

金融数据中心发展 白皮书



联合发布：北京软件和信息服务业协会 金科创新社

2023年12月

版权声明

本报告版权属于北京软件和信息服务业协会及金科创新社，并受法律保护。
转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明来源。违反
上述声明者，本团队将追究其相关法律责任。

编委会

主编：魏生

执行主编：李庆莉

编委会成员：刘莉

编写组成员：戴科冕、黄秋宜、张一斌、童阳

前言

在当今的数字化时代，金融数据中心作为金融行业的核心支撑设施，正在经历前所未有的发展和变革。本白皮书旨在深入探讨金融数据中心的发展历程、当前状态以及未来趋势，为金融行业的持续创新和卓越运营提供指导和洞见。

报告的第一部分，首先回顾了金融数据中心的发展历史，从最初的简单数据存储和处理设施，逐步演变为今天高度复杂和动态的环境。其次，深入分析了数据中心技术的演进路径，包括基础设施、运营模式、安全性和合规性等关键领域。报告重点强调了在云计算、大数据、人工智能等技术推动下，数据中心如何转型以满足日益增长的业务需求，并着重讨论了数据中心面临的一系列挑战，包括技术快速发展带来的适应性问题、日益严峻的安全威胁以及保障资源环境可持续性要求等。报告提供了应对挑战的策略和建议，指导金融机构在业务创新的同时，确保其数据中心的安全性、可靠性和合规性。最后，展望了金融数据中心的未来发展方向，特别是在技术创新、业务模式变革和全球金融市场中的角色定位。强调了人才培养、技术升级和策略调整的重要性，力求为金融数据中心转型升级提供一个清晰的路线图，助力其抓住变革时代的机遇。

报告的第二部分，探讨了数据中心在支持金融机构现代化转型中的关键作用。通过对多个实际案例的分析，如北京地区的几个主要数据中心项目，展示了如何有效地利用数据中心来优化运营效率、提升服务质量、增强风险管理能力，并最终加强机构的竞争优势。

本报告不仅为金融行业的决策者、技术专家和运营管理人员提供了深刻的洞见和实用的指导，也为广泛的业界人士提供了对金融数据中心发展的全面理解。我们希望，通过本报告，读者将更好地理解金融数据中心在现代金融生态系统中的重要性，并能够为应对未来的挑战做好准备。

目录

第一部分 金融数据中心发展报告	01
一、数据中心内涵的变迁	01
二、数据中心技术及应用架构的发展	02
（一）数据中心技术架构的发展	02
（二）数据中心应用架构的发展	03
（三）数据中心技术创新及其影响	05
（四）小结	05
三、金融数据中心发展历程及建设原则	05
（一）金融数据中心的发展历程	05
（二）金融数据中心的建设原则	06
（三）金融数据中心的安全措施及合规性	07
（四）金融数据中心的业务连续性和灾难恢复	09
（五）小结	10
四、金融数据中心未来发展趋势和要求	10
（一）集约高效，绿色低碳	10
（二）多地多活，分层协同	14
（三）数据驱动，智能运维	14
（四）人才和技能培养	15
（五）挑战和机遇	16
（六）小结	17
第二部分 金融数据中心应用报告	18
一、数据中心应用架构概述	18
（一）对象、目标和范围	18
（二）整体框架	20
（三）评价标准	22

二、数据中心应用发展趋势	24
(一) 数字化运维体系概述	24
(二) 数据驱动下的 DataOps 运维体系	24
(三) AIOps 智能运维体系	27
(四) DevOps 研发运维一体化	28
三、北京金融数据中心建设实践	30
一、华夏银行：全栈云数据中心实践项目	32
二、爱心人寿：云上云下异地灾备中心项目	35
三、北京农商银行：运行版本变更自动化项目	38
四、华夏银行：华夏同城双活机房网络建设及搬迁实施项目	41
五、大童保险服务：快保云服平台	50
六、阳光保险集团：云杉容器云平台	53
七、爱心人寿：DevOps 实践	56
八、华泰人寿：安全运营中心	60
九、瑞泰人寿：智慧审计信息云系统	62
十、北京农商银行：高端 NAS 存储双活建设项目	64
十一、人保科技：中国人保集团北方信息中心建设项目	68
十二、阳光保险：小审阳 1 号——智能关系网络分析平台	69
十三、阳光产险信保事业部：智能运营管理可视化平台	74
十四、阳光财险：全能保双活建设	76
十五、时速云：分布式支撑平台建设解决方案	78
十六、新华三集团：SeerFabric 金融智能无损数据中心解决方案	80
十七、神州云科：云科透明湖应用交付弹性计算解决方案	83
十八、西骏数据：数据库统一操作平台	84
十九、博云：容器云平台解决方案	86
二十、嘉为蓝鲸：嘉为鲸翼多云管理平台解决方案	87
二十一、嘉为蓝鲸：灾备切换管理中心解决方案	90

第一部分 金融数据中心发展报告

一、数据中心内涵的变迁

数据中心作为信息处理和管理的枢纽，在金融行业的发展中扮演着至关重要的角色。随着信息科技的不断演进，金融机构的数据集中趋势日益显著，数据中心的作用与日俱增。广义上，数据中心被定义为一个集成的 IT 应用环境，它不仅支撑着各种应用服务，如数据计算、网络、存储、安全等，而且提供了数据备份、数据恢复、数据管理和联网控制等关键服务。随着计算机及网络通讯技术的发展，以及数字经济的兴起，数据中心的内涵和功能不断变化，大致可划分为四个阶段（如图 1-1-1 所示）。



图 1-1-1 数据中心内涵变迁的四个阶段

1. 数据存储中心阶段

这一阶段，数据中心主要作为金融机构办公自动化设施或电子文件的集中管理场所，尽管功能较为单一，仅支持数据的存储和基础应用，但已经具备基本的基础设施支持和数据安全性保障功能。

2. 数据处理中心阶段

随着金融行业内部基于局域网的管理信息系统（如 MIS、OA）的普及，数据中心的职能逐渐转变，开始承担核心的计算和数据处理功能。这一阶段的数据中心配备了专业的维护团队，关注提升处理能力和整体运营效率，特别是在支持金融服务和操作能力方面，成为金融机构运营中不可或缺的部分。

3. 数据应用中心阶段

互联网技术的普及和数据资源的日益增长使得数据中心逐步承担起更多的核心业务支撑功能。数据中心开始面向具体的业务需求，提供更为可靠的业务支持服务。这一阶段，数据中心的系统维护要求显著提升，管理逐渐从事后处理升级到事前预防。运行效益和高可用性成为关键指标，虚拟化技术的广泛应用使得数据中心的服务更为高效和灵活。

4. 数据运营服务中心阶段

在数字经济的推动下，数据中心的角色进一步演变。这一阶段，数据中心不仅是信息资源服务、

核心计算、数据存储和备份的提供者，还成为了金融机构核心运营的支撑，确保了业务的连续性和稳定性，提供了可靠和高度定制化的服务。在这一阶段，数据中心的管理和维护实现了自动化，更加注重从运维到运营的转型，从成本中心转变为价值中心。

随着信息科技的演进，金融数据中心的角色和功能也发生了巨大变化。这种变化不仅体现在技术层面，更体现在如何更好地服务于金融机构的核心业务需求上。在这个过程中，数据中心的发展可视为对金融服务日益增长的数据处理和分析需求的响应。随着金融产品和服务的复杂性增加，对数据处理的速度、安全性和准确性的要求也随之提高。因此，数据中心的进化不仅反映了技术的进步，更是金融机构业务创新、效率提高和竞争力提升需求下的必然选择。

当前以及未来，金融数据中心将继续扮演至关重要的角色，不仅要满足日益增长的数据量的处理和存储需求，还要提供高效、灵活且安全的服务，以支持金融机构在快速变化的市场环境中保持领先地位。此外，随着金融科技的快速发展，如云计算、区块链、人工智能和大数据等新技术的应用，数据中心将面临更多新的挑战 and 机遇。

综上所述，金融数据中心是一个不断演进的实体，其发展脉络深刻体现了金融服务行业对信息科技的依赖和应用。从最初的数据存储，到现在的数据运营服务，每个阶段都是对前沿技术的适应和对市场需求的回应，展示了金融业务与技术的深度融合和创新应用。

二、数据中心技术及应用架构的发展

（一）数据中心技术架构的发展

数据中心技术架构经历了从集中式 IOE¹ 技术体系到云化分布式技术体系，再到云原生技术体系的演变过程（如图 1-2-1 所示）。这一进程在金融行业尤为重要，因为技术架构的每一次变革都直接影响着金融服务的效率、安全性和创新能力。



图 1-2-1 数据中心技术架构发展的三个阶段

¹ "IOE" 通常指的是三家大型 IT 公司：IBM、Oracle 和 EMC。这个术语经常用来指代传统且成本较高的 IT 基础设施，通常与较为昂贵的维护费用和复杂的系统集成挑战相关，尤其是在企业级市场中。

1. 大型机时代（1940-1980 年代）

这一时期，数据中心总体依赖大型计算机支持系统运作。最初，大型计算机的能力有限，经常需要多台计算机共同完成复杂功能。随着计算能力的提升，单台计算机足以支撑大型信息系统的运作。这一时期的计算架构是集中式的，使用的是封闭和专有的并行计算架构。终端设备主要用于数据输入和输出，无计算能力，而网络通常局限于单一建筑或小范围内，使用专用网络技术。在金融行业中，这意味着所有关键运算和数据处理都在中央大型机上完成，这在当时是银行等金融机构处理大量交易和记录的唯一可行方式。

2. PC 机时代（1980 年代至 21 世纪初）

这一时期，计算架构转变为“服务端和终端并重”。服务端主要采用 Unix 小型机和 X86²服务器，每台机器可单独运行与计算，同时采用容灾备份和负载均衡技术。终端则以 X86 PC 为主，采用更开放的架构。网络技术也发生了显著变化，从局限于单一机房扩展到局域网和园区网，以太网开始成为主流。在金融领域，这一变化使得银行和金融机构开始能够在多个服务器上分别处理任务，提高了数据处理的效率和可靠性，同时也为后续更复杂应用的发展奠定了基础。

3. 云计算时代（2006 年至今）

随着云计算和云原生技术的兴起，数据中心开始采用“服务端为主，终端为辅”的模式，服务端主要使用 X86 服务器，采用分布式计算架构，构建集中式海量信息及数据的计算和存储能力。云计算技术最早可以追溯到 20 世纪 90 年代，经过多年发展，逐渐从一种技术演变为服务模型，它允许随时随地、方便快捷地从可配置计算资源共享池中获取所需资源（如网络、服务器、存储、应用及服务）。这一模式大幅降低了资源管理调度的工作量和与服务提供商的交互，使云计算与数据中心结合的云数据中心成为传统数据中心的迭代升级，对金融行业的数据中心产业产生了深远的影响。对于金融机构来说，云计算时代意味着能够实现更高效的数据处理、更强大的计算能力和更灵活的资源分配。云数据中心能够迅速扩展以应对市场波动，如交易量激增时，无需投资于额外的物理基础设施。此外，云计算还为金融服务提供了更高的数据可用性、可靠性、安全性和合规性保障，这对于处理敏感的金融交易和客户数据至关重要。

（二）数据中心应用架构的发展

随着信息技术的发展，数据中心的应用架构不断演进。从单机应用时代到面向服务的架构（Service Oriented Architecture, SOA）³再到微服务时代（如图 1-2-2 所示），每一次变革都是对技术挑战的响应。

² Intel 在早期以 80x86 这样的数字格式来命名处理器，包括 Intel 8086、80186、80286、80386 以及 80486，由于以“86”作为结尾，因此其架构被称为“x86”。

³ SOA（Service-Oriented Architecture，面向服务的架构）是一个组件模型，它将应用程序的不同功能单元（称为服务）通过这些服务之间定义良好的接口和契约联系起来。SOA 是一种粗粒度、松耦合服务架构，服务之间通过简单、精确定义接口进行通讯，不涉及底层编程接口和通讯模型。SOA 可以看作是 B/S 模型、XML（标准通用标记语言的子集）/Web Service 技术之后的自然延伸。SOA 将能够帮助软件工程师们站在一个新的高度理解企业级架构中的各种组件的开发、部署形式。



图 1-2-2 数据中心应用架构发展的三个阶段

1. 单机应用时代

在这个时期，信息系统主要依靠单台计算机作为服务器支撑大型信息系统的运作。虽然单体应用成为软件架构的主流，但这种架构的性能受限，且缺乏自治和隔离能力。对于金融机构而言，这种架构限制了其处理大规模交易和复杂运算的能力。

2. 面向服务的架构（SOA）时代

SOA 作为微服务架构的前身，呈现出服务间的松散耦合、注册、发现、治理和隔离等特征。SOA 是一种架构设计模式，其软件应用功能模块以独立、分布式和互操作的服务形式组织和提供，这使得不同的应用程序间能够无缝集成和交互。然而，由于 SOAP 协议及其衍生协议⁴的复杂性，SOA 在广泛应用和推广方面遇到了挑战。在金融领域，SOA 的引入标志着从单一应用到分布式计算的转变，这对于处理越来越复杂的金融服务和产品至关重要。

3. 微服务架构时代

微服务架构追求更加自由和灵活的架构风格，摒弃了 SOA 中的许多约束，提倡以“实践标准”替代“规范标准”。它将单一应用程序划分为一组小的服务，每个服务运行在其独立的进程中，并通过轻量级的通信机制（如 HTTP API）相互协作。微服务架构以业务能力为中心，通过细粒度、松散耦合的服务，提高应用的灵活性和可扩展性。这种架构非常适合快速交付、大型、复杂的互联网应用需求，但也带来了规模大、交付难度提升、对自动化测试和持续集成要求高等挑战。

微服务架构提供了极大的灵活性和扩展性，让金融机构能够快速适应市场变化，同时更有效地管理和维护大量的金融服务和产品。尤其在数字化转型加速的今天，微服务架构使得金融机构能够更快地推出新产品和服务，同时保持系统的稳定性和可靠性。如银行可以通过微服务架构快速开发和部署新的支付系统或客户服务平台，同时确保新服务能够在不影响其他服务运行的情况下，无缝集成到现有的系统中。此外，微服务架构还支持金融业务系统在云环境下运作，使其能够有效利用云资源，为高峰期的大规模业务交易、数据分析和风险管理等提供有力支撑。

⁴ WSDL, UDDI 和 SOAP 协议是 SOA 基础的基础部件。WSDL 用来描述服务；UDDI 用来注册和查找服务；而 SOAP, 作为传输层，用来在消费者和服务提供者之间传送消息。SOAP 是 Web 服务的默认机制，其他的技术可以为服务实现其他类型的绑定。一个消费者可以在 UDDI 注册表（registry）查找服务，取得服务的 WSDL 描述，然后通过 SOAP 来调用服务。

（三）数据中心技术创新及其影响

除了云计算外，人工智能、大数据、量子计算、边缘计算等新技术也在重塑数据中心的运作方式，并对金融服务行业产生深远的影响。人工智能在数据中心的应用，特别是在自动化运维、预测性维护和智能数据分析方面，正逐步成为标准配置，有助于提高数据中心的运营效率，优化资源配置，并在金融服务如个性化投资建议和客户服务中发挥重要作用。利用大数据技术，金融机构可以更准确地评估风险和制定个性化的投资策略，可以深入分析客户行为、市场趋势和风险模式，提供更加精准和高效的金融服务，制定更符合市场需求的策略和产品。量子计算通过其超越传统计算的处理能力，在金融数据分析和安全加密领域展现出巨大潜力。量子算法能够在复杂的金融市场分析和风险评估中提供更加深入的洞察，量子加密技术为金融数据提供了更高级别的安全保护。边缘计算将数据处理的任务从数据中心转移到网络的边缘，有利于提高数据处理的效率，减少延迟，并降低带宽使用，这对于实时金融交易处理和分析至关重要，可极大提高金融服务的响应速度和效率。

综上所述，技术革新大大促进了金融业的数字化转型，也带来了新的机遇和挑战。新技术改变了数据中心的运作方式，提升了数据中心的效率 and 安全性，为金融机构带来业务模式和服务创新的可能性。一方面，利用先进技术，金融机构不断提升数据处理能力，优化内部操作流程，提高客户服务质量，提升客户体验。另一方面，技术创新也为金融数据中心带来了新的安全和合规性挑战。金融机构需要确保新技术的应用不仅要满足业务发展需求，还要符合日趋严格的数据和个人隐私保护相关规定。

未来，随着 5G、元宇宙、大模型等更多创新技术的进一步成熟和广泛应用，金融数据中心将迎来新的发展机遇。

（四）小结

从早期的集中式大型机，到 PC 机时代的服务端和终端并重，再到当今的云计算和云原生技术时代，金融数据中心经历的每一个发展阶段都标志着金融服务能力的提升和业务复杂度的增加。从单机应用到面向服务的架构，再到微服务架构的演进，则反映了金融机构对于更高效、灵活和可靠的业务系统的需求。随着技术的不断进步，未来的数据中心将更加注重自动化、智能化和可持续性。同时，绿色计算和能源效率也将成为数据中心设计和运营的重要考量因素。对于金融机构而言，积极拥抱新技术不仅是提升自身竞争力的关键，也是在不断变化的市场环境中保持领先地位的必然选择。数据中心的未来发展将继续深刻影响金融服务的质量、效率 and 创新能力。

三、金融数据中心发展历程及建设原则

（一）金融数据中心的发展历程

金融数据中心的发展经历了三个重要阶段（如图 1-3-1 所示），每个阶段都反映了技术的发展和业务的特定需求。



图 1-3-1 金融数据中心发展历程的三个阶段

1. 区域机房阶段（1980-1990 年代）

以银行为例，在这一阶段，数据中心多以省级分行的服务器机房为雏形，规模较小，运维能力参差不齐，面临的主要挑战是设备的可靠性和业务连续性。由于故障导致的业务中断时有发生，反映出了早期金融数据中心在技术和管理上的局限。

2. 数据集中阶段（2000-2010 年）

这一阶段，以国有银行为代表的大型商业银行开始实施数据大集中工程。数据中心的规模和技术手段显著的提升，建设了现代化、集中式、超大规模的数据中心，组建了专职运维团队，设计了标准化的管理制度等，显著降低了生产故障发生的频率，开启了更高效、安全的运营模式，为后续更先进技术的应用打下基础。

3. 治理转型阶段（2010-2020 年）

这一阶段，金融数据中心开始重视灾备建设和全面治理。采用“两地三中心”的架构，从集中式向分布式架构转型，从物理资源向虚拟化转变，更加关注灵活性和效率，运行模式从传统运维向现代化管理转变。

当前，面对全球技术竞争，金融机构积极推进分布式架构转型，从“两地三中心”向“多地多活”云数据中心演进。新老架构并存、技术快速发展以及信创生态的逐渐成熟，将推动数据中心架构和技术栈更加多样化，更加复杂但功能强大的双模或多模架构或将到来。

（二）金融数据中心的建设原则

为确保金融数据中心高效、稳定、安全运行，可持续发展，应遵循以下建设原则。

1. 整体性原则

金融数据中心建设应进行统一规划，确保系统的一体化和通用性，设计时应考虑整体架构的兼容性和扩展性，确保未来技术升级和功能扩展的可行性。

2. 先进性与实用性原则

金融数据中心应采用行业内的先进技术，构建合理超前的技术架构，在保持技术领先的同时，结合实用性进行综合分析，避免过度投资尚未成熟或不切实际的技术。

3. 可靠性原则

安全性和可靠性是金融数据中心的核​​心诉求，设计时应考虑合理的冗余和灾难备份能力。此外，基础设施如电力和制冷系统的设计应匹配可靠性目标，以最小化运行中断的风险。

4. 标准性原则

金融数据中心的设计应遵循国际和国内的相关规范标准，合理解读和融合这些标准，以实现国际化和本土化的平衡，确保数据中心的全球兼容性和效率。

5. 可扩展性原则

金融数据中心应具备适应未来发展需求的能力。采用模块化设计，可为数据中心预留足够的扩展空间，并具有灵活性。同时，需注意保持数据中心的可持续发展能力，便于未来的技术升级和功能扩展。

6. 经济性原则

数据中心建设阶段应在满足功能和可靠性要求的前提下，通过复用物理资源和充分利用现有投资等方式，最大限度节约成本；运营阶段应考虑长期运营成本，提高产出效率，降低总体拥有成本。

7. 安全性原则

选用高标准的材料和设备，确保基建设备运行和工作人员安全。同时，采用完整的安全策略和有效的安全手段，确保数据中心的 IT 系统及基础设施的安全。

8. 节能环保原则

利用先进技术，进行科学规划，提升能源利用效率，最大限度实现节能减排，满足环保要求。

9. 可管理性原则

数据中心的各系统应具有强大的集中式管理能力，并为分布式实施提供清晰的管理逻辑。

10. 总体集成性原则

考虑到各系统间的相对独立性和差异性，数据中心的整体系统架构应通过信息网络化管理平台进行有效集成，以保证系统间的顺畅协作和互联互通。

（三）金融数据中心的安全措施及合规性

数据中心的安全性在金融行业尤为重要，因为其处理和存储大量敏感的信息和数据。金融数据中心面临的安全挑战不仅仅是技术上的，还包括环境安全、数据安全、合规安全及客户信息保护等更多维度。

1. 物理安全

- (1) 访问控制。数据中心必须实施严格的物理访问控制，如使用生物识别系统、门禁卡和监控摄像头等，以防止未经授权进入。
- (2) 环境监控。监控温度、湿度和水浸等环境因素，采取防火、防洪和其他灾害的预防措施。
- (3) 冗余系统。确保关键系统如电力供应和冷却系统有备份和冗余，以防任何单点故障。

2. 网络安全

- (1) 防火墙和入侵检测系统。使用先进的防火墙和入侵检测系统监控和防止未经授权的访问。
- (2) 网络隔离和分段。通过网络隔离和分段技术，确保敏感区域的网络安全，防止潜在的内部和外部攻击。
- (3) 持续监控和响应。实施 7x24 小时的网络监控，配合快速响应机制，第一时间处理任何安全事件。

3. 数据安全

- (1) 数据加密。实施端到端数据加密，确保数据在任何时候都不会暴露给未授权的个体。
- (2) 访问管理。实施严格的访问管理策略，确保只有授权人员才能访问敏感数据，可采用多因素认证进一步强化安全性。
- (3) 密钥管理。采用安全、高效的密钥管理手段，并确保加密密钥和访问控制的安全性。

4. 合规安全

- (1) 国际标准。遵守 ISO/IEC 27001 等国际信息安全管理标准，确保数据中心达到全球安全标准。
- (2) 地区法规。遵守全球各地区的数据保护法规，如欧盟的 GDPR⁵、美国的 CCPA⁶等，确保跨境数据处理的合法性。
- (3) 合规性报告。定期进行内部和外部审计，生成合规性报告，以证明数据中心符合所有相关法规和标准。

5. 金融行业特色要求

- (1) 事务完整性。确保所有金融交易的完整性和不可否认性，这对于维护客户信任至关重要。
- (2) 风险管理。实施全面的风险管理策略，识别、评估和缓解潜在的安全威胁，包括网络攻击、物理破坏和内部风险。
- (3) 敏感数据保护。特别关注敏感金融数据（如交易记录、个人账户信息等）的保护，确保其安全性和机密性。

⁵ GDPR.(General Data Protection Regulation), 全称为《通用数据保护条例》，是欧洲联盟于 2018 年 5 月 25 日生效的一项数据保护法规。

⁶ 《加州消费者隐私法案》(CCPA) 是继欧盟《一般数据保护条例》(GDPR) 颁布后又一部数据隐私领域的重要法律。它于 2018 年 6 月 28 日正式颁布。

(4) 合规性数据报告。为了应对监管要求，金融数据中心需要具备高效的合规性数据报告能力，快速响应监管查询和审计。

综上，金融机构的数据中心在保护敏感金融数据方面的安全措施是其核心竞争力的一部分。随着技术的发展和威胁的不断演变，金融数据中心必须不断更新和强化其安全策略。同时，遵守国际和地区的法律法规，对于维护客户信任、保护客户数据及确保业务的合法性和稳定性至关重要。金融机构的数据中心面临的挑战不仅是技术性的，更是管理和合规性的。因此，建立一个全面、动态和适应性强的安全框架，以及一个响应迅速、符合法规要求的运营模式，是确保数据中心长期成功和可持续发展的关键。

(四) 金融数据中心的业务连续性和灾难恢复

确保业务连续性和有效的灾难恢复机制对于金融机构来说至关重要，任何停机事件都可能导致重大的财务损失、客户信任损害和监管合规性风险。金融服务高度依赖数据中心的稳定性和可靠性，业务连续性计划（BCP，Business Continuity Plan）是确保金融服务在任何情况下都能持续运行的关键。BCP 的目标是在面临自然灾害、系统故障、网络攻击等突发事件时，能够快速恢复运营。这不仅关系到机构的运营效率和市场信誉，还涉及客户资产的安全。

1. 灾难恢复计划

灾难恢复计划（DRP，Disaster Recovery Planning）是 BCP 的关键组成部分，专注于数据和 IT 基础设施的恢复。有效的 DRP 开发包括以下步骤。

- (1) 风险评估和业务影响分析。识别可能影响数据中心运营的各种风险，并评估其对业务的影响，包括从技术故障到自然灾害的一系列潜在风险。
- (2) 恢复策略。基于风险评估，制定具体的恢复策略，包括数据备份、系统冗余、灾难恢复站点等。
- (3) 实施计划和测试。制定详细的恢复步骤，定期进行测试和演练，以确保计划的有效性。

2. 业务连续性技术和策略

为了实现业务连续性和有效的灾难恢复，以下技术和策略至关重要。

- (1) 数据备份。定期备份关键数据，包括离线和云端备份。确保在数据中心受损时，可以从备份中迅速恢复数据。
- (2) 数据复制。使用同城双活和异地多活架构的实时数据复制技术，确保关键数据在多个地点的实时可用性。
- (3) 容错和冗余设计。对数据中心电源、网络 and 冷却系统等关键组件实施冗余设计，确保部分系统失效时，整体系统仍能继续运行。

3. 业务连续性测试和维护

定期测试和维护灾难恢复计划对于确保其有效性至关重要，包括模拟灾难场景、测试恢复程序和更新计划以应对新的威胁和技术变化。持续的维护和改进确保灾难恢复计划与当前的业务需求和技术环境保持一致。

4. 业务连续性法规遵从和标准

(1) 国际和地区法规。金融数据中心必须遵守国际和地区的数据保护、隐私和业务连续性等的相关法律法规，如欧盟的 GDPR 或美国的 Sarbanes-Oxley Act (SOX) 等。

(2) 标准和认证。数据中心应遵循行业标准，如 ISO 22301 (业务连续性管理系统) 和 ISO/IEC 27001 (信息安全管理)。这些标准提供了构建和维护有效业务连续性计划的框架。

5. 面向金融机构的特定需求

金融机构由于其服务性质，对数据中心的业务连续性和灾难恢复有特别的要求。

(1) 交易系统的连续性。金融交易系统需要达到近 100% 的可用性，任何业务中断都可能导致巨大的财务损失和市场信任危机。

(2) 客户数据保护。金融机构需保护客户数据不受灾难影响，包括确保所有个人和交易数据的完整性和可用性。

(3) 监管合规性。金融机构必须确保其业务连续性计划符合所有相关的行业监管要求，以避免潜在的法律和监管风险。

综上，随着技术的发展和威胁的不断演变，金融机构必须持续投资数据中心的业务连续性策略，包括技术、人员和流程。同时，遵守相关的法规和标准，这不仅是法律义务，更是维护客户信任和市场声誉的关键。一个强大的业务连续性和灾难恢复计划将成为金融机构抵御未来挑战、保护客户利益并保持市场领先地位的基石。

(五) 小结

金融数据中心的发展历程与建设原则在反映了技术进步的同时，也体现出金融行业对于数据管理和保护的认知不断深化，从最初的区域机房，到数据大集中，再到向现代化治理转型，每个阶段都标志着金融行业对于数据处理能力和服务质量提升的追求，以及风险管理策略的逐渐完善。在安全措施和合规性方面，金融数据中心面临着保护敏感数据的重大挑战，需在物理安全、网络安全、数据安全等方面采取强化措施。随着网络环境的复杂化和监管要求的严格化，金融数据中心必须适应国际和地区法律法规的要求，确保安全性和合规性，这对维护客户信任和市场声誉至关重要。同时，业务连续性和灾难恢复成为保障金融服务稳定性的关键，通过制定和实施有效的业务连续性计划和灾难恢复策略，金融数据中心可有效应对自然灾害、技术故障或网络攻击等潜在风险，确保金融服务不间断。上述措施和策略的执行和制定不仅需要技术层面的考量，还需要有效的组织管理和迭代升级，以应对不断变化的技术环境和业务需求，支持金融机构长期发展和保持市场竞争力。

四、金融数据中心未来发展趋势和要求

(一) 集约高效，绿色低碳

在全球环保和可持续发展的大背景下，金融数据中心的未来建设必须遵循集约高效、绿色低碳的原则。这不仅符合国家“碳达峰碳中和”重大战略，也是数据中心行业可持续发展的必然趋势。未来，金融数据中心将更多地采用绿色建材、高效能源和废热回收技术，大幅提升能源使用效率。

近年来我国及地方关于数据中心低碳环保的政策汇总见表 1-4-1。

表 1-4-1 国家及地方关于绿色数据中心的政策

发布时间	发布部门 或地方	政策名称	重点内容
2019 年	工业和信息化部、国家机关事务管理局、国家能源局	《关于加强绿色数据中心建设的指导意见》	打造一批绿色数据中心先进典型。到 2022 年，数据中心平均能耗基本达到国际先进水平，新建大型、超大型数据中心的电能使用效率值达到 1.4 以下，高能耗老旧设备基本淘汰，水资源利用效率和清洁能源应用比例大幅提升。
2021 年	国家发展改革委、网信办、工信部、国家能源局	《全国一体化大数据中心协同创新体系算力枢纽实施方案》	布局全国算力网络国家枢纽节点，启动实施“东数西算”工程，构建国家算力网络体系，推动数据中心合理布局，供给平衡，绿色集约及互联互通，实现数据中心绿色高质量发展。 对于服务金融交易、车联网等领域，网络时延要求极高的数据中心，允许在城市内部发展（数据中心端到端单向网络时延原则上在 10 毫秒范围内）；对于服务后台加工、存储灾备等，网络时延要求不高的数据中心，要优先向贵州、内蒙古、甘肃、宁夏节点转移。
2021 年	工业和信息化部	《新型数据中心发展三年行动计划（2021-2023 年）》	规划提出了建设布局优化行动、网络质量升级行动、算力提升赋能行动、产业链稳固增强行动、绿色低碳发展行动、安全可靠保障行动等六个专项行动，包括 20 个具体任务和 6 个工程，着力推动新型数据中心发展。新型数据中心建设布局优化行动要求加快建设国家枢纽节点、按需建设各省新型数据中心、灵活部署边缘数据中心、加速改造升级“老旧小散”数据中心等措施。到 2023 年底，全国数据中心机架规模年均增速保持在 20% 左右，平均利用率力争提升到 60% 以上。新建大型及以上数据中心 PUE 降低到 1.3 以下，严寒和寒冷地区力争降低到 1.25 以下。国家枢纽节点内数据中心端到端网络单向时延原则上小于 20 毫秒。

发布时间	发布部门或地方	政策名称	重点内容
2021 年	国家发展改革委、网信办、工信部、国家能源局	《贯彻落实碳达峰碳中和目标要求推动数据中心和 5G 等新型基础设施绿色高质量发展实施方案》	到 2025 年，数据中心运行电能利用效率和可再生能源利用率明显提升，全国新建大型、超大型数据中心平均电能利用效率降到 1.3 以下，国家枢纽节点进一步降到 1.25 以下，绿色低碳等级达到 4A 级以上。全国数据中心整体利用率明显提升，西部数据中心利用率由 30% 提高到 50% 以上，东西部算力供需更为均衡。
2021 年	北京	《北京市数据中心统筹发展实施方案（2021-2023 年）》	按照“四个一批”总体思路，通过关闭一批功能落后的数据中心、整合一批规模分散的数据中心、改造一批高耗低效数据中心、新建一批计算型数据中心和人工智能算力中心及边缘计算中心。
2021 年	广东	《广东省 5G 基站和数据中心总体布局规划（2021-2025 年）》	全省按照“双核九中心”的总体布局，形成 9 个数据中心集聚区。按照“先提后扩”的建设思路，先提高上架率，后扩容和新增，单个数据中心项目上架率达到 60%，方可申请扩容和新建项目。到 2022 年，平均上架率达到 65%，设计 PUE 值平均小于 1.3。到 2025 年平均上架率达到 75%，设计 PUE 值平均小于 1.25。
2021 年	山东	《关于加快构建山东省一体化大数据中心协同创新体系的实施意见》	重点建设 6 数：数网、数纽、数基、数链、数脑、数盾；通过存量优化、整体提升，到 2025 年，全省数据中心在用标准机架数达到 45 万个以上，平均利用率提升到 60% 以上，总算力超过 12EFLOPS，高性能算力占比达到 15%，实现大型数据中心运行电能利用效率降到 1.3 以下。“十四五”期间，创建 50 个以上的新型数据中心，布局一批低时延敏捷型的边缘数据中心

发布时间	发布部门 或地方	政策名称	重点内容
2021 年	浙江	《浙江省推动数据中心能效提升行动方案（2021-2025 年）》	提高算力能效：加强区域资源统筹整合，对已建数据中心“整合一批、改造一批、淘汰一批”；节能创新：支持采用新型机房精密空调、高效电源设备、液冷技术、机柜式模块化、削峰填谷应用、余热综合利用等方式建设数据中心，引导数据中心在新能源发电侧或沿江沿湖自然冷源侧建设。
2021 年	江苏	《江苏省新型数据中心统筹发展实施意见》	到 2023 年底，全省数据中心机架规模年均增速保持在 20% 左右，平均利用率提升到 65%，全省新型数据中心比例不低于 30%，高性能算力占比达 10%，新建大型及以上数据中心 PUE 降低到 1.3 以下。到 2025 年底，全省数据中心机架规模达 70 万标准机架，新型数据中心占比进一步提升，算力算效水平显著提高，网络质量明显优化，能效水平稳步提升，可再生能源利用率逐步提高，基本形成“双核三区四基地”发展布局体系。
2021 年	云南	《云南省“十四五”大数据中心发展规划》	新建大型及以上数据中心绿色等级达到 4A 级以上，PUE 达 1.3 以下，改造后 PUE 达 1.4 以下。存量“老旧小散”数据中心高能耗设施与设备普遍实现优化，改造后 PUE 值不高于 1.6。

区别于传统数据中心，绿色数据中心具有以下建设重点。

1. 高效能源管理

金融机构应着重关注数据中心的能效比（PUE，Power Usage Effectiveness），并采取相关措施达到或超过国际标准。如通过采用高温服务器和液冷技术，提高热管理效率；使用高压直流供电和市电直供模式，优化电力使用等。

2. 绿色节能技术

在设计和运营数据中心时，应用绿色节能技术成为关键。模块化设计、异构加速计算、自然冷却系统等有助于降低能耗和减少碳排放。

3. 推动清洁能源使用

未来的数据中心将更多地依赖风能、太阳能等清洁能源。通过建立微电网和优化“源网荷储”系统，可以进一步降低碳足迹，实现绿色零碳目标。

4. 智能化管理

采用智能楼宇管理系统和绿色照明技术，可进一步提升能源效率，降低运营成本。

（二）多地多活，分层协同

分布式架构的发展推动金融数据中心向“多地多活”的模式演进，从而提高数据的可用性和灾难恢复能力。

1. 分布式架构

随着微服务架构和分布式技术的成熟，金融数据中心可以在多地布置，实现数据的实时同步和一致性，提高系统的稳定性和可靠性。

2. 云计算架构

金融数据中心正在向混合多云架构转型。在保持企业私有云的同时，与公有云和行业云协作，构建更加灵活和高效的云服务平台。

3. 边缘计算的融入

边缘计算的发展将带动微型边缘数据中心的建立，进一步丰富云网、云边、边边、端边之间的多层级资源和数据协同，提升服务网络的层次和用户体验。

（三）数据驱动，智能运维

数智化是金融数据中心未来发展的重要方向。随着数据中心规模的扩大和业务复杂度的增加，传统的运维模式已无法满足高效管理和运营的需求。

1. 智能化运维

金融数据中心将越来越依赖智能化的运维方式。通过运维大数据平台和先进的智能算法，可以实现事前预测、事中监控、事后分析等多场景的运维能力，从而提高数据中心的服务能力和效率。例智能运维机器人能够实现自动化的故障诊断和排障，减少对人力的依赖。

2. 数字化转型

人工智能、边缘计算、数字孪生等新兴技术的使用，推动数据中心的运营模式从传统、僵化向数字化、网络化、智能化转变，有效提升数据中心规划、建设、运营的投资效益和运营效率。

3. 大数据、大算法、大模型与场景结合

将大数据、人工智能等新技术与运维场景、业务规则和专家经验相结合，实现最佳的运维效果，驱动数据中心从“人力密集”的运维模式转变为“技术密集”和“数据驱动”的模式。

（四）人才和技能培训

数据中心不断演进，对专业技能和人才的需求也在持续增长。金融机构需要重视人才培养，特别要重点提升运维、安全、云技术等关键领域的人才技能。

1. 运维专家

运维专家负责系统性能监控，确保硬件和软件高效运作，对系统故障或性能下降等问题及时响应。运维专家需具备系统知识，如服务器管理、数据存储和网络配置等，还需要掌握自动化工具和脚本语言。在数据中心自动化、智能化趋势下，运维专家需要不断更新技能，以适应人工智能等新兴的技术在运维中的应用。

2. 网络安全专家

网络安全专家负责制定和实施安全策略，监测网络活动，防范和抵御网络攻击。网络安全专家需要熟悉各种安全协议、加密技术和防火墙配置，还需要了解最新的网络安全趋势和威胁，具备强大的分析和解决问题的能力。

3. 云技术专家

云技术专家负责管理和优化云环境，包括云基础设施的设计、部署和维护，需要熟悉各种云服务模型（如 IaaS、PaaS 和 SaaS）⁷ 和云提供商的平台（如阿里云、华为云、腾讯云、天翼云、AWS、Azure 和 Google Cloud），深入了解容器化技术和微服务架构等，同时要具有创新思维，以应对云技术快速发展的需要。

信息技术发展日新月异，金融机构需要采取多元化的人才培养策略，以应对不断变化的技术和市场需求。一是建立培训和发展计划。为员工提供定期培训和专业发展机会，以确保他们的技能与行业的最新发展保持同步。鑫知教育在过往金融数字化培训中提供了大量诸如“数据中心基础设施运维管理体系实战”、“高效数据中心运维策略与实践”、“云计算在金融数据中心的应用与最佳实践”。二是鼓励自我学习与认证。鼓励员工参与在线课程、研讨会和行业认证，以促进他们的专业成长和技能提升。这种自我学习和认证过程，可以通过与教育机构的合作得到加强，为员工提供最

⁷ 根据服务类型的不同，云计算服务可以分为三类，即基础设施即服务 (IaaS)、平台即服务 (PaaS) 和软件即服务 (SaaS)，后又衍生出 aPaaS。

前沿的技术教育和培训。三是建立知识共享文化。通过内部研讨会、技术论坛和学习小组促进知识共享，这不仅有助于个人成长，也有利于团队的整体技能提升。当前，在培训机构的课程设计中，旨在鼓励这种知识共享和团队合作精神的培训活动仍在不断优化和创新。鑫知教育在给唐山银行“盛唐创新营”的培训体系设计中，在分组案例工作坊的基础上，增加外部实战导师一对一辅导，增强内外部联动式的小组学习。四是与教育机构和行业组织合作。与大学和专业培训机构合作，为员工提供最前沿的技术教育和培训。

随着金融数据中心技术的不断进步，从自动化到智能化，从云计算到量子计算，数据中心工作人员面临着前所未有的挑战。这些挑战不仅在于掌握新技术，还包括了解这些技术如何影响金融行业的运作模式和服务提供。一是跨学科技能的培养。未来的数据中心工作人员需要具备跨学科的技能，不限于技术领域，还包括对金融服务行业的深入理解。二是适应快速变化的环境。能够快速适应新技术和 workflows 的能力将成为数据中心人才的关键特质。

综上，人才和技能成为金融数据中心未来发展的核心要素，拥有高技能和不断学习的专业团队，金融数据中心才能够有效地支持金融服务的创新和优化。

（五）挑战和机遇

随着金融科技的不断进步，数据中心不再仅仅是数据存储和处理的地方，而是支撑金融机构核心业务和创新的基石。处于转型关键期的金融数据中心面临如下挑战和机遇。

1. 数据增长的双重影响

（1）更广泛的数据集成。随着物联网（IoT，Internet of Things）和在线交易量的增长，数据中心面临来自多种渠道的数据整合挑战，不仅对存储和处理能力提出更高要求，而且需要更复杂的数据管理和分析技术。

（2）数据治理和合规性。数据的增长也带来了数据治理和合规性的挑战。金融数据中心需要确保所有数据的处理符合 GDPR、CCPA 等国际和地区的法律法规。

2. 技术迭代的压力和潜力

（1）技术更新的速度。随着 5G、量子计算和先进加密技术等出现和快速发展，数据中心需要不断更新基础设施和软件，以保持技术领先。

（2）云服务和混合云策略。云服务的普及使得数据中心需要适应不同的云环境和服务，如公有云、私有云和混合云。这要求数据中心具备灵活性和可扩展性，以适应多变的业务需求。

3. 威胁与防御的博弈

（1）日益复杂的网络攻击。随着黑客攻击手段的日益高超，数据中心必须采用更为先进和多层次的安全策略保护敏感金融数据。

（2）安全技术的发展。网络安全态势日趋紧张的同时，安全技术也在不断发展。如基于人工智能的威胁检测和响应系统、区块链技术在数据完整性保护方面的应用等，为数据中心提供了新的安全工具。

4. 人才培养和技能提升的需求

(1) 人员技能多元化。随着技术的发展，数据中心需要配备具有多元化技能的人才，如云计算专家、大数据分析师、网络安全专家等。

(2) 持续的职业发展。金融机构应为数据中心员工提供持续教育和培训机会，帮助其持续提升职业技能和职业素养。

(六) 小结

金融数据中心面临着前所未有的变革，必须适应新的发展趋势，如绿色低碳、分布式架构及智能化运维。未来，金融数据中心将更加注重清洁能源的使用、云计算和边缘计算的结合以及运维的智能化和数字化。这些变化在带来技术挑战的同时，也为金融企业带来了提高效率、降低成本和增强竞争力的机遇。金融数据中心作为支撑金融服务和创新的关键基础设施，将成为金融机构智能、高效和可持续发展的关键资产，为金融行业乃至整个社会的数字化转型贡献力量。

未来，在新的挑战和机遇下，金融数据中心应采取全面和积极的策略，不断加强基础设施建设，持续投资人才和技能发展，并保持对新兴技术的敏感性和适应性，以有效支撑金融机构在复杂和竞争激烈的市场环境中持续发展。

第二部分 金融数据中心应用报告

本章节详细介绍金融行业数据中心应用案例和最佳实践，通过研究、分析其成功因素，为金融机构提供有价值的参考和启示。

一、数据中心应用架构概述

（一）对象、目标和范围

金融数据中心架构应结合企业级架构开发方法进行系统性规划，企业架构规划如图 2-1-1 所示，具体内容包括以下几方面。

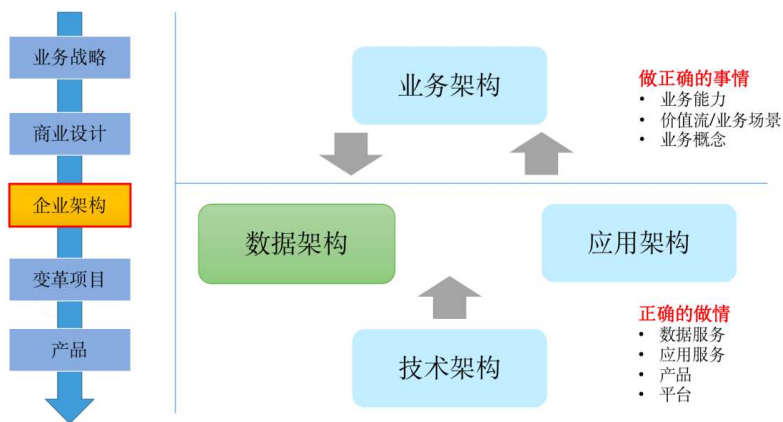


图 2-1-1 企业架构规划示意

1. 企业架构实现路线

- (1) 业务战略，明确企业的业务目标和战略方向是企业架构规划的第一步。
- (2) 商业设计，将业务战略转化为具体的商业模型，包括收入来源、成本结构等。
- (3) 企业架构，是整个架构规划的核心，定义了企业的整体结构，包括技术架构、数据架构、应用架构等。
- (4) 变革项目，根据企业架构制定具体的变革项目，以实现企业的战略目标。
- (5) 产品，根据变革项目设计具体的产品，以满足企业的商业需求。

2. 技术架构、数据架构、应用架构和业务架构

技术架构、数据架构、应用架构和业务架构共同构成了金融机构的信息技术架构，它们相互配合，共同支撑业务运营。

技术架构是金融机构在实现业务目标过程中所采用的各种技术的总和，包括硬件、软件、网络和通信等。技术架构需要与金融数据中心的数据处理能力相匹配，以确保数据的准确性和实时性。

数据架构是金融机构在处理和存储数据时所采用的组织方式，包括数据的定义、分类、存储和管理等。数据架构需要与金融数据中心的数据处理能力相匹配，以确保数据的高效和安全。

应用架构是金融机构在开发和实施应用系统时所采用的结构和组织方式，包括应用的模块化、组件化、可扩展性和可维护性等。应用架构需要与金融机构的业务架构相匹配，以确保应用的实用性和可靠性。

业务架构是金融机构在设计和实施业务流程、服务和支持体系时所采用的结构和组织方式，包括业务的战略目标、业务流程、服务和支持等。业务架构需要与技术架构、数据架构和应用架构相匹配，以确保业务的效率和可控性。四类架构的内涵、差异与关联可参考表 2-1-1。

表 2-1-1 四类架构的内涵、差异与关联

类型	企业业务架构	企业数据架构	企业应用架构	企业技术架构
目的	识别企业如何为用户和相关利益者提供价值	描述数据应该如何组织和管理	描述企业应用的结构和功能	描述能使系统发挥功能和传递价值的实体技术
元素	业务模型、流程、功能、服务、事件、策略词汇	数据模型、数据定义、数据映射规范、数据流、结构化数据应用编程接口	业务系统、软件包、数据库	技术平台（数字化底座）、网络、安全、整合工具
依赖项	制定其他架构的需求	管理业务架构创建和需要的数据	依据业务需求来处理制定的数据	承载并执行应用架构
角色	业务架构师和分析师、业务数据管理员	数据架构师、建模师、数据管理员	应用架构师	基础设施架构师

3. 技术架构、数据架构与应用架构

技术架构、数据架构和应用架构是数据中心设计的三个核心要素，一个高效的数据中心需要这三个架构相互协调和优化，以满足业务需求和服务质量以及规范需要。正确的做法是提供数据服务、应用服务并开发和推广相关的产品，同时构建和维护一个稳定、高效的平台，支持各种数据应用和服务的运行。

- (1) 数据服务。数据服务是数据中心的基础功能，包括数据存储、数据处理、数据安全等。
- (2) 应用服务。应用服务是数据中心的主体，包括各种业务应用，如信贷系统、支付系统等。
- (3) 产品。产品是数据中心的应用成果，包括各种面向用户的服务，如网上银行、手机银行等。
- (4) 平台。平台是数据中心的基础设施，包括各种技术平台，如云计算平台、大数据平台等。

4. 应用架构、业务架构、数据架构

在企业架构规划的过程中，应着重提升业务能力，优化价值流 / 业务场景，并深化对业务概念的理解和应用。

(1) 金融数据中心的应用架构

金融数据中心的应用架构由数据接入层（负责接收来自前端应用的数据请求，并将数据存储到数据中心的数据库中）、数据存储层（负责存储和管理数据中心的所有数据，包括原始数据、中间数据和最终数据）、数据处理层（负责对数据中心的数据进行处理，包括数据清洗、数据转换、数据分析等）、数据应用层（负责将数据中心的数据应用到前端应用中，为前端应用提供数据服务）、数据安全层（负责保障数据中心的数据安全，包括数据加密、数据备份、数据恢复等）组成。

(2) 金融数据中心的目标实现

- 一是提高数据处理能力。通过优化数据处理流程，提高数据处理的速度和效率。
- 二是保障数据安全。通过数据加密、数据备份、数据恢复等手段，保障数据中心的数据安全。
- 三是支持数据应用。通过提供数据服务，支持前端应用的开发和运行。
- 四是提高数据可用性。通过数据冗余、数据备份等手段，提高数据中心的可用性。

(3) 金融数据中心的实施范围

金融数据中心的实施范围包括：硬件设施（服务器、存储设备、网络设备等）、软件系统（操作系统、数据库系统、数据处理系统等）、运维管理（数据中心的运行监控、故障处理、性能优化等）、业务应用（金融业务的数据处理、数据分析、数据服务）等。

综上所述，金融数据中心应用架构是一个复杂而重要的系统，通过对金融数据中心应用架构的分析和研究，可以更好地理解金融数据中心的工作原理，为金融行业的数字化转型提供有益的参考。

(二) 整体框架

金融数据中心是一个复杂的系统，涉及多个技术领域，包括基础设施、数据存储和管理、数据安全、数据处理和分析、数据应用和服务等（金融数据中心的应用架构示例如图 2-1-2 所示）。

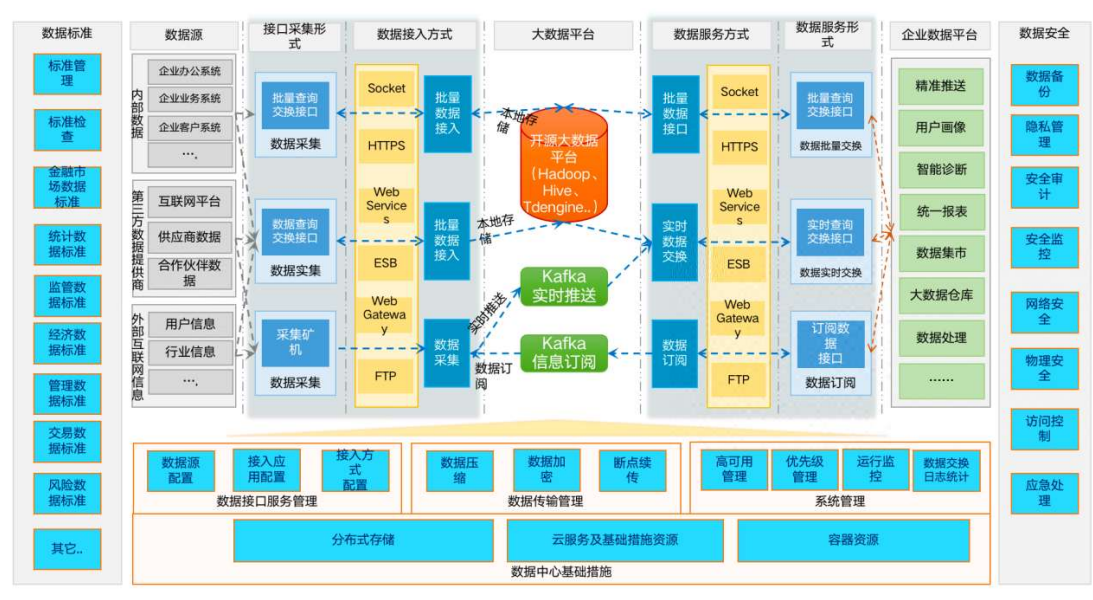


图 2-1-2 金融数据中心的应用架构示例

(1) 数据标准。包括标准管理、标准检查、金融市场数据标准、统计数据标准、监管数据标准、经济数据标准、管理数据标准、交易数据标准、风险数据标准及其它相关内容。

(2) 数据源。包括企业办公系统、业务系统、客户系统等内部数据，互联网平台、合作伙伴等第三方数据及用户信息、行业信息等外部数据。

(3) 接口采集。包括数据采集和数据集成（数据交换接口）。

(4) 数据接入。Socket、HTTPS、Web Services、ESB 等批量数据接入和 Web Gateway、FTP 接入。

(5) 大数据平台。开源大数据平台（如 Hadoop、Hive、TDengine 等）、Kafka 实时推送、Kafka 信息订阅。

(6) 数据服务。包括批量数据接口（Socket、HTTPS）、实时数据交互（Web Services、ESB）、数据订阅（Web Gateway/FTP）。

(7) 数据服务。批量查询（数据批量交换）、实时查询（数据实时交换）、订阅数据接口（数据订阅）。

(8) 数据平台。精准推送、用户画像、智能诊断、统一报表、数据集市、大数据仓库、数据处理等。

(9) 数据接口管理。数据源配置、接入应用配置、接入方式配置。

(10) 数据传输管理。数据压缩、数据加密、断点续传。

(11) 系统基础管理。高可用管理、优先级、运行监控、数据交换日志统计。

(12) 数据平台基础设施。分布式存储、云服务及容器资源。

(13) 数据中心基础设施。包括电力、空调、机房、网络等设备。

(14) 数据存储和管理。数据存储包括数据的收集、存储、备份和恢复等环节；数据管理包括数据的分类、命名、权限、审计等环节。

(15) 数据安全保障。覆盖数据备份、隐私管理、安全审计、网络安全、物理安全、访问控制、应急处理等领域。数据安全涉及数据的保护、检测、响应和恢复等环节。

(16) 数据处理和分析。数据处理包括数据的清洗、转换、整合等环节；数据分析包括数据的描述、解释、预测、挖掘等环节。

(17) 数据应用和服务。数据应用包括数据的报告、展示、应用等环节；数据服务包括数据的咨询、培训、支持等环节。

总的来说，金融数据中心是一个多层次、多功能、多技术的系统，需要多种技术结合，如云计算、大数据、人工智能、物联网等；需要多种资源的整合，如人力、物力、财力等；需要多种服务的提供，如数据存储、数据处理、数据安全、数据应用等；需要多种制度的保障，如管理制度、技术标准、安全规范等。因此，建设一个高效、安全、可靠的金融数据中心是一项复杂的任务，需要多方面的努力。

（三）评价标准

金融数据中心的设计可以从企业战略愿景、用户体验、组织流程、技术能力 4 个方面展开，并建立一套适合企业自身需求的评价方法。

1. 战略愿景评价指标

金融数据中心的战略愿景主要体现在其未来的发展规划和目标，包括定位、在企业整体战略中的角色以及要实现的具体目标。评价金融数据中心战略愿景可以有如下标准。

(1) 战略定位。金融数据中心在企业整体战略中是否具有明确且重要的地位，是否与企业的整体战略相一致。

(2) 目标设定。金融数据中心设定的目标是否具有可衡量性、可实现性以及与企业战略目标的关联性。

(3) 长期规划。金融数据中心是否具有长期的发展规划，以及其对于未来市场变化和技术发展的应对策略。

2. 用户体验评价体系

金融数据中心的服务对象是人，因此用户体验是重要的评价标准之一。

(1) 界面设计。金融数据中心的界面设计是否简洁明了，易于理解和使用。

(2) 功能设置。金融数据中心提供的功能是否满足用户的需求，是否具有足够的灵活性以适应不同用户的使用习惯。

(3) 响应速度。金融数据中心的响应速度是否足够快，是否能够满足用户对于数据处理速度的需求。

(4) 易用性。金融数据中心是否易于使用，用户在使用过程中是否容易遇到问题。

3. 组织流程的评价标准

金融数据中心的组织流程包括内部管理结构、工作流程以及与其他部门的协作方式。金融数据

中心组织流程的评价标准设计思路如下。

- (1) 管理结构。金融数据中心的组织结构是否清晰，管理层的管理和决策是否有效。
- (2) 工作流程。金融数据中心的流程是否高效，是否能够确保数据的安全性和准确性。
- (3) 协作方式。金融数据中心是否能够与其他部门进行有效的协作，是否能够满足企业对数据的需求。
- (4) 适应能力。金融数据中心是否具有较强的适应能力，是否能够应对市场变化和技术发展带来的挑战。

4. 技术能力体系的评价标准

金融数据中心的技术能力是其核心竞争力的体现，包括数据处理能力、安全性、稳定性等。金融数据中心技术能力评价标准如下。

- (1) 数据处理能力。金融数据中心的数据处理能力是否足够强大，是否能够满足企业对数据处理速度和质量的需求。
- (2) 安全性。金融数据中心是否具有足够的安全防护措施，是否能够确保数据的安全。
- (3) 稳定性。金融数据中心是否具有高度的稳定性，是否能够在面临各种突发情况时保持稳定运行。
- (4) 技术创新。金融数据中心是否具有较强的技术创新能力，是否能够紧跟技术发展的步伐，不断推出新的功能和优化方案。

总之，金融数据中心的评价标准和分析指标涵盖了多个方面，包括性能、安全性、可靠性、节能性、成本效益、服务质量和技术创新。这些指标可以帮助我们全面地评估金融数据中心的性能和表现，从而为决策提供依据。

5. 法规贯标体系的评价标准

金融数据中心设计还需要考虑相关法律要求，涉及金融数据中心的国内法律主要包括以下内容。

- (1) 涉及数据保护的要求。根据《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》，金融数据中心需要确保用户数据隐私和安全，包括数据加密、访问控制、数据备份和恢复等方面的措施。
- (2) 涉及数据共享和传输的要求。根据《全国人民代表大会常务委员会关于修改〈中华人民共和国合同法〉的决定》和《全国人民代表大会常务委员会关于修改〈中华人民共和国电子商务法〉的决定》，金融数据中心需要遵守数据共享和传输的相关法规，如数据出口许可、数据跨境传输协议等。
- (3) 涉及知识产权保护的要求。根据《中华人民共和国著作权法》和《中华人民共和国专利法》，金融数据中心需要尊重和保护知识产权，如禁止转载、禁止使用未经授权的软件等。
- (4) 涉及竞争方面的要求。根据《中华人民共和国反垄断法》和《中华人民共和国反不正当竞争法》，金融数据中心需要遵守竞争法规，如禁止滥用市场地位、禁止不正当竞争行为等。
- (5) 涉及金融法规方面的要求。根据《中华人民共和国银行业监督管理法》和《中华人民共和国证券法》，金融数据中心需要遵守金融法规，如禁止非法金融活动、禁止内幕交易等。

二、数据中心应用发展趋势

（一）数字化运维体系概述

数据中心的发展与数据治理是分不开的。一是在组织保障和数据治理方面，需要建立一套完善的管理体系和流程，确保系统的建设和运行得到有效监管，包括明确组织结构、职责划分、人员配置等，以及建立数据收集、整理、分析、应用的数据治理机制。二是在系统建设方面，需要关注系统的需求分析、设计、开发、测试等阶段，确保系统能够满足业务需求，同时保持良好的可扩展性和可维护性。在这一过程中，运维中台的作用是提供底层支持，包括基础设施、工具、平台等方面，以便于系统的建设和运行。三是在系统运行阶段，需要关注系统的监控、故障处理、性能优化等，确保系统的稳定运行。在这一过程中，运维中台可以提供各种工具和服务，帮助发现问题、解决问题，提高系统的运行效率。通过运维中台沉淀底层能力，可以实现运维服务的四化转型，即服务标准化、自动化、可视化和智能化。这有助于提高运维效率，降低人力成本，减少错误，提高系统稳定性。

建立完备的金融数据中心数字化、智能化运维管理体系，可以从以下几个方面入手：一是引入 DevOps 理念，打造 DevOps 研发运维一体化管理体系，实现开发与运维的深度融合，提高协同效率，缩短反馈周期，降低故障风险；二是引入大数据、人工智能等技术，升级建立 AIOps 运维体系，实现对系统的智能监控、预测和优化，提高系统的运行效率和质量；三是引入敏捷运维理念，实现对变化的快速响应，提高系统的适应性和灵活性。

金融数据中心的数字化运维体系建设参考图 2-2-1。

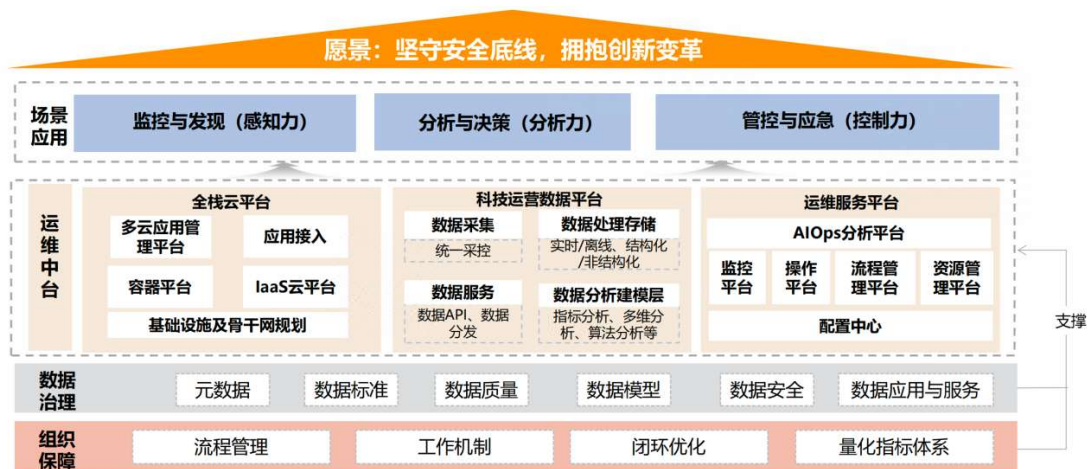


图 2-2-1 金融数据中心的数字化运维体系示例

（二）数据驱动下的 DataOps 运维体系

随着经济社会的数字化转型加速，新一代信息技术不断升级，数据中心运维管理方式也在发生深刻变革。为有效应对数据中心向绿色化、集约化、高密化、智能化建设发展演进过程中的新需求，

数据中心运维需要由“人力密集型”向“技术密集型”演进，实现程度更深、水平更高的信息化变革，并在此基础上进一步向更高级别的数字化、网络化、智能化迈进。这种新型运维模式与综合解决方案被称为基于数据驱动的运维体系。

基于数据驱动的运维体系是集人工智能、大数据等新一代信息技术应用管理平台与数据中心自动化运行设施等深度融合的新型运维模式与综合解决方案。通过对运维设施、平台、体系与服务的全面建设，一方面充分利用数据中心基础设施管理（DCIM，Data Center Infrastructure Management）、数字化运维服务管理平台（DOSM，Digital Operation Service Management）等管理平台叠加自动化运行设施尽可能的实现系统自发现、自控制与自应急；另一方面，通过对海量数据的积累和分析，实现对数据中心运行状态的精准预测和智能决策，从而提高运维效率和质量。

1. 基于数据驱动的运维体系设计

图 2-2-2 是基于数据驱动的运维体系设计示例，通过将数据采集、存储、分析、可视化、自动化等环节紧密结合，同时采用流程化运维 ITIL 和数据化运维 DataOps 等方法，实现更高效、更智能、更稳定的运维管理。

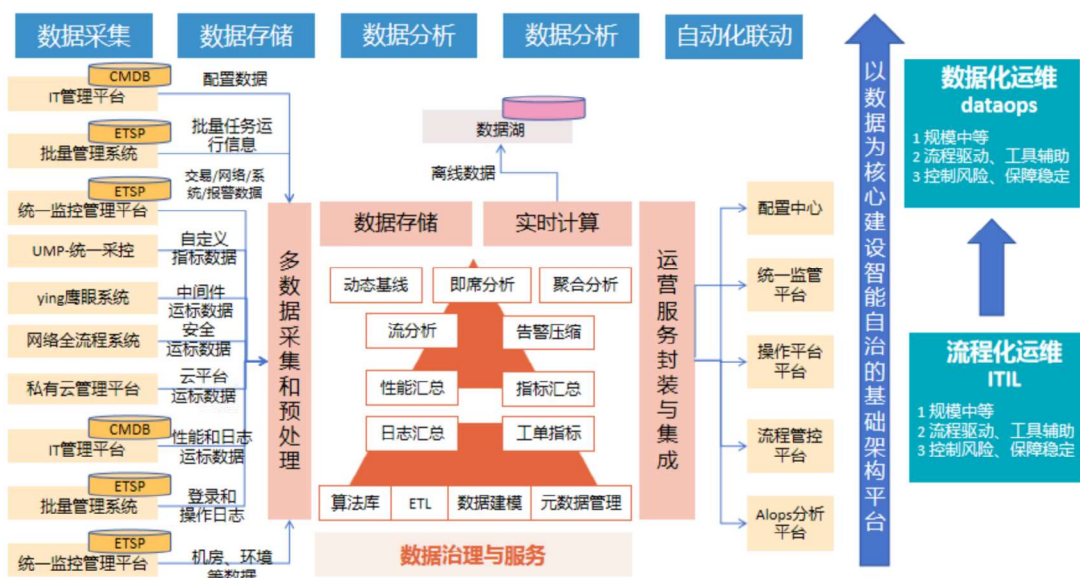


图 2-2-2 基于数据驱动的运维体系示例

(1) 数据采集、数据存储环节。平台从各渠道收集数据，包括传感器、日志文件、数据库等；将收集到的数据进行清洗、整合并存储在适当的数据库或数据仓库中，以便后续分析和处理。

(2) 数据分析、数据可视化环节。平台利用机器学习和人工智能技术对收集到的数据进行分析，以发现潜在的问题和改进点。数据可视化工具将帮助用户更直观地理解数据分析结果，从而做出更明智的决策。

(3) 自动化联动。根据数据分析结果，平台将自动执行相应的操作，如调整系统参数、发送警报或执行修复任务。这将大大提高运维效率，减少人为错误，并确保系统稳定运行。

(4) 流程化运维 ITIL。ITIL（信息技术基础设施库）是一种标准的 IT 服务管理方法，它将运维流程化、规范化，有助于控制风险、保障系统稳定。在智能自治的基础架构平台上，ITIL 可以与其他技术和方法相结合，如数据化和 AI 驱动，以实现更高效、更智能的运维。

(5) 数据化运维 DataOps。DataOps（数据运维）是一种以数据为核心的运维方法，它将数据视为一种重要的资源和资产。在 DataOps 中，大量的数据被用于驱动决策、优化流程、提高效率。结合 AI 技术，DataOps 可以实现更高级别的智能协同和自动化运维。

2. 基于数据驱动的运维体系的发展历程

基于数据驱动的运维体系的发展历程包括四个阶段：一是初始阶段，以人工巡检和故障响应为主，缺乏有效的监控和管理手段，运维效率低下，难以应对大规模数据中心的运维挑战；二是自动化阶段，引入自动化工具和系统，实现部分运维工作的自动化，提高了运维效率，但仍需人工干预和处理复杂问题；三是数据分析阶段，开始利用大数据技术对运维数据进行分析 and 挖掘，实现对数据中心运行状态的实时监控和预测，但数据分析能力有限，难以应对复杂多变的业务需求；智能运维阶段，深度融合人工智能技术，实现对数据中心运行的全面智能管理，提高运维质量，降低运维成本，提升业务连续性。

3. 基于数据驱动的运维体系的目标

基于数据驱动的运维体系的目标是实现数据中心的全面智能化，包括生产连续性、运维即服务以及数据驱动管理等。

(1) 生产连续性。指数据中心基础设施层面进行智能化运行的过程，设施根据既定的设计标准和架构冗余度，结合业务需求和管理要求，在不超过设计运行目标的异常情况下，可以按照预定义模式持续运行。

(2) 运维即服务。在借鉴了 SaaS（Software as a Service，软件即服务）和研究了业界数据中心服务转型的基础上提出新理念。

(3) 数据驱动管理。以数据为驱动，通过数据分析和建模，实现对数据中心运行状态的精准预测和智能决策。

4. 基于数据驱动的运维体系的发展趋势

基于数据驱动的运维体系的发展趋势主要包括：一是智能化，随着人工智能、大数据等技术的发展，基于数据驱动的运维体系将更加智能化，实现更全面、更精准、更高效的运维；二是自动化，自动化将成为运维体系的重要组成部分，通过自动化工具和系统，实现运维工作的高效、低成本运行；三是服务化，运维将逐渐转变为服务，以用户需求为导向，提供个性化的运维服务，提高用户满意度；四是云平台化，随着云计算的发展，基于数据驱动的运维体系将逐渐向云平台转移，实现云边端一体化的运维管理。

总的来说，基于数据驱动的运维体系是一种新兴的运维模式，它将人工智能、大数据等技术应用于数据中心运维，实现了运维工作的智能化、自动化和高效化，为数据中心的运行提供了强大的支持。未来，随着技术的不断发展，基于数据驱动的运维体系将在数据中心中发挥更加重要的作用，推动数据中心创新发展。

（三）AIOps 智能运维体系

AIOps（Artificial Intelligence for IT Operations）智能运维体系是一种集人工智能、大数据等新一代信息技术应用管理平台与数据中心自动化运行设施等深度融合的新型运维模式与综合解决方案。它是一种基于人工智能的科学，旨在提高数据中心运维的效率和质量。

1.AIOps 智能运维体系的发展阶段（如图 2-2-3 所示）



图 2-2-3 AIOps 智能运维体系的发展阶段

（1）数据化运维。通过数字化技术，将运营过程中的各种信息以数据的形式进行记录和存储，包括客户信息、业务数据、运营动作等。通过对这些数据的分析，可以发现运营中的问题和机会，从而优化运营策略。

（2）智能化运维。在数据化运维的基础上，引入人工智能技术，实现对运营过程的智能化管理。如通过机器学习算法，可以预测运营过程中的各种问题，提前采取措施进行优化。此外，还可以利用自然语言处理技术，自动分析和处理大量的文本数据，提高运营效率。

（3）智能化运营。在数据化运维和智能化运维的基础上，实现对运营过程的全面智能化管理。全流程包括统一决策、统一分析、统一监控、统一告警和统一数据五个方面：统一决策指通过

小步试错和创新，总结有效场景和局限性，输出精确结论，构建决策体系，实现业务需求联动技术决策；统一分析指通过全景可观测，智能化分析，构建反馈机制，实现基于统一监控和统一告警构建反馈机制；统一告警指集中处置问题，一体化协作，实现智能收敛，自动处置，沉淀有效经验；统一数据指建立数据团队，破除竖井化数据管理，夯实平台基础和智能化底座，完善数据消费机制，主动开展数据治理。

2.AIOps 智能运维体系的发展历程

AIOps 智能运维体系的发展历程包括三个阶段：一是初始阶段，在这个阶段，AIOps 的概念和理论框架刚刚开始形成，相关研究和实践主要基于传统的 IT 运维方法，尚未充分融入人工智能技术；二是发展阶段，随着人工智能技术的不断发展，AIOps 开始融入更多的 AI 技术，如机器学习、自然语言处理等，开始尝试对 IT 运维过程进行智能化改造；三是成熟阶段，在这个阶段，AIOps 已经形成了较为完善的理论体系和实践方法，广泛应用于 IT 运维领域，成为推动 IT 运维发展的重要力量。

3.AIOps 的目标与理念

AIOps 的目标与理念主要包括：一是提高运维效率，通过 AI 技术，实现对 IT 运维过程的自动化和智能化，从而大大提高运维效率，减少人力成本；二是保障系统稳定，通过 AI 技术，实现对系统运行的实时监控和预测，及时发现和解决潜在问题，保障系统稳定运行；三是优化运维决策，通过 AI 技术，对大量运维数据进行分析，为运维决策提供数据支持，帮助运维人员做出更加科学和合理的决策；四是提升用户体验，通过 AI 技术，实现对用户需求的快速响应和满足，提升用户体验。

4.AIOps 的发展趋势

AIOps 的发展趋势主要包括以下几个方面：一是 AI 技术将更加深入地融入 IT 运维领域，推动 IT 运维向更加智能化、自动化的方向发展；二是 AIOps 将与其他新技术如云计算、大数据、物联网等更加紧密地结合，形成更加完善和高效的运维体系；三是 AIOps 将在更多行业和领域得到应用，如金融、医疗、教育等，推动这些行业的信息化建设和运维管理；四是 AIOps 的研究和实践将不断深入，形成更多的理论体系和实践方法，为 IT 运维提供更多支持。

总的来说，AIOps 是一种将人工智能技术应用于 IT 运维领域的体系，其发展目标是通过 AI 技术提高运维效率，保障系统稳定，优化运维决策，提升用户体验。随着 AI 技术的不断发展，AIOps 将发挥更大的作用，推动 IT 运维创新发展。

（四）DevOps 研发运维一体化

DevOps 是一套研发运维一体化的体系和方法，旨在实现更快速、更可靠的应用开发和部署。它的核心理念是通过打破传统的研发和运维之间的隔阂，使得两者能够更好地协同工作，从而提高软件交付的效率和质量。在数据中心智能化、高效化管理的趋势下，DevOps 亦可融入到数据中心运维体系中，助力数据中心的高效治理。

DevOps（Development 和 Operations 的合并词）是一种软件工程文化和实践，它强调开发（Dev）和运维（Ops）团队之间的紧密协作，以实现更快速、更可靠的应用交付。在传统的软件开发过程中，开发和运维通常是分离的，开发团队负责编写代码，运维团队负责部署和维护。然而，这种分离导致了效率和质量的降低，因为开发和运维之间的沟通和协作存在障碍。DevOps 通过打破这种隔阂，使得开发和运维团队能够更好地协同工作，从而提高软件交付的效率和质量。

DevOps 的核心实践包括持续集成（Continuous Integration）、持续交付（Continuous Delivery）和持续部署（Continuous Deployment）。持续集成指开发团队频繁地将代码集成到主分支，以尽早发现和修复问题；持续交付指运维团队能够快速、可靠地将代码部署到生产环境；持续部署指开发团队能够自动化地将代码部署到生产环境，而无需人工干预。

1.DevOps 的发展历程

DevOps 的发展历程可以分为以下几个阶段：一是传统软件开发阶段，在这个阶段，开发和运维是分离的，开发团队负责编写代码，运维团队负责部署和维护，分离导致了效率和质量的降低，因为开发和运维之间的沟通和协作存在障碍；二是 DevOps 实践阶段，随着云计算和自动化技术的发展，开发团队开始尝试将开发和运维结合起来，以实现更快速、更可靠的应用交付，这个阶段的典型实践包括持续集成、持续交付和持续部署；三是 DevOps 成熟阶段，在这个阶段，DevOps 已经成为一种广泛的实践，开发团队和运维团队能够更好地协同工作，以实现更快速、更可靠的应用交付，这个阶段的典型实践包括容器化部署、微服务架构和持续监控。

DevOps 的目标是提高软件交付的效率和质量，通过打破传统的研发和运维之间的隔阂，使得两者能够更好地协同工作。其理念是“以用户为中心”，强调快速响应变化，持续学习和改进，以及跨团队的紧密协作。这种理念使得开发团队和运维团队能够更好地理解彼此的需求和挑战，从而提高软件交付的效率和质量。

2.DevOps 的发展趋势

随着云计算、容器化、微服务等技术的发展，DevOps 正在向更深入、更广泛的方向发展。以下是 DevOps 的发展趋势。

（1）DevOps 与云原生技术的融合。随着云原生技术的发展，DevOps 正在与云原生技术融合，以实现更快速、更可靠的应用交付。如容器化部署和微服务架构已经成为 DevOps 的核心实践，很多数据中心的治理应用都可以深度集成在 DevOps 中。

（2）DevOps 和数据管理相结合。DevOps 和数据管理相结合可以带来许多好处，包括更快的数据交付、更高的数据质量和更好的数据安全性。一是数据管道自动化，通过自动化数据管道，可以确保数据从源头到目的地的传输和处理过程更加高效、可靠和安全，包括数据清洗、转换和加载（ETL）过程的自动化；二是持续集成和持续交付（CI/CD），将数据管理过程与 DevOps 实践相结合，可以实现持续集成和持续交付，这有助于确保数据质量始终得到维护，同时还可以加速数据交付速度；三是数据监控和分析，通过在 DevOps 环境中集成数据监控和分析工具，可以实时了解数据的状况，从而更好地控制数据质量，包括对数据偏差、数据完整性问题和数据安全性的实时监控；四是数据治理，将数据治理原则和实践融入 DevOps 流程中，可以确保数据在整个生命周期

中得到适当的保护和管理，包括对数据的创建、存储、访问和使用进行严格的控制；五是跨部门协作，鼓励数据管理人员与开发人员、测试人员和其他相关团队紧密合作，以便更好地了解数据需求、优先级和限制，有助于确保数据在整个开发过程中得到适当的考虑和处理。通过将 DevOps 和数据管理相结合，企业可以更快地交付高质量的数据，从而提高业务效率和竞争力。

(3) DevOps 与安全管理相结合。在传统的软件开发过程中，安全和质量往往是相互矛盾的。在 DevOps 中，安全和质量是相辅相成的。通过打破传统的研发和运维之间的隔阂，使得安全和质量团队能够更好地协同工作。

(4) DevOps 的自动化和智能化。随着人工智能和机器学习技术的发展，DevOps 正在向自动化和智能化的方向发展。如通过使用 AI 和机器学习技术，DevOps 可以实现更快速的故障诊断和恢复。

总的来说，DevOps 是一种新兴的软件开发模式，它通过打破传统的研发、运维、数据治理、安全管控之间的隔阂，使得整个软件开发过程能够更好地协同工作，从而提高软件交付的效率和数量。随着云计算、容器化、微服务等技术的发展，DevOps 正在向更深入、更广泛的方向发展。

三、北京金融数据中心建设实践

数据中心作为数据应用和数据运转的基础，是数据的枢纽和算力的载体，同时也是数字经济的关键要素与核心资源，正在发挥着越来越重要的作用。

当前我国数据中心产业正在由通用数据中心占主导，演变为多类型数据中心共同发展的新局面，数据中心间协同，以及云边协同的体系将不断完善。以应用为驱动，多种类型的数据中心协同一体，共同提供算力服务的模式，将成为我国数据中心算力供给重要形态，能更好地服务于生产和生活各个环节，成为各行业数字化转型的重要支撑，推动数字经济快速发展。

“2022 中国数字经济企业发展报告”和“数字经济企业 TOP500 发展指数”显示，目前北京在全国数字经济领域的发展中处于领先地位。作为国家的政治、科教和文化中心，北京拥有丰富的数据资源和高科技人才，为建设和发展金融数据中心提供了良好的基础。为了加大数据中心的建设力度，北京各级政府和相关行业企业推出了“建立数据基础制度先行区、全面推进首席数据官制度”等多个支持政策。

本报告收集、整理了北京金融数据中心项目参考案例，案例名称见表 3-1-1。

表 3-1-1 金融数据中心项目参考案例

序号	案例项目名称	分类
1	华夏银行：全栈云平台建设实践	云平台建设与架构转型
2	爱心人寿：云上云下异地灾备中心项目	灾备建设
3	华夏银行：华夏同城双活机房网络建设及搬迁实施项目	基础设施建设

序号	案例项目名称	分类
4	大童保险服务：快保云服平台	云平台建设与架构转型
5	阳光保险集团：云杉容器云平台	云平台建设与架构转型
6	爱心人寿：DevOps 实践	运维与安全
7	华泰人寿：安全运营中心	运维与安全
8	瑞泰人寿：智慧审计信息云系统	云平台建设与架构转型
9	北京农商银行：高端 NAS 存储双活建设项目	灾备建设
10	北京农商银行：运行版本变更自动化项目	运维与安全
11	人保科技：中国人保集团北方信息中心建设项目	基础设施建设
12	阳光保险集团：小审阳 1 号——智能关系网络分析平台	
13	阳光产险信保事业部：智能运营管理可视化平台	
14	阳光财险：全能保双活建设	
15	时速云：分布式支撑平台建设解决方案	云平台建设与架构转型
16	新华三集团：SeerFabric 金融智能无损数据中心解决方案	
17	神州云科：云科通明湖应用交付弹性计算解决方案	云平台建设与架构转型
18	西骏数据：数据库统一操作平台	运维与安全
19	博云：容器云平台解决方案	云平台建设与架构转型
20	嘉为蓝鲸：嘉为鲸翼多云管理平台解决方案	云平台建设与架构转型
21	嘉为蓝鲸：嘉为蓝鲸灾备切换管理中心解决方案	灾备建设

一、华夏银行：全栈云数据中心实践项目

1. 项目背景

华夏银行在新的五年规划中提出，秉承“服务新时代、建设新华夏”主题，以综合金融服务巩固对公业务基础地位，着力提升数字化和零售业务发展新动力，打造绿色金融和财富管理发展的新特色，畅通服务实体经济的血脉。高效安全的新发展格局离不开新技术，新架构的支持。在业务稳健发展背后，华夏银行确立并实施首批数字化转型重点工程，如旨在提升数据管理与应用能力的“禹治”工程；旨在提升科技智慧安全运营能力的“神盾”工程等。作为“神盾”工程的一项重要任务，全栈云平台项目深入探索 IT 架构转型，利用分布式云原生技术栈、全链条安可技术栈，实现系统稳定运行、智能控制、信息交互便利、金融信息安全可靠，为华夏银行 IT 系统全面转型打下基础，为解决我国在“卡脖子”的技术场景以及相关技术验证做出贡献。

本项目以全栈云为技术核心和落地实体，包含了多层级、多能力的一系列硬件、软件、系统和服务的集合，明确了华夏银行未来基础设施的发展方向，确定了未来技术架构，降低了基础设施成本投入，充分发挥数字资产价值，带来显著的经济效益，有效支撑了全行业务拓展和金融创新，全面提升新技术应用支撑能力。

本项目旨在确保信息系统运行安全、稳定、快捷的前提下，创新性建设云原生平台以及全栈技术体系和全面的服务能力。在兼容性、全栈互通性等方面进一步带动全栈云平台安全能力以及开放的产业链生态发展。

金融级全栈私有云平台是华夏银行自主建设的云计算产品服务平台，以云原生技术框架为支撑，提供包含云主机、云存储、弹性 IP、虚拟私有网络等基础云服务，以及容器、负载均衡、服务网格、云数据库等高级云服务，为各应用系统提供高可用、高弹性、安全合规的云计算服务，同时通过云架构 AZ 设计、一云多“芯”、多云管理、智能运维等能力保障业务高可靠。

2. 项目创新点

一是金融云平台涉及金融信息，具有多层分布式云原生架构、系统性平台安全、开放性多云管理、一云多“芯”、可持续的多生态兼容、智能运营等创新点。

二是基于 Kubernetes 集群架构提供云原生应用的资源交付能力，构建操作系统 + 容器 + k8s 的云原生不可变基础设施；PaaS 层面提供统一的编排框架，支持数据库、中间件和消息平台提供分布式服务和标准化交付，结合行内自研 DevOps 形成华夏银行云原生架构，实现从传统架构向敏捷架构演进。

三是在充分发挥云原生安全能力优势的基础上，持续筑牢具备“安全内生、主动免疫、智能感知、动态适应”等特色的纵深安全防护体系。增强云平台网络结构安全性，完善云平台安全措施，提升云基础平台安全防护能力，增加云服务安全纵深防御，全面满足合规管控要求。有效抵御日趋复杂的网络威胁，充分保障云平台的持续稳定运行，支撑业务的安全可靠发展。

四是规划全行五朵云面向全行全业务场景提供服务：生产云、分行云、中间业务云和金融生态云，其中全行生产云主要承载总行生产应用系统、各分行的前置及重要的、无特殊需求的关键应用系统；金融生态云（托管云）主要承载子公司、行外客户生产业务以及未来服务其他产业，实现产融结合。

五是建设统一云管平台，实现稳敏态、总分行等不同资源池的统一管理和全局调度，屏蔽稳敏态底层资源及技术差异，实现云服务门户、云服务管理、云服务运维三项主要功能，提供统一的IaaS、CaaS、PaaS、SaaS等服务，包括计算、存储、网络、安全、数据库、中间件和批量等资源，支持统一监控、数据报表和计量计费等功能。

六是云服务门户通过 Web 方式为最终用户提供统一入口和使用界面，主要包括服务请求管理和服务目录管理。云服务管理负责云服务的申请、审批、交付、使用和回收等各个环节的全生命周期管理，主要包含服务目录设计、服务实例配置、服务编排和执行、服务计量管理。云运维平台主要负责云环境的监控、配置、容量和应急等日常管理维护，提升云资源与云服务管控能力。

七是自研云魔方运维服务平台，凭借先进的技术架构和前卫的运维理念，在云平台的运行监控、变更操作、弹性供给、故障定位、问题处置等方面提供一键式解决方案，并在安全可控的前提下，推出了移动端 App 工具，极大提升了私有云平台的运维水平和技术掌控能力，在同业中处于领先水平。按照体系化建设思路，围绕安全生产关键环节和重要部位，以安全技术和安全运营两大体系为主，梳理差距短板，明确努力方向，从运维工具箱建设、智慧化生产运维、数据安全保护 3 个方面入手，细化工作任务，确定实施路线，确保各项措施落实到位。同时制定了 5 分钟发现、3 分钟定位、2 分钟解决问题等运维目标。规划以运维数据为核心建设智能运维数据平台，为运维数据应用场景提供一体化支持。

3. 项目技术方案

(1) 整体方案设计

为保障信息系统建设持续支撑全行及各子企业业务发展，华夏银行按照统一建设规划、统一技术路线、统一管理底座和统一版本控制的原则，建设完成自主规划、建设及运维的云计算平台（整体架构见图 3-1-1），支撑了传统应用平台、云原生平台、数据平台三种生态应用的统一部署和运行。



图 3-1-1 华夏银行全栈云整体架构

该平台采用“一横、五纵、两技术栈”的方式进行规划和建设。“一横”指统一的管理平面和运维平面，云上的所有系统均按照相同的技术标准使用云计算服务；“五纵”指总行、分行、子公司、龙盈和信用卡五个相互隔离的虚拟资源区，通过租户划分和权限控制共同使用云平台资源；“两技术栈”指云平台分为两条技术路线，即支撑传统应用的稳态技术路线和支撑云原生应用的敏态技术路线。

(2) 云平台逻辑架构

华夏私有云平台由基础设施层、资源池层、云服务层、管理域和展现层组成，如图 3-1-2 所示。



图 3-1-2 华夏银行私有云逻辑架构

①基础设施层。华夏银行私有云实际运行的物理设施，包括 X86、ARM 或 GPU 服务器，提供块存储的 SAN 或者分布式存储设备，提供对象或者文件的存储设备，通过网络交换机、路由器、防火墙组网互联，形成大规模集群；集群在云平台的管理下，为上层业务提供具有云平台能力的资源服务使用方式。本次设计基础设施层主要以 X86 服务器和网络设备组成。

②资源池层。将基础设施层提供的硬件设备按照逻辑功能的不同划分为不同功能的资源池。按照提供服务能力的不同分为基础服务资源池和数据服务资源池；本次设计虚拟化资源池、物理机资源池、网络资源池、分布式块存储资源池、分布式对象存储资源池。

③云服务层。作为云服务的后端实现实体，主要完成服务的封装和对资源的自动化分配、使用。通过对资源池层相关资源的封装，实现云资源服务的发现、路由、编排、计量、接入等功能，实现从资源到服务的转换。

④管理层。管理层分为运营管理和运维管理两部分：运营管理提供运营管理功能，如云服务申请和自助服务能力，包括租户管理、组织管理、流程审批、统一认证、云服务管理、经营优化等运营管理功能；运维管理提供运维管理功能，支持对多个数据中心的统一运维管理，包括告警、性能、监控、日志以及报表等功能。

⑤展现层。展现层是云管理平台的对外呈现，分为用户门户及管理员门户：用户门户面向最终租户 / 用户，管理员门户面向系统运营 / 运维管理员等。租户 / 用户可通过服务控制台自助实现对服务的申请、使用、监控、删除等生命周期管理的操作；运营 / 运维管理员可以通过管理员门户完成对系统的管理。

（3）云平台技术路线

华夏金融云采用全链条安全可控技术，构建全新生态的云原生技术栈，并对应用提供有效支撑和运维，建设领先的新型 XC 平台，在硬件平台、SDN 及安全、云平台及云操作系统各层面全面实现自主可控。充分运用云计算、大数据等先进理念和技术，按照“集约高效、共享开放、安全可靠、按需服务”的原则，以“云网合一、云数联动”为构架，建成云平台，实现各部门基础设施共建共用、信息系统整体部署、数据资源汇聚共享、业务应用有效协同，开展大数据开发利用，为企业管理和公共服务提供有力支持，提高服务水平，提升用户数据治理能力。

整体方案的硬件基础设施层使用国芯计算型、存储型服务器资源池，以及基于国芯的 GPU 服务器资源池构建，为银行业务发展提供充足高效的算力。在平台技术层，全栈云采用分布式技术实施。首先，在应用架构设计上遵循三个原则：松耦合（微服务，松耦合与组件化的服务架构）、分布式（复杂服务简单化、每一层考虑分布式部署）、实时化（各层之间保持数据实时连接）。其次，在基础平台技术上走分布式路线，包括计算、存储、网络、数据库等单元。最后，通过本项目的建设，系统采用微服务架构、国产操作系统、国产中间件、国产 CPU 服务器，相较于传统架构，大幅度降低整体解决方案的软硬件成本，单账户管理成本降低了 80%-90%。采用云魔方运维服务平台大幅减少了因故障导致的系统中断时间，项目上线后因云平台故障造成的系统中断时间较之前降低了 5 倍。

综上，华夏银行金融级全栈私有云平台建设从底层芯片到上层应用生态均满足开放和持续发展的要求，覆盖互联网、生产网、开发测试等环境，提供了计算、存储、网络、大数据、数据库等基础软硬件服务，以及容器、应用网关、服务网格等云原生服务，有力支撑各类信息系统云化及微服务化改造。云魔方运维服务平台重在运维平台及工具的开发，虽然不能直接产生经济效益，但大幅减少了因故障导致的系统中断时间，从而间接创造了业务价值。

二、爱心人寿：云上云下异地灾备中心项目

1. 项目背景及目标

为保障爱心人寿重要业务系统安全、可靠、稳定运行，提升各类信息系统突发事件应对能力，有效防范重要信息系统风险，满足监管对业务连续性的要求，公司决定启动异地灾备中心建设。根据公司生产中心的部署特点，以及与未来灾备中心的关系和定位，项目组分别考察了以下三套方案：跨云异地灾备方案、同云异地灾备方案、云上云下异地灾备方案。在综合考虑公司的业务发展规划与成本投入约束等条件下，最终选定云上云下异地灾备方案。项目目标旨在针对公司主要业务系统构建异地的应用级灾备中心，满足监管要求的同时，确保当灾难发生时可快速在灾备中心恢复主要业务系统运行并开展正常的业务经营。

2. 创新点

爱心人寿灾备中心建设以开放性、先进性、可扩展性、经济性为原则，最大化涵盖公司主要业务系统，组织以自有人力为主，外包人力为辅的科技力量，采用新模式、引用新技术，建设具有爱心特色的跨云异地应用级灾备中心。

灾备中心建设具有以下四大创新特性。

(1) 云上云下异地灾备

异地灾备建设对于跨域网络环境要求较高，灾备数据中心与生产中心通过两条 30MB 专线互联，无法满足实时数据同步传输要求，经过多方考察调研，最终使用裸光纤将灾备数据中心与同园区腾讯北京公有云 POP 点对接，并将北京至上海金融云的云专线通道扩展至 1GB，且打通灾备中心与腾讯北京金融云网络，为云上云下异地灾备建设打造数据传输高速通道。公司生产系统使用了较多的云平台产品和技术，为保证灾备环境与生产环境系统代码一致性，灾备建设还面临基础平台产品的同构问题，通过调研沟通，最终采用腾讯云产品私有化部署的模式保持与云平台的技术兼容，借助腾讯 DTS 软件实现云端至云下的异地数据实时同步，实现从腾讯上海金融云到北京数据中心的云端至云下的异地灾备建设。

(2) 新技术与传统架构结合

爱心灾备中心项目整体采用传统架构模式，通过单独采购硬件服务器，搭建虚拟化平台，部署灾备所需的应用服务器、腾讯私有化版的 TDSQL 及 Redis 平台，确保与生产环境的一致性。在传统架构基础上引入了超融合技术、网络虚拟化技术、英方数据同步、DevOps、流程自动化等新技术，新技术与传统架构融合，为爱心灾备项目赋能，提升灾难恢复效率。

(3) 技术可控

爱心灾备中心项目建设全程以自有人员为主，践行爱心保险 + 科技，从项目的调研、分析、规划到项目的设计和落地，全部由 IT 自主引领实现，通过项目实施锻炼了爱心自有科技队伍、提升对系统自主掌控能力，也是爱心保险 + 科技核心能力的践行过程。

(4) 成本控制

有效成本控制也是此次灾备中心建设的重要目标之一，爱心灾备项目采用以最优性价比的传统架构模式搭建，最大限度利用自身技术资源降低成本投入，将自主可控贯穿项目全过程，加强项目各环节定制化，融合新技术赋能业务，以较低的成本投入完成云上云下异地应用级灾备中心建设。



图 3-2-1 爱心人寿异地灾备中心整体架构

3. 项目技术方案

爱心灾备中心建设，以监管《保险业信息系统灾难恢复管理指引》文件要求为准则，结合爱心自身业务发展规划，对生产中心展开充分的业务风险识别和业务连续性影响分析，经过详尽的市场调研和测试，形成了适合爱心发展战略的灾备中心建设方案。整体方案见图 3-2-1。

(1) 网络架构设计

网络是实现灾难恢复数据传输最重要的一环，将灾备中心与腾讯 Pop 点的连接从专线更换为光纤直连，保证数据传输的稳定性，是实现云上云下异地灾备方案的最有效保障。公司生产网络采用腾讯金融云 VPC 架构，在灾备数据中心新建网络区域与其他业务区域逻辑隔离，提供控转分离、业务平面隔离、弹性扩展快速交付的大二层 Fabric 网络。网络架构采用松耦合的网络架构，使用云融合 SDN 技术搭建业务网络基础平台，同时利用 SDN 网络快速交付能力及大二层灵活扩展性，快速实现业务搭建。同时具备全面的网络防护能力，满足监管合规及业务经营需求。

(2) 数据同步设计

有了网络基础，通过腾讯云 DTS 软件实现灾备中心数据库与腾讯云 TDSQL 之间的数据实时同步，构建灾备数据中心。数据同步设计如图 3-2-2 所示，当腾讯云出现灾难时，可快速将业务切换到灾备数据中心并恢复服务，保证业务的可持续性。大量生产业务数据存储在腾讯云金融云的 COS 对象存储中，为保障灾备中心使用同类型服务，通过与腾讯协商，打通灾备中心与北京腾讯云金融云之间内网连接。通过腾讯 COS 存储的跨域同步复制功能将数据实时同步至北京腾讯云金融云，灾备中心可通过内网直接访问北京金融云 COS 数据，从而提升灾备中心快速切换并恢复业务运行效率。

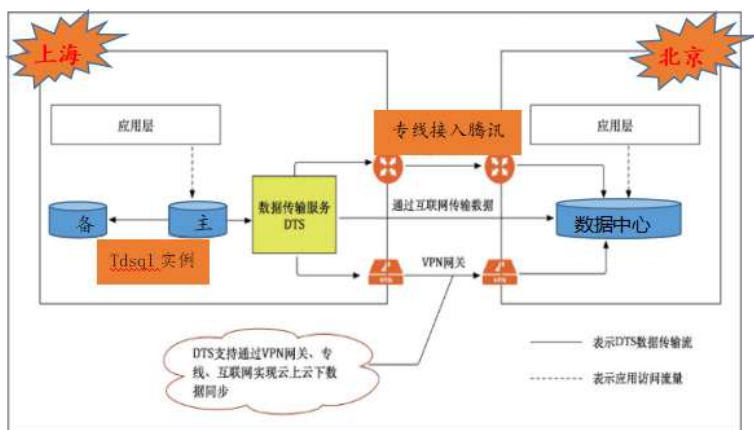


图 3-2-2 数据同步设计示意

(3) 数据库设计

选定数据同步技术后，数据库平台采用了腾讯 TDSQL 一体机方案，实现与生产系统同构，保证灾备系统的数据一致性。业务系统使用的 MQ 和 Redis，为保证程序代码一致性，引入了私有化版本的腾讯软件，采用 VM 部署方式，软件平台版本每年升级一次，保证与腾讯金融云接口兼容，各业务系统通过内网可直接访问。

(4) 虚拟化资源池设计

灾备中心计算及存储资源采用虚拟化技术，自有人力可维护，采用最优成本方案。资源池使用 Nutanix 超融合一体机，由高配的 PC 服务器组成，在资源池中创建灾备所需的各类规格 VM，实现生产与灾备最低 2:1 的配置比。虚拟化资源池设计见图 3-2-3。

(5) 应用同步发版

公司 IT 团队以 CI/CD 为轴心，整合了 GIT 和 SVN 代码管理、统一了 JIRA 需求管理全流程、引进先进的代码扫描和度量工具 Merico、集成了自研的自动化测试框架、构建多云部署架构，创

新性的融合了 IT 服务流程和资产管理，建成了具有高度可扩展性和兼容性的先进的 DevOps 基础体系，实现灾备中心各系统与生产系统的自动同步发版，保证灾备中心业务应用程序版本与生产环境完全一致。

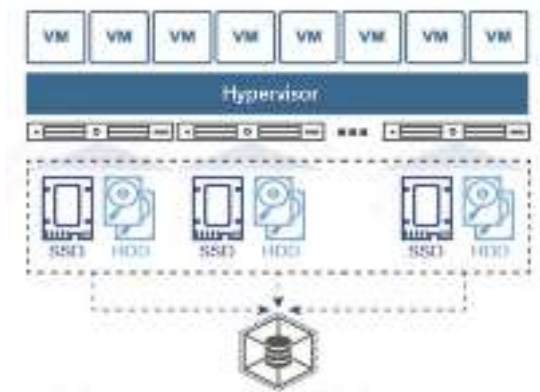


图 3-2-3 虚拟化资源池设计

4. 项目成效

爱心人寿灾备中心项目充分整合 IT 资源，以新技术与传统架构结合，实现保险主要业务系统从云端至云下的异地灾备中心建设，为公司开展混合云的系统部署模式奠定坚实基础。

(1) 满足监管要求。不仅满足了“重要信息数据需异地备份；关键类业务系统灾备系统须满足电子传输及完整设备支持”的监管要求，且大幅高于监管所要求的灾备建设标准。

(2) 灾难防范能力。当生产中心遭受重大灾难时，公司可以快速在灾备中心恢复主要业务系统运行并开展业务，确保公司业务的连续性，保障公司可持续正常经营及客户的权益。

(3) 数据保护能力。当生产中心遭遇重大灾难而导致数据销毁或丢失时，灾备中心将保证公司业务数据库接近零丢失，进一步加强了爱心的信息安全防护能力，增强客户对公司的信任感和依赖性。

(4) 技术能力支撑。通过灾备建设验证了公司业务在公有云和私有云之间的可迁移性，为公司将来信息系统建设模式提供更多选择性，并为公司开展混合云建设提供技术支撑。

三、北京农商银行：运行版本变更自动化项目

1. 背景

2021 年上半年，北京农商行的新核心银行项目建设到了最关键、最紧要的冲刺阶段，1 个新核心银行系统、1 个新柜面系统、100 余套外围系统需要同期上线。在这次大规模、集群式上线中，各系统间关系复杂，投产窗口有限，操作步骤繁杂。如何有效提高效率、确保版本变更 100% 成功、压降操作强度和风险，成为新核心项目的一项重点工作内容。

版本变更自动化投入使用前，各业务系统版本变更以手工操作为主，其存在以下问题：一是版本变更操作复杂，绝大多数系统的版本变更包含程序上传下载、备份、服务启停、程序更新、配置文件修改、数据文件更新、投产后技术检查等，操作比较复杂；二是版本变更操作耗时长，由于各

业务架构复杂，服务器数量多，每个系统每次版本变更需耗时 1 个小时以上，耗时长；三是版本变更人员投入大，出于版本变更成功率控制及风险管控，95% 以上的变更都要在变更窗口期进行，时间紧、任务重，在短时间内，每套系统的变更需要执行人和复核人共同完成变更还需要对他人的操作进行复核，工作强度大；四是版本变更技术检查落实不到位，版本变更完成后由系统负责人根据经验进行检查，可能会因为工作强度大、服务器数量多而导致个别服务器的技术检查不到位。

2. 实现目标和实施方向

(1) 实现目标。一是落实多次新核心周例会要求，实现至少 100 套新核心银行建设项目涉及系统的版本变更自动化；二是落实疫情常态化防控要求，最大限度降低操作人员的聚集密度。

(2) 项目实施方向。一是实现变更流程标准化、自动化，从投产程序，包版本校验、备份、更新到技术检查，全流程实现自动化，应用负责人在平台进行复核确认，降低版本变更工作强度；二是提升版本变更操作水平，降低版本变更过程中人为操作风险；三是实现变更流程规范化，如投产程序版本检查、技术检查均作为变更流程的关键环节自动进行，降低版本变更风险；四是提高版本变更效率，缩短版本变更耗时。

3. 技术实现

系统逻辑架构如图 3-3-1 所示



图 3-3-1 系统逻辑架构

(1) 用户层。基于系统提供的如流程设计、版本管理、变更管理、权限控制等调度功能，提供了 3 个重要的工具允许开发人员及管理员进行变更流程设计、变更调度及变更过程监控。

(2) 业务功能层。应用系统通过代理 Agent，根据业务关系进行分组管理，通过调度接口，执行具体的作业任务，实时监控作业情况，及时将变更步骤的作业信息及日志反馈给版本变更自动化调度服务器，最终由客户端进行操作、监控、管理。

(3) 系统核心层。具备调度集群、心跳检测、负载均衡及失效备援等高可用机制。

(4) 受控系统层。实现版本下载、投产校验、程序备份、服务启停、程序变更、配置文件修改及变更检查等综合应用功能。

4. 项目实施

通过制定标准开发规范，对变更操作进行统一管理，根据开发规范，开发版本变更自动化流程及脚本，实现版本变更自动化。

开发规范的制定及落实，为版本变更流程及脚本的开发提供了标准及规范参考；要实现版本变更自动化，还需制定变更流程及脚本。变更流程囊括了应用系统所有的变更步骤及各步骤之间的逻辑依赖关系，变更脚本是实现变更步骤的具体操作。

目前，各应用系统的变更步骤不相同，同一应用系统每次的变更步骤也不尽相同，各应用系统的备份、更新等步骤脚本也各有差异，若纳入版本变更自动化平台进行统一管理，则脚本开发工作量大，大规模推广困难。

为解决以上问题，推动版本变更自动化系统的全面推广，必须制定版本变更自动化开发规范，一是按系统分类（文件覆盖类、WAS 类等）进行备份、更新、启停服务等变更脚本的标准化，使脚本具有通用性，减少重复开发，提高效率；二是规范各应用系统版本变更时的变更步骤，将技术检查等操作统一纳入版本变更自动化的范围，形成标准的变更流程；三是标准化各应用系统的变更操作，以降低变更操作步骤对经验的依赖性。

5. 创新点

银行新核心银行项目建设涉及 100 余套外围系统，各个系统已形成自己的发版方式，本着“不影响新核心已有发版方式、最大程度兼容各个系统投产”的原则，对版本变更自动化进行了全新的设计，按照组件、模块、场景进行归纳整理，具备模块化、参数化、强兼容等特点，主要体现在以下几方面。

(1) 投产作业流控和参数灵活设置，保证投产平台高可用性。平台以“灵活可配置”为原则，抽象出 6 类作业模板，根据每次变更程序资源动态配置对应作业流控。抽象出投产参数，通过参数配置实现当数据集发生变化后直接修改配置参数，不需要改动程序，最大限度确保平台高可用性。

(2) 流程形成闭环。只需登录运维自动化平台即可完成流程相关操作，流程操作分散到主机程序投产的各个环节，用户无需额外操作，减化了操作流程。

(3) 变更流程兼容性。增加对各环节的裁剪、略过、禁用等功能，应变临时调整，增加服务器优先级设置，增加模板实例，为不同需求建立不同的模板实例。

(4) 变更流程敏捷性。变更流程的开发采用模块化方式，通过复制同类业务系统的变更流程，再经过简单的个性化调整即可上线。

(5) 投产记录可追溯。运维自动化平台设计了完善的变更日志与统计功能，详细记录投产各环节的操作人、操作时间和操作对象，并对变更实施结果进行保存。同时，设计变更统计模块，对各项变更分类进行统计汇总。

(6) 异常投产可回退。对于投产后出现问题的程序，设计开发了逆向的程序回退模块，便于快速进行程序回退。

6. 项目难点及解决成效

版本变更自动化初期，面临系统架构复杂、环境差异较大、操作无统一的规范、应用负责人操

作习惯不同等困难。以新核心银行系统项目为例，历经 8 轮投产演练，通过对各系统手工部署方案进行梳理，历时 2 个多月，实现 126 套系统应用版本变更自动化，纳管设备 429 台。新核心系统一次性大规模、“集群式”使用变更自动化进行投产，如此大规模使用，在同业中也属首次；变更自动化成功率为 97.62%，投产平均耗时为 542 秒，与手工部署相比，平均节约时间 92% 以上，大大提高投产部署效率，为新核心银行系统上线节省了宝贵的时间。变更自动化实现了测试环境、投产演练环境、生产环境应用版本的自动化部署，保障了新核心银行系统顺利上线，为实现开发、测试至生产的 DevOps 一体化奠定基础；同时，可将运维中心日常自行发起的变更任务分类，针对每类变更实现模板化和标准化，通过运维自动化进行实施，进一步提高变更效率和准确性，降低操作复杂性和风险。

经过摸索与实践，解决以下难点问题（见表 3-3-1）。

表 3-3-1 项目成效

类型	难点	解决成效
程序打包规范	打包规范需覆盖多种操作系统。 兼顾新核心项目组原来打包习惯。 不能影响管理员手工部署。	统一程序打包与提版规范。 统一配置文件书写与提版规范。 完善系统技术投产手册。
变更流程兼容性	系统变更方式多样(was控制台增量发布、程序文件替换、jar包增量更新等)。 变更逻辑多样(步骤的先后关系不定，服务器优先级不同)。 变更需求多样(停不停服务部署等)。	完成100多个基础脚本开发。核对类功能完成4个java类包开发。 增加对各环节的裁剪、略过、禁用等功能，应变临时调整，增加服务器优先级设置。 增加模板实例，为不同需求建立不同的模板实例。
推广应用	新的事物都有接受期，变更又是系统管理员重要且敏感的操作，影响推广的主观或客观原因都存在。	通过集中培训和一对一培训完成技术转移。
变更流程敏捷性	如何加快新增系统的版本变更自动化开发速度？	变更流程的开发采用模块化方式，通过复制同类业务系统的变更流程，再经过简单的个性化调整即可上线。

四、华夏银行：华夏同城双活机房网络建设及搬迁实施项目

1. 项目背景及目标

①项目背景。华夏银行信息科技部紧紧围绕总行“智慧金融，数字华夏”的愿景和“建设一流智慧生态银行”的战略目标，规划部署重点项目工作，随着总行业务的快速发展，现有同城灾备机房的容量和基础设施环境已无法满足 IT 基础架构发展的需求，华夏银行于 2022 年启动实施了新同城灾备中心机房（以下简称“新机房”）的建设和搬迁工作，作为此次项目的配套工程，华夏银行在一年时间内先后完成了新机房的网络设计、建设以及网络搬迁实施工作。

②项目目标。采用标准化、模块化架构设计，引入面向应用的设计理念，按既定计划完成新机房网络的建设工作，旨在建设具备高效交付能力的数据中心网络。新机房网络须保障各应用系统多批次、原 IP 地址搬迁，并确保搬迁期间各应用系统稳定运行。

2. 创新点

- ①新机房互联网 DMZ 区采用数据中心 SDN 技术实现了互联网区网络资源池化，降低网络部署成本的同时提升了网络部署效率。
- ②新机房带外管理网通过采用 SDN 技术解决了机房搬迁所带来的跨楼层大二层问题。
- ③通过建设北京同城二层环网，实现各应用系统多批次、原 IP 地址搬迁以及跨数据中心同网段的稳定运行。
- ④自研网络 Pingmesh 系统实现对机房各区域网络通信质量的实时监控，基于流量分析系统研发网络流量可视化产品，部署在新机房网络 DMZ 区，实现基于域名的网络流量可视化监控，确保搬迁期间重要业务系统网络异常问题的快速根因定位。

3. 项目技术方案

(1) 新机房网络技术方案

华夏银行数据中心网络整体采用两地三中心的架构（如图 3-4-1 所示）。

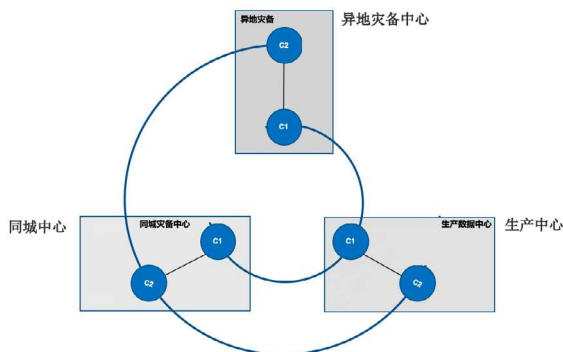


图 3-4-1 新机房网络架构

此次新机房规划替换现有同城灾备中心，基于华夏银行网络架构标准并结合业务需求，新机房网络总体规划 10 个模块，具体网络功能区域设计如图 3-4-2 所示。

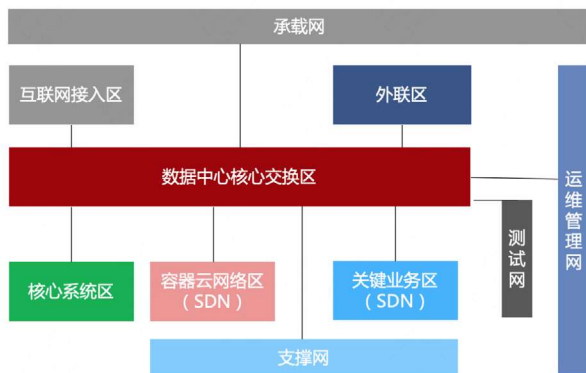


图 3-4-2 网络功能区域设计

新机房网络架构按照模块化原则划分为广域网互联区、数据中心核心交换区、测试网（区）、互联网区、外联网区、核心业务系统区、关键业务区、容器云网络区、支持网、运维管理网（区）共计 10 个区域。

数据中心分区主要根据业务功能划分，功能分区不同主要体现在业务的不同，因此以“业务分类”为主，分区标准分为网络设备逻辑隔离和物理隔离两个维度。

基于上述网络功能区域规划，新数据中心网络架构设计见图 3-4-3。

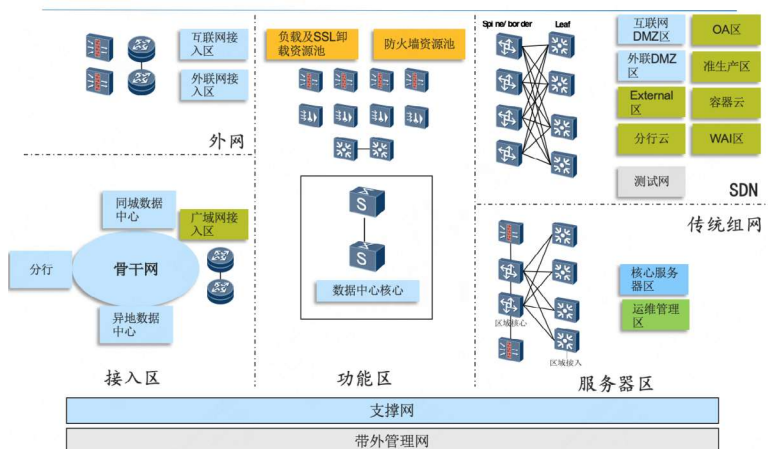


图 3-4-3 新数据中心网络架构设计

数据中心网络整体路由规划见图 3-4-4。

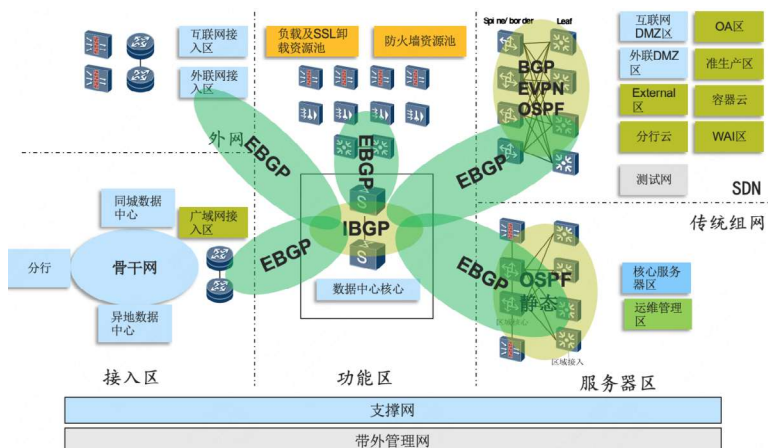


图 3-4-4 数据中心网络整体路由规划

此次机房搬迁涉及应用系统多，存在同一系统 / 平台多批次搬迁的情况，且应用系统须保留原 IP 地址搬迁，为保障上述搬迁需求，华夏银行设计搭建了北京同城数据中心二层环网（见图 3-4-5），主要解决 2 点搬迁痛点问题：一是应用系统多批次搬迁的场景下，实现系统跨数据中心

的平滑迁移；二是搬迁期间新旧两个灾备中心之间网络链路故障时，业务流量实现自动切换绕行，确保搬迁期间业务稳定运行。

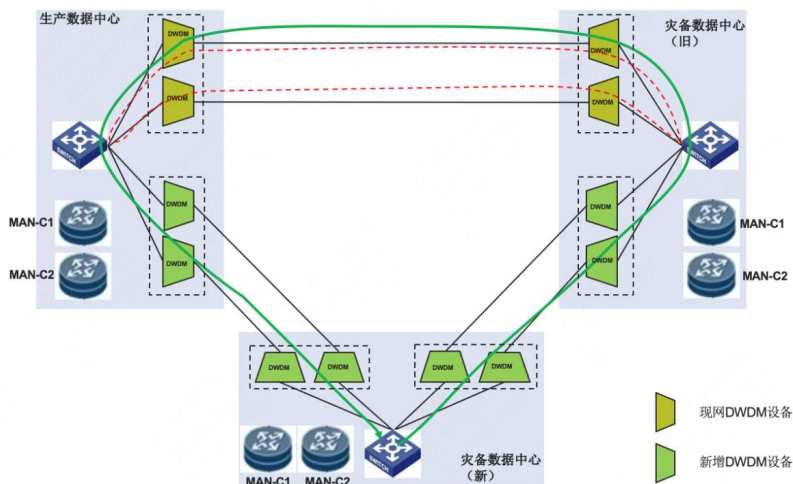


图 3-4-5 北京同城数据中心二层环网

为优化新机房网络 and 系统运维管理能力，新机房网络对运维管理网进行了优化设计，主要由带外管理网、运管服务器区和 ECC 区接入三个子网构成，具体网络架构设计如图 3-4-6 所示。

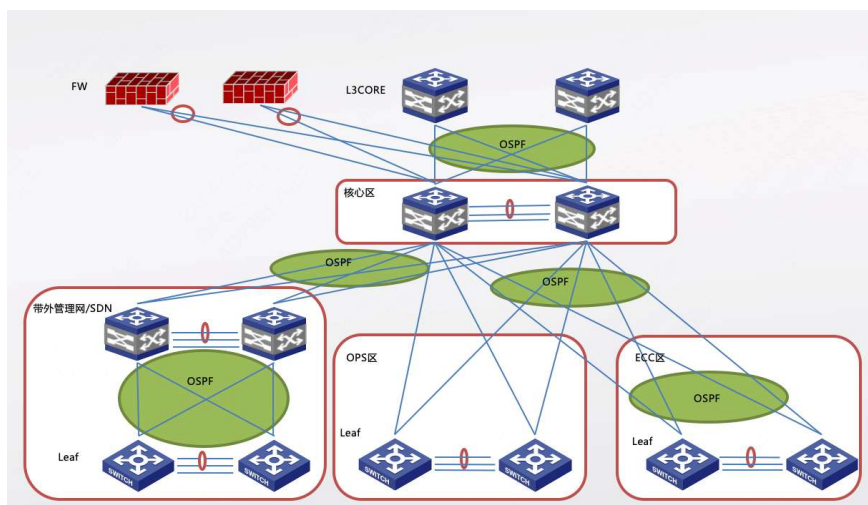


图 3-4-6 网络架构设计

各分区主要承载业务流量规划如下：一是带外管理网，包括网络设备、服务器 BMC 的监控、日常运维、网络自动化；业务系统监控管理和虚拟机管理通过支撑网接入，支撑网通过数据中心大核心与运维管理网互通，运维管理网出口部署防火墙。二是运管服务器区，所有运维管理类的服务器统一接入至此区域；三是 ECC 接入区，机房操作间、运维管理接入。

相较原有灾备机房，新机房容量有较大增长，存在同一业务 / 平台跨楼层、多机房模块部署的情况，此情况将导致带外管理网二层域过大的问题，新机房带外管理网通过采用 SDN 技术完美解决了上述问题，同时实现了 SDN 控制器与交换机产品的解耦，消除了 SDN 技术被单一厂商捆绑的风险，带外管理网架构设计如图 3-4-7 所示。

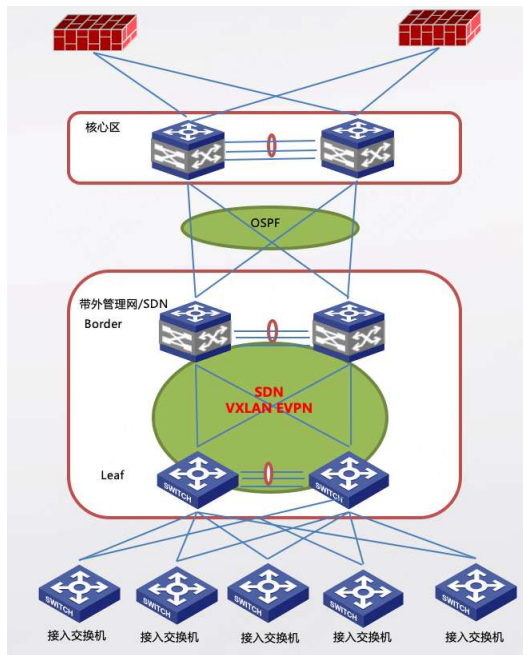


图 3-4-7 带外管理网架构

此外，考虑到运维管理网架构相对复杂，此次对运维管理网安全控制进行了优化设计（见图 3-4-8），通过虚拟防火墙技术将运维管理网各子区进行隔离。

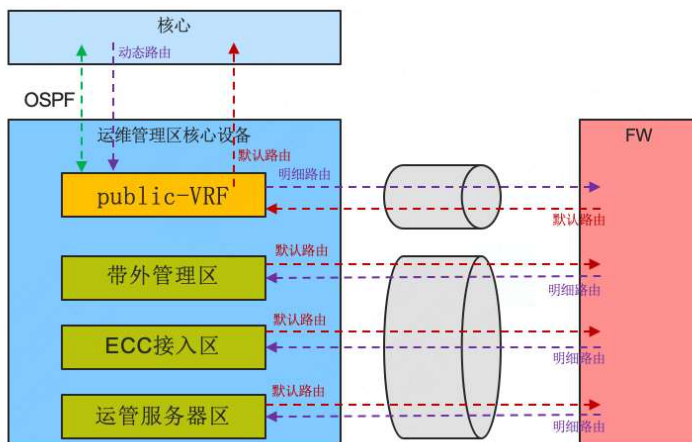


图 3-4-8 运维管理网安全控制

一是部署第三方防火墙和负载均衡设备旁挂至区域核心交换机，防火墙 / 负载均衡采用 HA 部署方式，以保证网络的高可用性；二是负载均衡系统通过静态路由引流，目的地址为 VIP 路由下一跳，负载均衡互联地址。

新机房在互联网 DMZ 区设计时考虑到面向应用的高频运维和交付场景需求，通过采用 SDN 技术实现了互联网区网络资源池化，降低网络部署成本的同时提升了网络部署效率。

互联网 DMZ 区网络架构设计如图 3-4-9 所示。

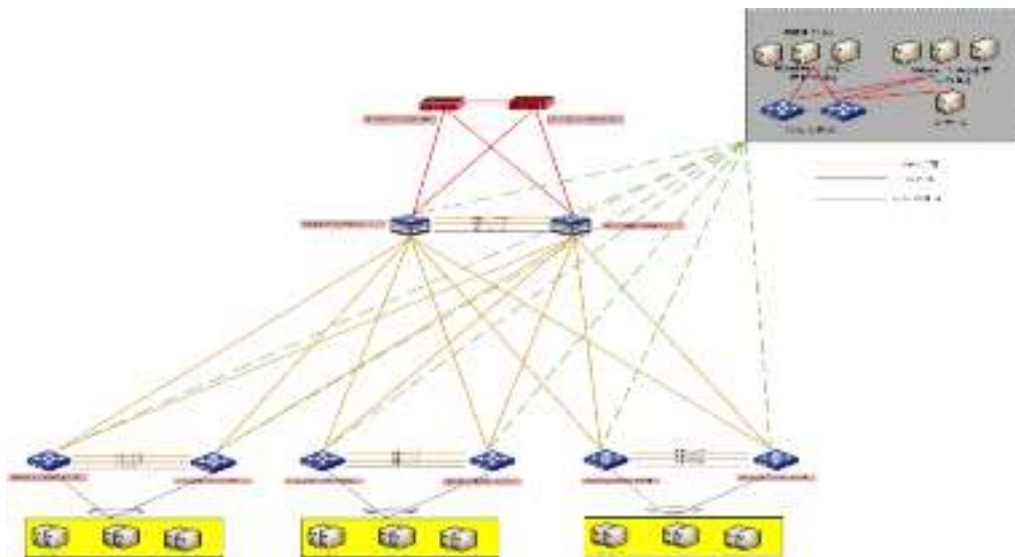


图 3-4-9 互联网 DMZ 区网络架构

通过在互联网 DMZ 区部署 SDN，将 DMZ 七层设备池化，可实现负载均衡、SSL 卸载等七层设备灵活调度、无缝扩展和物理位置解耦，交换机 PBR 由 SDN 控制器统一管理，可有效降低运维管理难度，有效提升网络运维效率。

互联网 DMZ 区流量模型如图 3-4-10 所示。

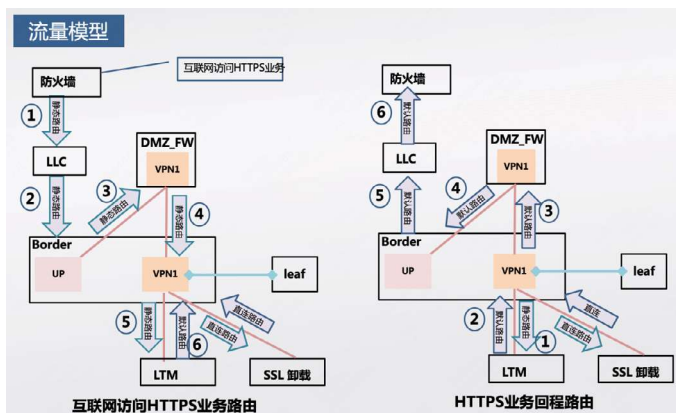


图 3-4-10 互联网 DMZ 区流量模型

此次新机房网络关键业务区采用硬 SDN 的技术方案，与原灾备机房网络环境保持一致，满足业务平滑迁移的需求。根据所部署业务需求，关键业务区网络共划分 7 个业务子分区，分别部署在新机房的三个机房模块，网络采用两层 Spine-Leaf 架构，Leaf 交换机分别上连至两台 Spine 交换机，所有其他设备包括服务器、负载均衡、防火墙等外设均连接至 leaf 交换机，整网采用 Multi-Pod 结构，每个机房模块作为一个 Pod，三个机房模块之间用 IPN 设备进行互联，三个机房模块通过 IPN 网络在 Fabric 内实现大二层功能，关键业务区网络整体架构如图 3-4-11 所示。

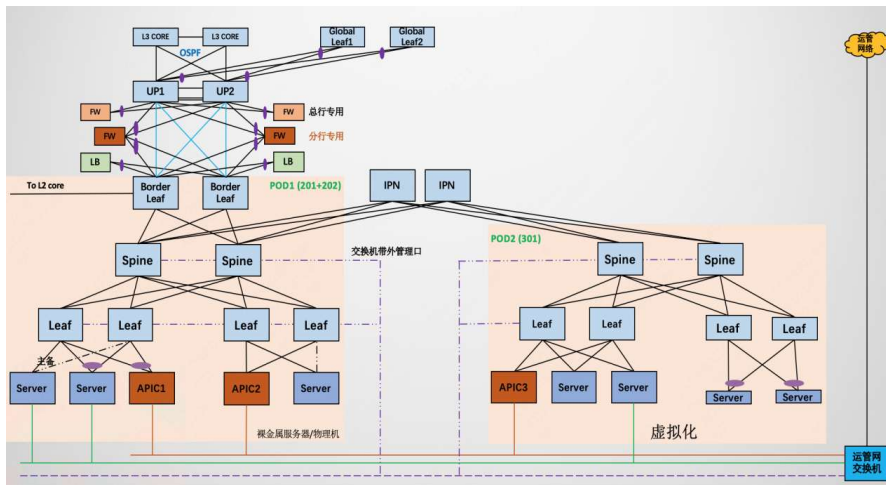


图 3-4-11 关键业务区网络整体架构

(2) 新机房网络监控

新机房在网络规划和建设方面已充分考虑后续搬迁需求，网络架构可支撑整机房应用系统多批次搬迁，华夏银行在机房网络搬迁阶段，重点加强网络监控体系建设，确保对搬迁过程中的网络运行状态实时感知以及后续机房投产后的运维需求，除部署现有网管、监控等产品外，同步自主研发网络 Pingmesh 系统对机房各区域通信质量进行实施监控，同时基于流量分析系统针对 DMZ 区用户访问的关键系统研发网络路径可观测产品，实现基于域名的业务系统流量可视化监控，上述产品重点说明如下。

① 网络 Pingmesh 系统

Pingmesh 系统是一个用于数据中心网络延迟测量和分析的大型系统，利用所有服务器启动 TCPPing，以提供最大网络延迟测量覆盖率并形成多层次的完整图表，系统采用松散耦合式架构，系统主体由 Pingmesh Controller、Pingmesh Agent、数据聚合存储和分析三个模块构成。

系统架构如图 3-4-11 所示。

华夏银行 Pingmesh 系统通过 API 接口对接网络自动化系统，获取网络拓扑信息，并结合分段 Ping 的优化算法，实现快速定位网络故障区域。监控告警方面，华夏 Pingmesh 系统具备对接行内智能分析引擎并通过机器学习算法生成动态阈值的能力，以最大程度降低网络误告警的情况。

在机房搬迁过程中，Pingmesh 系统作为网络监控重要手段，较大幅度提升了网络问题快速发现的能力，提升了网络监控保障能力，Pingmesh 系统应用情况如图 3-4-12 所示。

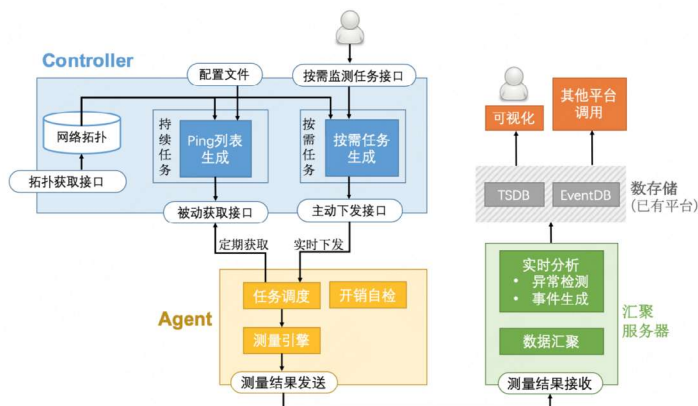


图 3-4-12 系统架构



图 3-4-13 Pingmesh 系统应用情况

② DMZ 区网络流量可视化

基于流量分析系统平台进行开发，将业务网络路径中各个节点关联到多源数据，如流量、日志、SNMP、Syslog等，实现基于业务主线的多源数据管理分析，同时基于设备及应用的配置文件，精确梳理出业务路径，DMZ 区业务系统流量自动化呈现，提供网络到业务端的全路径可视化支持，系统拓扑示意图如图 3-4-13 所示。

4. 运营情况

华夏银行新灾备机房网络正式投产运行后为后续业务系统扩容及新增提供了良好的网络环境，网络具备容量快速扩展的能力，满足总行业务快速发展的网络保障需求，投产后机房网络运行稳定，后续还将通过网络监控体系的持续运营，推进网络架构的优化迭代。

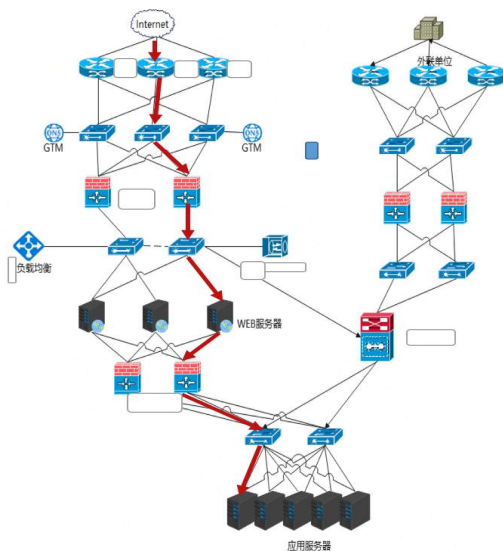


图 3-4-13 系统拓扑示意

机房生产环境应用案例展示见图 3-4-14。

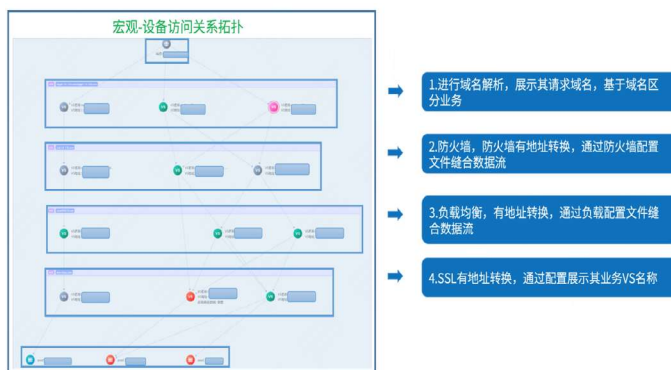


图 3-4-14 机房生产环境应用案例展示

5. 项目成效

此次华夏银行新同城灾备机房网络建设和搬迁项目达到了既定目标，取得了较好的成果。在机房网络建设方面，采用标准化、模块化架构设计，引入面向应用的设计理念，旨在实现面向应用的高效网络运维和交付能力，在网络核心区域引入 SDN、网络流量智能分析等行业新技术，同步部署新一代网络监控管理系统，实现数据中心网络可用性和运维效率的进一步提升。在机房应用系统搬迁过程中，构建跨数据中心网络大流量通信能力和网络流量监控调度能力，为业务系统多批次、保留原生产系统 IP 地址搬迁提供了可靠的网络支撑，最终圆满地完成了各项网络保障工作。

本次项目网络采用最小化新建方案，通过对各批次搬迁的网络设备进行精准动态调度，最大化利用现有网络设备资源，根据项目复盘统计，新机房网络设备利旧使用率达到 50%，同时，搬

迁过程中通过部署自研数据中心拨测系统用于对新机房网络各区域通信质量实时监控，替代原有商业化产品，在完成各项网络保障任务的同时，网络实施成本也得到了有效的控制。

本次项目，历时 8 个月时间，累计保障华夏银行及合作伙伴 10 个批次，3000+ 台 / 套设备的搬迁实施工作，期间还完成 240000 余根网络线缆的布线实施工作。

五、大童保险服务：快保云服平台

1. 项目背景及目标

随着集团战略推进，多子公司推进，业务快速发展，原有系统基础架构、建设方式和迭代周期已不能满足系统开发建设需要，精细化数字化运营管理服务已经迫在眉睫，应对业务场景快速迭代上线和业务活动快速反应高并发量的需求势在必行。

大童保险 2020 年 3 月启动整体规划设计与项目建设评估，确定了项目建设目标：构建业务服务组件化、业务一般性功能版本迭代 2 周上线、版本实现热发布、关键业务服务快速弹性扩容、全链路服务业务数据回流。

2. 创新点

打造基于保险生态业务应用的群组模块化划分，以微服务为核心技术架构，提供插拔式组装化服务组件，支持业务模式高度扩展 (2a、2c、2b、2a2c、MGA 等) 的保险新营销数智化解决方案。

3. 项目技术方案

项目技术方案如图 3-5-1 所示。



◆◆ 关键数据可视化

统一客户视图

1. 多维度定义客户视角，公司视角、业务伙伴视角；
2. 公司战略端-基于客户健全场景的客户服务，客户运营、客户分层、客户画像、客户权益等；
3. 业务伙伴端-为用户提供客户信息管理、家庭成员维护、客户导入、客户标签、服务跟进、数据回访等客户服务；
4. 为客户价值多次挖掘提供重要的数据决策。

统一产品视图

1. 归集所有产品类型，根据产品标签库对产品进行打标；
2. 为产品智能搜索、智能推荐提供基础数据源；
3. 为构建全品类产品库，细分产品频道，精准产品搜索建立基础。

统一保单视图

1. 非同类型保单统一管理(寿险、互联网、高端医疗、车险、团险、服务型产品等)；
2. 结合保单托管司内外保单统一收集，为客户家庭保障缺口测算、分析、智能产品推荐提供专业且精准化服务；
3. 为业务伙伴、客户、运营人员查询保单降低难度；
4. 为客户价值多次挖掘提供重要的数据决策。

统一用户视图

1. 通过用户特征、行为、交易、活动数据，为用户数据标签化提供基础；
2. 根据用户标签提供用户画像；
3. 实现用户个性化推荐和定制化服务。



◆◆ 多元连接最大化



◆◆ 场景交互智能化



客户服务智能化



内容推送智能化



搜索提醒智能化



知识推荐智能化



场景问题智能化



图 3-5-1 项目技术方案

4. 项目过程管理

2020 年 3 月启动整体规划设计，分阶段实施交付的模式；2022 年 7 月完成了全部规划功能的开发和原有系统历史数据迁移。

5. 运营情况

自 2020 年各服务系统分阶段交付上线以来，系统稳定运行率达到 99.9%。2022 年年度实现保单交易服务 230+ 万笔，计划书展业支持服务 2300 万次；2022 年度交付了 132+ 亿次业务页面访问调用服务；

2022 年度累计服务迭代发布次数生产及测试 8 万多次。

6. 项目成效

项目成效如图 3-5-2 所示。

(1) 全链路数据回流



图 3-5-2 项目成效

由传统业务部门发起需求再开发数据分析指标，转变为预定义标准化数据指标，由 IT 数据产品线主导标准数据指标同步埋点开发，构建统一的引用数据规范，实现数据快速融合业务场景上线。实现了标准定义将近 1000 个采集指标，上线累计采集处理将近 20 亿数据量。

(2) 缩短产品开发上线周期

保险新产品开发与保险公司对接上线周期由原来 4 周左右缩短至 1-2 周，最短可至 1-2 天。

(3) 统一消息降本增效

整合与规范站内信、邮箱、短信、微信生态、企业微信的消息触达代理人和客户，赋能业务场景灵活定义多通道触达消息方式，节省短信消息触达费用 15+ 万元 / 年；开发规范化，统一调用网关，提升了安全开发和开发集成效率。

六、阳光保险集团：云杉容器云平台

1. 项目背景及目标

容器技术因具有弹性伸缩、敏捷部署、资源利用率高、安全稳定等优势，近年来在互联网和大型金融企业越来越广泛应用，但商业的容器平台价格昂贵、个性化开发难度大，而且绝大部分的商业产品都是基于 Kubernetes 的容器管理平台，平台功能也大同小异，核心功能包括容器集群统一管理、用户权限管理、容器资源管理、资源监控、资源排行、容器网络管理等。

为了最大程度降低成本，增强核心技术自主可控能力，并且可以与公司现有系统无缝集成，按照公司云原生架构的整体规划，承载更加丰富的云原生技术，强化云原生架构底座，阳光保险自主研发了公司自己的容器云平台云杉，云杉能够实现多容器集群的统一管理，实现容器资源从申请、审批、自动部署，到运营监控等的一体化管理，功能相较商业产品更丰富，更加适合阳光科技管理模式。

云杉容器云平台的建设目标是实现全集团容器资源的一站式管理，大幅降低 IT 运营成本，提升应用系统的高可用性，并且提升公司底层核心技术的自主可控能力，符合国家信创战略。同时，能够满足公司个性化需求，平台可以与公司现有的各类企业级系统集成，并作为公司云原生架构的底座，未来可以扩展成为一个更加完整的技术生态。

此外，平台能够大幅提升容器运维人员和开发人员的效率，简化企业用云和上云的门槛，解决企业使用容器技术中的痛点及难点，提高企业在云计算领域的核心竞争力。

2. 创新点

云杉容器云平台具有完全自主可控、一站式管理、产品生态丰富、全栈信创化、自动化水平高、支持各类应用等多项创新点，目前已申请多项专利，可以为应用系统提供高效、安全、稳定的云端基础运行环境。

①技术完全自主可控。平台是公司内部技术骨干从 0 到 1 完全自主研发的，技术完全自主可控，不依赖于商业系统，具有完全自主知识产权，可以快速开发迭代，满足公司多样化的需求。

②一站式管理。平台实现了多容器集群、用户权限、基础资源的一站式管理，包括从申请、审批、自动部署、运营监控等环节的一体化管理，极大地提高了管理效率和运维效率。

③产品生态丰富。云杉容器云平台是全集团云原生架构的底座，平台集成了容器安全、镜像

管理等功能，而且还与公司现有的各类企业级系统无缝集成，包括 CMDB、统一认证、OA 等，实现了容器资源的一体化、规范化管理，增强了平台与其他系统的互通性和扩展性；未来，云杉平台还将与服务网格、服务架构、边云协同等集成，持续完善产品生态。

④全栈信创化。平台从服务器、操作系统到数据库等各个层面都实现了全栈信创化，解决了关键技术卡脖子问题，提高了平台的独立可控性和安全性。

⑤自动化水平高。平台简化了应用部署的流程，具有多功能，包括项目创建、资源分配等都是系统自动完成的，不但大幅提升了运维效率，减少了运维成本，而且降低了企业应用上云的门槛。

⑥支持各类应用系统。平台可以承载各类移动应用、核心业务系统、大数据平台、人工智能应用、云原生中间件等各类系统，为全集团所有科技项目提供了一个强大的技术底座，平台上线不到半年即管理了 109 个应用系统，快速完成了在全集团的推广工作。

3. 项目技术方案

云杉容器云平台整体功能架构如图 3-6-1 所示。

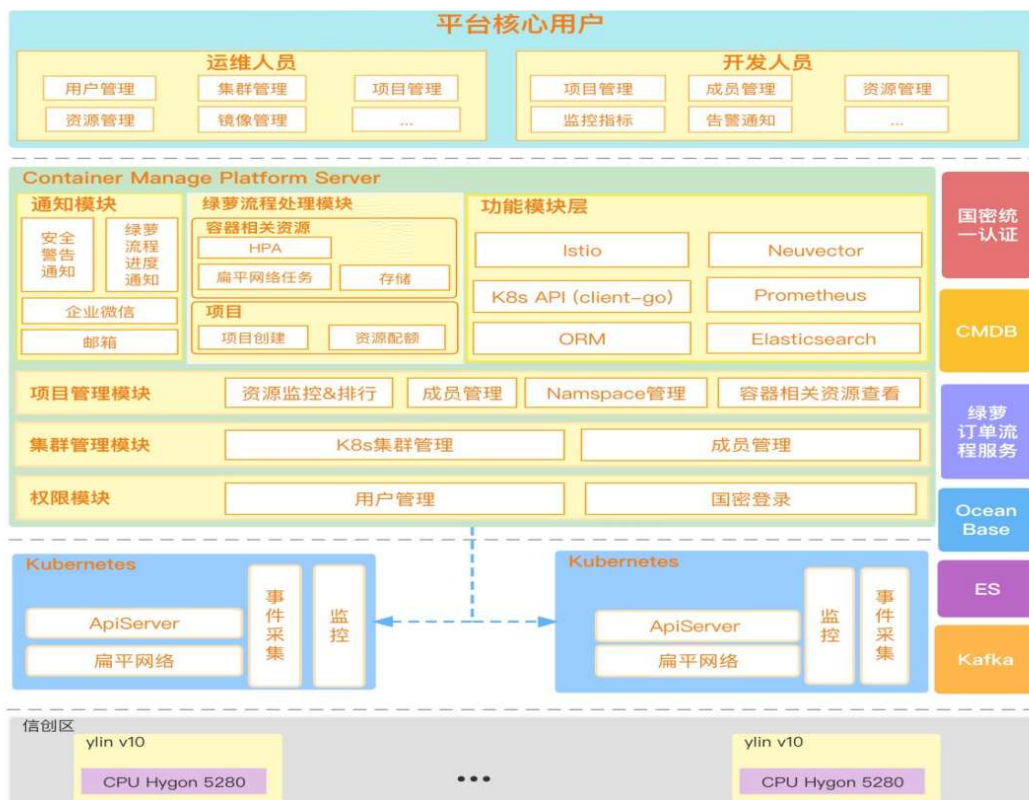


图 3-6-1 云杉容器云平台功能架构

云杉容器云平台主要面对运维人员和开发人员，内部具有权限管理、集群管理、项目管理、通知模块、流程模块和功能集成模块等五大功能模块，涉及如下技术架构。

(1) 前端。采用 Vue 等现代化的 Web 前端技术，实现平台前端组件的开发及页面交互效果，使得容器云平台的操作更加可视化、简单易操作；

(2) 后端。采用 Golang 微服务架构 (Kratos), 具有高性能、高可靠性、易扩展性和易调试性等优点，提高平台的稳定性和可靠性，为企业提供高效、安全、可扩展的容器云服务。

(3) 数据库。采用 OceanBase 数据库实现平台数据的存储和管理，同时支持分布式存储，提高容器云平台的数据处理能力。

(4) 容器。采用 Kubernetes 等容器编排技术，实现容器资源从申请、审批、部署，到运营监控等环节的一体化管理，提高容器资源利用率与运维效率。

(5) 安全。采用 OAuth2.0 和国密登录等安全认证技术，保障数据安全性和平台可控性，并且实现了对容器、镜像等资源的权限控制。

项目的业务模式采用如下两种：一是平台即服务 (PaaS)，为企业提供容器云平台的基础设施，企业通过订阅的模式获得服务，对云平台的资源进行申请、调用和管理；二是软硬件一体化，针对大型企业提供容器云平台的软硬件一体化服务，包括容器云平台、监控、存储等综合服务，可以根据业务团队的需求定制服务。

项目的商业模式为按需付费，研发团队可以按照实际使用量付费，实现灵活计费，降低企业的成本。

云杉容器云平台是集团一个全新的基础技术平台，有着完善的技术支持、优秀的业务模式和创新的商业模式，可以为公司提供高效、安全、可扩展的容器云服务，满足公司多样化的需求。

4. 运营情况

云杉平台上线后不到半年时间，完成了 8 个 Kubernetes 集群的纳管，承载了 109 个应用系统的稳定运行，其中包括车险承保、非车承保、车险理赔等保险核心业务系统，包括大数据平台等计算密集型的应用，也包括消息、监控等高并发的中间件平台，实现了全集团容器资源的统一管理。

云杉容器平台系统多副本部署，平台 24 小时全天候运行，平台使用 OceanBase 分布式数据库，平台数据实时存储和备份，确保平台数据的可靠性和安全性，系统代码经过安全扫描，不存在安全漏洞。

平台上线后尚未出现生产事故，并且保持着每半个月或每周一次小版本、每两个月一次大版本的快速升级迭代，能够快速满足全集团多样化的容器需求。

5. 项目成效

云杉容器云平台是一款轻量级、高可靠、易扩展的容器管理平台，与传统商业产品相比，具有成本低、安全性高、效率高等优势。通过引入云杉容器云平台，企业可以极大地降低服务器和软件成本，提升生产效率，进而实现更高的经济效益。按照目前规模，云杉平台较购买商业产品每年可以节省 120 万元以上的软件成本，同时应用所需的硬件成本较传统物理机或虚机可节省 20% 以上的资源。随着容器技术的快速推广，将节省更多成本，预计 3 年后，每年可节省 200 万元以上软件成本；5 年后，每年可节省 300 万元以上软件成本。

平台推广应用后，可以大幅缩短研发和上线时长，减轻运维人员工作负担，提升工作效率。平台具有自我恢复能力、故障隔离能力和双重验证等多重安全措施，可以大幅提高云平台的安全性，降低企业面临安全威胁和风险的可能性。

同时，云杉容器云平台可以实现服务器资源的最大化利用和功耗的最小化，让公司在提高效率的同时，实现节能减排目标，从而实现更高的节能环保效益。

七、爱心人寿：DevOps 实践

1. 项目背景及目标

项目之初，IT 开发运维管理工作没有形成完整的体系，各个项目都有自己独立的研发管理方案，管理方式不统一、管理水平参差不齐，IT 部门整体效率及质量难以保障。随着业务的飞速发展，需求数量大幅增加、需求发布频率越来越高，亟待提高交付质量及效率，以支撑快速发展的业务。

在此背景下，IT 部经过深入调研及分析，借鉴先进研发体系，结合当前系统建设情况，制定了一套具有爱心特色的 DevOps 体系。新体系旨在提升效能、降低成本，为公司战略、IT 部门规划提供保障。

2. 创新点

爱心人寿 DevOps 体系建立贯穿开发、测试、运维、运营四大场景的流水线，形成有效连接、紧密配合的应用研发闭环。具有以下四大创新特性。

(1) 高度的可扩展性

该体系是以业界先进主流的开源工具 Jenkins 为核心，各个功能环节均模块化采用先进的开源技术，如 GITAB、NEXUS、SVN、MAVEN、ANT、ARTIFACTORY 等，对于新技术的功能随时可以配置对接，如 DOCKER 等。对于各个项目可以灵活、自定义地选择 DevOps 工具和模块，完全满足各应用不同语言、不同架构的 DevOps 改造需求（详见图 3-7-1）。

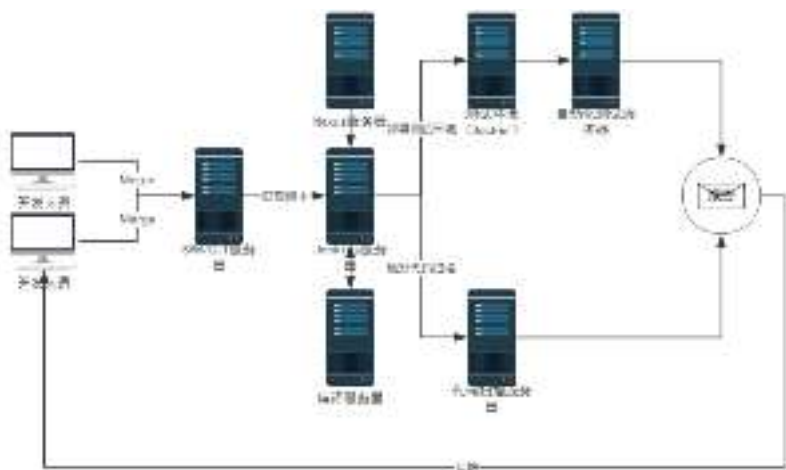


图 3-7-1 高可扩展性的 DevOps 体系

(2) 强大的兼容性

模块化设计带来的就是强大的灵活性，以满足各业务场景的不同需求。这种创新的 DevOps 模式拥有强大的兼容性，支持 SVN 和 GIT 等多种代码管理工具、支持传统虚拟机部署和容器部署、支持传统架构和微服务架构、支持 JAVA、C、OBJ-C、H5、VUE、PYTHON 等主流开发语言、ant、maven、gcc、xcode、gradle 等多种编译方式，支持增量构建、增量发布和全量构建、全量发布。

(3) 较强的自主掌控性

本次 DevOps 体系的建设工作均由自有员工完成，具备较高的自主掌控性。同时模块化的设计带来了权限模块化区分，不同的用户在不同的模块定制不同的权限，充分保证应用和数据的安全。

(4) 较低的建设维护扩容成本

基于先进的开源技术，自主掌控，自主建设，极大地降低了开发和维护成本。同时也避免了成熟商业软件定制化、功能扩展带来的高额费用。

3. 项目技术方案

在 DevOps 体系的规划下，打通开发、测试与运维，研发与运营，打造需求管理、工作协同、代码管理、发布管理、质量管理、度量服务等功能，适应多元云环境，为快速的用户响应、高效稳定的产品提供基础（详见图 3-7-2）。

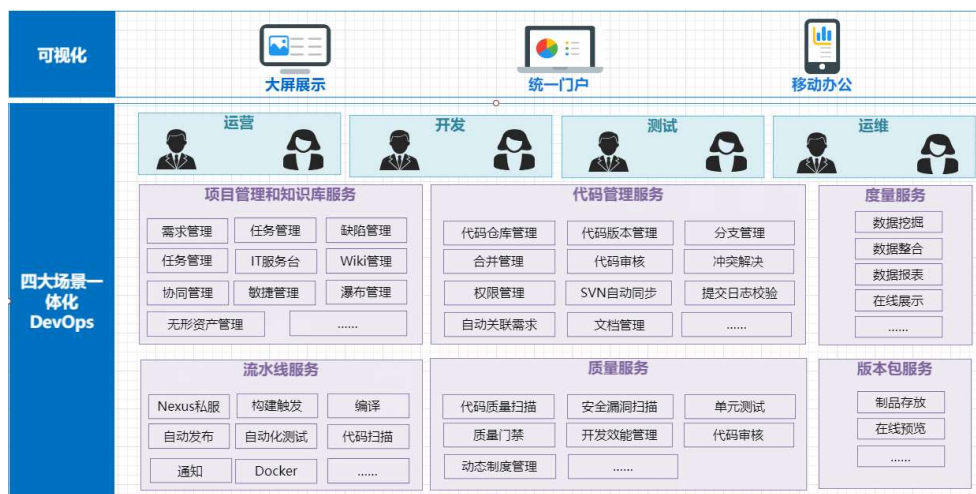


图 3-7-2 项目技术方案

(1) 项目管理和知识库服务

在 DevOps 的实践过程中，采用了主流的需求管理工具 JIRA 和知识库工具 Confluence，面向全公司提高 IT 服务支持、知识库支持、项目管理支持。通过 JIRA 标准化的项目管理方式，有效地推广 DevOps 文化，使每个人以正确的方式参与到 DevOps 的研发运维工作中，信任、分享、协作、共同进步。同时全面对接 SVN 和 GIT，每一次变更都有据可查可依，JIRA 界面也可清晰的展示需求对应的每一次变更清单和发布记录、相关人员工作量，为度量数据服务提供数据支撑。

(2) 代码管理服务

代码管理服务兼容主流的 SVN 和 Gitlab 两种代码仓库服务，通过可视化的界面结合经验丰富的技术人员对外提供统一的代码管理、版本管理、分支管理、合并管理、冲突解决等功能和技术支持，以满足项目实际情况要求。以分支管理为例，代码分支的创建主要是根据版本、环境、功能特性等创建。爱心人寿结合保险行业和公司业务情况，创新的提出了以环境分支为固定分支，需求分支为临时分支的分支管理策略。通常情况下存在 DEV 开发分支、SIT 测试分支、UAT 测试分支、PROD 生产分支 4 个固定分支，以及各个需求对应的临时分支，随着需求的完成，相应需求分支将同步删除。

基于存量项目使用 SVN 的现状，积极引导满足条件的项目从 SVN 迁移至 GITLAB，充分利用 GIT 的先进性。为不具备 SVN 迁移 GIT 条件的项目，提供 SVN 提交实时同步至 GITLAB 服务，为 SVN 用户带来更加方便的代码审核界面。

(3) 流水线服务

通过 Jenkins、Nexus、Docker、代码扫描、自动化测试等服务，结合代码管理服务，提供模块组合的标准化流水线。流水线包括代码服务选择、构建触发、质量门禁、编译环境、自动化测试 5 个部分（详见图 3-7-3）。



图 3-7-3 流水线服务

流水线均由配置管理员统一配置管理，项目组可根据项目实际场景选择合适的模块形成标准化的流水线。流水线标准化是规范标准的延伸，也是建设 DevOps 的关键。标准化流水线安装发布类型结合部署服务器对象分为 Docker 测试流水线、传统服务器流水线、Docker 生产流水线和传统服务器生产流水线，共计 4 大类流水线。

(4) 质量服务

质量服务使用先进商业软件 Merico 提供代码扫描、代码审核、单元测试、质量门禁等功能。采用制度建设与硬件建设相结合的方式，制度先行，硬件配合。制度上形成了有效的代码扫描、单元测试制度，质量人员审核相应的报告。硬件上，建设代码扫描平台和质量门禁，结合流水线自动化的审核代码并实施阻断。质量门禁随着项目管理水平和项目团队能力的不断提高，门禁的要求也会随之严格，促使管理水平和团队能力进一步提升，达到相互促进，螺旋上升的效果。

（5）版本制品库服务

版本制品库服务采用开源软件 Artifactory 提供版本包管理、版本信息、在线预览、下载功能以及权限管理。根据发布环境的不同提供测试版本服务和生产版本服务。测试版本服务分为两种方式：一是流水线发布测试环境，同步测试版本包和版本信息至制品库；二是编译流水线把测试版本包和版本信息推送至制品库，发布流水线从制品库获取版本应用包进行发布。

（6）度量展示服务

度量展示服务有效地将代码扫描结果、JIRA 数据及其他服务数据整合，进行数据分析和关联，形成页面化的报表展示。使度量可视化，从而有效跟踪 DevOps 的实施效果。

可视化的度量服务获取项目研发全生命周期数据，结合 PMO 管理目标导向，展示各指标数据视图，实时反应团队情况，促使团队持续改进。

4. 运营情况

DevOps 基本体系已经全面在公司试运行成功。目前已有 20 多个项目，100+ 应用的研发过程纳入 DevOps 体系，已建立的流水线超过 800 个，可在 1-2 人的控制下完成日均 200 次的流水线发布，有效的提升了版本发布效率。

5. 项目成效

爱心人寿 DevOps 实践整合了 IT 资源，同时为需求、开发、测试、运维、配置、运营等环节带来了更高水平的协作，形成有效连接、紧密配合的应用研发闭环，有效助力公司实现第二曲线的跃升。

（1）增强研发效率

单次应用发布效率由 30 分钟缩短至 3 分钟。截至 2023 年 3 月底，流水线执行总次数超过 80455 次。整体研发交付效率提升 30% 以上。

（2）提高资源利用率

各项目资源整合，有效的将分散的资源集中起来统一管理，释放出大量重复资源。容器的自动伸缩特性可以充分的利用服务器资源。DevOps 的推动整体提升了 20% 左右的资源利用率。

（3）DevOps 理念深入人心

DevOps 是一种文化，也是一个实践。它是提倡协作、沟通及相互学习的文化，也是为了使软件开发与 IT 团队之间的流程自动化的一组实践。爱心人寿通过组织学习，积极宣导和相互分享等方式，从自有员工至外包人力使 DevOps 理念深入人心，形成了具有爱心人寿特色的 DevOps 文化实践。

6. 经验总结

爱心人寿 DevOps 平台是对新技术、新理念积极探索与实践的产物。在技术上，落地了众多先进工具，并推动研发过程自动化、研发度量数字化、研发全生命周期可视化。在管理上，打破研发职能边界，促使研发团队之间协作分享，最终有效的提高了研发效率和质量。本项目所采用的低成本自主可控的建设模式，为中小保险公司带来一定的借鉴。

八、华泰人寿：安全运营中心

1. 项目背景及目标

在当今数字化的时代，互联网技术的发展使得信息的传递和交流更加便捷，然而这也为网络安全带来了挑战，网络攻击手段也日益复杂和隐蔽，网络安全威胁不断增加。其中，参数注入攻击成为网络攻击中的一种常见类型，攻击者通过在 HTTP/HTTPS 请求的参数中插入恶意代码，达到非法获取数据或者控制服务器的目的。传统的防护手段往往只能检测已知的攻击行为，难以对未知的攻击行为进行有效的防范，针对此类痛点，华泰人寿安全运营中心展开科研攻关，进行技术创新。

华泰人寿安全运营中心采用机器学习算法对 HTTP/HTTPS 请求中的参数进行异常检测，实现对请求中的参数自动建模，建立正常的参数引擎，以及对异常参数的解释性，方便使用人理解并处置问题。

2. 创新点

华泰人寿安全运营中心通过机器学习（人工智能）算法，自动识别 HTTP/HTTPS 请求中正常及异常参数，对正常参数建立安全基线，避免了人工重复性工作，对异常参数进行评估其攻击行为的可能性，在异常标签未知的情况下无需堆砌人力统计上线项目和页面的参数限制，算法会生成参数系统的规则引擎。

3. 项目技术方案

图 3-8-1 为项目技术方案，安全运营中心使用机器学习算法对 HTTP/HTTPS 请求中的参数进行异常分类。采用了基于嵌入式特征选择方法的模型，该模型可将请求参数分为正常和异常两类，并对正常参数建立安全基线。

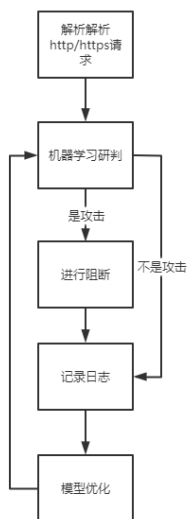


图 3-8-1 项目技术方案

图 3-8-1 为项目技术方案，安全运营中心使用机器学习算法对 HTTP/HTTPS 请求中的参数进行异常分类。采用了基于嵌入式特征选择方法的模型，该模型可将请求参数分为正常和异常两类，并对正常参数建立安全基线。

4. 运营情况

(1) 推广应用

一是安全运营中心宣传推广。通过内部培训、会议演讲、宣传资料等方式向组织内部员工推广安全运营中心的重要性和价值。

二是战略合作与共享。积极与其他团队、合作伙伴以及安全社区合作，共享安全运营中心的经验和资源，推动整体安全水平的提升。

(2) 系统运行情况

①监控系统运行状态。定期检查和监测安全运营中心的关键系统和工具，确保其稳定运行和高效性能。

②故障和事件处理。及时响应和解决系统故障、错误和安全事件，保障安全运营中心的正常运行和服务质量。

③性能和容量管理。定期评估和优化系统的性能和容量，确保安全运营中心能够满足日益增长的安全监测和响应需求。

(3) 安全报告和分析

①定期安全报告生成。安全运营中心定期生成安全报告，汇总和分析安全事件、威胁情报和安全运营中心绩效指标，为管理层提供决策依据。

②威胁情报分析和评估。安全运营中心分析收集到的威胁情报，评估其对组织的威胁程度，并提供相应的建议和应对措施。

(4) 风险管理和漏洞修复

①风险评估和管理。安全运营中心定期进行风险评估，识别和评估组织面临的安全风险，并提供建议和措施进行风险管理。

②漏洞扫描和修复。安全运营中心进行定期的漏洞扫描，发现系统和应用程序中的漏洞，并与相关团队合作进行及时的修复和漏洞管理。

(5) 项目成效

①预防损失。安全运营中心通过监测和响应安全事件，帮助组织及时发现和处理潜在的安全威胁，减少安全事件对组织造成的财务损失。包括避免数据泄露、系统瘫痪、网络攻击导致的停机时间和业务中断，从而保护组织的资产和业务连续性。

②提高生产效率。安全运营中心的监控和分析能力可以减少误报和虚警，帮助组织准确识别和优先处理真正的安全事件，以减少安全事件调查和响应的时间和成本，提高团队的工作效率。

③提升品牌声誉。通过建立一个高效的安全运营中心，组织能够有效地保护客户和用户的数据隐私和安全，提升品牌声誉和信任度。有助于吸引更多的客户和用户，并增加销售和市场份额。

九、瑞泰人寿：智慧审计信息云系统

1. 项目背景及面临挑战

随着新时代的迈进，国家步入前所未有的发展阶段，党和国家及各级政府组织及监管部门越来越重视内部审计工作，对保险公司的管理日趋严格。根据《保险机构内部审计工作规范》（保监发〔2015〕113号）第八条要求，保险公司审计的工作范围逐渐增大，内容逐渐复杂，同时随着信息技术在企业业务和管理中的广泛运用，信息科技成为企业竞争的重要支撑，但与此同时，信息系统在安全性、效率性、合规性、成本性方面都存在风险，传统的控制、管理、检查和审计技术都受到了巨大的挑战。信息化的经营管理环境使得内部审计面临的审计环境也更加复杂，手工审计作业未能在内审报告送达后一定期限内对问题进行后续跟踪，导致审计意见和建议不能引起被审计部门足够重视，造成整改不彻底，甚至完全不整改的现象发生，严重浪费了审计资源，也不利于企业管理和提高经济效益，为了解决如上痛点，满足行业监管政策要求，瑞泰人寿领悟时代使命，强化审计担当，自主研发并于2020年2季度成功建设智慧审计信息云系统，构建内部审计管理及作业一体化的在线智慧审计云平台，打造信息系统“安全卫士”。

2. 项目方案

智慧审计信息云系统是基于自主研发，引入移动互联网发展的创新理念，落实信息化建设科技赋能目标，基于大数据采集、分析、SaaS服务云架构构建的内部审计信息系统。相比传统架构，智慧审计信息云系统架构具有以下明显优势：一是面向服务，通过松耦合方式，提升应用程序的整体敏捷性和可维护性及一致性，业务响应更速度，系统开发成本更低，系统延展性、拓展性更强；二是容器化封装，以容器为基础，提高整体开发水平，形成代码和组件的重用；三是自动化管理，通过DevOps+Jenkins持续交付+Docker容器+云计算SaaS服务+云存储技术手段实现自动化管理。

3. 创新点

（1）技术创新

基于DevOps，通过JIRE、Maven、Jenkins实现持续集成，持续部署，结合自动化测试工具Selenium，由Jenkins定时周期性触发/手工触发自动化测试案例的执行，实现无人值守的自动化测试及发布。以互联网为平台，引入SaaS云，实现多租户，通过网络部署便捷按需使用。

（2）业务创新

一是系统兼容性强，支持单点登录，实现域账号统一管理，待办待阅整合。

二是业务系统拓展性强，通过统一接入平台对接数据平台，支持各种业务系统数据接入，实现全覆盖审计系统集成等数据互联互通服务，解决众多信息系统数据的审计。

三是审计分析模型化，支持指标数据采集，包含各类业务数据采集，以信息系统项目风险为导向，实现审计数字化，审计分析智能化。

四是成果管理数字化，指标数据采集后，自动进行疑点智慧分析，并可对分析结果进行查询，数字化展示结果，对风险项进行高亮提示，可进行预警分析，规避风险。

五是审计系统自我审计，记录审计系统所有操作，实现审计系统操作视频记录，支持回访调阅，实现操作轨迹全留痕，从而达到审计系统自我审计。

六是标签化，系统标签化管理，支持自定义标签、通过标签查询数据，增强系统扩展性。

4. 技术实现特点

(1) 云存储

以项目管理为中心，支持各种格式文件上传、下载。采用对象存储的方式，可扩展性强，灵活性强，减少灾备恢复成本，不需要额外数据中心，可实现快速云复制。

(2) 痕迹化管理

以审计信息化手段，实现审计计划至审计结论的全过程跟踪管理，可进行证据链的完整追踪，实现对审计程序的刚性约束和痕迹化管理，有效规避审计自身风险，保证审计质量。

(3) 云计算 SaaS 服务应用

以互联网为平台，系统上云，SaaS 化，实现多租户，可以通过网络便捷按需使用资源（包括计算资源、存储资源、应用资源、服务和网络等），且可扩展，灵活易于管理，具备大规模、虚拟化、高可配及弹性配置，提高资源配置效率，降低信息化建设成本和生产运营成本，提升企业管理水平。

(4) 便捷性管理

支持域账号统一管理，用户同一个域账号密码实现统一管理，无需各个系统维护单独密码，系统待办待阅任务统一整合，使用户直观掌握任务情况，工作任务实时提醒，逾期自动提醒，便捷开展作业。

(5) 统一接入接出

通过统一接口平台，支持各种业务系统数据接入，实现全覆盖审计系统集成等数据互联互通服务，解决众多信息系统数据的审计问题。

(6) 智慧化

支持指标数据采集，包含财务数据采集、业务数据采集、精算数据采集、投资指标采集，以信息系统项目风险为导向，实现审计数字化，审计分析智能化，结果展示数字化。做到事前、事中、事后识别风险、分析风险、规避风险，提升风险防范能力，有效降低审计风险。

(7) 标准化

按照不同的审计作业类型，分别定义项目管理、审计实施、审计报告、审计底稿，下发资料需求，整改追踪各个阶段中需要开展的关键任务，形成审计工作流程方案。按照不同的审计类型，定义审计实施的范围，具体体现在审计目标、审计事项、审计程序、审计方法，构成审计实施方案。使审计工作有规可循，规范高效，确保审计工作质量，有效降低审计风险。

5. 运营情况

(1) 构建和谐内审环境

在线智慧审计信息云系统的使用推广，使得企业各部门能够理解并积极配合审计人员进行审计工作，能够在系统中清晰明了查看审计问题并进行整改反馈，并让其转变思想，意识到审计工作并非要查其不足，而是为了找出工作上的漏洞并及时补救，构建了和谐的内部审计环境，提升了审计工作质量，降低了审计风险，为企业经济效益提升减少了阻碍。

（2）监测风险，预警分析

一是通过大数据采集、数据检测等手段对数据关键风险点进行全面监控预警，有效贯彻风险导向审计，降低风险；二是通过对审计问题设定、提醒、反馈，有效跟踪审计整改；三是通过流程化的复核、审批及方案约束，有效控制审计工作质量；四是利用查询、分析、报表、指标等工具，快速提升审计工作效率；五是直观反映审计工作效率效果，获取决策信息，辅助领导科学决策。

6. 项目成效

（1）节约成本，提高效率

通过在线智慧审计信息云系统，转变传统的手工审计方式，突破人力、财力、物力、时间等资源“瓶颈”，破解审计组织模式和管理机制等要素的制约，实现审计资源集约化、审计业务信息化、审计管理数字化、审计方式现代化，最大限度的发挥内部审计的价值，对现有资源进行综合评估，并根据企业的实际情况提出整改方案；整合企业资源，节约企业成本，提高企业经济效益。

（2）加强管理，增加价值

在线智慧审计信息云系统作为一个监督评价系统，渗透企业管理的各个环节，可以在线对企业各环节进行有效的监督评价，并通过系统邮件主动通知被审计部门，规范了审计流程，增加了部门粘性，从而加强企业管理，增加品牌价值。

（3）规避风险，减少损失

通过非现场数据监测，设置业务指标、财务指标、精算指标、投资指标，通过大数据采集、分析、监测，对风险提前预警，做好风险规避，减少损失。

（4）加强内部审计后续监督

项目全流程管控，从项目计划、审计作业执行、审计结论、审计整改跟踪，到绩效统计分析，自动生成报告并发送至被审计部门，在一定期限内进行有效的整改跟踪，便于及时跟踪处理整改问题，强化审计监督。

十、北京农商银行：高端 NAS 存储双活建设项目

1. 项目背景和建设必要性

目前北京农商银行非结构化数据主要存储在 IBM GPFS 并行文件系统上，如一体化客服、应用服务网关等业务系统生成的文件。这些非结构化数据的文件数量和容量随着业务规模的发展呈逐年激增的趋势，而这些数据主要存储在传统集中式的块存储上。

这种使用存储的方式灵活性不高同时带来了过高的成本开销。另外，由于和数据库类的应用争抢存储资源，也给联机交易类系统带来了一定的性能冲击。为此，我行 2018 年引入了中低端 NAS 存储设备，用于存储文件类的数据，为数据的分类存储提供了便利，使得存储的使用方式更趋于合理化。然而，按照存储资源池的分级架构建设规划，需要额外建设具备双活能力的高端 NAS 存储系统，满足 GPFS 场景中重要业务系统的文件共享需求和同城双活的高可用需求。而现有的中低端 NAS 存储，可以继续承载 GPFS 场景中的一般重要业务系统的文件存储需求。

除了非结构化数据存储架构优化之外，另一个需要逐步优化的场景是系统间的文件交互。目前，

使用专门的文件传输工具进行各系统间的文件传递，软件架构较为复杂，同时运维难度也略大。此外，由于各业务系统分布在不同的网络区域，跨区的文件传输流量也会给各区域的边界防火墙带来性能压力。为此，我们可以借助 NAS 存储构建文件交互平台，不但省去了文件在各系统间的频繁传递，提高业务系统效率，同时，依托 NAS 存储的多网络区域覆盖能力，可以避免产生跨区流量，进而规避对边界防火墙的性能冲击。

2. 项目建设方案和实施进度计划

由于首次引入高端 NAS 双活系统，因此在运维人员技术储备和项目实施技术细节的全面掌控上以及开发人员对 NAS 存储平台的使用经验上比较欠缺，所以项目立项之初需要进行详细的项目架构规划。

首先运维中心作为项目的建设部门积极和开发中心进行沟通，收集业务系统使用场景和需求；其次和业界主流 NAS 存储厂商以及银行同业进行技术交流，探讨 NAS 双活平台的使用场景以及技术实现方案；最后选取了在 NAS 存储双活细分领域领先的两家厂商进行了长达 5 个月的产品 POC 测试。在测试的过程中，运维人员全程深度参与，测试用例涵盖 6 大使用场景以及 20 个高可用场景。通过详细的测试，不但验证了 NAS 双活产品可以满足业务需求，也验证了在各种故障场景下，高端 NAS 双活系统的架构健壮性。同时运维人员也积累了丰富的产品使用经验。

运维中心作为该项目的牵头部门，基于前期的产品和技术调研，结合 POC 测试过程中总结的经验，编制了 NAS 存储使用规范。为了解决开发中心对新的 NAS 平台使用经验不足的问题，我们将规范进行了宣贯和多次沟通，这也很大程度上保证了该项目的建设质量以及应用系统开发的质量。在完成产品 POC 之后，项目通过科技三部门的技术方案汇报会，然后通过集采流程完成了招标采购，最终完成了 NAS 存储双活系统的集成上线。

整个项目的实施进度计划如下：技术调研和需求收集，2020.6 - 2020.7；产品 POC 测试，2020.8 - 2020.12；商务采购流程，2021.1 - 2021.3；系统集成调试和上线，2021.4 - 2021.5。

3. 项目创新点

本项目的创新可以分为管理创新和技术创新两个方面。在管理创新方面，首先，通过高端双活 NAS 存储系统的引入，完善了 NAS 文件存储的分级资源池建设，满足了业务系统分级建设的需求。中低端 NAS 存储资源池采用生产中心本地部署模式，满足一般重要和较重要业务系统的文件共享需求。高端双活 NAS 存储资源池满足核心系统、重要和重要支撑系统的文件共享需求以及文件跨中心的高可用需求。其次，通过项目建设，进一步优化了非结构化数据存储系统架构，不同类型业务数据的存储布局更加合理，实现了降本增效。最后，项目建设本身也完成了一次管理创新，通过立项前的深度 POC 测试，提升了运维人员的技能，运维中心和开发中心的紧密联动也很好地保证了项目建设质量和信息系统建设和运维的规范性。

在技术创新方面，一是同城双中心高端 NAS 双活是银行业相对较少的实施案例，提升了重要业务系统文件类数据的地域级抗风险能力。二是对于高端存储，从物理层面隔离 SAN 结构化数据和 NAS 文件类非结构化数据，在提升了存储系统可管理性的同时也规避了两种不同特性的 IO 对存储资源的争抢和性能干扰。三是在高端 NAS 双活系统实施方面，采用四网隔离的方案，实现了

业务网、数据复制网、仲裁网和管理网络的分离，提升了网络安全性和性能。此外，双活系统采用了物理主备双仲裁双隔离 VLAN 的方案，极大提升了双活系统的健壮性。四是借助双活系统提供的租户特性，实现了不同于其他整体存储切换方案的基于单业务系统的细粒度站点级灾备切换方案。五是借助 NAS 系统构建了文件交互平台，在提高业务系统效率的同时，也避免了先前方案中文件传输软件带来的跨区流量，进而规避了对边界网络防火墙的性能冲击。

4. 技术方案

按照前期规划，两台高端双活 NAS 设备分别部署在亦庄机房和空港机房，构建同城 NAS 双活系统，为新核心、重要以及重要支撑系统提供文件交互、文件共享服务和文件高可用容灾服务。

图 3-10-1 是高端 NAS 双活系统网络拓扑图，共涉及 4 个网络平面，分别是业务网络平面、复制网络平面、仲裁网络平面以及管理网络平面。每张网络的拓扑和功能介绍如下。

(1) 业务网络平面

高端 NAS 双活系统同时接入新核心区和业务三区，其中 A、B 控接入业务三区；C、D 控接入新核心区，形成两个故障漂移组（fail group）。每个控制器通过 2 条 10GbE 光纤接入业务交换机，形成一个 20GB 的端口组（LACP）。接入同一网络区域的控制器之间采用 A-A（双 Active）互备的工作模式，当任一控制器出现硬件故障或业务网络中断时，存储系统会自动将业务地址切换到另一个活动的控制器上，切换时间控制在 5 秒以内，对前端业务系统可以做到无感知。

(2) 复制网络平面

每台存储通过 4 个 40GB 的全互联连接接入 2 台 40GB 的内部复制交换机，两中心的 4 台复制交换机通过 2 条平行连接的 10GB DWDM 线路连接，构建了 NAS 同城双活数据复制链路。通过存储系统内部的配置，共形成 8 条负载均衡的冗余 ISL（Inter Switch Link）数据复制链路。

(3) 仲裁网络平面

每台存储设备通过 2 块仲裁网卡和 2 台仲裁物理服务器（HA 主备架构）构建成 2 个独立 vlan 的高可用仲裁网络。对于仲裁模块，从仲裁网络链路到仲裁软件，再到底层的仲裁服务器均实现了双冗余，规避了仲裁系统的单点故障，从而极大提升了仲裁的高可用性。

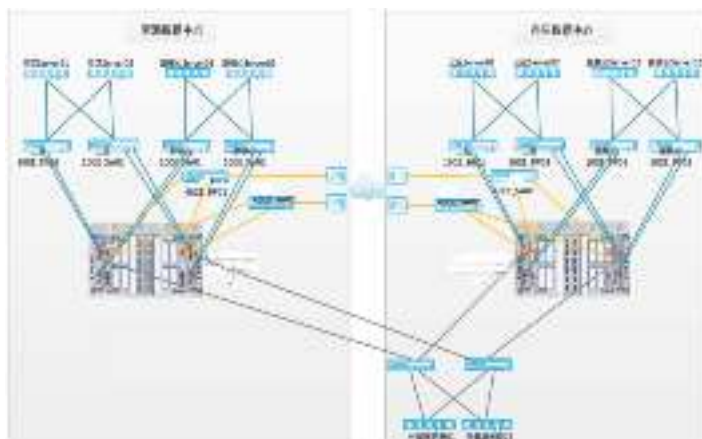


图 3-10-1 高端 NAS 双活系统网络拓扑

（4）管理网络平面

每台存储通过 2 个管理网口接入网管网，用于存储设备的日常管理和存储监控管理。

如上所述，高端 NAS 双活系统的网络按照功能划分为四个物理隔离的平行网络平面，每个网络平面只承载各自功能模块的流量。这样的网络架构设计，既保证了各个网络的安全性，也提升了每个网络平面的吞吐性能。

在软件层面，为了提升安全性和易管理性，高端 NAS 系统采用基于租户的方式实现业务系统逻辑隔离。租户是文件系统、网络逻辑端口的存储资源集合。针对实际业务场景，设计了两类租户，一类是业务系统交互，另一类是业务系统独自使用。对于业务系统间交互的租户，会按照业务系统网络区域配置不同的逻辑端口，业务系统会使用同区域的网络端口接入 NAS 存储，从而提升存储访问效率，同时还能规避边界网络防火墙的跨区流量。

除了安全性、易管理性和性能因素外，租户也是高端 NAS 双活系统细粒度站点级容灾的底层支撑要素。每个租户在双活架构下会配置双活租户 pair 对，由于双活租户 pair 是双活系统的最小单元，因此，可以实现基于单个业务系统的站点级灾备切换方案。

5. 项目运营情况

高端 NAS 双活系统自投产以来运行平稳高效。其中，业务系统间文件交互场景随着新核心银行系统工程项目一并上线。截止目前，该平台已经承载了和新核心银行系统交互的 54 个业务系统场景。

对于 GPFS 迁移 NAS 的非结构化数据存储架构优化事项，已经完成了两个批次系统的迁移，目前正在推进后续批次的迁移实施。

在高端 NAS 存储双活建设项目立项之初，便已经考虑了系统的可扩展性和架构弹性。为了满足新核心以及其他重要业务系统的文件异地灾备建设需求，目前正在推进异地 NAS 存储建设项目。对于文件异地容灾将采用基于 NAS 存储的复制技术，通过直接在现有高端 NAS 双活系统上增加第三台 NAS 存储，实现在线构建两地三中心架构。整个项目实施过程可以做到对现有业务系统无感知和性能无损。

6. 项目成效和经验总结

通过本项目的实施，无论是对存储系统架构体系建设，还是业务系统的设计都取得了显著的优化和成效。

一是实现了 NAS 文件存储资源池的分级建设，填补了高端 NAS 存储资源池的空白。二是降低了块存储使用成本，提高存储的使用灵活度，实现不同类型业务数据的合理存储。三是借助高端 NAS 存储设备构建同城双活架构，实现重要业务系统对于文件存储的高可用需求。同时，也为接下来的 NAS 存储两地三中心建设做了很好的铺垫。四是开创性地利用 NAS 存储构建业务系统间文件交互平台，显著提升了业务处理效率。

十一、人保科技：中国人保集团北方信息中心建设项目

1. 项目背景及目标

2020 年人保集团确立了“卓越保险战略”，并把信息化定位为中国人保的核心竞争力和基本生产力，将“建立数字化支撑的发展基础”确立为“1+7”战略框架中七大举措之一。为了落实“卓越保险战略”，科技板块持续完善数字基础架构，打造“两地三中心”的金融数据中心体系。

中国人保集团北方信息中心建设项目是打造“两地三中心”金融数据中心体系中重要的一个节点。其作为主生产中心，将承载人保集团当前生产应用，为公司业务长期运营保驾护航。

2. 创新点

（1）高标准高等级的物理环境

基础设施参照 Uptime Tier IV 和国家 A 级标准建设，暖通系统按照 2N 容错设计，配备完全独立的 AB 双路冷源供冷并相互备份，当市政水中断时，亦可保障系统持续制冷。同时每套系统均设置了满负载 15 分钟蓄冷罐的第三重冷源保障，形成双冷站、双冷源、三备份的可靠支撑。高等级 T4 标准的全链路 2N 系统保障，两路 10KV 供电 +18 台备用柴发 + 满负载 15 分钟不间断 UPS 系统，为北中心奠定了高可靠的供电基础。接入近 8 万个物理点位、70 多万逻辑点位的智能化系统，每秒数十万条的数据采集，为北中心自动化、智能化运维奠定了良好的数据支撑。机房运营管理平台构建了数字孪生的数字化北中心，DCIM、BA、安防、电力能源、电力投切、柴发并机等系统实现对数据中心运行关键设施 -- 供配电、暖通、机房环境、门禁、柴发等设备的监控管理，当市电中断、冷机故障、温度过高等情况发生时，能够自动切换、智能调节。消防系统采用 IG100 气体灭火系统，与消防报警系统自动联动，中控室 7 x 24 小时监控，保证数据中心安全运行；双路由进园的光缆能够有效避免单点故障，保障北中心网络出口的安全稳定运行。

（2）异地多活的顶层架构设计

基于中国人保位于廊坊、佛山、北京等地的数据中心，建设了多云多芯云平台，结合稳、敏态基础算力资源建设，设计并构建了同城双活、异地多活的架构体系，完成基础资源云服务模型和多云多芯资源供给设计，实现全栈信创云资源供给能力。未来，两地三中心将进一步升级为“多地多中心多活”。

（3）面向多云多芯、自主可控的 IaaS、PaaS 平台

多云多芯云平台建立了面向全集团的自主可控的分布式微服务技术体系 PDF-C，自主研发了支持敏稳双态、多云多芯、多地多活，并具备智能扩缩、水平扩展和流式计算等能力的 PaaS 云平台，实现了多中心任务调度互斥、数据库双向复制、应用服务单元化管理、智能引流以及全链路引流等面向多云多活运维侧的管理功能，在多云、多芯以及传统基础设施环境下能快速部署和高效运维应用系统。

3. 项目技术方案

北方信息中心项目整体建设用地面积约为 385 亩，分南北两区分期实施。其中，北中心南区一期建设内容为 ECC 和运维楼、数据机房一以及 110KV 变电站，共计 18 个模块机房，3240 个机柜。

南区一期项目于 2020 年 12 月 27 日开工建设，729 天后，首批 3 个模块机房交付试运行。2023 年 3 月 28 日第一电力路由完成市电送电入机柜，北中心一期具备全量上线条件，并于 5 月 16 日顺利通过竣工验收。目前，已部署超过 7 百多台设备，已上线集团统一技术平台、健康险商保核心系统等多家子公司的 13 个系统。

北方信息中心的投产使用，标志着中国人保异地灾备及同城双活的两地三中心架构形成，为未来建成东南西北四个数据中心集群为核心的多地多中心多活 / 灾备架构打下坚实的基础。

4. 运营情况

根据集团信息化建设规划自主可控要求，按照统一规划和部署，通过逻辑迁移和物理迁移等方式，稳步推进运行的业务系统迁移至北方信息中心，持续保障核心生产业务连续性。

稳步推进自主可控、绿色低碳的数据中心算力建设。遵循多措并举、分类推进、试点先行、确保稳定等信创建设方针，推动 IaaS 层建设，持续提升机柜算力资源供给能力，并积极贯彻高效、绿色理念，运用自动化运维、绿色能效管理、智能容量管理、高效制冷等技术，不断降低数据中心 PUE。

提供敏稳双态、弹性可扩展的基础资源服务，赋能集团为社会提供全面风险管理服务。按照“保险 + 服务 + 科技”的保险新逻辑，推动建成集团全面风险管理平台的技术底座，聚焦保险业务从风险等量管理向风险减量管理转变、从事后损失补偿向事前防范处置转变。并聚焦无人驾驶、绿色能源、万物互联、元宇宙等行业新兴风险的识别、计量、分析，从技术平台、数据分析、产品研发等方面提供有力支撑。

5. 项目成效

中国人保集团北方信息中心建设项目获得了国家 A 级机房认证、CQC 数据中心场地基础设施认证和 Uptime Tier IV 设计认证，其中，数据机房楼获得绿色建筑一星标准认证，ECC 和运维楼获得绿色建筑三星及 LEED 银级认证。同时，借助 3D 可视化统一运维管理平台和巡检机器人等数字化工具，具备了自动化、智能化的运营能力。

十二、阳光保险：小审阳 1 号——智能关系网络分析平台

1. 项目方案

(1) 业务方面

车险理赔欺诈一直是保险行业难以攻克的顽疾，是一个全行业都需要高度关注的问题，但车险欺诈类型日益多样，作案手法专业性越来越强，传统人工筛查难以有效应对复杂多变的欺诈手段。传统的理赔监察工作中，由于精力、时间和技术的限制，无法对车险理赔案件进行全面检查，只能对高风险案件进行抽样检查，大多基于单一风险因素进行排查，无法对多个风险因素的内在关系进行直观显示，较难发现复杂的团伙欺诈案件。针对该业务痛点建设关系网络分析平台，以车险团伙欺诈为切入点，基于大数据、知识图谱等可视化智能产品，结合人员关系、时间、空间等数据，

揭示风险因素之间的关联关系，突破单一风险因素排查，揭示多个风险因素之间的内在关联关系，更直观、有效的识别保险欺诈团伙。

项目架构如图 3-12-1 所示。



图 3-12-1 项目架构

(2) 技术方面

关系网络分析平台基于大数据、知识图谱等人工智能技术，对车险理赔案件进行全样本检查，自动分析案件中的风险关系，通过数据模型可视化展现风险因子间的关系网络，精准揭示人、车、电话等多个风险因子的内在关联关系，智能推送疑似欺诈的高风险案件进行重点核查，有效发现车险欺诈团伙。再将风险网络中验证的欺诈案件回流至数据池，基于此反哺和提升关系网络平台的反欺诈能力，形成反欺诈全流程管理的反馈迭代机制。

(3) 实施方面

项目实施共分为 4 个阶段，分别为需求阶段、开发阶段、测试阶段和正式上线，历时 6 个月完成系统正式上线运行。包括：案件智能推送、案件智能查询、关系网络侦测、风险地图展示等模块。主要功能有：自动收集理赔数据，定期推送风险关系网络；对风险关系网络进行智能分析；对异常风险因子进行定制检索；对高频出险地等地域信息采用风险地图标识。

2. 创新点

(1) 自主知识产权

该系统设计、开发全部自主独立完成，拥有自主知识产权。在大数据时代下，审计模式的创新变革，运用知识图谱智能技术，分析多维立体关系网，实现监察手段突破性提升。

(2) “AI 图谱技术 + 理赔打假场景”

小审阳 1 号将理赔数据与图数据库技术相结合，联合图挖掘、图计算等人工智能技术，通过优化“规则 + 算法”策略，精准揭示人、车、电话等多个风险因子的内在关联关系，助力稽核人员有效识别车险团伙欺诈。

系统自动收集历史车险理赔数据，结合实际业务特点及稽核日常工作模式，采用大数据技术对车险理赔数据进行知识的抽取，包括多组实体及其关系，完成车险赔案图谱的构建。通过 AI 图

谱技术中的社区发现算法、中心性算法、路径寻找算法等将车险赔案涉及的人员、车辆、案件等节点划分为多组车险团伙，并进行车险欺诈团伙的检测，进而锁定疑似欺诈团伙及骨干因子。

针对业务对风险的侧重方面的不同，从以下维度对欺诈团伙进行检测：一是基于风险配置规则，将多个风险因素的内在关系进行直观显示，发现复杂的团伙欺诈案件，综合考虑人员、车辆、案件等节点、关系及其附带的属性，如角色等，通过将多组风险因子进行组合，筛选满足触发多组高风险规则的车险团伙，完成欺诈团伙检测；二是基于车险团伙网络结构集群拓扑特征维度，根据车险团伙生成相对应的网络集群拓扑关系，采用图谱技术中的中心性算法筛选核心节点，进而计算相应节点及其 N 度邻居所在网络的聚集紧密程度，结合网络中节点的聚集程度及风险映射的关系，完成欺诈团伙检测。

两类欺诈团伙检测联合互相补充，一主要侧重人员与车辆、车辆与案件、人员与案件的节点属性及关系和相关阈值来定义欺诈，由于团伙作案涉及成本等因素，会出现多人多车进行角色互换在不同案件中多次出险的情况，可以通过出险次数的严重程度来衡量整个团伙的风险度，进而检测欺诈团伙；二对已划分社群抽取图谱集群结构拓扑特征、中心性特征，联合两类指标计算风险得分，此类方式不需业务人员预先设定具体风险规则及相应阈值，更加灵活，大大提升对未知类型团伙欺诈的检测，给保险公司带来另外的增量维度。

以上 AI 图谱技术，能够结合人员、车辆、案件的关联属性对团伙的欺诈行为进行研判，提高了车险反欺诈管理的灵活性、完整性、严密性和识别效率。

(3) 车理赔数据 100% 全量稽查

构建全国产险中支机构多年的案件图数据库，自动分析案件中的风险关系，进行理赔案件多维智能分析，全样本挖掘理赔虚假案件，防范内外部欺诈风险，挽回理赔损失。

(4) 形成严打高压震慑效应

依托小审阳 1 号智能关系网络及持续的理赔监察打假，保持高压监控态势，从而形成对内外部欺诈团伙的强大震慑作用，持续提升公司业务价值。

3. 技术实现特点

技术架构如图 3-12-2 所示。

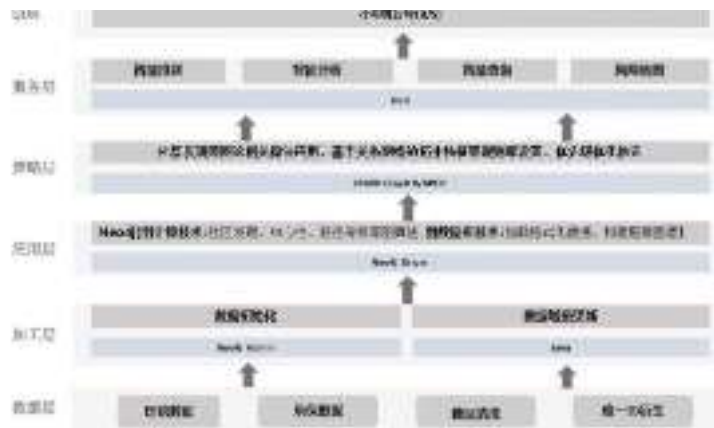


图 3-12-2 技术架构

（1）加工层

自动收集历史车险理赔数据，通过大数据技术完成数据检验、实体与关系的抽取。

（2）应用层

利用图数据库技术，加载格式化数据、构建赔案图谱，采用图计算技术，如社区发现、中心性、路径寻找等图算法，社区发现算法在复杂网络中发现连接紧密的节点簇（社区结构），将图中节点划分到不同社区，使得社区内部连接紧密，社区之间连接稀疏；中心性算法用来发现欺诈团伙中最重要、最具影响力的人物，为业务人员提供欺诈人员、车辆等核查线索，进而提高线下查处效率。

（3）策略层

基于应用层的图算法技术和关系网络的集群拓扑特征等规则库设置，对已分社群抽取图谱结构、中心性指标，联合两类指标计算风险得分，综合考虑图谱紧密程度和核心影响节点，推断新的高风险专家规则，通过不断迭代，提炼规则，规则验证，规则应用，不断优化和调整欺诈团伙检测规则库。

（4）服务层

基于 AI 图谱相关技术，根据触碰风险规则等优化排序，定期推送风险关系网络，并对风险关系网络进行智能分析，综合分析骨干人物、核心车辆及其关联关系等信息。同时实现对异常风险因子进行定制、灵活、差异化的检索，联合标的、三者修理厂等地址，对高频出险地域信息采用风险地图进行标识。

通过以上 AI 图谱技术能够有效地提升车险欺诈团伙锁定精准率，进而提升线上质检成功率，改善线下问题查处效率，精准识别打击车险欺诈团伙，防范内外部欺诈风险，为公司挽回赔款损失。

4. 运营情况

（1）推广应用

①用户情况。通过线上、线下分享和讲解，推广小审阳 1 号系统的应用。系统上线后，集团监察稽核部全体人员每人每天都在使用小审阳 1 号开展各项稽核项目，截止 2021 年 5 月 19 日，部门当前在职员工账户 167 个，上线运行期间含入离司变动人员账户共 391 个。

②数据情况。小审阳 1 号每月推送产险全国城市型分公司及三级机构的车险赔案风险线索及案件清单，推送量 8000 条 / 月。“智能推送”中，包括 3 类风险模型：疑似风险网络、老旧车型风险网络和修理厂风险网络。“智能查询”是在对已发现的异常案件中的风险条件进行相关案件的拓展串联，包括人员姓名、身份证号、报案电话、车牌号、VIN 码、修理厂、查勘定损员等条件。

③系统运行。推送接口支撑周边系统，包括服务层 4 个应用模块：智能推送、智能分析、智能查询和风险地图；与各系统接口运行情况正常。

随着数字化转型进程进一步加快，查勘、定损、理赔、稽核等业务节点开始使用系统对理赔案件进行管理和审查，系统带来的便捷、智能和高效逐步显现，使用情况更加规范和完善，并且持续不断迭代优化系统算法及计算规则，提升欺诈团伙锁定精准率。

5. 项目成效

(1) 经济效益

小审阳 1 号上线应用后，极大提升了监察人员打假效率，有效发现车险欺诈团伙，追回虚假赔款挽回理赔损失，为公司降赔增效发挥重要作用。如 2020 年理赔监察项目中，打掉欺诈团伙（含修理厂）和欺诈个人 10 名，追回赔款 58.26 万元，尚有已签署协议尚未退回赔款 10 余万元；2021 年理赔监察项目中，已成功追回赔款 16.35 万元。

图 3-12-3 是一个真实案例，通过查证人员、车辆、案件的关联关系，锁定欺诈团伙，团伙中涉及的虚假赔款占总赔款的 85%，已全部追回，同时发现欺诈修理厂 2 个，欺诈人员 2 名。

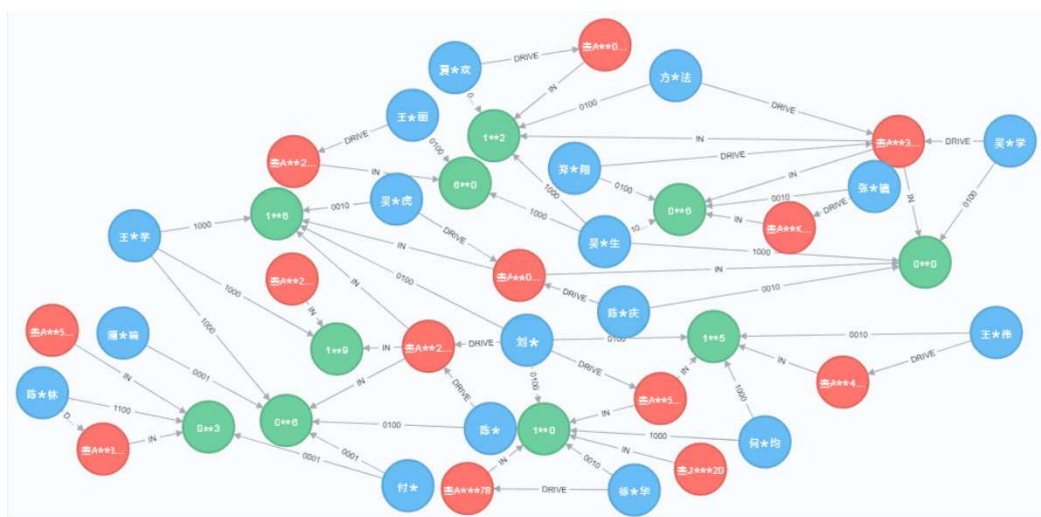


图 3-12-3 真实欺诈案例

(2) 社会效益

据中国银保监会数据统计，我国每年因车险欺诈所赔付的保险金约占全部理赔金总额的 20% - 30%，涉案金额惊人。我司每年均开展常规及专项稽核进行理赔打假，通过小审阳 1 号，让“数据 + 科技”真正赋能保险稽核监察业务，助力监察人员精准识别打击车险欺诈团伙，为公司挽回赔款损失，肃清理赔队伍，震慑外部不法分子，切实做好风险管控的第三道防线，构建健康和谐的保险环境，为社会稳定和长治久安作出积极的贡献。

十三、阳光产险信保事业部：智能运营管理可视化平台

1. 项目方案

阳光产险对于数字化运营有着清晰的规划和设计，从公司层面设立了自上而下的推动机制，并且定位于公司新时期发展战略，从数字化平台建设到客户洞察价值最大化，再到五大能力全面实现，稳定的三步走战略为数字化转型奠定了良好的基础。经过 9 年的打磨，各环节业务流程趋于成熟和稳定，积累了大量数据。

本项目通过运用数据可视化技术，将客户行为、承保信息、销售业绩追踪、运管时效等信息集中归一，避免了信息孤岛问题；通过三维立体、二维图形、曲线和其他形式对数据进行实时展示，对数据的相互关系以及模式进行可视化分析；通过不同终端、不同场景进行展示。

2. 创新点

①技术创新

使用大数据引擎，通过把多个业务系统的关键业务流数据统一抽取到 CDH 集群，实现订单的全链路关键节点的打通；通过维度建模技术，实现了多维度、多终端、多场景的数据分析应用。

②应用创新

实现企业经营的数字化、可视化、透明化，洞察管理盲区，提供决策支持，同时提升公司客户服务运营时效。在订单全流程的核心业务节点数字化改造的基础上，对各个核心节点时效进行可视化、多维度展示，能够直观反映各个节点的时效，帮助各业务部门及时掌握流程堵点，及时改进节点效率。

3. 技术实现特点

技术架构见图 3-13-1。



图 3-13-1 技术架构

4. 运营情况

2021年6月底完成一期平台上线，进行初期推广，经过数据治理与优化，二期于11月底完成上线，12月中旬上线开门红运营监控大屏，按时达成项目目标。

平台已完成测试并投入生产，推广至总公司各部门以及各分支公司。目前聚焦在管理层，上线投产后四季度用户超过100人，预计2022年深化推广，用户群体扩大至400人。结合总部分部管理层级调研，用户满意度达到96.08%。

管理考核上已经应用到信保全国运营中心活动量考核，并出具时效优化目标考核值，供不同环节的管理主体进行优化监测。

5. 项目成效

①行业应用

目前行业尚未有类似的时效管理平台 and 工具，本项目开创了行业应用的先河。项目借鉴物流和制造业，根据阳光产险信保业务特点进行本土化应用。

②客户感知维度

从客户角度出发，从客户意向产生、注册APP触发，到客户承保出单，并拆分出客户等待时间和客户操作时间，时刻注重客户体验与感受。

③全集全量埋点

平台采集全集埋点，细化到页面级及按钮级别，可查看最细颗粒度的业务实时动态数据，将全流程拆解成106个子节点，深入客户交互的每个页面，最终选择17个节点作为管理的主要阶段。

④聚焦作业单位

从客户经理端、核保端、签约端，到线下运营端、合作银行端，根据耗时长短，定位问题。

⑤可视 & 多维 & 实时

采取实时大屏，展现时效趋势和保单生命轨迹，全国各省时效红黄蓝达成，环节占比分布，并根据最新作业情况展示最新时效情况。

⑥独立研发

可视化方案由数据团队和产品团队联手打造，全部由我司开发人员研发，具有自主知识产权。

6. 经验总结

搭建纵观全流程业务管理视角的考核标准体系，通过构建用户和销售全流程事件流和业务操作数据流，在大数据平台上搭建全业务时效主题域全流程节点数据模型，实现了多维度、多终端、多场景的数据分析应用；可以实时监测作业团队排队作业量、当前人力配比、当前处理时效以及预估处理耗时等。业务全流程时效数据可视化，为业务流程优化提供依据，在分部推广应用的过程中体验良好。

十四、阳光财险：全能保双活建设

1. 项目背景及目标

随着移动互联网技术的不断发展，传统保险公司的经营模式从线下转向线上线下一体化，传统的 APP 展业工具不再是以满足出单功能为前提，而是以平台化的角度进行建设与升级，从而使公司业务具备透明度更强、参与度更高、协作性更好、中间成本更低、操作更便捷等一系列的变革。阳光产险自 2016 年上线面向销售人员展业的出单工具全能保后，经过 4 年的不断建设，用户规模不断扩大，系统功能不断完善，为适应上述变革带来的系统层面的挑战，以及工具本身从科技赋能业务发展的角度出发，保证系统 7x24 小时稳定在线已经是开发人员的必答题。

全能保系统双活旨在打造一个稳定的，集业务员展业与销售管理于一体的全流程双活体系。具体目标：一是实现 APP 登录服务高可用与双活快速切换，保证 APP 登录稳定；二是实现关键展业功能车险出单高可用与双活，保证业务稳定；三是双活切换以后实现数据归集，保证业务操作的连贯性与完整性。

2. 创新点

全能保 APP 充分整合现有资源，按照复用与易于维护的标准进行设计。在原来建设的底层系统之上，运用全新的互联网微服务架构，从建设一个 APP 需要的功能、标准、稳定性与扩展性出发，实现了符合自身发展特色的双活方案，保证了系统的双活建设顺利落地。系统具有以下创新点。

①基于 APP 打造了统一用户登录服务，重点解决全能保 APP 用户、角色、技能、菜单、权限之间的关系，通过梳理上述关系建设成标准统一的双活登录服务，重点保障了全能保的全员登录。

②如何保证登录双活服务的稳定性，则依赖搭建登录微服务双中心，通过双机房部署，对外提供两套网络通道，APP 接入时出现故障可以实现自动切换。底层数据搭建一主双从数据中心，一主写库主要保证数据一致性，双从读库为双机房读服务提供支持，写操作通过异步消息 MQ 系统解耦，保证了系统的高并发。

③出单双活的基础是登录双活，两种相辅相成，统一用户登录服务双活保障了 APP 的 7x24 小时在线，而关键出单功能系统的双活建设，则通过打造车险多中心完成。

④车险多中心可以实现快速切换，具备高可用性，任一中心可以保证全量的业务操作具备横向扩展与灾备的能力。统一对接接入方式，保证了保险公司各个渠道标准化接入。

⑤为保证多中心切换的时效，基于登录双活服务，建设后台管理系统，完善数据字典等基础服务。可以实现多中心切换可视化配置，支持机构、渠道、工号、系统多个维度。

3. 技术实现特点

APP 核心功能的双活建设主要针对之前 APP 建设遇到的瓶颈问题，综合分析影响 APP 稳定性的因素，主要包括网络层、中间件层、数据库层等，通过有的放矢的解决问题，确定解决方案，具体实现特点如下。

①系统采用 Spring Cloud 分布式服务化架构进行系统改造，采用无状态服务原则进行设计，保证了服务模块可以随时进行横向扩容及部署，通过服务拆分降低服务之间的耦合，同时支持后续

续服务推广容器化 Docker 进行管理。

②实现网络层面高可用双活，鉴于业务高峰期间，网络带宽出现瓶颈问题，使用阿里云与公司外网双网络通道，支持通过配置域名，实现客户无感切换。

③实现中间件高可用双活，主要依赖双中心部署，在原有架构基础上，应用服务中间件搭建双中心，同城异地双机房部署，保证了网络入口切换时应用中间件的扩展能力与支撑能力。

④实现数据库高可用与双活，基于单一数据库存在的 IO 性能瓶颈，在中间件多中心的基础上，实现数据多写，同时通过分库分表、读写分离、增加两地缓存，进一步保障数据库的连续稳定性。

⑤实现数据切割与归集，全能保双活建设为保证前端系统的轻量级，及功能不重复建设，充分利用核心系统的全量数据、读服务双活及读库多节点等系统优势，通过核心接口与数据同步实现移动端双活切换后的数据归集，保障业务操作连贯性，同时增加大表数据的自动切割保障数据库的持续稳定。

4. 运营情况

①全能保统一用户登录双活服务

可以支持全体销售人员各类用户总量达 10 万人以上，日活跃用户约 20000 人。同时支持公司同类 APP 统一管理，为实现 APP 工具融合奠定基础。

②出单系统多中心

全能保关键业务系统车险出单完成多活中心建设，支持域名灵活切换，保证业务峰值时系统的稳定性，围绕出单的切换，增加配置管理，保障系统的灵活可扩展性。出单系统多中心不仅支持全能保线上出单功能，同时为内部多个 APP 与渠道提供报价与出单服务。目前全能保车险日均保费约 4000 万元左右，产险线上化车险出单率达 98%，助力公司释放柜面人员，节约人力成本。

5. 项目成效

①系统持续稳定

移动全能保 APP 包括登录系统和关键业务系统，从保障系统稳定性的角度进行全链路优化，包括网络、中间件、数据库等各环节实现双活部署。在确保高可扩展性的同时，集成展业、业绩统计、结算、活动管理等功能，形成了功能全面的移动端专属工具。

②具备快速输出的服务能力

基于全能保统一登录服务层，可以实现快速服务输出，最大程度的实现资源复用，目前我司多个 APP 借助于的全能保双活服务完成孵化。

③助力线上化展业能力提升

借鉴互联网思路，支持公司线上化业务的开展，疫情期间，通过移动 APP 系统保证了公司整体业务稳定推进。

6. 经验总结

通过移动全能保 APP 系统双活的建设，完成了移动工具开发的标准化建设，以平台化的思路建设配套的后台管理系统，为保险公司通过科技赋能业务发展提供了有价值的参考。

十五、时速云：分布式支撑平台建设解决方案

时速云分布式支撑平台建设解决方案基于云原生技术打造，采用服务网格技术对企业数量繁多的微服务进行统一管控，帮助企业完成分布式架构改造，通过发挥分布式系统敏捷、弹性、易用等特点帮助企业适应不断变化的市场需求。

1. 解决方案简介

时速云分布式支撑平台建设解决方案能够帮助企业构建分布式 IT 系统架构，实现对跨集群、跨区域，公有云与私有云混合部署的服务的统一治理，同时支持容器、虚拟机等多种部署形态的服务统一接入，以及存量服务的平滑迁移，并可与 PaaS 平台集成实现全周期统一管控。同时在服务网格的标准服务组件和服务治理方面有一定创新。

该解决方案通过标准服务组件，可支持多种微服框架接入、多服务协议发布，形成一致的服务注册、服务发现标准与规范，将企业内的服务进行统一管控，降低不同业务部门、不同开发框架、不同协议带来的系统部署及管理的复杂性，且便于从整体视角审视企业内的服务部署、调用、资源使用情况，增强了平台管理的可观测能力。

在服务治理方面，平台在数据面上采用 Sidecar 的部署模式，使应用开发阶段需要引入或者编码的工作逐步下沉到基础设施（服务网格），既可以避免服务治理模块升级带来的服务重新构建升级，也为企业服务开发语言的多样化提供了支持，降低应用开发、构建的成本。同时，通过配置的增量下发，降低了数据面代理的性能损耗。

该解决方案已经历了多个行业核心业务应用的生产上线与流量洪峰考验，大大提高了业务应用运行的易用性、可靠性、可观察性等特性。

同时在安全性上除了通用的 mTLS、RBAC 安全机制，还支持国密安全。

由于其在跨架构跨云统一服务管理方面的优势和全面的功能，使其尤其适用于金融行业的架构转型，并能够满足合规、安全方面的要求。

2. 应用场景痛点

在传统架构下，企业的服务治理面临着治理应用范围过窄、治理难以落地沉淀、多项目多环境易交叉等挑战。

因此，从传统架构向分布式架构过渡成为企业探索的重点。利用微服务、服务网格技术实现分布式架构，可以有效解决服务间通信、流量治理等方面的问题，并能够将服务注册与发现、流量监控与智能路由、服务熔断、限流与降级等服务治理能力沉淀到平台层。从而实现多框架统一治理、常用治理功能工具化、多租户多项目管理，极大地提升了业务开发部门的研发效能、简化运维部门工作流程，推动自动化运维。

金融行业是分布式架构转型的先行者，主要原因在于金融行业有一定的技术储备，能够采用有一定技术门槛的新技术；金融行业业务量大、架构复杂、数据庞杂、对于转型的迫切性更高，痛点也更为突出。分布式支撑平台建设解决方案所针对的具体痛点包括：①服务依赖管理，服务间直接调用，依赖混乱；②服务调用统计，调用记录无迹可寻，调用统计与分析无从谈起；③服务安全管理，安全靠白名单各自为战；④服务治理能力，不同业务系统中存在大量重复代码，多语

言支持困难；⑤服务接口测试，拆分过程中跨服务接口调用异常不可预测；⑥服务灰度发布，上线功能实现灰度借助大量 if-else；⑦服务历史峰值监控，对于峰值压力无历史数据参考，无容量规划；⑧服务调用链分析，当服务请求缓慢，难以快速定位问题点；⑨租户隔离治理，系统环境多，难管理，存在资源浪费。

针对上述痛点，可以归纳出 3 个主要的解决方案思路：一是扩充多框架治理范围，并实现多框架统一治理；二是沉淀治理能力，将服务熔断、服务降级、服务限流、服务路由等常规治理能力工具化；三是多项目多环境实现标准化管理。

3. 解决方案亮点介绍

（1）企业内的服务进行统一管控

形成一致的服务注册、服务发现标准与规范，降低不同业务部门、不同开发框架、不同协议带来的系统部署及管理的复杂性，也便于从整体视角审视企业内的服务部署、调用、资源使用情况。

（2）统一服务代理

采用 Sidecar 的部署模式，使应用开发阶段需要引入或者编码的工作逐步下沉到基础设施（服务网格），降低了应用开发、构建的成本，既可以避免服务治理模块升级带来的服务重新构建升级，也为企业服务开发语言的多样化提供了支持。

（3）多协议发布

主要是支持将同一个业务系统的多个端口，各自配置为单独的协议，并同时发布到统一的注册中心，进行服务发现。如传统应用开发中，一般会提供一种协议的业务实现，如 Rest 协议，但是调用方可能期望可以使用 Rest 或者 Dubbo 方式进行调用，此时则需要通过某种方式自动的实现多协议发布，而不是重新实现协议层的逻辑，来减轻业务开发方的负担。

（4）多种分布式框架

主要是指 Dubbo、Spring Cloud 等主流分布式开发框架，包括兼容框架自身的服务注册、发现机制，以及处理分布式服务框架与框架本身能力的冲突问题，如注册冲突、负载均衡冲突等，保障原有分布式框架的服务可以平滑的接入到分布式服务框架的统一框架下，以最低的成本接入已有业务系统。

（5）开放性更佳

多种部署方式、多注册中心的能力支持使得平台的开放性更佳。支持容器部署与虚拟机部署的服务统一接入至平台实现统一治理；可以将多种外部注册中心的服务逐步平滑地接入服务网格，减轻业务人员对应用的改造，实现服务的统一治理、统一观测。

（6）丰富且稳定的治理能力

服务治理能力包括服务监控、健康检查、服务熔断、熔断告警、服务限流、服务降级、服务依赖、灰度发布等功能。

①服务监控：包括服务注册、服务使用资源的实时 / 历史监控，用来对服务及其资源使用情况进行管理。

②健康检查：主要允许服务主动上报健康状态，或者通过注册中心探测服务健康状态，以便随时了解服务的监控情况；同时允许基于策略处置异常服务，包括采取服务的降级、熔断、限流、弹性扩容等行动，最大程度保障系统的平稳运行。

③服务熔断及熔断告警：在服务不可用时，依据规则触发熔断，避免串联故障导致的雪崩效应；同时发送告警通知，以便运维人员可以采取相关行动。也可以根据策略定义熔断动作，以及在访问正常后的熔断服务恢复。

④服务限流：允许用户定义限流规则，当流量超过了服务能够支撑的范围时，拒绝服务访问，以确保服务在可以承载的容量内稳定运行。

⑤服务降级：当一个服务调用多个外部服务，结合服务依赖的分析，对于劣质服务可以采取降级处理，防止对劣质服务依赖影响应用自身服务能力，确保应用自身的稳定运行。

⑥灰度发布：是指能够在多个版本之间平滑过渡的一种发布方式。

⑦流量管控、智能路由、认证与鉴权：主要是指允许用户定义限流、路由和认证规则，并由系统自动将对应的配置下发到对应服务的服务代理（Sidecar），进而由 Sidecar 按照配置执行限流、路由转发、认证鉴权等行为。

4. 金融行业客户名单

目前时速云分布式支撑平台已在保险、能源、通信、交通等各行业企业客户的生产环境中获得应用。此外，银行、气象、通信等行业也有成熟应用，累计服务的大型企业客户数量已达数十家。其中金融行业客户包括：大家保险、中国人保、中信银行、国元证券等。

5. 客户评价

大家保险研发部技术负责人：行业内率先应用下一代微服务架构 Service Mesh，将服务治理下沉到基础设施，并与业务系统解耦，提供一个可视、便捷的微服务“交通治理监控”网，为集团数字化转型提供了技术支撑保障。

十六、新华三集团：SeerFabric 金融智能无损数据中心解决方案

新华三 SeerFabric 金融智能无损数据中心解决方案包含交换机、SDN-DC、集中式 / 分布式存储、超融合、安全等产品，将 RDMA、RoCE、iNoF、SDN、可视化、无损以太网、大带宽融为一体。方案整体基于云边 AI 协同架构，能够借助智能学习为不同业务场景构建智能无损控制模型，并能实现对业务场景的智能识别，进行相应模型参数的动态匹配，以大带宽、低时延、零丢包的精确转发和可确定性网络体验，广泛应用于金融行业的生产业务、大数据 / AI 计算、存储环境等多个场景的统一 IP 化承载，从而实现金融新一代无损数据中心建设。

1. 应用场景痛点

传统数据中心一般建立在多个架构（Fabric）上，包括用于服务器互连的以太网、用于存储网络的光纤通道（Fibre Channel - FC）以及用于高性能计算集群的 Infiniband（IB）。金融核心生产数据以数据库的形式集中存储存放，数据传输通过 FC 协议的 SAN 网络实现；备份归档数据，作为生产数据的副本，通过备份方式构建，以近线集中存储和离线磁带存储为主，传输网络采用 SAN

网络；AI 大数据由大数据平台构建，数据采用大数据平台的分布式存储，AI 网络则以 Infiniband 网络为主；而金融业务则是通过以太网承载。上述三部分的数据采取了不同存储方式和网络联接方式。但 IB 和 FC 在全球都是只有少数个厂商提供技术，并且与以太网完全不互通。在金融核心技术自主可控建设背景下，需要突破 IB 和 FC 两个最主要的技术垄断。

全融合以太网

全融合以太网网络，将数据中心运营成本降低40%以上。



应用场景

化繁为简：以太网一统三大网络场景

- 智慧客服
- 智能信贷
- 智能获客
- 行情分析
- 智能理财
- 智能监管
- 移动银行
- 生态渠道
- 智能投顾
- 智能营销
- 智能风控
- 互金业务

证券

银行

保险

生产业务、大数据/AI计算、存储环境等
多个场景的统一IP化承载。

零丢包、低时延、高吞吐，满足金融全场景转型需求

随着以太网的新发展，无损以太网技术、支持 RDMA 和 MPI 的高性能以太网网卡、以及 NVMe over RoCE 全闪存存储系统等的出现，基于以太网的数据中心网络解决方案开始取代光纤通道（Fibre Channel - FC）和 InfiniBand 解决方案，提供等效或更好的表现。此外，以太网解决方案通常更具有成本效益，并得到了更多供应商的支持。由于这些原因，现代数据中心正在从多协议模式转向全融合以太网。

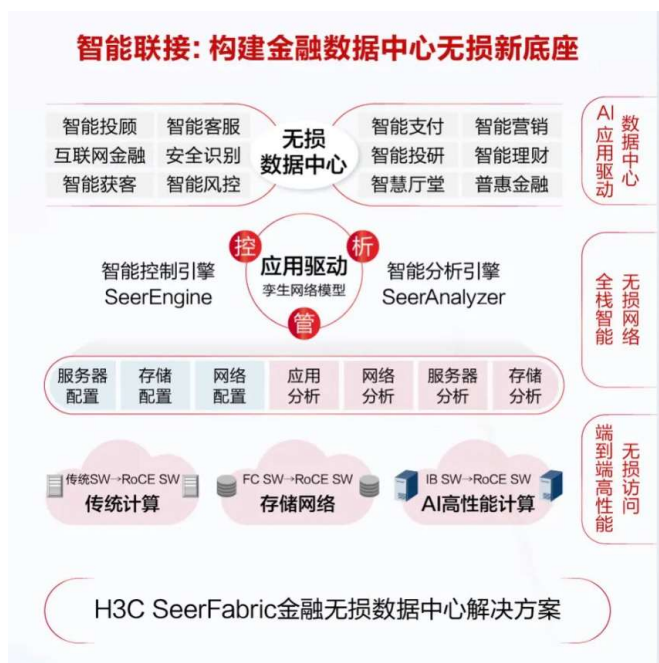
2. 解决方案亮点

一是国产化：网络、计算、存储领域系统级端到端国产化；

二是低成本：相较于 IB、FC 组网更低的采购成本；

三是性能高：更低的网络拥塞延时，核心领域协议升级，性能提升显著；

四是简运维：全以太网组网三大场景 IP 全融合，交付与业务上线提供便捷性能评估工具，跨领域全线无损运维支持能力，SDN 智能运维管理，问题快速定位，业务深度可视化，帮助更有效优化业务流程，场景化网络性能自动调优，存储自动发现，便捷部署。



3. 金融客户案例

贵阳农商行采用云计算、虚拟化技术基于海光服务器建设无损信创云；同时采用超融合、海光服务器、RoCE 交换机替换传统光纤交换机组网，实现无损传输功能的落地。创新性的端到端 RDMA 方案，实现了 RoCE SAN 替换 FC 的实质性突破。

十七、神州云科：云科透明湖应用交付弹性计算解决方案

1. 解决方案简介

金融行业在构建云计算平台时都会考虑弹性计算，因为它可以根据工作负载的需求，动态、灵活调整服务器计算资源，弹性计算真正使云计算中心具备智能性，最终为用户提供按需所求的服务，但如何实现智能弹性计算，业务不中断，需要一套完整的方案来解决。

云科透明湖应用交付控制器弹性计算解决方案将流量管理、资源调度与虚拟化技术紧密结合，通过与云计算虚拟机管理平台的集成，为云计算环境提供一个完整的弹性计算解决方案。

云科透明湖应用交付控制器在判断业务繁忙方面具有得天独厚的天生优势。应用交付控制器是应用交互数据的承载平台，对业务负载的变化非常敏感并最先感知。同时云科透明湖应用交付控制器提供强大的服务器健康检测机制，可以实时掌握后台服务器的运行状态。最为关键的是，应用交付控制器负责整体协调后台服务器计算资源的负载调度，那么对于业务的变化以及所需计算资源的多少，应用交付控制器作为控制点是最为合适的。但问题的关键是，无论传统的负载均衡设备还是当前的应用交付控制器，通常都是负责固定服务器群的负载调度，即使遇到业务的高峰或低谷，计算资源依然是固定的。除非人为的干预，通过调整服务器池中的参数，才能完成这种变化，可是这种管理方式是非常不灵活的，而且操作性较差。不过我们也欣喜的发现，在云计算环境下，虚拟化技术的特点正好可以弥补上述的不足，虚拟机的灵活调度在云计算环境中根本不是什么问题，那么应用交付技术与虚拟化技术的完美结合，为弹性云计算提供坚实的技术基础。

云科透明湖应用交付控制器正是基于这种理念进行设计，其内置的弹性调度引擎是四大核心任务引擎之一。它首先利用云科设备对业务变化的实时跟踪数据，利用决策模型确定业务的高峰和低谷，并计算出满足对应业务情况下的合理计算资源配置，然后通过基于事件驱动的触发器（例如通过预置应用负载的阈值作为计算资源调配的触发器），向云计算资源管理中心发送指令，例如唤起或关闭虚拟机。通过云计算资源管理中心进行相应的计算资源调配，实现计算资源的弹性调度（见图 3-17-1），保证用户以最佳的资源配置为应用提供服务，实现绿色 IT。

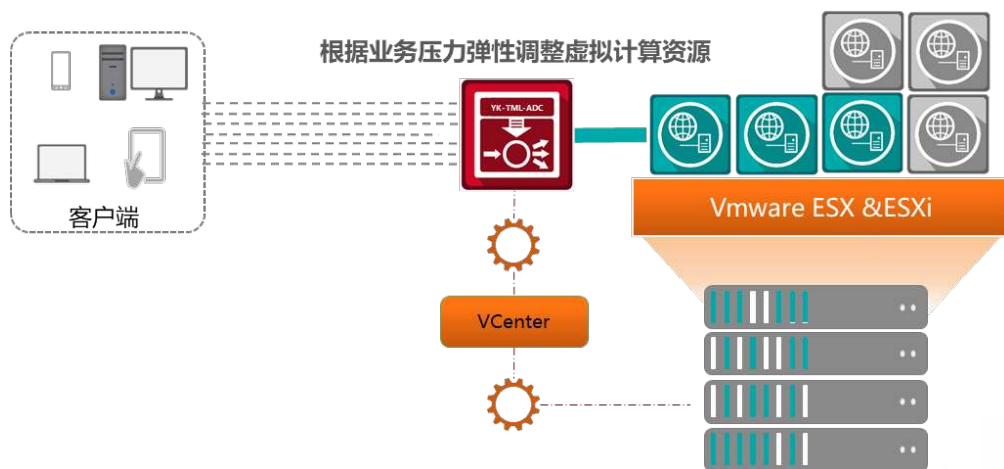


图 3-17-1 计算资源的弹性调度

在实现计算资源弹性调度解决方案中，云科透明湖应用交付控制器将作为云计算资源管理中心的第三方应用者角色，通过资源管理中心提供的开放式 API，与资源管理中心进行集成，如通过调用 VMware vCenter 提供的 API，远程执行唤起或关闭后台应用服务器策略，动态掌控应用服务器资源的规模。

云科透明湖应用交付控制器弹性计算解决方案适合银行根据业务的高峰低谷来动态调整基础资源，高峰期实现轻松拓展，操作无需中断，保证业务连续性；低谷期实现自动缩放，降低资源浪费，可以节省资源和电力等 IT 成本。

2. 应用场景痛点简介

由于业务办理量会受到工作日、周末，白天、夜晚等时间段的影响，工作日的白天工作时间段业务量要远远大于夜晚时间段，为了适应流量最大峰值，业务不得不选择 N 台服务器集群来支撑，这样在非高峰时期就必然浪费了很大一部分资源。所以如何合理化利用资源满足业务需求，是行业必须考虑的问题。

3. 解决方案亮点介绍

云科透明湖应用交付控制器是应用交互数据的承载平台，对业务负载的变化非常敏感并最先感知。同时云科透明湖应用交付控制器提供强大的服务器健康检测机制，可以实时掌握后台服务器的运行状态。最为关键的是，应用交付控制器负责整体协调后台服务器计算资源的负载调度，那么对于业务的变化以及所需计算资源的多少，云科透明湖应用交付控制器作为控制点是最为合适的，更为及时和精准。

十八、西骏数据：数据库统一操作平台

1. 应用场景痛点

随着金融科技、数字化转型战略的实施和信息技术应用创新的推进，证券公司在数据库领域已经进入多元混合数据库应用场景。在如此复杂的数据库应用场景下，如何实现对数据库资源接入、操作、权限等进行统一管理，落实各项精细化管理措施，满足数据安全相关法律和监管部门要求，对证券公司而言，具有重要意义。

复杂的数据库应用场景催生出了复杂的数据库类型的使用需求，某头部证券公司拥有较多的不同类型的数据库实例，需要对数据库进行操作的各类研发、测试、运维人员较多，对于不同类型数据库的庞大的数据访问操作，如何进行有效的审计和管控，防止出现数据泄露、数据误删、数据篡改、性能影响等各类事件成为数据库运维管理的难题。

2. 解决方案亮点

本项目方案设计采用一种全新的数据工作台替换原有的 PLSQL、Navicat 等前端工具，实现所有操作的汇聚扎口。采用全新的工作台的模式能够实现平台访问账号与数据库实际账号的完全隔离，

彻底解决账号权限细粒度管控的难题。

数据库统一操作平台可以有效解决访问数据库存在的无审计留痕、无权限校验、无法拦截、容易误删除等传统工具无法规避的风险，数据库统一操作台是人工访问数据库的一种“工作台”，也是一款数据访问操作“网关”，能够代替 PL/SQL、Navicat 等传统工具访问数据库，并实现访问及操作结果留痕、细粒度权限校验、访问拦截管控、多人复核、操作备份、重大变更确认等功能；能够提供统一的数据操作访问网关接口，对接其他各类工具平台，进行 SQL 脚本执行，节省其他各类工具平台的开发成本、降低各类平台连接数据库的风险，并能够实现统一审计和管控。

数据库统一操作平台采用微服务架构，分为接入层（SQL 编辑器、调用 API、应用对接 API 等）、引擎层（SQL 引擎、鉴权引擎、脱敏引擎、审计 AI 引擎、流程引擎、任务编排引擎）、数据层（权限数据库、审计数据库、管理数据库）、分析层（SQL 分析、脚本解析、细粒度权限分析、审计分析、授权追踪分析、智能脱敏扫描分析、密码安全性分析等）、展现层（统一门户、数据工作台、告警推送等）等部分。

平台的核心是提供基于 SQL 引擎的 SQL 编辑器。该编辑器支持多种 SQL 语法的输入和智能适配，即 SQL 语法和 NoSQL 语法及不同数据库的特性语法都可以解析，从而无需为不同数据库配置不同客户端；提供强大的 SQL 智能带出、SQL 美化、执行计划、多语句执行以及结果集编辑等功能；能够在 SQL 编辑器发起授权工单，实现提权申请。

在 SQL 引擎方面，支持 SQL92、SQL999 标准，支持 30 多种数据库特性 SQL 语句的解析和执行，包括传统 SQL 数据库及 NoSQL 数据库。目前已支持 Oracle、MSSQL、MySQL、MariaDB、达梦、TiDB、OceanBase、GoldenDB、Hive、ClickHouse、MongoDB、Redis 等 30 多种数据库。

在权限管控方面，支持实例、Schema、表、列级别的细粒度权限管控；支持按照对象、操作类型、时间段、返回数等进行精准控制；支持按照数据库实例设置管控模板和白名单；开发了交易日历功能，支持按照交易日历进行不同交易数据库的操作管控。

重点开发了数据操作安全管控功能，包括提供动态脱敏配置、敏感数据智能扫描等功能；支持水印功能；支持导出数据权限管控与导出数据脱敏；支持导出数据不落地。并且能够实现敏感数据的增量扫描，极大地提升了敏感扫描的效率。

作为一款完全自主研发的产品，数据库统一操作平台同时满足信创建设要求，所有组件支持信创环境部署，与主流国产芯片、国产操作系统、国产数据库等均完成兼容适配。

3. 金融行业客户名单

南昌人行、新疆建行、福建农信、华泰证券、中金证券、易方达基金、银华基金等。

4. 客户评价

经过客户的论证，本平台的上线，实现了对各类数据库操作访问的统一扎口管控，在提质、增效、降本方面产生了明显的成效。

① 提质方面

由于采用细粒度权限管控和误操作恢复技术，大幅提高数据库运行的稳定性，大幅降低了数据库操作对数据库安全的影响，提高了系统运行的稳定性，大幅减少了误操作业务中断的几率。

②增效方面

首先是提高了普通用户访问数据的效率，无需进行多个客户端的切换；其次，提升了管理效率，DBA 管理以及审计管理由以前的纯手动操作变为自动化实现，将以往复杂流程变更为高效审批，效率大幅提升；再次是解决了误操作快速恢复问题后，将数据库误操作恢复时间由数小时、数天降低到数秒钟。

③降本方面

节省采购其他各类数据库管理工具的直接成本。同时节省了学习、使用和运维管理成本。

十九、博云：容器云平台解决方案

1. 解决方案简介

容器云平台解决方案由云原生应用管理（BKA）、混合异构 Kubernetes 管理（BKM）、博云企业级 Kubernetes 发行版（BKE）三部分组成，提供企业级 Kubernetes 平台管理能力，全面解决多集群管理、异构集群纳管、应用管理、应用上云、多租户管理等业务场景的容器化落地，简化金融客户以互金业务为代表的敏态业务上云后管理的复杂性。

①云原生应用管理（BKA）：提供应用开发支持、应用发布和应用运行管理能力；

②混合异构 Kubernetes 管理（BKM）：提供应用开发支持、应用发布和应用运行管理以及多云异构集群管理、运维管理和运营管理能力；

③博云企业级 Kubernetes 发行版（BKE）：提供容器的运行时、网络、存储、负载均衡、镜像等能力。

容器云平台解决方案全面解决云原生应用的多集群管理、异构集群纳管、应用编排发布、中间件容器化、应用上云（高性能计算、大数据、人工智能、老旧业务等）、多租户管理等业务场景的容器化落地，简化上云后管理的复杂性，让应用管理既快又稳、降低成本；全面适配国产化软硬件环境，满足用户对一云多芯的管理需求。

2. 应用场景痛点

为应对金融用户互联网业务的快速发展需求，解决传统 IT 架构不满足业务灵活变化、不满足弹性伸缩场景、能耗高、运维难、密度低等问题，通过容器云平台建设，可以提高资源利用率、提升运维自动化水平、提高新系统部署速度，同时有效提升金融用户的开发、测试、运维的整体信息化管理水平。

随着市场政策的引导和信创发展趋势，金融行业正在加速推进国产化适配。金融行业应用具备大数据量和高并发的典型特征，这刚好是容器云的优势，金融行业的国产化适配可以一步到位采用信创容器化架构，既避免了不同芯片架构的多次适配，又实现了极致弹性扩展的系统架构升级。

3. 解决方案亮点

（1）长期生产验证的稳定性

①方案拥有大量生产案例，稳定性、可靠性、安全性经历了长期生产级验证；

②累计装机 10 万 +，Pod 数 100 万 +；

③首批通过可信云金融场景容器云集群性能最高级认证 - 卓越级。

(2) 深度的底层掌控能力

①在 Kubernetes 上运行时，计算、网络、存储、负载均衡、安全性等基础底层都有独到的能力增强；

② Kubernetes 社区贡献位居全球第 10 名。

(3) 第三方权威机构的认可

①连续三年进入 IDC《中国容器基础架构软件报告》，国内市场规模前五（创新厂商第一）；

②连续三年进入 Gartner《成熟度曲线报告》- 容器技术代表厂商。

(4) 完善的信创支持

①产品全面支持国产化软硬件，包括芯片：飞腾、鲲鹏、海光、兆芯、龙芯，操作系统：银河麒麟、统信 UOS、中科方德、欧拉，数据库：达梦，满足客户对国产化安全可控的要求，降低客户的局部和重复试错成本；

②产品通过工信部、中国电子技术标准化研究院（四院）、中国软件评测中心（赛迪）、央行金融信创生态实验室等严格测试验证，同时，通过了国家工业信息安全发展研究中心（一所）源代码知识产权评估，代码自主率超 75%。

4. 金融行业客户名单

金融行业客户用户包括中国建设银行、中国民生银行、中国民生银行信用卡中心、中国银联、江苏银行、大连银行、昆仑银行、湖北银行、潍坊银行、自贡银行、广东华兴银行、山东省农村信用社联合社、苏州农商行、无锡农商行、张家农商行、江阴农商行、常熟农商行、江南农商行、紫金农商行等银行；银河证券、东方证券、中泰证券、东吴证券、东莞证券、国盛证券等证券公司；中国人寿财险、中国太平保险、东吴人寿、汇添富基金、海富通基金等保险公司，以及山东城商行合作联盟、中国对外贸易信托、中银消费金融、海尔消费金融、奇瑞汽金、中国信托登记有限责任公司等金融企业。

二十、嘉为蓝鲸：嘉为鲸翼多云管理平台解决方案

嘉为鲸翼多云管理平台解决方案致力于帮助金融企业实现多云架构下海量云资源的全生命周期管理，通过异构云对接纳管、资源集中规划、组织适配、用户自助服务、多云资源编排、自动化交付及资源容量成本分析等服务能力，综合提升企业对于云资源的有效利用率、流程合规性，全面满足业务云化发展的需要。

1. 解决方案简介

嘉为鲸翼多云管理平台解决方案（见图 3-20-1）为客户提供基于腾讯蓝鲸 PaaS 平台打造的从

IaaS、PaaS 到 SaaS、从基础设施、软件到应用的全栈一体化云管平台，提供云管理、云服务、云运维、云运营、云门户等综合性多云管理能力；面向业务开发运维人员提供应用运行资源环境服务以及全生命周期管理，整合运维支撑工具；面向 IT 管理员提供多云环境下的运维、管控、运营服务，为 IT 管理员简化多云环境下的工作。通过多云管理平台的跨云管理能力，实现跨云厂商的资源调配，提升云资源的利用率，降低企业成本，帮助企业的数字业务获得竞争力。



图 3-20-1 嘉为鲸翼多云管理平台解决方案

2. 应用场景痛点

①异构云统管困难：无法一站式纳管各类公有云、私有云、虚拟化、容器云、物理机资源，陷入烟囱管理。

②租户资源规划难：多租户、部门、项目边界不清晰，无资源池规划，云资源交付不规范、难管理。

③云监管局限：缺乏从云平台、云资源、系统组件到业务应用的全方面运行监控与日常运维操控。

④用户服务体验差：用户申请资源或服务渠道单一、流程欠缺规范、效率低下，影响业务构建。

⑤统计分析难：难以清晰统计各租户单位资源使用情况、成本情况，缺乏有效容量分析、成本核算分析手段。

⑥云管集成能力弱：缺乏统一调度手段，无法打通和调用 CMDB 配置管理、监控告警、自动化运维流程编排、流程服务、可视化分析等能力，难以融合集成外部云服务产品，从而难以满足保障业务稳定运行的要求。

3. 解决方案亮点

- ①基于资源编排引擎的编排能力，实现从网络到应用的全栈标准化资源的自动化交付。
- ②通过服务编排引擎的编排能力，实现跨技术资源的全流程交付。
- ③通过可配置化的云纳管插件实现对不同公有云和私有云的快速对接和纳管。
- ④通过基于基础设施即代码理念的自动化工具与 CMDB 的原生集成，实现从交付、管理到下线的资源全生命周期管理。
- ⑤基于功能原子单元的自定义编排，具有灵活的资源对象交付场景扩展能力，并可在企业内部持续自生长和沉淀。
- ⑥通过运营编排引擎的编排能力，能够快速跨业务、跨云，全盘展示资源、成本、容量等分析报表，并提供优化建议，助力企业提升资源使用效率，构建成本优化闭环，实现精益化云业务运营。
- ⑦灵活的计量计费管理，通过自定义计费项和计费周期，实现多云环境下面向不同租户的多种资源、不同平台提供自定义的计费规则，满足企业灵活可控的计费要求。
- ⑧多级租户体系实现企业多层次、多应用维度的资源隔离和资源配额，满足企业组织架构多样性、管理要求复杂性诉求。
- ⑨通过服务编排引擎的编排能力，提供内置常用的自助服务目录，帮助企业实现跨云资源申请及调度管理；用户可根据自身需求通过可视化编排自定义服务，无需开发即可快速通过服务流程引擎实现服务创建和修改，满足企业的个性化服务提供需求。

4. 金融行业客户名单

已采购该解决方案的金融行业客户名单见图 3-20-2。



图 3-20-2 金融行业客户

5. 客户评价

四川省农村信用社联合社：蓝鲸平台帮助我行提高了运维效率，让运维人员有更多宝贵的时间投入到更具创新的实践中去。

富滇银行股份有限公司：随着平台的落地，富滇银行稳固多元业态的发展，由更高的效能、可控的风险建立银行的核心竞争力。往后运维团队将基于平台，进一步实现更多场景的建设，借由大量的能力与数据沉淀，建立更智能的运维体系。

二十一、嘉为蓝鲸：灾备切换管理中心解决方案

嘉为蓝鲸灾备切换管理中心解决方案（见图 3-21-1），基于跨系统调度自动化能力，帮助金融企业实现业务系统在生产机房和灾备机房之间的一键切换和回切，并提供可视化大屏跟踪控制，通过保障企业定期灾备切换演练活动的高效成功进行，从而保障企业业务连续性。



图 3-21-1 灾备切换管理中心解决方案

1. 应用场景痛点

近年来，金融企业的信息化程度不断提高，信息系统已经成为金融企业经营管理和业务操作中不可或缺的一部分，金融数据的安全问题也变得尤为重要，一旦金融企业的数据中心发生灾难，将有可能引起巨大的经济损失，影响金融企业的社会声誉，甚至引发金融秩序混乱。因此，灾备建设成为金融业保障业务稳定运行的最后一道屏障。

灾备建设的核心是建立数据灾备中心，建设了灾备中心之后，企业每年还需要通过灾备演练检验系统的可用性、有效性。同时检验灾备切换预案是否能够满足业务恢复的需求和业务连续性的要求。但随着企业业务的不断发展与规模的扩张，业务系统及相应的服务器数量也与日俱增，传统的手工切换已经很难满足企业灾备切换的要求，面临着如下挑战。

①随着业务系统及相应的服务器数量与日俱增，灾备切换过程中所需要执行的脚本 / 命令次数也在不断增加，导致切换所耗费的时间变长，无法满足 RTO 时间目标。

②随着 IT 架构设计不断演变，灾备切换的场景变得越来越复杂，灾备切换软件难以满足复杂场景的流程配置。

③预案在灾备切换系统中起着关键作用，明确了在突发事件发生后如何快速地将系统恢复至可用的状态。因此预案的维护就变得尤为重要，在预案修订后，需要及时更新预案，保证预案的新鲜度和准确性。

④如何在演练或真实切换时，确保切换过程有序平稳的进行，让相关人员都能够实时了解到切换的执行进度，避免因跨团队协作问题导致切换现场出现“混乱”的场面。

2. 解决方案亮点

①海量支持：系统可同时对海量主机批量执行脚本 / 命令，降低海量主机切换的复杂度，提升切换效率（见图 3-21-2）。即使企业在后期面临因业务增长带来的系统数量和服务器数量激增的问题，也无需考虑性能问题。

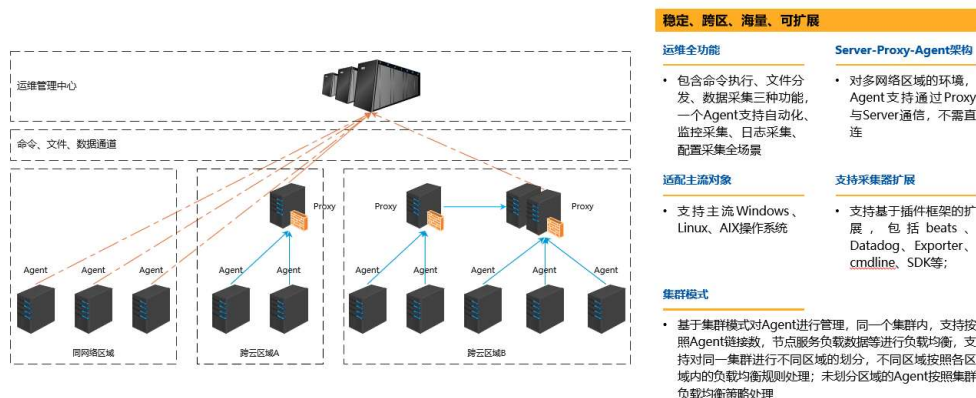


图 3-21-2 对海量主机批量执行脚本 / 命令

②异构兼容：在传统架构和云原生架构下，组成应用的各类软硬件设备多种多样，基于蓝鲸成熟的主机和容器纳管能力以及标准运维的可扩展原子框架，可以实现对各类 IT 设备的各类自动化操作（见图 3-21-3）。

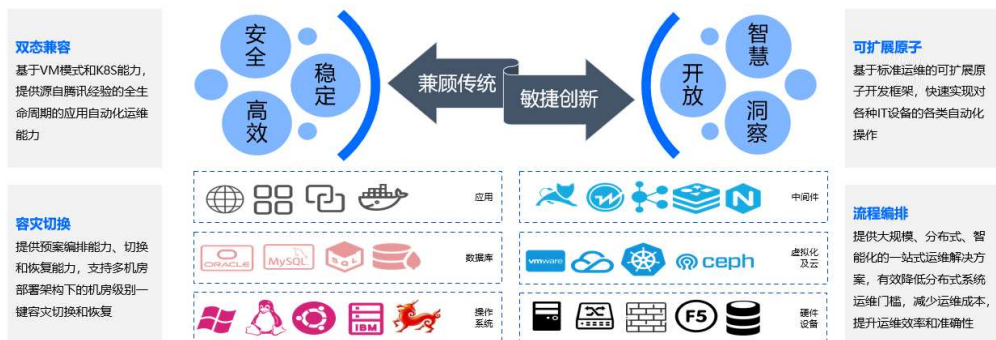


图 3-21-3 自动化操作

③可视化编排能力：系统提供友好的图形化编排界面（见图 3-21-4），支持串行、并行、跳过、重试和人工干预等，可应对企业多种切换场景。同时也降低了编排工作的难度，简化流程编排人员的工作量。编排好的预案用户可一键执行，减少人工操作，实现自动化目标。

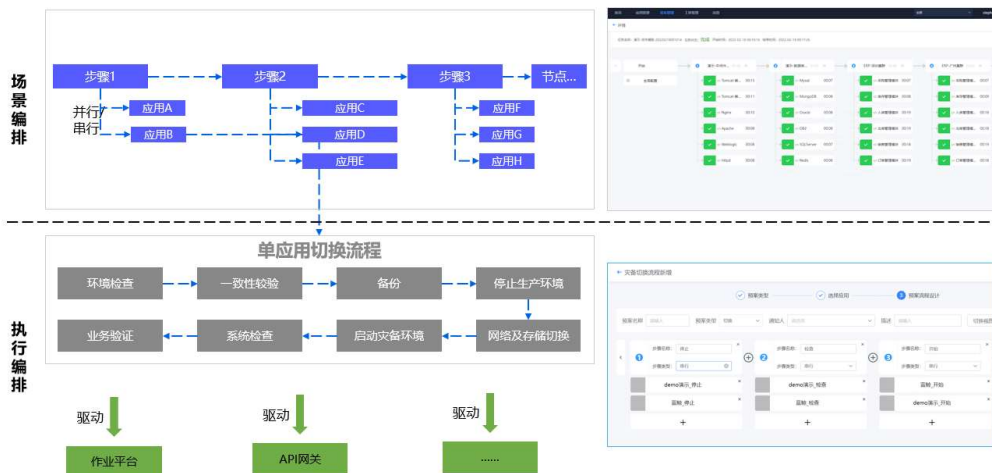


图 3-21-4 图形化编排界面

④切换可视化：系统提供大屏展示功能（见图 3-21-5），动态展示切换过程，向决策层、指挥层、操作层提供切换过程的展示，实现跨团队协作，提高跨部门沟通效率，确保切换过程有序平稳的进行。



图 3-21-5 系统大屏

3. 金融行业客户名单

已采购该解决方案的金融行业客户名单见图 3-21-6。



图 3-21-6 金融行业客户

4. 客户评价

赣州银行股份有限公司：自动化的流程解放了我们的双手，而我们基于蓝鲸平台又能开发出更多场景化的运维、运营工具，让工作变得更加高效。未来，我们会加强与嘉为蓝鲸的进一步科研合作，共同推进更多自动化场景的落地，探索智能化运营的路径，为我行的业务发展提供从保障到决策的一体化技术支撑。

厦门国际银行股份有限公司：嘉为蓝鲸灾切管理中心的引入，助力厦门国际银行向着“敏、稳、智”的数字化运维目标迈进，进一步推动银行的敏捷创新组织机制改革，为数字化生态经营模式提供安全保障支撑。