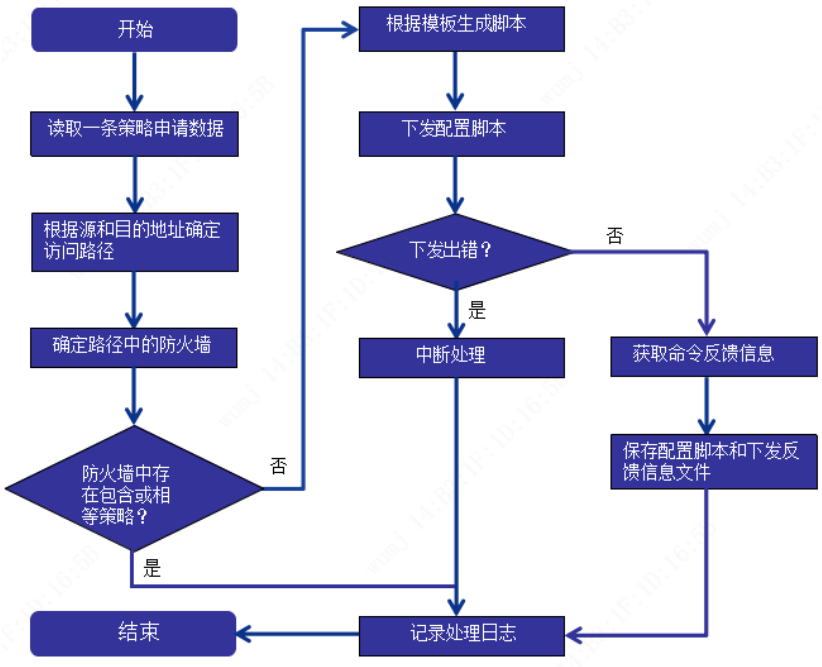

图 2：访问权限流程处理

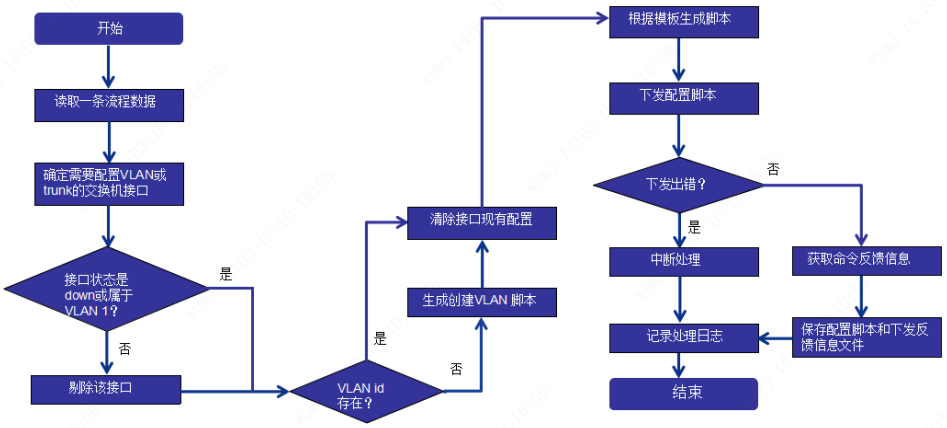

图 3：交换机端口配置流程处理

交换机的端口配置，包括将交换机指定端口划分到指定 VLAN，或将指定端口配置为 trunk 模式。同时，还要考虑是否有指定速率需求等因素。

同样地，自动化系统只保存完成配置需要的流程编号、选中的交换机端口、VLAN id 等参数。这些参数申请人员在流程审批系统中输入，并由流程审批系统通过外部系统接口传给自动化系统。

自动化系统在每天指定的变更时间窗口内，间隔一定的时间，读取流程数据，按照图 3 所示步骤进行处理：

（四）策略查询

假定需要查询主机 H1 能否访问 H2 的 TCP 80 端口，处理思路是首先确定 H1 访问 H2 的完整路径中经过了几台防火墙，并查询每台防火墙中是否都开放了 H1 能否访问 H2 的 TCP 80 端口的策略，如是，则满足访问条件。简单起见，这里只介绍单台防火墙设备中查询是否满足 H1 访问 H2 的 TCP 80 端口的策略，且不考虑 NAT 的情况。

首先按顺序比较防火墙中每条策略，只要存在一条源地址包含 / 等于 H1，同时目的地址包含 / 等于 H2，同时服务包含 / 等于 TCP 80 端口，并且安全域、动作都满足条件的策略，即可以认为该防火墙满足条件。

由于防火墙匹配策略时是按照先后顺序进行的，因此要考虑动作是“禁止”的策略。如果先匹配到了 1 条动作为禁止访问的安全策略，既可以终止查询，认为该防火墙不满足访问条件。

图 4 所示是在单台防火墙设备中查询是否有满足条件策略的处理流程：

5、系统运行效果

在克服了人手不足、疫情影响等不利因素后，经过近两年的艰苦努力，基本上实现了预期目标，一个功能完备的网络系统自动化运维平台初具雏形，日常运维工作中，涉及到重复性强、或操作对象数量庞大的操作类型，自动化覆盖率达到 90% 以上。以下是自动化运维平台功能以及日常应用中实际例子展示，因访问权限自动化开通系统在以前的文章中已经由详细介绍，这里不再讲述。

（一）策略查询

策略查询可以查询当前防火墙上主机之间的访问策略开放情况。根据查询模式的不同，分为六种查询模式；根据指定主机所处交易网、非交易网和互联网不同，提供多种查询范围。图 5 所示为系统提供的策略查询模式。

图 6 所示是查询办公网的一台指定主机（10.

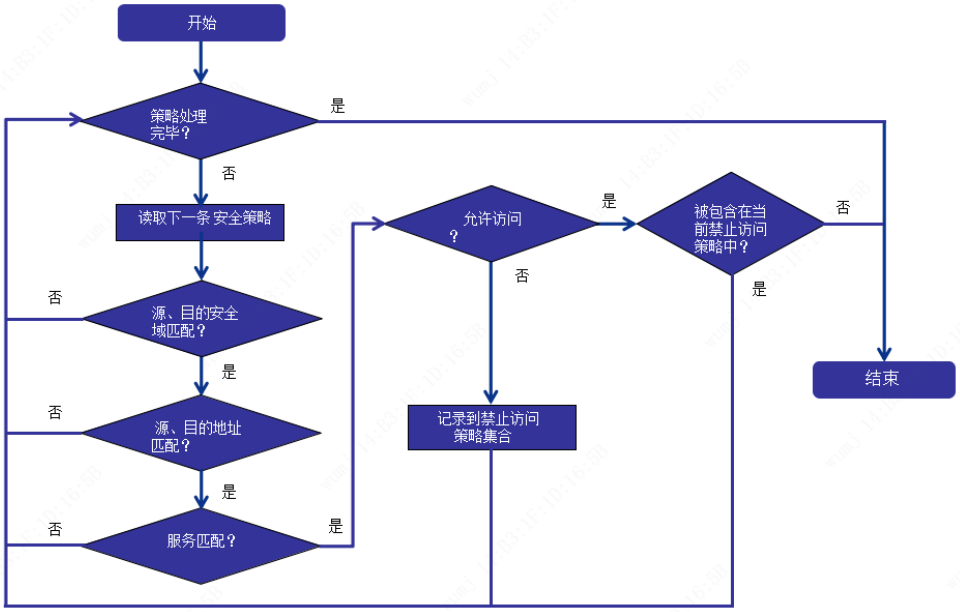

图 4：策略查询处理流程

图 5：查询模式

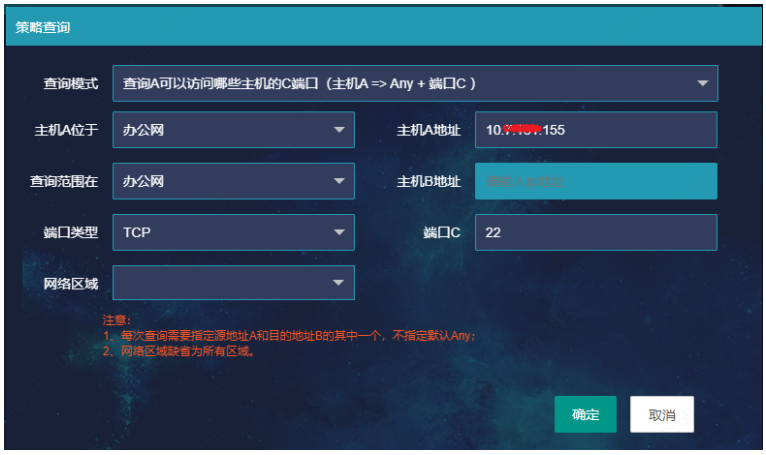

图 6：查询操作

x.x.155），能访问办公网内哪些主机的 22 端口的操作界面。

图 7 所示是查询结果的一部分，列出的主机都开了 TCP 22 端口服务，且指定主机具有访问权限。

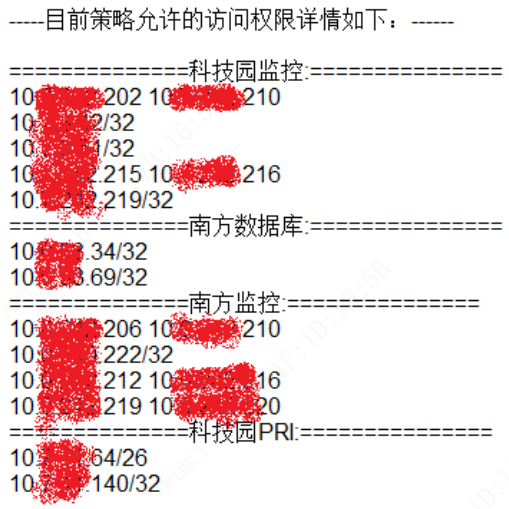

图 7：策略查询结果

（二）交换机端口自动化配置

因物理机上架流程在 CMDB 系统中流转，因此交换机端口配置流程中的参数由申请人在 CMDB 系统中输入并提交，如图 8 所示。

每个工作日的下午 4 点开始，系统自行扫描数据库，读出需要处理的参数，生成交换机配置脚本保存，下发后，将下发结果保存到另外一个下发结果文件中。

该模块自 2022 年 10 月份试运行，至今处理了近 200 条流程，配置端口约 700 个，可以配置指定端口到某指定 VLAN，或配置为 trunk 口。为确保配置的交换机端口准确性，系统提供给一线人员选择的可用交换机端口，必须满足连续两天状态为 down。

图 9 所为一份根据配置参数生成的配置脚本文件样例。

```
default interface Eth1/35
interface Eth1/35
switchport
switchport access vlan 2080
no shut
exit
default interface Eth1/37
interface Eth1/37
switchport
switchport access vlan 2080
no shut
exit
default interface Eth1/39
interface Eth1/39
switchport
switchport access vlan 2080
no shut
exit
default interface Eth1/41
interface Eth1/41
switchport
switchport access vlan 2080
no shut
exit
default interface Eth1/32
interface Eth1/32
switchport
switchport mode trunk
switchport trunk allowed vlan 32-254,301-331
no shut
exit
```

图 9：交换机端口配置脚本文件

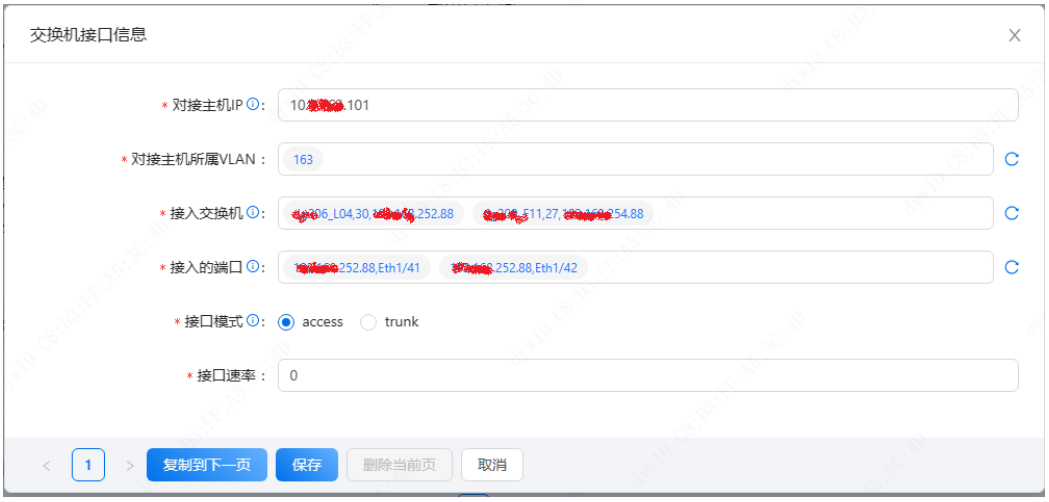

图 8：CMDB 交换机接口参数输入界面

图 10 所示是一份下发结果文件样例。

```
S-N9K-N07-05U-S(config)#
default interface Eth1/40
S-N9K-N07-05U-S(config)#
interface Eth1/40
S-N9K-N07-05U-S(config-if)#
switchport
S-N9K-N07-05U-S(config-if)#
switchport mode trunk
S-N9K-N07-05U-S(config-if)#
switchport trunk allowed vlan 32-254,301-331
S-N9K-N07-05U-S(config-if)#
no shut
S-N9K-N07-05U-S(config-if)#
exit
S-N9K-N07-05U-S(config)#
default interface Eth1/42
S-N9K-N07-05U-S(config)#
interface Eth1/42
S-N9K-N07-05U-S(config-if)#
switchport
S-N9K-N07-05U-S(config-if)#
switchport mode trunk
S-N9K-N07-05U-S(config-if)#
switchport trunk allowed vlan 32-254,301-331
S-N9K-N07-05U-S(config-if)#
no shut
S-N9K-N07-05U-S(config-if)#
exit
S-N9K-N07-05U-S(config)#
Copy complete, now saving to disk (please wait)...
Copy complete.
S-N9K-N07-05U-S#
```

图 10：配置脚本下发反馈文件

（三）定期执行类任务

定期执行类任务目前完成 / 每天：

- 纳管设备配置文件备份
- 路由器 / 交换机物理接口信息采集
- 指定的设备巡检任务
- 指定的清理指令

目前纳管的设备主要为我司三个数据中心的近 600 台防火墙、交换机和路由器。物理接口信息的采集主要完成接口的工作状态、所属 VLAN 等基础信息，为其它应用提供数据支持；指定设备巡检任务，是对重要设备进行的日常巡检，对监控系统的一种补充。例如，重要通信线路接口的错包率、双工模式；光接口的光衰指标检查等。指定的清理类指令，是每天对特定设备执行的一种“无害化”指令。例如，为防止操作人员打开了设备的 debug 功能忘记关闭，可以每天在指定时间段内执行 1 条设备关闭 debug 功能的指令。

巡检类任务实际上是在设备上执行指定的查看类指令，然后对返回的结果进行分析，取回感兴趣的信息进行分析，并将巡检结果记录在巡检报告中。配置一个巡检任务的界面如图 11 所示：

上述配置的巡检任务，是检查指定交换机的指定接口 eth1/1，检查项为该接口的 CRC 参数和双工工作模式。其中，CRC 参数为实数类型，值不等于 0 即为异常，双工模式是字符串类型，值不等于 full-duplex 或 Full-duplex 即为异常。

另外，采集到的基础信息，还可以进一步做

图 11：配置一个巡检任务

“增值化”处理。例如，可以将昨天状态为 up，今天状态为 down 的接口信息筛选出来，也可以将状态为 err_disable 的接口筛选出来，提供给技术人员做进一步分析处理。

（四）策略管理

防火墙策略管理实现了垃圾策略清理，敏感策略筛选，策略批量迁移和策略优化分析等功能。绝大部分策略管理的功能是基于防火墙配置文件进行操作的，因此可以不限制操作时间段。图 12 所示为策略管理操作界面。

1、策略筛选

策略筛选功能，可以在指定防火墙中，根据事先定义的筛选条件，找出满足条件的策略。最常见的应用场景是，当网络结构发生变化，一个网段不再使用，那么这个网段有关的安全策略理论上都成了垃圾策略，都应该清理掉。另外，出于安全考虑，我们希望找出一些目的地址是 Any，或服务是 Any，或服务是一些高位端口的安全策略进行安全评估。

图 13 所示为筛选策略输入筛选条件的系统界面。

首先需要指定防火墙，然后输入筛选条件。通常，筛选出的策略需要做进一步的操作，例如删除，这时，可以将选中的策略提取关键字，比如策略 ID，和指定的前、后缀字符串组成删除命令，这样就可以很容易地顺带生成删除策略的脚本。目的安全域，源、目的地址，服务端口以及策略动作，都可以做为筛选的条件设定，设置的多个条件是与的关系，只有满足全部筛选条件的策略才会被选中。

源、目的地址作为筛选条件时，可以指定一

图 12：策略管理界面

图 13：策略筛选操作

个地址集合，设置策略地址等于或包含指定地址，或指定地址包含策略地址的条件。还可以限定策略中对应地址包含的地址个数，以提高匹配精确度。

假定因网络拓扑变化，地址段 192.168.1.0/24 这个网段取消，需要将源地址全部包含在 192.168.1.0/24 这个段的策略挑选出来并删除，则按图 13 设定条件筛选策略即可。

再假定删除策略的命令格式如下：

```
delete rule01
```

其中，delete 为删除策略命令关键字，rule01 是策略 ID，则前缀字符串设置为 delete，后缀设置为空，既可以根据所有筛选出的策略，顺带生成删除策略的脚本文本。

2、批量迁移

在设备更换、网络拓扑变更等情况下，通常需要将原有设备中的一部分安全策略提取出来，并将其迁移到另外一台设备中。手工迁移策略的做法通常是简单粗暴编辑设备配置文件，提取策略，再拷贝到目标设备中。因为很多安全策略中涉及到源、目的设备中的地址对象、服务对象等配置情况，因此手工方式不仅仅效率低下，且极易出错。自动化系统根据设定的策略迁移条件，代替人工自动完成上述工作。图 14 所示为策略批量迁移操作界面。

首先需要设定源、目的防火墙 IP，再设定源设备选择策略条件，即选择哪些策略需要迁移，设置条件同“策略筛选”。然后设置变换条件，即允许将迁移的策略做一定的变换，可以变更源、目的安全域，源、目的地址和服务端口。图中所示为将迁移策略中的源地址做转换：设定一个地址集合，迁移后的策略中源地址可以排除这个地址集合，也可以只保留这个地址集合，排除其它地址。

假定想要将一台防火墙中，策略中源安全域为 trust，目的安全域为 untrust 的策略全部迁移到另外一台防火墙中，同时，迁移后的策略中源地址为 192.168.1.0/24 这个网段内的地址去掉，保留其它地址，则筛选条件中设定源、目的安全域分别是 trust 和 untrust，变换条件中设置源地址限定值为 192.168.1.0/24，操作模式为“排除”即可。

假设源设备中有如下两条选中的策略：

```
rule 1
action permit
src-zone "trust"
dst-zone "untrust"
src-ip 192.168.1.5/32
dst-ip 202.0.0.2
```

图 14：策略批量迁移

```
service "http"
exit
rule 2
action permit
src-zone "trust"
dst-zone "untrust"
src-ip 192.168.1.15/32
src-ip 192.168.2.15/32
dst-ip 202.0.0.2
service "http"
exit
```

那么迁移后，rule 1 排除操作后，源地址为空，成为一条非法策略，不再迁移；rule 2 去掉源地址 192.168.1.15/32 后再迁移，最终生成的迁移脚本为：

```
rule
action permit
src-zone "trust"
dst-zone "untrust"
src-ip 192.168.2.15/32
dst-ip 202.0.0.2
service "http"
exit
```

（五）通用批量操作

批量设备操作根据下发的配置复杂度不同，分为几种情况：

· 单一固定命令集合

· 多个固定命令集合

· 单一带可变参数命令集合

· 多个带可变参数命令集合

· 复杂命令集合

单一命令集合是所有操作设备对象下发统同一个命令脚本，多个则是不同设备操作对象下发的脚本不同；固定命令集合是指脚本是固定不变的，例如所有设备更新为相同的超级用户密码；带参数的命令集合则是脚本中命令格式下发前需要按要求替换；复杂命令集合是指，需要从被操作对象取回一定的参数，根据这些参数动态生成命令脚本。

自动化系统实际上是根据要求和设定条件，为每一台操作设备对象生成配置脚本并保存，然后通过下发脚本功能批量下发。图 15 所示为设备批量操作界面。

篇幅所限，这里只介绍复杂脚本批量生成的界面。如图 16 所示。

首先要指定操作设备对象集合。这里输入的参数，系统组合后形成一个 SQL 语句的条件部分，从纳管设备库中筛选出操作对象。任务名指定对选中的设备执行的操作，并获取指定的参数集合，这些参数集合作为指定配置模板的输入参数，最终为每个选中设备动态生成一个配置脚本。这里的配置脚本是系统自定义格式，操作人员可以审核并随时修改，然后通过下发配置操作下发到指定设备中。

一个典型的应用场景是，将某个数据中心所有的接入层交换机，状态为 down 的网络接口，设置为 shut down。假定某台接入交换机（192.168.1.1）通过执行“获取所有接口状态”任务，得到其中以下接口状态为 down:

图 15：批量操作界面

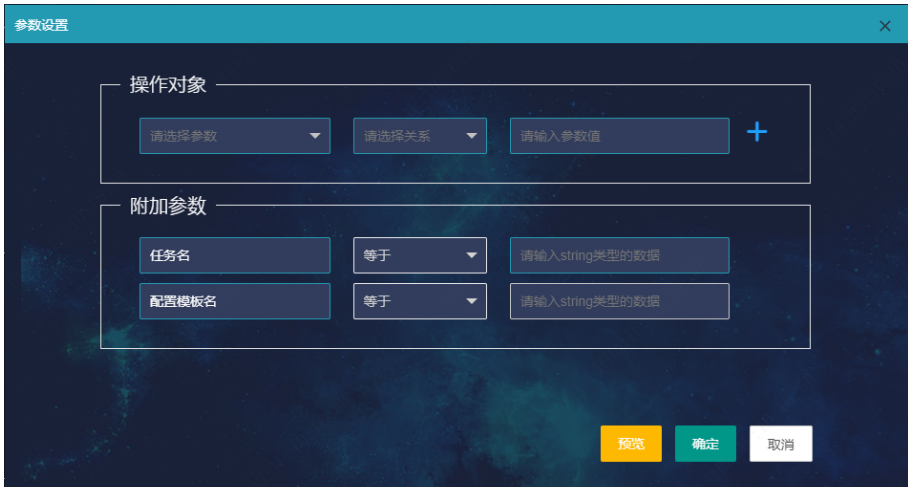

图 16：复杂脚本生成界面

Eth1/22,Etrh1/30,Eth1/35

另外一台接入交换机（192.168.1.2）以下接口状态为 down:

Eth1/2,Etrh1/3

则最终生成的配置脚本如图 17 所示：

```
@@ip:192.168.1.1
configure t
int eth1/22
shut
exit
int eth1/30
shut
exit
int eth1/35
shut
exit
@@save
@@ip:192.168.1.2
configure t
int eth1/2
shut
exit
int eth1/3
shut
exit
@@save
```

图 17：结果配置脚本

其中，@@ 开头的语句为自定义的脚本操作控制语句。这个脚本文件就是一个普通的文本文件，经过复核后，就可以通过下发操作，批量下发到指定设备。

（六）统一地址对象

统一地址对象有 3 类，个人终端、地址组和系统类。个人终端类只能有一个 IP 地址，地址组类可以有多个地址，但必须处于同一安全域，系统类地址成员不限，可以根据需要随意配置。

1、创建地址对象

申请人可以自行创建地址对象，但只可以创建个人终端或地址组类型的地址对象。创建的地址对象可以是私有，只有自己可以使用；也可以公有，所有人都可以使用。图 18 所示为创建地址对象界面。

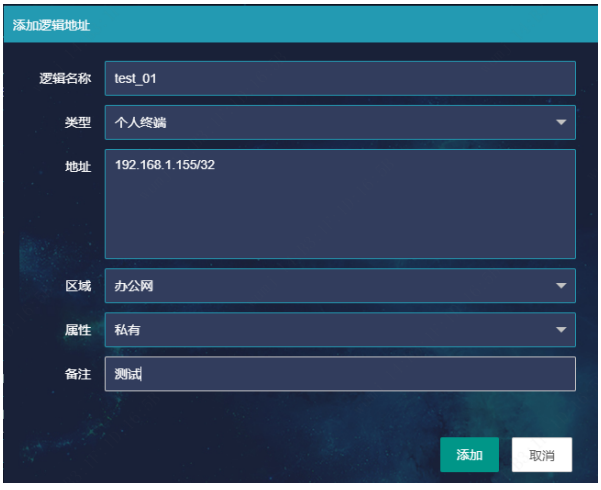

图 18：地址对象创建

创建好的地址对象，就可以用来申请安全策略了。后续，如果个人终端地址变化，或地址组成员发生增减，只需要提申请流程修改地址对象就可以具备和变更前相同的访问权限了。图 19 所示为地址对象变更操作界面。

图 19：地址对象变更

图 19 所示的流程申请，将地址对象 test 地址变更为 192.168.1.230/32。

2、系统地址对象

系统地址对象一般由网络管理员创建并管理使用，禁止在策略申请中使用。系统地址对象应用在特殊的安全策略中，且此类策略数量少，只须手工配置即可。通常频繁变化的是地址对象中的成员。图 20 所示为系统地址对象管理界面。

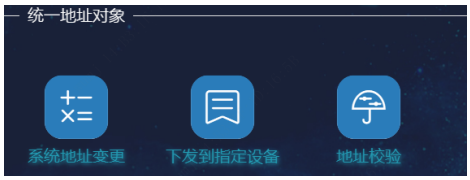

图 20：系统地址对象管理

例如，互联网边界防火墙通常会定义一组高危地址，此类地址被禁止访问内网。因为这个高危地址组成员是动态变化的，因此经常需要对它进行修改。如果有多台边界防火墙，就相当繁琐了。因此，这样一组高危地址，可以将其定义为一个系统地址对象使用、管理。

6、结束语

我司自 2020 年网络自动化项目一期上线运行至今，系统已经由一个单一处理访问权限申请流程的自动化处理工具，演变为一个可弹性扩展、功能完备的网络系统自动化运维平台。不仅可以自动化处理流程类申请引发的各类网络日常操作变更，还可以协助网络管理员自动化处理各类人工难以完成的运维工作和批量操作。

系统平台仍以处理访问权限开通申请流程为主要功能，图 21 所示为系统上线以来每年处理的访问条目数量增长情况。

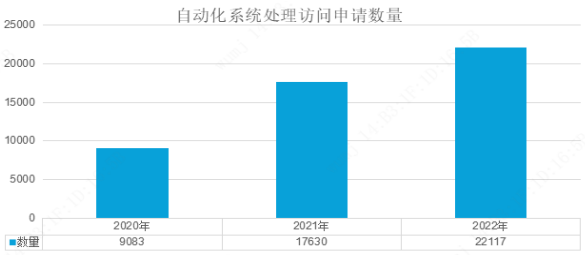

图 21：访问权限流程开通数量变化

由于我司近年来办公场地和数据中心屡次搬迁，导致每年涉及的网络访问权限申请剧增，2022 年自动化系统共处理了 22117 条访问申请，包括节假日在内，平均每天自动化处理 60 多条，基本上做到了流程“审批通过当天处理完毕”。剔除因为网络变更导致的基础数据配置错误以及申请人提交信息错误等原因，生成配置脚本、下发脚本处理过程正确率达到了 100%。

安全策略管理功能 2022 年上线试运行，至今已经完成 6 次因网络拓扑变更、设备更新引发的策略批量迁移，迁移策略总数约 700 条；清除因弃用网段、相互包含的垃圾策略 1100 多条；通过策略优化分析功能，清除无用地址对象、服务对象 4 批次，自动化操作处理准确率高于 99%。

应用自动化系统的意义不仅仅在于节省了人力，更重要的是自动化可以完成许多人工不能完成，或者说很难完成的工作。比如说在配置安全策略时，确定一条策略是否在目标设备上已经实现或被包含，是一件非常费时费力的事情，特别是当目标设备中的策略条数很多时，更加难以处理。又比如，只要配置足够强的算力，自动化系统可以在业务空闲时间段对所有网络设备接口进行自动化巡检，筛选出潜在风险点。这种操作需要登录大量设备，输入命令并处理天量的返回文本，再生成巡检报告。类似操作如果换成人力，是几乎不可能完成的任务。

兴业证券应用性能监控系统建设思路、方法和实践

刘洋、石良生、杨洋 / 兴业证券股份有限公司 金融科技部 福建 福州 350001
E-mail：yangyang2021@xyzq.com.cn

随着微服务框架在公司内的逐步推广落地，对分布式架构下的产线可观测性提出了新的挑战。业务的复杂化，给性能监控的内容和方式也提出了新的要求。同时，为数众多的外采的烟囱式的信息系统，使得应用的性能监控更加困难。本文针对公司现状，对应用性能监控系统的解决方案进行探讨，通过自主研发一套全新的应用性能监控系统，在传统的分布式链路跟踪技术的基础之上，实现丰富的接入方案，灵活的监控配置，动态的指标拉取，边缘化的数据存储，解决了公司产线观测的问题，在大量自研及外采系统中进行实践，取得了良好的效果。

1、建设背景

业务的复杂化和上层技术的升级是推动监控手段不断发展的原动力。企业级监控体系要面对众多信息化系统拓扑组成的复杂 IT 经营服务，其实际运行工作更为复杂，再加上微服务、云原生、函数计算等新技术的不断涌现，传统的日志加系统监控的手段已经难以充分地满足企业的监控需求。

系统监控领域由于其复杂性和普适性，是各类技术服务商和开源组织竞相角逐的战场，流行方案层出不求、创新不断。通过开源或商用工具快速构建监控能力是小型团队的常规路径，但对于有大量存量系统、或自研与外购混合、或多中心、或多技术栈的中型以上企业来说，明确监控体系建设质量目标，通过目标倒推监控工具和管理流程规划相比较而言更加具有长期成效。无论技术如何发展更迭、企业业务特性如何包罗万象，抛开层出不穷的新潮概念和流行方案，从主要监控步骤（日志采集 - > 发送告警 - > 故障定位）来看，衡量企业监控体系健壮性的关键指标依然是：监控覆盖度、告警有效性和可观测性。

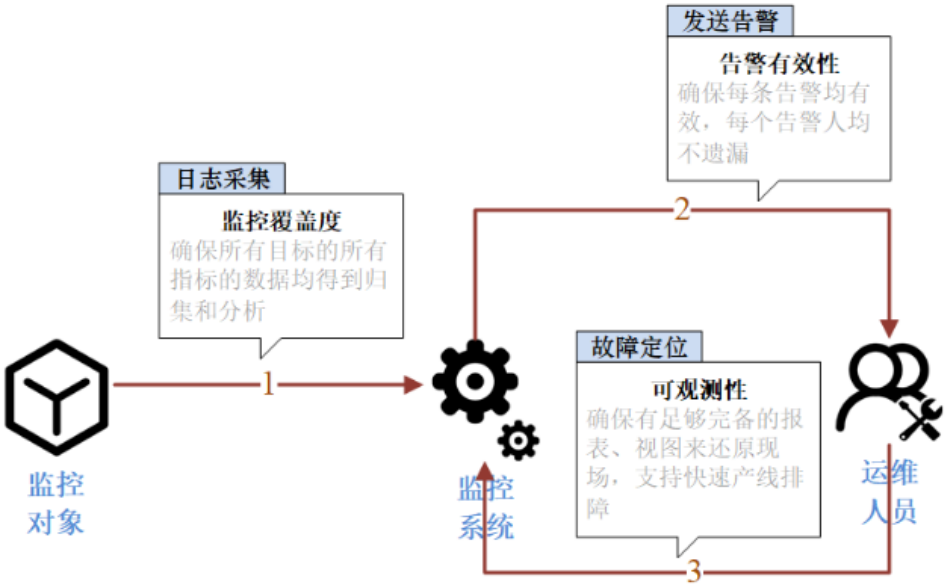

图 1：监控系统关键指标

1.1. 监控覆盖度

具体包括监控目标的覆盖度和监控指标的覆盖度。监控目标包括：应用、系统（运行环境）、数据库、中间件、硬件（机房、服务器、空调）、网络等。监控指标可以分为系统指标、应用性能指标、日志、业务指标等。通过设置标准化的监控管理流程和角色来保障监控覆盖度是非常有必要的。与之相反的是运动式、缺乏监督和检查点、缺乏针对性评估。

对于存量系统，打通 CMDB（Configuration Management Database，配置管理数据库）与监控系统，将 CMDB 系统清单和监控系统的指标清单匹配整合，通过日志有无采集来判断覆盖度是一种比较理想化的存量覆盖度检查手段。

1.2. 告警有效性

当完成监控覆盖度后最重要的工作便是维持告警的有效性，包括去除无效日志、告警降噪、触达审计等。告警有效性保障是监控体系最容易忽略的一环，有效性的缺失会导致整个监控机制的失灵。因此，通过管理机制和协同工具来保障每条告警的有效触达和被充分重视是至关重要的监控工作之一。

1.3. 可观测性

不同于狭义监控侧重于观察特定指标，可观测性则是强调通过分析系统生成的数据理解推演出系统内部的状态。可观测性是面向复杂分布式系统的现代监控理念，以应对云原生、大规模分布式协同等现代技术场景，同时，可观测性也是产线排障的重要支点。

可观测性内容非常多，是监控体系中最具技术挑战性的部分。大致可以分类为日志（Logging）、指标（Metrics）和追踪（Tracing）。全链路的可观测建设牵涉到诸多方面，易入门难完善，同时也间接反映企业整体 IT 研发实力水平。

1.4. 金融类企业其他要求

1.4.1. 多技术栈、多外购系统

不同于一个技术栈撸到底的互联网公司，大多数券商非常依赖技术供应商，其技术栈容易发散，同时还存在大量的外购黑盒系统，部分还自带监控子系统。对自研和外购的分层支持、对于不同技术栈系统保有一致性的监控水准需要一个

系统性解决方案。

1.4.2. 数据脱敏与研发协同

对于瀑布类的项目和外购系统，运维团队掌控力较强。但敏捷交付项目往往更需要开发人员参与稳定性的维护。因此，在开发和运维两类角色中进行数据隔离同时保证高效协同也是完善监控体系的重要内容。

1.4.3. 系统的健壮性

金融类企业的信息系统，涉及交易、资金等许多环节。对于监控系统的引入，需要非常谨慎。必须要保证监控系统不能对原有系统的正常运行造成影响。

2、建设思路

企业监控体系的搭建可以分为监控接入管理、监控服务、监控平台三项工作。良好的监控体系需要依赖可靠的平台系统和有效的工作制度，系统与制度缺一不可。

图 2：项目建设思路

2.1. 监控接入管理

监控接入管理是指通过清晰有效的工作机制，在研发交付流程环节保障监控覆盖面，避免死角。具体包括健全开发侧相关规范，在架构评审环节增加监控评估内容等；

2.1.1. 监控接入规范

监控接入规范旨在指导开发人员在应用设计阶段就考虑监控方面的需求。从日志、异常、探活和业务事件等方面着手主动适配企业监控体系。因此，我们需要制定可行的相关规范，包括日志输出规范、异常处理规范、应用探活规范、事件上报规范。

2.1.2. 监控覆盖评估

2.1.2.1. 监控基线

针对各类监控对象建立监控配置基线，由监控探针按照配置进行日志采集。基线的目的是面向常规系统监控和基础应用监控而设，可以满足绝大多数监控需求。基线往往由系统运维设立并打入交付设施中，与交付系统打通往往可以支持全自动化生效。同时，监控基线应该能自然支持市面上主流的中间件、基础设施。

2.1.2.2. 监控评估

监控评估主要在架构评审、采购评审等阶段开展，面向的是非基线约定的监控角度。除了复核常规监控配置基线外，主要评估内容为高可用自动切换等变更告警、关键 Transaction 监控、可观测性评估等，具有较大的自主性和主观性。因此有必要建立专人专岗，在研发交付的流程中设定专门评估环节来保障有效落地。

2.2. 监控服务

监控服务描述的是应用接入企业监控体系后，将监控告警和观测平台打包提供给项目人员的一系列标准化服务的集合，是由监控团队提供给开发和应用运维人员。

2.2.1. 告警工单服务

告警与工单的结合不但标准化了异常处理过程，同时也可以作为项目的应急处置能力的评估指标。自动化告警工单在监控体系中的价值包括：

· 对告警进行归纳和分类

· 无干扰地统计处理时长

· 度量 IT 团队的异常处置能力

· 在制度上有助于收敛无效告警

2.2.2. 观测支撑服务

监控团队集中建设的观测平台是面向项目组

提供合规、脱敏的产线运行状况的观测通道。观测支撑服务支持开发工程师、应用运维两类角色，分别提供不同程度的数据查看权限。同时，也支持应用运维即时授权给开发查看更多内容。可观测的数据包括：

· 日志数据
· 统计数据
· 分析数据
· 事件数据
· 交互数据

2.3. 监控平台

当下市场上流行的监控平台层出不穷，对于金融企业需要重点兼顾的需求包括有：

· 多语言支持
· 多中心支持
· 与 IT 资产管理、交付工具、工单系统、成效分析系统的打通和集成

抛开各类流行监控产品的上层能力图谱的影响，从监控工具的运行流程来看，监控平台可以拆分为如下阶段性子系统或模块。

3、技术方案

3.1. 产品定位

目前公司拥有包括 Zabbix、Prometheus、日志易、动环监控、天旦、APM（Application Performance Management，应用性能管理）、服务治理以及其他专项监控设施共同组成的多方案企业监控体系。监控不同于通信框架，可以适度冗余，通过有限交错的监控工具可以增加容错率。目前公司在应用层监控采用以 Prometheus 为主，以自研的 APM、服务治理为补充的整体结构。

图 3：监控平台链路

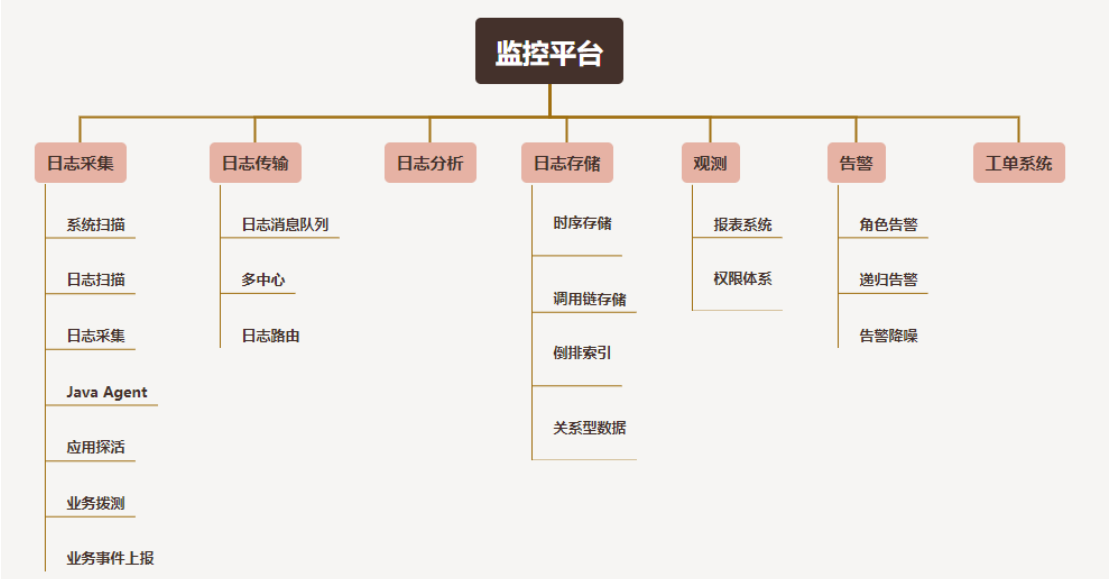

图 4：监控平台功能细分

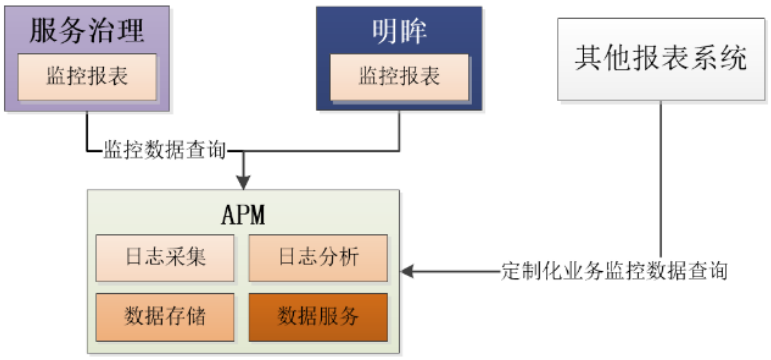

图 5：产品边界

3.2. 系统设计

3.2.1. 整体设计

兴业证券 APM 是一个主要基于 Java 开发而成的分布式系统集，其包括多个子系统。系统设计的整体目标为高吞吐、海量存储，但在数据一致性、备份冗余方面需求不高。除了支持异地部署外，还需要强调对业务监控的支撑力度，同时在企业监控体系的定位上做了下沉，APM 新增的事件处理编排能力旨在构建灵活的业务监控能力，与其他监控设施做差异化服务。

3.2.2. 事件分析与存储

APM 以灵活配置事件消息处理流程为目的，基于 Kafka 流式处理能力自主设计了的可编排日志分析器。对于上报的事件消息，根据事件的“type”关键字，区分不同的事件类型。对不同的事件类型，可以配置一个或多个有序的事件消息处理器。分析器服务将会根据配置的分析器，按需对事件消息进行处理。链条处理器目前定义了 6 种基础的处理器。

处理后的事件消息，如需要持久化，则最终会通过特定类型的分析器落入到 3 类存储设施中。其中，BitCask 是我们基于 Riak 分布式数据库论文，结合边缘存储的理念做的自主实现。存储结构为 Key->Value List，具有较高的吞吐能力。目前我们测试数据结果为：单机 4 核 8G 的机械硬盘下 QPS 为 10K/S 左右。

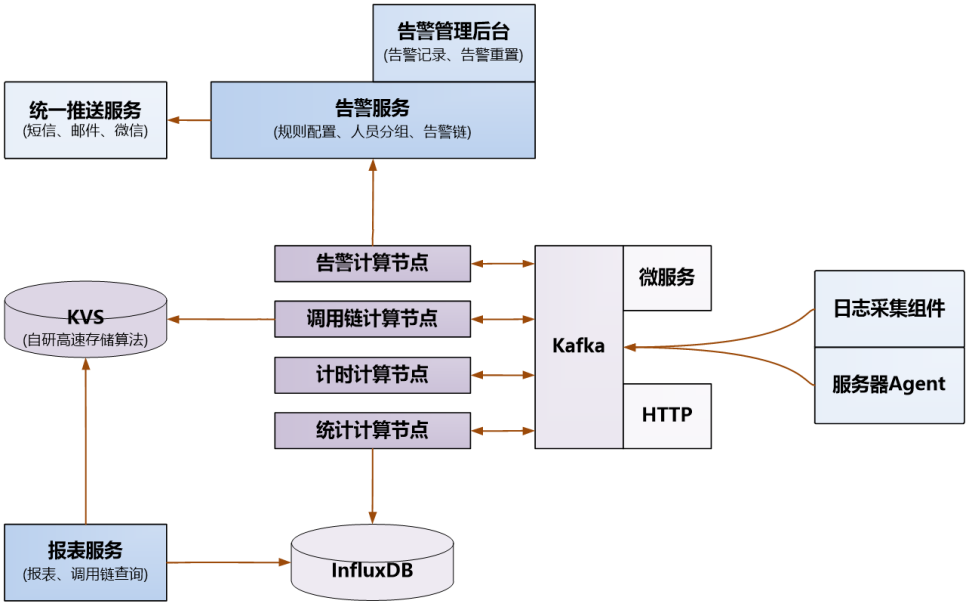

图 6：产品整体设计

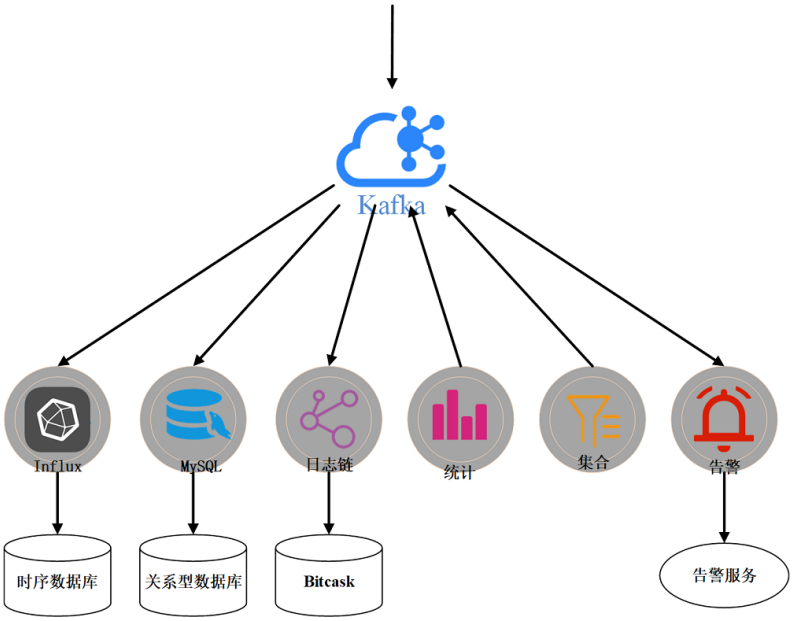

图 7：事件分析处理器

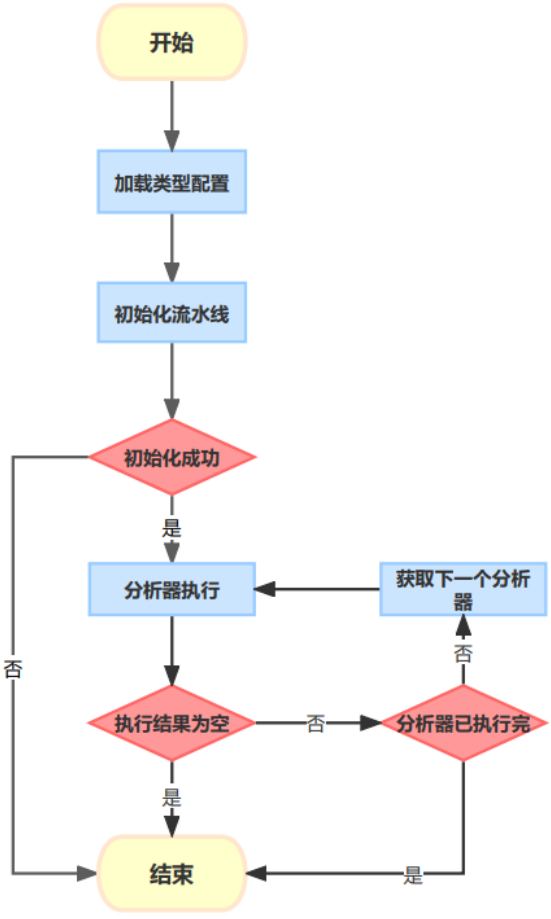

图 8：日志分析流程

我们针对 APM 事件消息详情数据写入频率远高于查询，且写入后不会修改的特点，将调用链详情数据写入本地 BitCask，运用边缘存储的方式，极大地节约了网络带宽资源，同时提高了数据的安全性和隐私保护。

3.2.3. 数据查询服务

APM 数据查询服务是实现了类似 MyBatis 的在线模板录入生成数据查询能力的服务，是 APM 重要的子系统。其查询脚本存储在 Zookeeper 中，同时脚本采用 Velocity 模板，有很强的灵活性，可以根据模板及传入参数形成复杂的数据检索逻辑。同时对外开放了检索的 RPC 服务与 HTTP 接口，周边系统开发人员可以通过接口提取采集到的 Metrics 数据。

通过灵活的事件分析存储、数据查询配置，我们就可以将业务与能力解耦。将业务交给接入方，使得他们在享受 APM 基础能力的同时，能够根据自己的需求，定义特殊的事件，做定制化的事件分析和分析结果查询，形成完整的自闭环。这种方式能极大提升系统的数据权限隔离和隐私保护能力，使之在金融行业内，能发挥更大的能动性。

表 1：分析器功能说明

分析器	功能	说明
MySQL	MySQL 分析器	将数据插入 mysql 数据库
InfluxDB	InfluxDB 分析器	将数据插入 influxdb 数据库
Counting	计数分析器	按参数，对指定维度，指定关键字进行计数
Set	集合分析器	通过配置的 keys 进行去重，对新数据进行转发
Tracing	跟踪分析器	将调用链数据持久化写入 BitCask
Alarm	告警分析器	触发告警

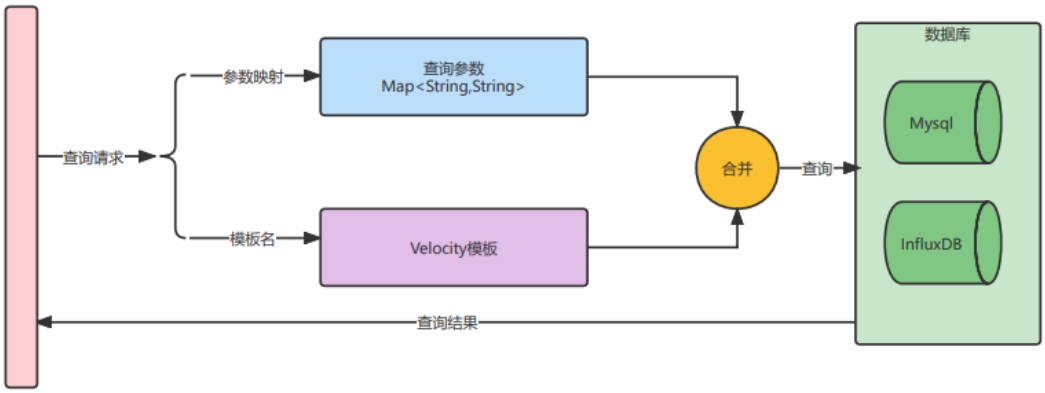

图 9：数据查询服务执行流程

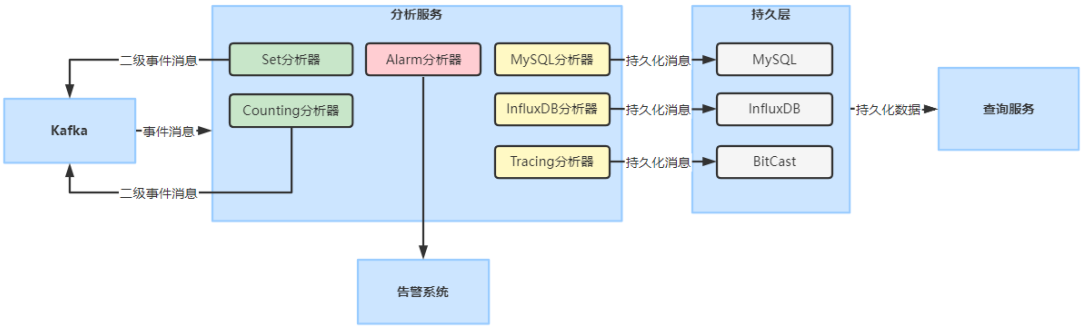

图 10：事件消息数据流图

3.2.4. 跨中心同步

公司系统有多个数据中心，有的系统仅部署在一个数据中心，有的系统部署在多个数据中心，就会导致我们有跨数据中心的请求。而数据中心间的网络资源，往往是比较紧缺的，APM 的数据量又是比较大的，因此，我们设计了一种跨数据中心的调用链存储和查询方式，能够极大地减少跨中心请求时伴随着的跨中心调用链数据上报。

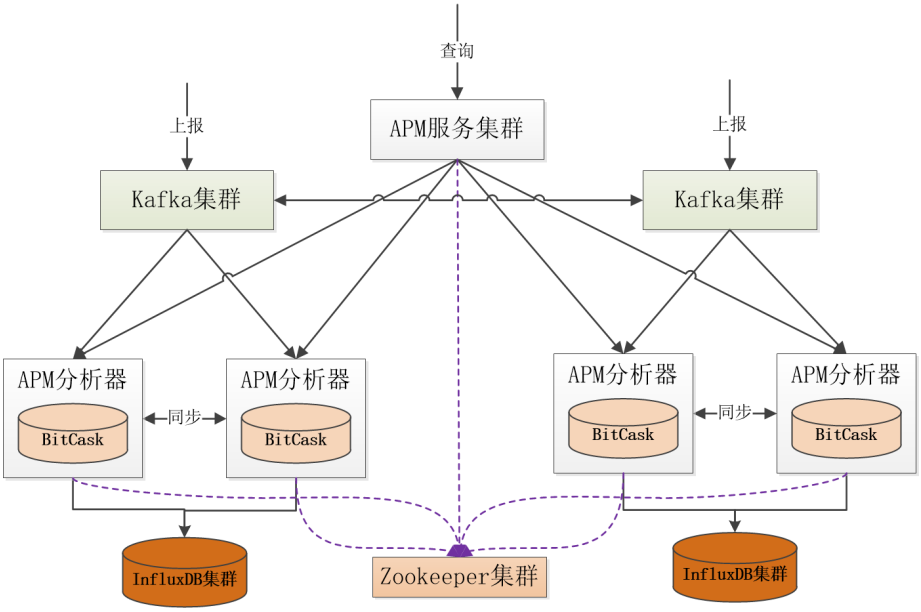

图 11：跨中心同步部署架构

4、成果及展望

本文主要介绍了兴业证券在应用性能管理系统上的建设思路和实践。不同于外购和开源方案，系统在复杂模块使用开源组件的基础上，自主研发底层存储和事件分析查询能力，使系统对公司技术栈和潜在技术变更有着更好的兼容性和适应能力。

该系统在公司内上线运行以来，经过反复地迭代升级，对特殊业务、协议、中间件的陆续支持，已取得了良好的效果，成为应用性能管理提供了有力的抓手。

4.1. 监控体系

兴业证券自研的 APM 系统自 2018 年上线以来，经过不断地完善和优化，在性能上和兼容性上持续提升，目前已成为应用性能监控的标准方案，配合 Prometheus 的中间件监控和 Zabbix 的主机监控，共同构成了我司完整的监控体系。

4.2. 减少带宽占用

基于新中心网络规划进行技术攻关解决跨中心海量数据同步和传输网络带宽占用问题。在今年的新中心搬迁工作中，对于新中心的两地三中心网络规划，自研 APM 发挥了完全自主可控的优势，攻关了应用运行数据集中存储与异地网络带宽限制，满足数据就近存储，减少跨机房数据同步，禁止应用跨机房数据上报的需求，实现多中心部署并支持弹性伸缩，避免对机房间网络带宽的占用。

4.3. 支持自研与外购系统

APM 凭借多语言支持，目前已成为中台、优理宝、兴证 e 家、财富梦工厂和集团 CRM 等几大自研产品线运行观测和生产排障的主要工具，外购系统接入率也在持续提升，极大提高开发运维人员性能监测、故障感知与定位的效率。

4.4. 未来展望

未来，我们会持续深耕，探索现场还原、风险预判、自动剖析等更前瞻的观测能力，探索边缘存储方案和应用场景，持续沉淀和输出相关的通用方案，提供更加丰富的观测指标和能力，为产线系统稳定运行保驾护航。

一种可扩展的多因素访问控制方法及实践

姜洪涛、宫珂、于慧 / 上交所技术有限责任公司 上海 200120
E-mail：htjiang@sse.com.cn

在数字化转型浪潮下，通过科技创新和数字化变革寻找发展动能已成为必然趋势。在企业内部，各业务条线正在朝着信息化、自动化、智能化的方向转变，对 IT 带来前所未有的挑战。应用系统需要更加开放，提供更好的使用体验，同时需要必要的访问控制技术，保证在非保护网络环境下的信息安全，而且对于存量系统来说存在一定的改造成本。本文就如何构建多因素可扩展的访问控制能力进行阐述，并结合自动化运维平台的需求，提出比较合适的实践方法。

1、背景

互联网技术的发展促进了用户对于系统使用便利性的需求，那些部署在受保护网络下的信息系统逐步显露出不能有效满足用户需求的问题，在需求驱动之下需要向更加开放的外部网络环境延伸。而外部网络环境的多样性和复杂性会对信息系统的受保护内容带来新的挑战，因此有效的访问控制手段是这些系统首先要具备的能力。

在运维领域，随着 DevOps 等模式的发展，去后台操作的白屏化运维逐步成为趋势。而且，在一体化运营、业务与技术联动等企业数字化转型的战略安排下，传统的在 ECC 内完成的运维工作，尤其是不涉及敏感数据和不影响生产运行的相关工作，在逐步向日常办公环境甚至是互联网环境延伸。为避免产生数据泄露及破坏到生产安全运行，需要通过访问控制技术来保证只对授权用户、授权场景开放服务。

2、问题与挑战

对于访问控制模型，较为普遍常见的就是基于角色的 RBAC(Role Based Access Control)，通过赋予不同角色不同权限来进行访问控制。对于一

个主体（往往是组织内的人员或者某个客户端），可以拥有多个角色以应对多种不同的操作权限。RBAC 与组织内的实际业务组织架构相近，往往是系统首选的原生访问控制技术，但随着环境变化，尤其是对于安全防御要求提高，需给系统增加更多因素的访问控制技术，如用户使用环境、访问途径、时间段等。

在现有系统上增加访问控制因素，一种简单明了的做法是将相关控制逻辑嵌入到代码中，比如在认证模块或代码段增加访问控制相关代码。该方法虽然有效但也存在两个比较明显的局限性。一方面，增加访问控制逻辑需要重构现有模块，且与系统现有功能有强耦合性，甚至在一些特殊情况下，一些系统不一定能支持新版本的上线。另一方面，其它系统无法复用相关能力，容易形成竖井式的功能孤岛。访问控制技术在一个组织当中，属于安全基础设施，是一种基础能力，应具备在各系统中共享的能力。在实现上，可以借鉴中台建设的思路，在架构上以松耦合方式独立于各应用系统，且又能满足不同应用系统的差异化需求。

本文介绍一种针对基于互联网架构的，可扩展地增加访问控制的方法，而且通过在构建自动化运维平台的实践场景验证，其不仅可以按需灵活地添加控制因素和策略，而且能够加强现有存量系统的访问控制能力。

3、方法阐述

运维操作白屏化是 DevOps 重要组成部分，敏态的运维过程带来了收益，但也同样带来了一系列安全隐患，比如：网络攻击、运维操作权限控制和审计问题等。因而，需要一个可灵活配置、扩展的访问控制模块，为运维操作、故障问题排查提供安全防护，为提高安全运行的能力提供支撑。

3.1 总体架构

本文中设计的多因素访问控制模块，在架构上与后端各应用节点间独立解耦。原则上用户访问行为均基于策略进行控制，策略规则支持动态扩展，灵活设置。总体架构如图 1 所示。

用户的访问请求首先经过负载均衡层，此时

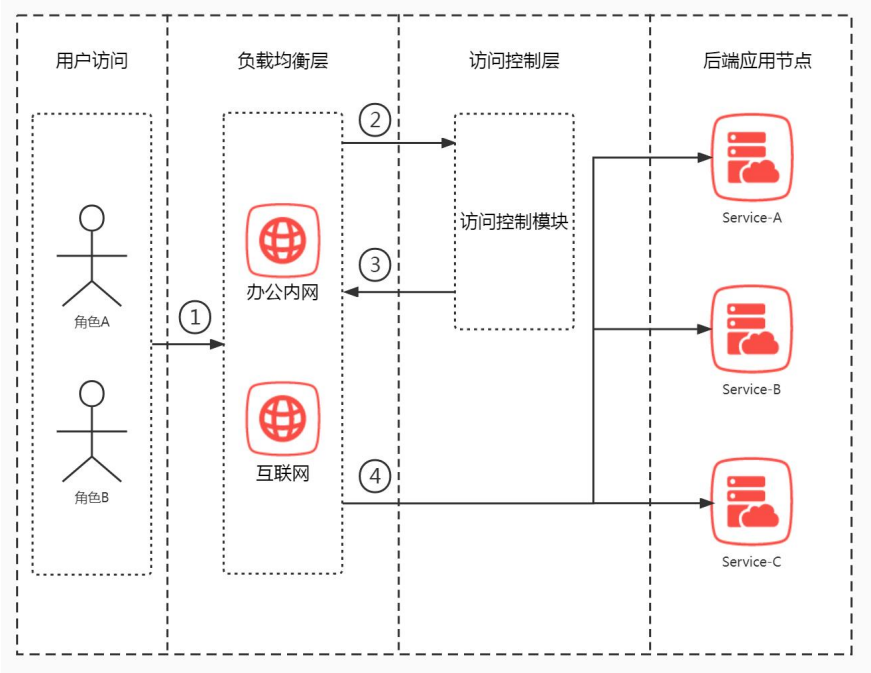

图 1：总体架构图

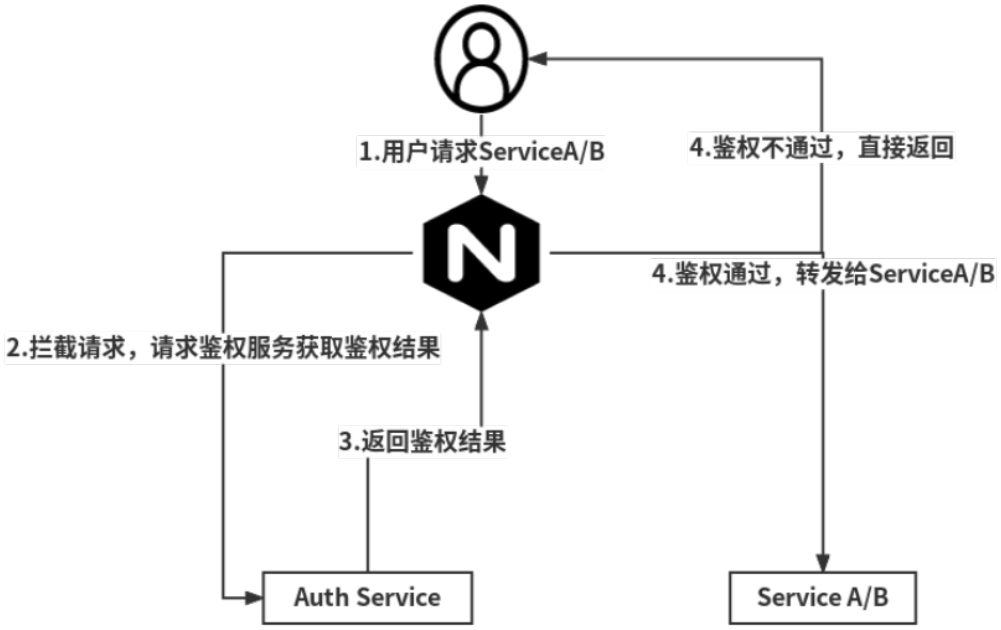

图 2：基于 Nginx 中 auth_request 模块访问控制架构图

请求首先被转发到访问控制层进行验证，只有验证通过的请求才会被转发到后端服务。负载均衡层的该转发能力将访问控制可动态插入到请求处理链条，与流量镜像不同的是，这里是一个同步顺序执行关系。

访问控制模块在整体架构中处于用户和目标应用服务器之间，属于保护代理结构，用户请求经过此模块完成策略规则的校验判定后，可根据判定结果获取到对应的目标服务器资源。原则上，访问控制模块是无状态的，不负责代理应用的用户认证和权限校验，只做多因素访问控制，但在实现过程中，也可将鉴权作为检查因素之一，如设置一条策略校验当前用户请求的 Token 是否有效。

3.2 基于 nginx auth_request 实现负载转发能力

基于总体架构方法，需要一个可以拦截用户请求并进行鉴权的工具，将用户的请求都先发送给鉴权服务进行访问控制鉴权后，根据鉴权结果决定是否可以访问应用服务。拦截用户请求最直接的方式是从负载均衡层进行拦截，前期调研发现常用的负载均衡工具 Nginx 提供的 ngx_http_auth_request_module 模块，可以协助实现访问拦截和访问鉴权。在 Nginx 访问 ServiceA/B 的配置里添加 auth_request /auth 参数后，当用户访问 ServiceA/B 时，Nginx 会先将请求拦截，先请求 /auth 访问鉴权模块 Auth Service，当 Auth Service 返回鉴权通过时允许继续访问，Nginx 会将请求发给 Service A/B; 当鉴权服务返回无访问权限时，可以将指定的拦截页面返回给用户。

基于 Nginx 中 auth_request 模块进行访问控制逻辑改造，可将访问控制模块与现有功能模块分离，将用户请求内容拦截到访问控制模块进行统一鉴权，使控制策略逻辑内聚到访问控制模块中，其他服务只做 Token 有效性验证，轻量级适配现有权限控制体系，从而，降低存量系统访问控制改造成本。

3.3 访问控制模块

本文设计的访问控制模块架构主要分为三层：策略层、执行层、校验层。架构设计如图 2 所示。

图 3：策略执行架构图

整体架构主要遵循两点设计原则：1. 策略层中支持多种访问控制策略的逻辑组合；2. 执行层可针对不同的访问要素类型设计不同的执行器，执行器在验算策略过程中需保证幂等性，执行器支持组合使用。在实现过程中可基于实际业务需求设置策略组合，各执行器对策略组合进行幂等运算后，输出校验结果的布尔值。

运维平台使用人员、场景复杂，需要一个灵活的、多维度的访问控制策略，基于此，我们设计一种可灵活拆分、组合的策略执行方法。首先，将系统所需的访问控制规则打散，变成一个个不易分割的原子策略，比如：基于访问时间限制的控制策略 P1，可以拆分成允许访问的时间区间；基于访问地点限制的控制策略 P2，可以拆分成允许访问的指定 ip 或者指定 ip 前缀；基于访问请求路径限制的控制策略 P3, 可以拆分成允许访问的指定 url 路径或者 url 路径前缀；基于角色的访问控制策略 P4, 可以拆分成角色或者角色集合等等，然后借助组合数学中交集、并集的概念，将不同子策略组合在一起，实现复杂的策略的组合，例如：公式（1）可以表示允许 P4 角色的用户在 P1 时间区间内使用 P2 指定 ip 访问请求路径 P3，而公式（2）可以表示允许 P4 角色在 P1 时间区间内访问请求链接，或允许 P4 角色在 P2 指定 ip 访问请求链接，或允许 P4 角色访问 P3 请求路径。

$$P1 \cap P2 \cap P3 \cap P4 \quad (1)$$

$$(P1 \cup P2 \cup P3) \cap P4 \quad (2)$$

运维平台对操作审计信息十分敏感，基于本文访问控制方式改造后，所有审计信息都可以在访问控制鉴权模块进行采集，统一记录访问人、访问路径、请求设备（ip 地址或者 MAC 地址）、请求时间等信息，为审计工作提供便利。

基于策略组合实现的访问控制方式相较于传统单独基于角色的访问控制方式更为灵活，它允许通过流程审批临时增加或者变动访问控制策略，这种访问控制策略变动的方式，无需更新系统版本，也无需进行其他适配性改造，就可以达到临时赋权访问的效果，而流程审批记录也可以为审计记录留痕，例如可以让某一用户通过 IP 为 1.1.1.1 的主机在 1 个小时区间内访问指定资源。

4、应用实践

4.1 在运维平台的实践情况

随着运维工作数字化转型的推进，运维平台能力变得更加开放和服务化，如何做好访问控制，避免敏感信息泄露和对安全运行造成破坏是不得不解决的一个难题。基于本文所述架构，在存量运维平台上进行了相关实践验证，根据运维

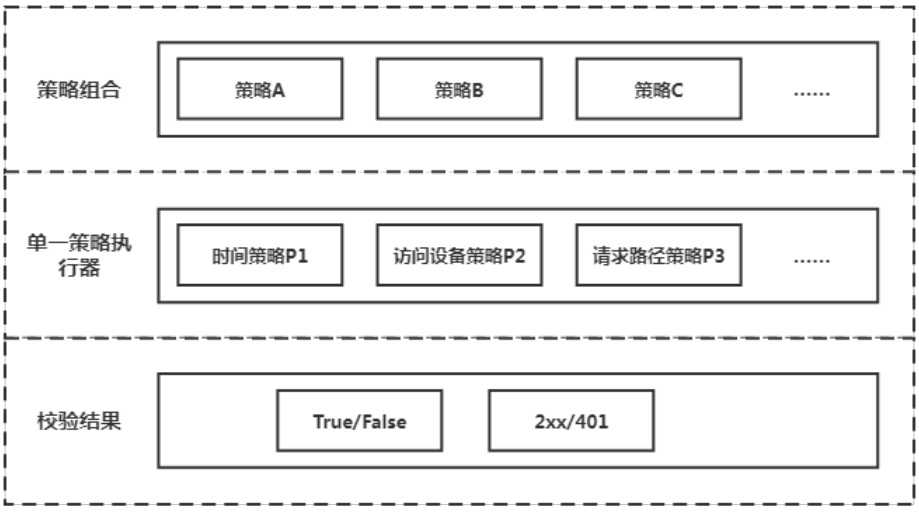

图 4：策略方法层次架构图

实际场景要求，提取所需访问控制元素，内聚在新建的访问控制模块中，对用户请求进行统一拦截鉴权。

从生产安全性考虑，运维平台不能在公网直接开放使用，但如遇紧急情况时，运维人员、二线支持人员短时间内无法赶去现场，极有可能导致定位问题、处置问题时间被拖长，给生产安全运行带来隐患。基于本文多因素访问控制方法，通过访问控制策略，临时访问策略审批流程，可允许运维人员、二线支持人员在指定设备终端在持有 CA 证书的情况下在指定时间区间内访问运维平台，及时定位、解决生产问题。

本系统基于 SpringBoot 框架创建了一个访问控制服务 AC Service，用于进行访问控制权限校验。并在控制层 AuthController 开放了一个权限校验接口 /auth，供 Nginx auth_request 模块拦截鉴权，该接口实际调用策略执行器 StrategyExecutor，而 StrategyExecutor 根据单一策略要素校验结果按照复合策略进行组合计算，将访问控制策略结果返回给 Nginx。用户可灵活化自定义单一策略要素和组合策略，本运维平台已纳入的单一策略要素有：限制访问 IP 前缀的 IPPolicyExecutor、限制访问时间区间的 TimeRangePolicyExecutor、限制是否交易日访问的 TradeDayExecutor、限制用户是否可以远程访问的 UserPolicyExecutor、限制使用指定 CA 证书访问的 CertPolicyExecutor 等，如图 5 访问控制策略实现图所示。

为满足生产环境实际需要，本平台根据访问日期、访问时间、访问网段等元素，设计了一系列不易拆分的单一策略，部分策略如表 1 所示。以应用发布功能为例，涉及生产操作需双岗复核，不应允许用户在交易时间内访问操作，仅允许用户在办公内网非交易时段进行访问，它的复合策略应为 {{P1，P2，P3}，{P1，P5}}，如公式（3）；而对于应用日志下载、应用状态检查功能，不涉及生产环境敏感操作，应既允许用户在办公内网访问，也允许用户在非交易时间通过外网访问，它的复合策略应为 {{P1}，{P4，P5}，{P2，P3，P4}}，如公式（4）。

$$(P1 \cap P2 \cap P3) \cup (P1 \cap P5) \tag{3}$$

$$P1 \cup (P4 \cap P5) \cup (P2 \cap P3 \cap P4) \tag{4}$$

经过实践验证，通过灵活的策略组合及 Nginx 可插拔的 auth_request 模块应用，本文所述架构能够较好地对现有运维平台访问控制能力增强，起到相关的预期作用。

4.2 扩展场景实践

本文所述方法及架构不仅可用于访问控制技术，而且可以推广到对系统能力进行的其它场景，结合实践情况列举以下两个场景进行描述。

4.2.1 用于 IPV6 过渡方案

随着社会数字化、智能化的体系建设不断深入，大部分政企单位均面临着数字化转型及创新体系构建的挑战，其中加快建设部署 IPv6，快速

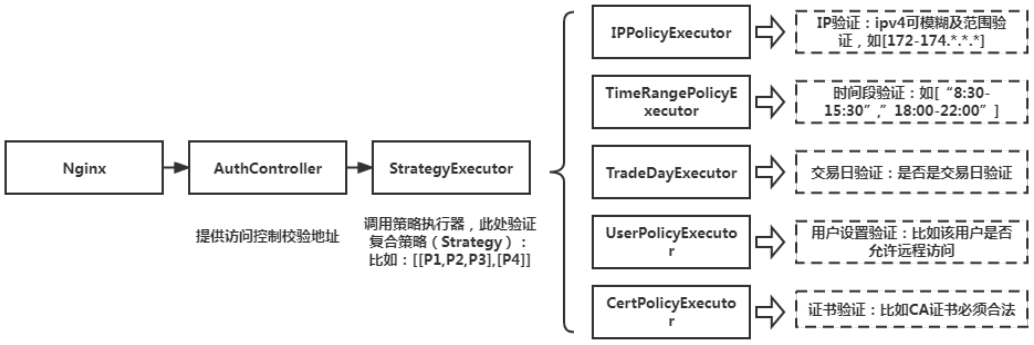

图 5：访问控制策略实现图

单一策略标号	策略名称	策略方向	策略内容
P1	仅允许办公内网 IP 访问	Positive	[“172.*.*.*”]
P2	仅交易日允许	Positive	
P3	非交易时间段	Negative	[“9:15-15:30”]
P4	证书 ID	Positive	[“cert1”, “cert2”]
P5	节假日允许	Positive	

表 1：单一策略表

完成现有 IPv4 业务系统转换，具备一定的战略意义。本文设计实现的多因素访问控制方法同样可以用于 IPv6 与 IPv4 之间的服务转化，用户可以在策略层中增加 IPv6 与 IPv4 服务间的映射策略，设计具体执行器完成服务请求校验及转发规则判断，此设计模式可以在不改造现有架构的基础上，快速帮助存量 IPv4 业务系统具备 IPv6 终端和用户访问能力。

4.2.2 用于系统保护机制

在传统 IT 系统架构中，应用系统一般会通过专业压测来获取性能指标，如接口并发响应时延、最大并发用户数量、数据库记录数等等，这些指标不仅能够帮助运维及开发人员评估应用系统在高负载情况下出现故障的可能性，也可用于应用监测告警，有效避免系统安全运行风险。但在实际的生产环境中，同样可能面临击穿性能容量的情况，本文设计实现的多因素访问控制方法同样可以用于系统性能容量保护，在不调整后端服务架构的基础上，通过在策略层增加多因素拦截策略，如限制同一设备单位时间内请求次数，请求响应延时超过阈值后弹回处理等等，不仅提升了整体架构的灵活性，也是一种有效的安全防护手段。

4.3 收益分析

通过将本文所述方法在运维系统中进行实践验证，访问控制模块的引入不仅可以有效加强系统安全性，而且，在成本、架构管理等产生一定的收益。

安全方面，架构在负载均衡层接入到现有系统，可以对所有请求进行分析处理。访问控制模块可以灵活制定原子策略并加以组合，可以按需添加访问控制的要素，能够较好满足系统的安全需求。 在该架构下，安全审计仅需要针对访问控制模块进行，不需要逐个系统模块进行审计确认，节省审计日志的存储及审计人员的重复检查工作。

成本方面，架构以 Sidecar 形式灵活接入到现有系统，对现有系统几乎无改造需求。架构上解耦后，通过将访问控制能力沉淀为中台服务，避免单个系统的改造，规避不同系统或模块的重复开发和适配，若按照 20 个系统或模块接入该鉴权方式，可节省 90% 以上的开发成本。而且，访问控制服务就绪后，各系统可快速对接，大大缩短推广周期。

架构管理方面，安全控制通过集中化的访问控制模块完成，减少各系统因系统架构、鉴权逻辑不统一产生的设计疏漏和运行风险，进一步降低管理成本和提升系统健壮性。

5、总结与优化

通过对现有运维平台增加基于 IP 地址、时间段范围、CA 证书等验证要素的实践，证明本文所述方法不仅可以做到架构上对现有系统无侵入性，而且通过策略的灵活组合，可以实现对于不同保护等级的功能模块进行细粒度访问控制。后续，除进一步支持更多访问控制要素外，可以结合智能分析技术提前识别潜在风险并阻断相关访问，而且可以进一步加强审计能力，定期回顾访问控制的有效性。

证券公司智慧营销与服务平台建设

潘建东、徐政钧、刘逸雄、谷航宇 / 中信建投证券股份有限公司 信息技术部 北京 100010
E-mail：xuzhengjun@csc.com.cn

随着居民可投资资产的快速增长以及资本市场改革红利的充分释放，券商财富管理业务正迎来蓬勃发展的新时代，而互联网运营模式的逐步推广，使得传统大规模线下金融业务以及传统营销模式受到诸多限制。对证券公司来说，充分发挥大数据、云计算、人工智能等新兴技术的优势，大力发展线上营销服务，以智能化方式提升顾问营销与服务能力，提高客户服务体验是大势所趋。本文阐述了中信建投证券通过对传统电话营销服务的智能化改造，实现了高效、合规的全流程精细化服务，最后本文总结客户服务中智慧营销的经验与未来展望。

1、概述

随着数字化转型的不断深入，金融科技领域迎来了蓬勃发展的黄金时期，金融机构运用人工智能、大数据、云计算、区块链等技术改变传统业务的经营模式和业务场景，建设端到端的智能化生态，实现运营效率提升与经营成本降低已成为行业共识。对证券公司来说，随着越来越多投资者涌入金融市场，如何以更完善的方式实现服务与营销的结合，如何结合科技能力实现高效营销，成为了一项重点的攻关项目。

线上开户是证券公司的核心开户渠道，开户引流效果也是衡量业绩的重要指标，开户流程分为手机号注册、营业部选择、身份证上传、风险测评等十余个步骤，此外需添加身份证核验，人工核验，回访确认等诸多需等待步骤，很大程度上会使客户停留并遗忘。此外，在产品推介、业务办理等众多过程中，均存在各种原因导致的客户停留。及时地识别客户停留原因，为客户提供陪伴式的服务引导，将在增强客户体验的同时提升经营业绩。因此，为实现智慧营销，增强引流和转化能力，进一步提升公司的核心业绩，中信

建投证券以全流程数字驱动的理念为引领、以数字化手段为支撑，着力建设全流程、多维度智慧营销服务平台。该平台提供客户行为跟踪、IP 电话呼叫、客户画像、智能分析引擎、数据统计与分析等功能，通过智能监听客户业务办理及产品购买流程，实现基于模型及流程的客户意图预测，最终智能生成任务并路由分配。此外平台在对话过程中引入实时知识与话术推荐等一系列功能，实现全流程、多维度、精细化的智慧营销。

2、营销服务平台智能化建设

2.1 功能与架构

营销服务平台整体划分为任务管理单元、数据统计单元、行为监控单元和智能化单元四个部分，对外提供客户行为跟踪、IP 电话呼叫、客户画像、智能分析引擎以及数据统计与分析等功能。

行为监控单元是平台中的数据获取中心，它通过数据埋点，轻量级地收集各界面上客户的状态信息，并发送至统一后台消息队列，消息队列提供全流程客户信息，任何监听消息队列的用户均可获取全量客户状态信息。过滤管理则是面对海量客户信息，精准地实现信息漏斗，过滤掉无关的监听信息，平台提供了基于渠道、流程状态的监听配置，该过滤管理功能也可实现基于业务的信息过滤，以达到个性化监听的目的。数据扩容模块则是为了向营销人员提供更多客户信息而设置的，该模块对接公司其他数据中台，在流程监控中拉取的部分信息进行数据补全，收集用户的历史营销信息、个人信息和历史办理业务信息等，为营销人员决策提供数据支撑。

智能化单元是平台的核心单元，是平台的决策大脑。智能分析单元提供数据画像的分析能力，并且通过基于自然语言处理（Natural Language Processing，NLP）技术实现自动画像生成，可在对话过程中实时分析客户的意向。行为预测则是平台的辅助单元，该单元收集用户的特征，并基于流程信息对客户的后续行为进行预测，该预测采用深度学习模型，决策出用户后续办理业务成功的概率，并将概率反馈给营销人员，营销人员则可根据该单元决策是否电话营销。用户增长是平台中的员工数据分析单元，该单元可将平台中的全部信息进行实时分析，实现基于不同维度的分析数据，实现漏斗分析、行为分析、成功率分

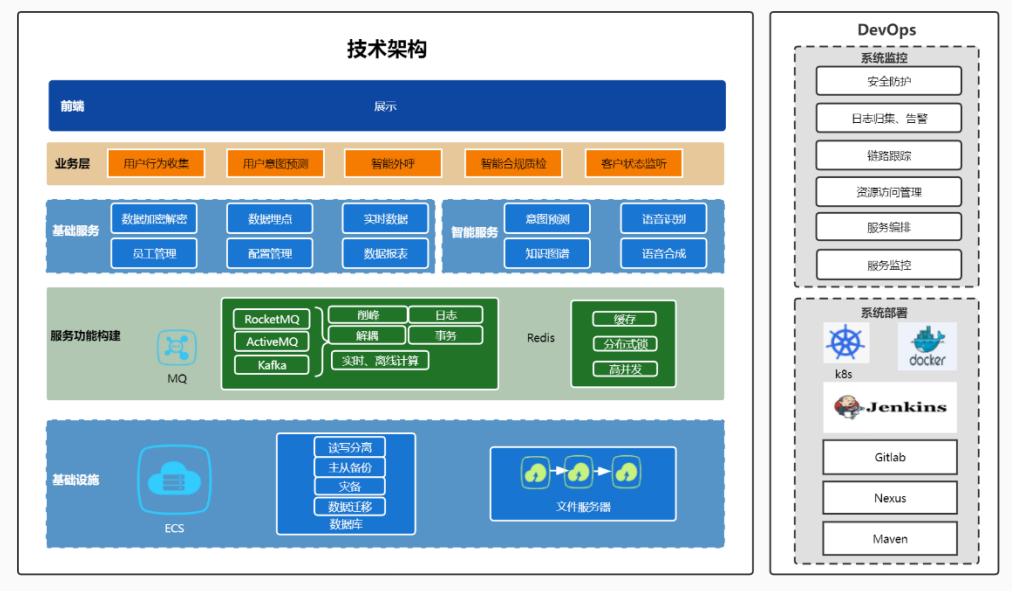

图 1：整体架构图

析等营销的质量报告。

任务管理单元则是平台运行的控制单元，该单元连接智能化单元和行为监控单元，从行为监控单元中抓取数据，并实时生成任务，然后将该任务分配给公司内的营销人员。任务生成单元内置任务生成引擎，采用可配置模型实现任务的自动生成和匹配。任务管理则是为管理员用户提供的核心功能，可实现任务的重定向、删除等操作。任务执行实现了基于公司 IP 电话的一键拨打功能，该模块同时提供话术推荐服务，可针对客户的停留步骤和其他配置信息提供优秀话术。数据统计单元则提供了基础的管理员服务，实现员工、渠道、总览的报表数据服务，为运营决策提供数据支持。

2.2 核心技术

2.2.1 轻量级用户行为埋点监听

埋点是数据采集领域的术语，指的是针对特定用户行为或事件进行捕获、处理和发送的相关技术及其实施过程。埋点可以为后续的产品优化和用户运营提供可供参考的业务数据及其附带信息。根据部署的位置可以分为客户端埋点和服务端埋点，而客户端埋点可以根据埋点工具的方式划分，可以分为三种类型：代码埋点，可视化埋点和全埋点。综合考虑数据采集有效性、客户端可靠性以及移动端的电量、流量和内存消耗，本平台采用统一代码埋点，即部署完基础的 SDK 后，在需要采集数据地方添加跟踪代码，APP 启动的时候会初始化 SDK，数据采集位置被触发的时候就会调用 SDK 对应的数据接口把数据发送出去。基础埋点 SDK 将上报用户界面点击进度，并发至后端消息队列中。

本平台采用 Kafka 消息队列，通过监听 Kafka 消息队列即可完整接收全部客户的实时状态信息，基于客户全流程信息，即可实现流程信息的分析，通过用户的行为实现预测与诊断。

2.2.2 智能外呼系统

传统电话客服模式中，外呼人员的服务承载能力有限，无法应对数量庞大的电话交流场景，并且众多重复性问题会造成人力资源的浪费。为了保障营销服务的时效性，降低营销服务成本，智能外呼应运而生。智能外呼主要采用智能机器人进行电话外呼服务，用以提高公司主动与用户联系沟通的效率。智能外呼系统能够模拟真人与客户进行电话沟通，引导用户完成电话主流程任务，支持实时意图识别、开放域提问，且在回答开放域问题后能够引导客户关注主流程。智能外呼的核心是赋予产品语音识别、理解以及合成的能力。

智能外呼系统由话务模块、语音服务模块、算法模块、对话管理模块以及运营管理平台组成。其中话务模块管理话务能力方面的功能，例如语音通讯、录音等；语音服务模块负责语音方面的工作，包括自动语音识别以及自然语言合成；算法模块是外呼机器人的核心组件，需要完成数据的处理、模型的构建与训练等，让机器人具备识别与交互能力；对话管理模块的工作是在机器人识别客户的意图之后，对回复的内容进行生成；运营管理平台负责系统的日常管理，通过制定用户名单以及外呼策略，实现在限定时间范围内向目标客户进行自动呼叫。

为了更好地进行营销与服务客户，实现量质并举，平台会在对客户进行意图预测后依据预测的意向对客户进行分类。对于意愿较弱的客户，由智能机器人进行服务，智能机器人会告知客户开户流程未完成，并提供常见问题的智能问答。此外，平台会询问客户是否需要人工指引，若客户回复需要，则通过多轮对话的形式沟通客户需求，并将需求以工单形式发送给客户经理，客户经理则会根据工单及时服务客户，及时解答客户问题。

2.2.3 基于客户行为及画像的意图预测

目前大多数系统均将与客户的实时通话内容作为意图识别的主要特征来源，这导致在未与客户接触时缺乏对于客户的了解。传统外呼服务中

心缺乏一套智能决策系统来预测业务办理中断客户需要帮助的紧急程度以及业务办理意图强弱。为此，本平台根据预测模型，建立分级的外呼服务策略，将外呼服务分为直接人工外呼的高优先级，先进行智能外呼的中优先级，以及不进行外呼的低优先级，解决服务不及时和效率低下的问题，提升营销效果。

本平台设计了一种基于客户行为及画像的意图预测方法，该方法针对业务办理中断的客户进行实时预测，预测客户最终业务办理成功率以及客户中断的原因，并将办理高成功率客户作为高优先级，引导营销人员优先处理。该方法收集客户流程特征与个人信息，其中流程特征包括客户业务办理进行的步骤总数、客户回退的步骤总数、客户平均停留时长、客户历史停留超时次数、客户当前停留步骤、客户是否主动回退和客户历史意愿；客户个人信息包括客户的基本信息，即户籍地址、住址地址、教育程度、性别、年龄等。其中“客户历史意愿”即为用户历史对话中办理意愿的强弱，是根据该业务的客户历史对话语音，在提取文本矩阵后输入至双向长短时神经网络 BiLSTM 的意图检测模型获得的。

预测的整个流程为，将客户全部信息输入二分类器，该二分类器根据历史数据训练而来，用于对客户产品办理是否成功进行预测，并给出具体成功概率。考虑到模型运行的运行速度，该二分类器在本文中采用轻量级的 LightGBM 实现，LightGBM 以直方图算法代替 XGBoost 的与排序算法构建的数据结构，大幅度提升了训练速度减少了内存消耗，并且采用按叶生长（Leaf-wise）的策略代替按层生长（Level-wise）策略，增加了最大深度的限制，保证高效的同时防止过拟合。

2.2.4 实时合规质检的 IP 电话设计

本平台的营销电话采用基于 VoIP 协议软交换平台 FreeSWITCH 的电话语音呼叫系统，又称作两端呼，即一端通过 IP 电话机或 IP 软电话连接客服人员，另一端通过传统的 PSTN 电话网络连接客户。实现员工电话录音的集中管理，并对外开放接口以供第三方系统调用。员工在拨打客户电话时，员工侧采用 IP 电话（软电话）来拨打，不占用电话线路，节省线路资源与费用。此外，两端呼电话与系统自动挂接，实现了对话语音的自动上传与实时质检分析，设计架构如图 2 所示。

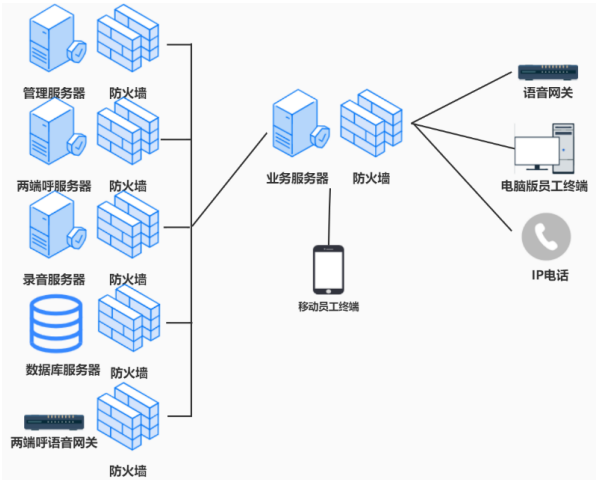

图 2：两端呼电话架构

两端呼电话采用云端部署，通过 TLS 对信令加密和 SRTP 对语音数据加密实现数据传输的安全性，同时底层构建管理服务器、录音服务器、知识库服务器、语音网关等底层服务单元。基于两端呼 IP 电话，可以实现录音的文件的实时获取，系统可在电话过程中实现实时话术提醒与实时语音质检，营销平台与电话系统通过 restful 接口进行对接，实现一键拨打，录音收听，智能质检等功能。

2.2.5 基于延迟队列的自定义监听方案

延迟队列就是进入该队列的消息会被延迟消费的队列。而一般的队列，消息一旦入队了之后就会被消费者马上消费。生产者把消息发送到消息队列中以后，并不期望被立即消费，而是等待指定时间后才可以被消费者消费，这类消息通常被称为延迟消息。一般通过最大生存时间（Time-To-Live）和死信交换机（Dead Letter Exchanges）两个特性模拟出延迟消息的功能。消息超过最大生存时间没有被消费就成为一条死信，便会被重新投递到死信交换机，然后死信交换机根据绑定

规则转发到对应的死信队列上，监听该队列就可以让消息被重新消费。

本平台实现可自定义的延迟管理单元，采用基于 RabbitMQ 的 delayed message exchange 插件实现任意时长的毫秒级监听，该插件支持延迟投递机制的 Exchange 类型，在接收到该类型的消息后不会立即将消息投递至目标队列中，而是存储在 mnesia 表中，检测消息达到可投递时间时再投递到目标队列，基于该插件的二次开发和封装，本平台实现了监听管理、延迟启停、延迟配置管理、延迟队列管理等一系列标准化功能，实现用户监听的千人千面，即可根据用户进度信息、客户个人信息等构建任务生成模型，使不同客户的状态监听时长自定义，例如某些直播渠道因为营销实时性高，延迟定义为较小。

3、智能化建设成效

3.1 实现精准且专业的营销

平台采用预测技术对客户综合信息进行快速评估，帮助员工在海量客户中过滤高潜力客户，提升工作效率，实现点对点的精准营销。本文提出的平台有效提升了服务流程的标准化与营销团队的专业化程度。此外，基于智能外呼、人工外呼及短信的营销方式能够全方位触达客户，营销与服务结合的模式能够以为客户解决问题为出发点附带营销，提升客户服务体验的同时兼顾业绩提升。

3.2 提高营销服务的规范性

平台实现了基于 IP 电话的智能合规质检功能，员工可以通过平台一键拨打电话，语音数据及拨打记录会实时存储在后端云盘。平台通过搭建完整的合规风险分析模型，建立员工合规风险画像，并通过对营销服务过程的实时合规监控实现对员工的潜在合规风险预警，有效提高员工的合规意识，保证营销服务的规范性。

3.3 降本增效与业绩提升

智慧营销服务平台创新性地引用了多种智能化组件，将传统电话营销系统进行数字化改造，实现智能客户行为跟踪、客户行为预测、客户画像分析等一系列创新性应用，平台应用后效果明显，依据智能预测开展的营销可有效降低对于客户的打扰，同时减少了外呼人员的人力资源成本。根据客户意图预测模型进行的精细化营销实现了客户开户率的稳步提升。上线以来，平台运行良好，实现了服务体验、合规管控与业务转化的齐头并进与良性发展，客户满意度稳步提升。

4、总结

中信建投证券以智能化为引领，在推进智慧营销平台建设上持续深入，努力打造贯穿用户全周期的数字化智能营销服务，通过数据驱动，智能地为客户匹配适宜的服务和产品，实现高效、合规、精细的服务。以数据为核心构建的智能化体系将成为支撑未来券商发展的关键，智慧化建设在金融行业具备广阔前景，将对未来证券业态发展产生深远影响，着力布局智能应用将成为券商的必由之路。随着区块链技术的快速发展，营销平台未来可以在营销结算、利益分配等方面发力，利用区块链技术去中心化、公正性和透明性、防伪、防篡改、准匿名性、交易可追溯等特点，可更好地在实现合规的前提下提高营销分配效率与完善奖惩机制。随着人工智能算法的不断进步，深度强化学习、自动化机器学习以及大模型为代表的新兴模型在解决问题的多样性、结构复杂度、训练数据规模等方面有了显著提高，为此营销平台要不断紧跟新技术、探索新方法、实现新突破。百舸争流千帆竞，乘风破浪正远航，未来中信建投证券将继续以时不我待、只争朝夕的精神，保持对智能化建设的敏感度，发挥自身资源优势，不断增强客户服务水平，以向客户提供优质高效服务为目标而不断努力！

参考文献：

[1] 于建彬，邱轲．智能化转型背景下提升现金服务的路径选择 [J]. 金融发展研究 ,2020(8):4.

[2] 李婕．商业银行网点智能化建设研究 [J]. 现代经济信息 ,2018(21):267.

[3] 王琛．国内证券公司客户服务变化趋势 [J]. 经贸实践 ,2017(03):67-69.

[4] 苗英哲．互联网金融背景下券商网络营销对策 [J]. 山西农经，2019(23):2.

[5] 刘艳丽，刘心义，林黎钦．基于适当性管理的用户画像助力智慧营销研究 [C]. 创新与发展：中国证券业 2017 年论文集 .2018.

[6] 刘新霞，廖信超．全渠道智能营销平台建设探索 [J]. 金融科技时代 ,2022,30(3):5.

[7] 张巍，唐琴．人工智能客服软件企业营销渠道管理探析 [J]. 现代工业经济和信息化 ,2021,11(9):3.

[8] 苏萌．隐私计算在智能营销中的应用 [J]. 金融电子化 ,2022(1):3.

[9] 侯晓．银行 " 零接触 " 营销服务体系建设 [J]. 中国金融 ,2021.

证券行业网站智能数据搜索服务的研究与实践

季晓娟、王中澎、李炜、赵冬昊、王汉杰、李蓉 / 上证所信息网络有限公司 上海 200120
E-mail：xjji@sse.com.cn

为加快推进数字化建设，打造数字智能型交易所，上交所积极研究探索技术创新，强化搜索对网站服务的赋能。本文主要介绍了上海证券交易所网站智能数据搜索服务的建设历程，重点讲述了建设目标、成果及未来方向等内容。希望可以给致力于科技赋能的读者以启发，共同探索以科技创新增强用户获得感之路。

1、概述

近年来，我所加快推进数字化建设，积极推动业务、技术、数据的深度融合。为切实服务市场主体，集中精力提升服务体验，我所完成了网站智能数据搜索服务的研究与系统建设，将人工智能和搜索引擎技术相结合，为网站用户获取披露数据提供更加便捷、有效、易读的服务体验。

2、系统建设效果

网站智能数据搜索服务体验版于 2020 年底上线并对市场提供试点服务，日均调用量超过一万次，陆续收到市场良好反馈。根据我所“我为群众办实事”实践活动中“持续听取广大群众和市场各方的合理诉求，扎扎实实办好大家关注、关心、关切的实事”的相关指示精神，我所常态化开展网站用户调研和搜索服务用户意见征集等活动，并以此为基础，积极改进搜索服务体验。从反馈情况看，用户对数据获取的效率与阅读体验提升的需求较为迫切。因此，我所开展了网站智能数据搜索服务的算法自研、数据扩展、语义模型训练、功能迭代、数据验证，将数据搜索服务由官网试点转为网站群全面服务。以下进行具

体建设效果介绍。

2.1 实现搜索意图的“智能处理”。

实现了将人类口语化语言转换为机器能识别的“数据语言”，进而从海量数据中搜索答案并精准高效地反馈结果。支持更口语化的表述作为系统输入，支持多实体组合及数据指标的处理，有效桥接用户需求和网站数据间的语义鸿沟，提升了用户获取披露数据的便捷性。

2.2 实现数据内容的“一键直达”。

扩展数据范围至网站群，扩展后的数据范围涵盖股票、债券、基金等多产品，贯穿注册审核、发行承销、上市交易等阶段，解决了站点栏目分散不易查找的问题，提升了用户获取披露数据的有效性。

2.3 实现搜索结果的“友好交互”。

统一搜索入口，根据用户搜索意图聚合展示数据、公告、规则等相关结果，并新增五大类搜索频道，支持细分用户搜索场景，提升了用户获取披露数据的易读性。

3、技术突破点

3.1 整体架构

网站智能数据搜索服务的整体架构图如图 1 所示，主要包括数据源层、数据采集层、数据存储层、逻辑处理层、应用层。

（一）数据源层：搜索的数据源来自于上交所官网、子网站、应用及部分行业知识。

（二）数据采集层：采集的过程通过解析文件、数据库，并通过 REST API 还有消息队列交互。

（三）数据存储层：数据被采集加工后被重新组织并存储，被存储为文件、ES 中的索引信息、还有经过逻辑清洗的结构化数据。

（四）逻辑处理层：在处理搜索 QUERY 请求时，运用了自然语言处理技术，分词、同义词、改写实体识别等技术将输入 QUERY 构建为多层（layer）语义信息。通过关键字段如证券代码将结构化数据建立关系，通过 NLP 模型判断权重，映射为可能性最高的 SQL 语句

图 1：整体架构图

去做查询。

（五）应用层：顶层在应用层构建，输出语义理解能力。

3.2 技术与功能创新

本项目基于证券行业先验知识和预训练模型构建了混合架构语义解析引擎。技术先进性及阶段性成果主要如下：

一是基于数据关系的自动发现方法，将数据知识化，构建数据实体间的关联关系，为智能分析提供决策依据。

二是基于行业先验知识，构建实体及意图识别模型，避免过度泛化，提升了实体及意图识别模型的准确率，模型训练过程中使用的训练语料达 300 万条。

三是优化推理模型网络结构，实现高效在线实时运算。采用粗排、精排、网络结构剪枝、GPU 和 CPU 混合计算、半浮点数运算等方法，突破了在线实时交互查询的运算瓶颈，在准确率得到保障的情况下，计算效率提升了 6 倍。

4、未来挑战

网站智能数据搜索服务是基于人工智能技术、搜索引擎技术与我所数据信息的综合应用。技术方面，涉及搜索引擎技术、人工智能技术等多种技术的研究发展。信息来源方面，接入数据的质量、用户行为数据粒度对结果产生直接影响。应用方面，市场对个性化与多元化搜索体验的要求不断提高。因此，作为数字化时代的基础设施应用，需持续进行技术迭代、行业反馈、服务运营的积累与更新。

5、总结展望

我所已初步完成网站智能数据搜索服务的建设，该服务提升了用户获取数据服务的效率与体验，基于搜索服务实践经验，我所将积极推进落实上交所网站搜索引擎建设，强化多源多态信息的融合搜索，持续提升数字化基础设施的服务能力，强化数字科技对资本市场的有效支撑。

关于ION GROUP遭遇勒索病毒攻击事件的分析思考报告

张涛、卢雅哲、徐广斌、谢毅 / 上海证券交易所 信息科技部 上海 200120
E-mail：yzlu@sse.com.cn

1 月 31 日，国际金融行业关键软件提供商英国 ION Group 遭遇勒索病毒攻击，攻击使得衍生品系统无法完成保证金计算、主要市场头寸监管报送等。美国财政部、商品期货交易委员会、欧洲央行等纷纷就此事件发声。据 2 月 9 日报道，大部分受影响的业务已恢复运行。事件发生后，上交所密切关注进展，持续跟踪境内外媒体报道，对事件进行思考分析，并对行业防范供应链网络与信息安全风险提出启示与建议。

1、事件整体综述

ION Group 是一家软件公司，其产品被金融机构、银行和公司广泛用于交易、投资管理和市场分析。1 月 31 日早间，ION Group 的服务器遭遇严重网络攻击，整个通信网络瘫痪数小时，导致期货交易匹配和保证金计算业务无法正常运行。该事件影响了其位于欧洲和美国的 42 个客户，其中包括荷兰银行清算所（ABN Amro Clearing）和意大利联合圣保罗银行（Intesa Sanpaolo）。该事件迫使多家银行和经纪人手动处理交易，美国商品期货交易委员会（CFTC）宣布推迟三周发布其交易商承诺报告，泛欧证券交易所（Euronext N.V.）宣布推迟发布大宗商品衍生品持仓周报。

黑客组织 Lockbit 于 2 月 2 日将 ION Group 添加到其数据泄露网站的受害者名单中，声称在入侵期间窃取了数据，并威胁 2 月 4 日前不缴纳赎金，将公布这些数据，对 ION Gruop 进行文件加密和数据披露的“双重勒索”。文件加密导致受害方无法访问和获取系统中文件和数据，系统崩溃，但此类攻击受害方可通过备份数据进行恢复；数据披露，即攻击方以公开其敏感数据要挟受害方缴纳赎金。2 月 4 日 ION Group 支付了赎金，

LockBit将其移出受害者名单,并对系统进行恢复,2 月 7 日 ION Markets 系统基本恢复运行。

2、事件影响

衍生品投资的结算具有时间敏感性，多家机构在 2 月 1 日表示此次攻击对其业务造成了严重影响。伦敦洲际交易所（ICE）宣布，已将维持头寸的截止时间从上午 10 点延长至中午，并警告，延期将导致未平仓合约延迟公布，受攻击影响期间可能错误陈述未平仓合约。商品期货交易委员会（CFTC）表示，ION 的中断正在影响其一些成员向其提供及时和准确数据的能力。多家交易所运营商表示，攻击可能会影响当天按时发布交易所报告。荷兰银行（ABN Amro Bank NV）的美国清算部门表示，中断将延迟其隔夜处理，并将在 2 月 1 日继续手动操作。美国期货业协会（FIA）正在评估该事件对 ION Group 造成的破坏后果，并在声明中表示，此次攻击影响了 ION 客户在全球交易所衍生品的交易和清算。英国金融行为监管局（FCA）正在与同行合作，帮助受影响的金融服务公司。

3、攻击过程分析

据分析，在过往攻击中，黑客组织 Lockbit 攻击过程大致可分为初始入侵、深入渗透和目标达成三个阶段。

初始入侵阶段，Lockbit 主要采用三种策略获取访问权限。一是单刀直入，非法购买或暴力破解远程登录账户。二是迂回包抄，采用社会工程学策略，向目标用户发送带有恶意附件的“钓鱼”电子邮件。三是大刀阔斧，借助大规模漏洞扫描定位潜在目标，利用应用程序漏洞获取初始感染机会。

深入渗透阶段，Lockbit 进一步提升权限，扩大感染面，探测内部网络敏感数据。一是通过渗透工具或诱饵文件得以加载执行。二是为进一步扩大感染面，通过各种权限提升工具来扩展对系统的访问权限，一旦进入域控制器，即可通过 SMB（一种通信协议）连接传播到其他系统，或在网络中横向扩展。三是躲避受害者系统安全防护产品检测，利用进程管理工具禁用安全软件，或直接利用域管理员权限关闭系统防护，再者伪装成常见的 PNG 图像格式来隐藏可执行文件。

目标达成阶段，Lockbit 在感染多台主机后实施数据加密和渗出。加密环节，收集各类系统信息，在不影响正常运行下，开始加密其可以访问的本地和远程设备上的所有数据。渗出环节，通过云存储工具上传所窃取的文件；使用窃密木马，盗取用户数据文件以对受害者进行数据披露勒索。

完成攻击后，lockbit 会在其网站公布受害者信息，并以邮件等方式向受害者进行勒索，赎金要求以比特币和门逻币等区块链货币支付。

4、思考与启示

网络和信息安全工作事关国家安全、政权安全和经济发展。此次 ION Group 遭遇勒索病毒攻击对全球衍生品交易产生了极大的负面影响。据知名网络安全厂商 Imperva 研究，全球网络攻击事件中，针对金融机构的攻击占比高达 28%，采取供应链或“跳岛”的方式进行攻击,越来越普遍。根据此次事件分析结果，结合我国证券期货行业的实际情况，从防范供应链安全风险角度，提出几点启示。

一是警惕供应链上下游的网络安全风险。随着金融交易向更快、更自动化发展，ION 这样的软件公司逐渐蓬勃壮大，已成为现代金融市场管道中越来越重要的部分。对 ION 的攻击，体现出金融系统的相互关联性和对软件的强烈依赖性。建议证券期货行业重点单位梳理重要系统供应链

上下游厂商，对其基础设施、工具、开源组件、源代码和配置开展评估，定位和降低漏洞风险。

二是加强证券期货行业的攻击面风险管理。攻击面指任何可能受到攻击的载体，包括与互联网连接的系统、供应商链、移动设备、物联网和员工。证券期货行业可联合加强攻击面风险管理，对行业依赖度较高的供应商和服务商进行常态化监测。

三是针对类似攻击事件开展应急演练和沙盘推演。金融领域的网络攻击不再仅仅是针对金融企业本身，而是转向攻击其数字化转型的关键供应商。证券期货行业可联合开展此类情况的应急演练，并针对供应链上下游厂商遭受攻击的各类极端情况，开展沙盘推演。

I 信息资讯采撷
nformation

监管科技全球追踪

监管科技全球追踪

12 月 22 日，国际清算银行发布报告《可持续金融中的信息治理》（以下简称报告）。

12 月 27 日，中国银保监会发布《外国银行分行综合监管评级办法（试行）》（以下简称《办法》），目的在于进一步完善外国银行分行监管评级体系，合理配置监管资源，加强分类监管，促进外国银行分行稳健运营。

1 月 4 日，英国首相表示，英国已通过 260 亿英镑有效保护了收入较低的人群，并稳定了国内经济与抵押贷款利率。

1 月 4 日，2023 年人民银行工作会议以视频形式召开。会议深入学习贯彻党的二十大和中央经济工作会议精神，总结 2022 年和五年来主要工作，分析当前形势，部署 2023 年工作。

1 月 4 日，日本金融科技公司 SmartPay 在日本、沙特阿拉伯及阿联酋推出了新的数字客户金融服务 SmartPay Bank Direct。

1 月 8-9 日，国际清算银行在瑞士巴塞尔召开行长例会，中国人民银行行长易纲出席了新兴经济体行长会、经济顾问委员会会议、全球经济形势会等会议，与会央行行长们就全球经济金融形势、新兴经济体如何面对全球冲击以及汇率调整的挑战等问题进行了交流。

1 月 11 日，英国国家网络安全中心发文建议机构通过托管服务提供商管理运维云服务。

1 月 11 日，丹麦央行及 7 家商业银行遭受了分布式拒绝服务攻击（Distributed denial of service attack，DDoS）。

1 月 12 日，欧洲银行管理局、欧洲保险与职业养老金管理局和欧洲证券和市场管理局联合发布了一份关于数字化国家金融教育计划的联合主题报告，重点关注网络安全、诈骗和欺诈等问题。

1 月 13 日，证监会、人民银行联合发布《公开募集证券投资基金信息披露电子化规范》金融行业标准，标准自公布之日起施行。

2 月 2 日，亚马逊云科技（Amazon Web Services，AWS）宣布，全球领先的保险公司苏黎世保险集团选择 AWS 作为其云服务提供商，并迁移其企业 IT 基础设施至 AWS。

2 月 4 日，人民银行易纲行长前往通州参加北京城市副中心打造国家级绿色交易所启动仪式并发表讲话。

2 月 8 日，英国央行（The Bank of England）

公布了针对金融市场基础设施（Financial Market Infrastructures，FMIs）外包和第三方风险管理政策。

2月9日，端到端金融科技和监管科技解决方案提供商CSI宣布，其全面的预构建开放API套件促进了金融科技公司ECHO Health和MOCA Financial与金融机构的合作伙伴关系，助力部署银行即服务（BaaS）和支付计划。

2月14日，上海银行火花平台发布会在上海城创金融科技国际产业园举办，在上海市国资委指导下，邀请了华东师范大学长三角金融科技研究院、上海金融科技产业联盟等政研企机构共同参与。

2月15日，英国金融行为监管局创新部门成立了合成数据专家组，成员包括监管机构、咨询公司、法律专业人士、消费者团体等，旨在研究金融市场中使用合成数据相关问题。

2月16日，金融科技公司Wedge宣布与Visa合作，共同推出连接到Wedge应用程序的借记卡，改善用户消费体验。

2月21日，新加坡金融管理局（Monetary Authority of Singapore，MAS）和印度央行（Reserve Bank of India，RBI）联合推出PayNow-UPI实时跨境支付服务，并启动了新印间统一支付接口的连接。

2月23日，人民银行会同银保监会、证监会、外汇局、广东省人民政府联合印发《关于金融支持横琴粤澳深度合作区建设的意见》和《关于金融支持前海深港现代服务业合作区全面深化改革开放的意见》。

2月27日，国务院印发《数字中国建设整体布局规划》。《规划》指出，建设数字中国是数字时代推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑。

2月28日，美国网络安全与基础设施安全局（Cybersecurity and Infrastructure Security Agency，CISA）发布网络安全警示报告。报告公布了CISA近期在大型关键基础设施（运营）机构红蓝对抗测评中的关键发现，提出了监测和强化网络环境的改进办法。

3月8日，英国央行、英国金融行为监管局、审慎监管局和支付系统监管机构就2013年签署的一份谅解备忘录进行了年度审查。该备忘录制定了监管机构在英国支付系统方面合作的高级框架，并要求各家机构每年对谅解备忘录进行审查。

2023年一季度《交易技术前沿》征稿启事

《交易技术前沿》由上海证券交易所主管、主办，以季度为单位发刊，主要面向全国证券、期货等相关金融行业的信息技术管理、开发、运维以及科研人员。2023 年二季度征稿主题如下：

一、云计算

（一）云计算架构

主要包含但不限于：云架构剖析探索，云平台建设经验分享，云计算性能优化研究。

（二）云计算应用

主要包含但不限于：云行业格局与市场发展趋势分析，国内外云应用热点探析，金融行业云应用场景与实践案例。

（三）云计算安全

主要包含但不限于：云系统下的用户隐私、数据安全探索，云安全防护规划、云安全实践，云标准的建设、思考与研究。

二、人工智能

（一）应用技术研究

主要包含但不限于：语音识别与自然语言处理，计算机视觉与生物特征识别，机器学习与神经网络，知识图谱，服务机器人技术。

（二）应用场景研究

主要包含但不限于：智能客服、语音数据挖掘、柜员业务辅助等。

主要包含但不限于：监控预警、员工违规监控、交易安全等。

主要包含但不限于：金融预测、反欺诈、授信、辅助决策、金融产品定价、智能投资顾问等。

主要包含但不限于：金融知识库、风险控制等。

主要包含但不限于：机房巡检机器人、金融网点服务机器人等。

三、数据中心

（一）数据中心的迁移

主要包含但不限于：展示数据中心的接入模式和网络规划方案；评估数据中心技术合规性认证的必要性；分析数据中心迁移过程中的影响和业务连续性；探讨数据中心迁移的实施策略和步骤。

（二）数据中心的运营

主要包含但不限于:注重服务，实行垂直拓展模式;注重客户流量，实行水平整合模式;探寻数据中心运营过程中降低成本和提高服务质量的途径。

四、分布式账本技术（DLT）

（一）主流分布式账本技术的对比

主要包含但不限于：技术架构、数据架构、应用架构和业务架构等。

（二）技术实现方式

主要包含但不限于：云计算 + 分布式账本技术、大数据 + 分布式账本技术、人工智能 + 分布式账本技术、物联网 + 分布式账本技术等。

（三）应用场景和案例

主要包含但不限于：结算区块链、信用证区块链、票据区块链等。

（四）安全要求和性能提升

主要探索国密码算法在分布式账本中的应用，以及定制化的硬件对分布式账本技术性能提升的作用等。

五、信息安全与 IT 治理

（一）网络安全

主要包括但不限于：网络边界安全的防护、APT 攻击的检测防护、云安全生态的构建、云平台的架构及网络安全管理等。

（二）移动安全

主要包括但不限于：移动安全管理、移动互联网接入的安全风险、防护措施等。

（三）数据安全

主要包括但不限于：数据的分类分级建议、敏感数据的管控、数据共享的风险把控、数据访问授权的思考等。

（四）IT 治理与风险管理

主要包括但不限于：安全技术联动机制、自主的风险管理体系、贯穿开发全生命周期的安全管控、安全审计的流程优化等。

六、交易与结算相关

（一）交易和结算机制

主要包含但不限于：交易公平机制、交易撮合机制、量化交易、高频交易、高效结算、国外典型交易机制等。

（二）交易和结算系统

主要包含但不限于：撮合交易算法、内存撮合、双活系统、内存状态机、系统架构、基于新技术的结算系统等。

投稿说明

1、本刊采用电子投稿方式，投稿采用 word 文件格式（格式详见附件），请通过投稿信箱 ftt.editor@sse.com.cn 进行投稿，收到稿件后我们将邮箱回复确认函。

2、稿件字数以 4000-6000 字左右为宜，务求论点明确、数据可靠、图表标注清晰。

3、本期投稿截止日期：2023 年 6 月 30 日。

4、投稿联系方式 021-68607129，021-68607131 欢迎金融行业的监管人员、科研人员及技术工作者投稿。稿件一经录用发表，将酌致稿酬。

《交易技术前沿》编辑部

证券信息技术研究发展中心（上海）

附件：投稿格式（可通过电子邮件索要电子模板）

标题（黑体 二号 加粗）

作者信息（姓名、工作单位、邮箱）（仿宋 GB2312 小四）

摘要：（仿宋 GB2312 小三 加粗）

关键字：（仿宋 GB2312 小三 加粗）

一、概述（仿宋 GB2312 小三 加粗）

二、一级标题（仿宋 GB2312 小三 加粗）

（一）二级标题（仿宋 GB2312 四号 加粗）

1、三级标题（仿宋 GB2312 小四 加粗）

（1）四级标题（仿宋 GB2312 小四）

正文内容（仿宋 GB2312 小四）

图：（标注图 X. 仿宋 GB2312 小四）

正文内容（仿宋 GB2312 小四）

表：（标注表 X. 仿宋 GB2312 小四）

正文内容（仿宋 GB2312 小四）

三、结论 / 总结（仿宋 GB2312 小三 加粗）

四、参考文献（仿宋 GB2312 小四）

电子平台

欢迎访问我们的电子平台 http://www.sse.com.cn/services/tradingtech/transaction/ 。我们的电子平台不仅同步更新当期的文章，同时还提供往期所有历史发表文章的浏览与查阅，欢迎关注！

联系电话：021-68607129
021-68607131
投稿邮箱：ftt.editor@see.com.cn

ITRDC
证券信息技术研究发展中心（上海）
上海证券交易所 SHANGHAI STOCK EXCHANGE
中国上海市杨高南路388号
邮编：200127
公众咨询服务热线：4008888400
网址：http://www.sse.com.cn

内部资料 免费交流
本资料仅为内部交流使用，本季度印200册，编印单位为上海证券交易所，面向证券期货行业发送，印刷日期为2023年5月，印刷单位为上海长鹰印刷厂。