

构建大型银行开放平台系统智能运维体系研究

徐丽俊著



上海交通大学出版社



构建大型银行开放平台系统 智能运维体系研究

Constructing Intelligent Operation and
Maintenance Framework on Open System of
Large Commercial Banks

徐丽俊 著



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书主要介绍了大型商业银行开放平台系统高效、智能的运维体系,包括基础架构建设、运维治理模型和风险防控体系设计。系统在成本约束下能够满足内外部客户的需求和监管对业务连续性的要求,同时,还具有高可用性以及智能应对突发事件、动态调度各类应急资源、实时恢复业务的能力,满足银行风险管理的要求。

本书适合大型商业银行数据中心系统运维人员、软件开发中心系统开发人员、商业银行管理人员以及银行监管和审计人员阅读和参考。

图书在版编目(CIP)数据

构建大型银行开放平台系统智能运维体系研究 /

徐丽俊著. —上海:上海交通大学出版社,2018

ISBN 978-7-313-20030-3

I. ①构… II. ①徐… III. ①电子银行-研究-中国

IV. ①F832.29

中国版本图书馆 CIP 数据核字(2018) 第 199486 号

构建大型银行开放平台系统智能运维体系研究

著 者:徐丽俊

出版发行:上海交通大学出版社

邮政编码:200030

出 版 人:谈 毅

印 刷:常熟市文化印刷有限公司

开 本:710mm×1000mm 1/16

字 数:172 千字

版 次:2018 年 10 月第 1 版

书 号:ISBN 978-7-313-20030-3/F

定 价:52.00 元

地 址:上海市番禺路 951 号

电 话:021-64071208

经 销:全国新华书店

印 张:12

印 次:2018 年 10 月第 1 次印刷

版权所有 侵权必究

告 读 者:如发现本书有印装质量问题请与印刷厂质量科联系

联系电话:0512-52219025

前 言

Preface

我国银行业信息化建设在过去几十年中取得了巨大的成绩。开放平台系统作为信息化的基础性设施,因其具有开发周期短、架构灵活易扩展、技术更新快、性价比高等优点,在银行业中得到广泛应用,数量规模不断壮大。随着大型商业银行全国数据大集中的完成,大型开放平台的运维面临着需求多样化、对象复杂化、模式集中化、风险集中化的形势。一方面,随着互联网金融和大数据浪潮的兴起,开放平台技术不断更新,对系统运维管理提出了新的需求;另一方面,公众对金融服务的全天候需求与监管机构日益严格的监管要求,对银行业的业务连续性提出了更高要求。大型银行开放平台的运维工作面临着严峻挑战,如何科学、高效、智能地运维开放平台,满足内外部对业务连续性的要求,成为值得深入研究的课题。

由此,原中国银行业监督管理委员会(以下简称“银监会”)根据《银行业信息科技风险管理课题研究管理办法》和《中国银监会办公厅关于银行业信息科技风险管理客体研究立项事宜的通知》,要求五大国有银行及部分股份制商业银行立项并开展相关课题研究,银监会高层指导委员会办公室联合北京银监局共同开展严格的课题验收工作。

本书的研究秉承银监会信息科技风险管理课题的指导思想开展工作,结合

开放平台系统运维特点,分析了大型银行开放平台运维面临的六大挑战:交易量增长快、系统异构性强、监控工具割裂、运维自动化不够、技术演进快和监管要求严。由于系统的高可用和业务连续性是衡量运维质量的重要标准,本书通过系统运维方法和智能技术革新的研究,提出了开放平台基础架构的高可用建设思路。在此基础上,梳理了开放平台的运维对象及其特点,明确了运维体系的设计目标、原则与建设内容,设计了符合大型银行特点的运维体系整体架构,包括开放平台治理模型、应急管理体系和风险防控体系等。

特别是在应急管理体系设计中,创新地依据管理学理论和系统工程理论,同时基于应急管理的多主体理论、信息多向交叉沟通机制和信息资源管理理论,统筹规划、综合协调多部门配合与冲突解决机制,建立了智能应急风险管理的关键要素分析智能模型。风险应急事件一般可分为潜伏期和发生期两个时期,相应的,将应急风险管理划分为应急潜态和应急显态两个过程。应急风险管理模型有应急准备、监测预警、应急响应和善后处置四大基本功能,分别体现在各个管理过程中。以事前应急事件风险评估为基础,建立完善的综合应急预案,通过应急事件的预测预警模型实现应急管理快速响应;通过生产运维视图的建立实现应急事件快速精确定位;进一步利用辅助决策和全局资源调度,实现应急恢复等快速处置;同时引入应急评估方法全面评价应急管理绩效,明确奖惩措施,达到总结回顾和提升的目的,实现风险管理自动化、智能化。本书的研究荣获银行业科技风险管理课题三类成果奖。

本书是基于大型商业银行总行开放平台系统的运维实际,通过理论化的运维体系构建指导实际运维工作。目前,提出的相关运维理念和运维成果已经应用于实际工作,取得了较好的成效,主要应用成果包括以下四个方面。

(一) 开放平台高可用基础架构的建设推广

为有效保证重要业务系统的高可用性,对企业级统一架构建设思路,运维团队从两方面着手落实。一方面对新投产系统均按照高可用基础架构建设,另一方面对已有的重要系统制订高可用改造实施计划,先后完成对综合应用系统中间层(ABIS 中间层)、贷记卡前置系统、银联前置系统、第三方存管和投资业务平台等系统的基础架构改造。

以 ABIS 中间层为例,总行每笔主机业务均需通过 ABIS 中间层统一接入主机系统处理。随着各类渠道业务的急剧发展,总行 ABIS 中间层业务量最高峰达到 7 100 万,巨大的交易量给系统带来很大压力,同时中间层业务关联系统超过 60 个,一旦中间层系统异常,业务影响范围广泛,异常处置难度大。面对这种情况,运维团队对原有系统进行高可用架构改造。首先硬件层面上实现多份冗余配置,特别在存储层面采用基于操作系统逻辑卷镜像的高可用架构,使单台存储故障时对业务透明。此外,协调软件开发部门改造应用中的单点设计,在中间层基础架构中引入了硬件负载均衡技术,采用对等式冗余设计,布置多套中间层应用,形成应用与数据库集群,提升系统处理能力和整体的高可用性。改造后的 ABIS 中间层运行平稳,系统标准可用率超过 99.999%。

目前,银行开放平台运维团队在基础架构建设中充分运用负载均衡技术、应用服务器集群技术、虚拟化技术、存储高可用技术及冗余技术等主要高可用技术,完整覆盖了系统架构中的各个层次,包括系统接入层、应用服务器层、数据库服务器层及存储层等,有效降低了由于单个设备可靠性低对系统服务连续性的影响。本研究成果目前已推广应用到某大型银行全行 36 家分行,取得了实际的经济效益。

(二) 自主建设开放平台生产集成管理系统

早期采用的监控管理工具包括 BMC 集中监控系统、AME 前置交易监控系统、MyAME 中间件系统监控软件、NBU 集中备份监控软件,这些工具功能单一,缺乏整合,信息无法共享,同时运维人员面对成千上万条告警信息缺乏有效的事件监控和诊断工具。这些不仅增加了运维成本和难度,而且无法保证快速有效的处置问题。

根据“快速响应、快速定位、快速处置”的运维理念,将开放平台治理模型的研究成果与银行总行开放平台的运维实际相结合,运维团队自主开发了开放平台生产集成管理系统(简称 OpenIMIS),同时根据开放系统运维出现的新情况,不断开发新功能,并集成到 OpenIMIS 中,从整体上实现了开放平台运维队伍专业化、运维工作流程化、运维手段自动化,推动运维工作从被动运维向主动服务的根本转变。

（三）电子银行系统的运维实践

电子银行系统部署于开放平台上,并直接面向客户提供基本金融服务,是对实时性、连续性和稳定性要求最高的系统之一。同时电子银行系统应用模块集中,架构庞大复杂,业务系统逻辑关联紧密,而开发和运维人员分处北京、上海两地,信息共享和人员协调的时空成本较高,客观上给运维工作带来更多困难。运维团队借鉴本书研究成果的相关理念,构建了完善的运维体系,很好地支撑了电子银行系统年均40%的业务增长速度。

首先架构上保证了高可用性,电子银行包括个人网银、企业网银、电子商务、手机银行、电话银行、客户服务六大类电子渠道类业务。每类业务对应的各子系统均采用统一框架开发,配置统一的基础环境,以提高整个电子银行系统的可扩展性和高可用性。除了满足系统横向扩展的要求,还为新的子系统保留扩展接口。交易均通过电子银行的总线服务处理发送到连接核心系统的各类网关系统,各类应用根据各自需要扩展前端应用服务器和基础环境。

其次,运维工作中以“主动运维”为指导方针。一是从应用系统投产立项开始,对架构设计和资源管理提出运维方面的建议。二是借助自主研发的集成管理平台,坚持全面的统一监控,对监控指标进行周期性统计,阶段性开展容量数据采集、数据分析、评估建模、预测及优化。三是标准化日常运维操作,及时规避技术风险和业务风险,主动识别风险和发现问题。四是在问题解决、日常变更和事件处理上遵循统一流程标准,采取精细化管理,统一运维视图,加强运维经验的知识积累,坚持重点问题分析与趋势分析,推进应用优化与架构整合。五是坚持以安全生产为第一要务,多举措落实“快速响应、快速定位、快速处置”的应急管理要求,如加强值班管理、优化监控质量,建立统一的运维视图,建立应急预案并开展应急演练等,整合各方运维力量,及时响应、科学处置,提升突发事件的处置效率。

最后,加强电子银行的风险防控。一方面,技术层面上,采取通过第三方对电子银行系统进行安全评估的方式及通过专业防攻击工具,周期性对电子银行系统的运维提醒进行考察,以针对性消除薄弱环节,并周期性优化方案,对体系进行加固。另一方面,加强风险防控管理,针对新出现的病毒和补丁更新,建立

定期更新制度。加强访问控制和密码管理,实行操作系统和数据库管理员的权限分离,对数据库的访问权限进行控制。对应用系统用户访问数据库采取最小权限原则。由于电子银行直接面向客户,且依托互联网,在安全上要求较高。在安全技术方面,通过完善的安全体系(包括CA系统、证书认证系统、动态口令卡系统等)保障客户端安全,并采用符合人民银行安全规范标准的专用安全设备构成安全体系,系统架构的网络安全层层递进以保障网络通信安全。

(四)全面提升开放平台系统的运维质量

在开放平台运维实践中,银行总行数据中心开放平台全面推进生产运行的标准化、规范化和精细化。开放平台的运维工作全面通过了英国标准协会BSI的ISO/IEC 20000-1:2005标准认证和ISCCC 27001:2005信息安全管理体系认证。

通过运维体系建设有效提升了开放平台运维效率和运维质量,逐步完成从被动运维到主动运维的转变。目前运维团队不足50人,运维的计算机数量超过3000台套,并且每年新投产项目增加迅速,开放平台系统数量年增长率超过30%,而重要系统的标准可用率已达到99.98%。

日常运维中,变更总量不断增加,变更成功率逐年攀升。开放平台变更数量年增长率超过45%,而变更成功率已达到100%。变更量的增加,一方面是因为系统数量的增加,另一方面则是主动运维导致的结果,主动运维通过变更来达到系统优化的目的,完善的变更流程则保证了变更的成功率。

围绕“三快”应急管理实践,运维团队梳理了应急场景并建立相应的应急预案,根据应用系统特性建立各系统的运维视图,每年应急场景演练覆盖率为70%,大幅缩短了应急情况下人员和资源协调的时间,提高了应急效率,应急时间平均缩短30%~50%。在事件的处理上,事件响应率和解决率不断提升,开放平台的事件响应率已达99.39%,事件的解决率已达100%。可用性方面,以电子银行系统为例,系统可用性不断提高。一方面得益于基础架构、开放平台治理优化及完善,另一方面通过应急管理体系的落地实施,应急事件的处理时间有效缩短。

构建全面的运维体系为运维工作长期发展打下扎实的基础,并从业务需求

视角进行 IT 风险管理。通过技术和管理两个方面防范操作风险,技术上应用安全审计平台加强用户痕迹管理,管理上职责和权限分离,使信息内部操作风险控制得到全面加强。生产运行标准化、规范化程度稳步提升,生产运行质量和服务效率进一步提高,逐步形成了符合银行数据中心管理目标的 IT 服务管理体系。

在互联网金融和大数据背景下,银行业在服务创新、竞争手段和经营模式上将出现巨大变化,大型银行开放平台的基础性支撑作用将得到进一步的凸显,科学智能的开放平台运维体系必将发挥更大作用。

目 录

Contents

第 1 章 引言	001
1.1 研究背景	001
1.1.1 银行业信息化现状	001
1.1.2 开放平台系统在银行业的发展与变迁	003
1.1.3 开放平台系统是银行信息化的重要组成部分	004
1.2 研究现状	006
1.2.1 开放平台的优势	006
1.2.2 开放平台引领业务作用凸显	007
1.2.3 银行业开放平台面临的挑战	008
1.3 研究目标及内容	011
1.4 研究整体说明	013
第 2 章 大型商业银行开放平台系统基础架构建设	015
2.1 开放平台基础架构的发展形势分析	015
2.1.1 集群技术	017

2.1.2	虚拟化技术	020
2.1.3	大数据技术	021
2.2	开放平台基础架构设计原则	023
2.2.1	高可用	023
2.2.2	可扩展	024
2.2.3	高性能	025
2.2.4	高安全	026
2.2.5	易维护	027
2.3	开放平台系统基础架构总体设计	027
2.3.1	总体目标	027
2.3.2	设计思路	028
2.3.3	物理架构	031
2.3.4	部署架构	033
2.4	开放平台基础架构建设主要内容	038
2.4.1	技术路线	038
2.4.2	工程实施	041
2.4.3	集中式运维管理平台	042
第3章 大型商业银行开放平台运维体系设计		044
3.1	开放平台运维对象	044
3.1.1	硬件设备	045
3.1.2	系统与数据	046
3.1.3	管理工具	048
3.1.4	人力资源	050
3.2	运维体系整体框架设计	051
3.3	运维体系设计目标及原则	052
3.3.1	运维体系设计目标	052

3.3.2 运维体系设计原则	053
3.4 运维体系设计内容	054
3.4.1 运维制度建设	054
3.4.2 运维流程建设	054
3.4.3 运维队伍建设	057
第4章 大型商业银行开放平台系统治理模型研究	059
4.1 制度管理	059
4.1.1 制度管理的必要性	059
4.1.2 制度管理层次模型	060
4.2 流程管理	061
4.2.1 事件管理	062
4.2.2 问题管理	063
4.2.3 变更管理	065
4.3 配置管理	066
4.3.1 配置管理的功能	067
4.3.2 配置项管理策略	070
4.4 容量管理模型研究	072
4.4.1 容量管理的概念及目标	072
4.4.2 容量管理的子流程	073
4.4.3 容量管理的建模	074
4.4.4 容量管理的实施	078
4.4.5 容量管理的指标	079
4.5 团队管理	080
4.5.1 运维团队的管理现状	081
4.5.2 运维团队的管理改革	083

第 5 章 大型商业银行开放平台应急风险管理体系构建	085
5.1 应急风险管理体系构建的总体原则	086
5.2 应急风险管理体系目标内容和运行机制	087
5.2.1 应急风险管理体系目标内容	087
5.2.2 应急风险管理运行机制	089
5.3 应急风险管理综合协调体系构建	090
5.4 应急风险管理模型设计与实践	092
5.4.1 应急风险管理模型设计	092
5.4.2 应急风险管理实践	103
第 6 章 大型商业银行开放平台系统风险防控体系建设	110
6.1 系统安全管理概述	111
6.1.1 安全管理方针	111
6.1.2 安全管理原则	112
6.1.3 安全管理框架	112
6.2 系统风险点识别	113
6.2.1 威胁识别	114
6.2.2 脆弱性识别	116
6.3 系统安全管理模型	117
6.4 系统风险防范措施	121
6.5 系统风险评估	128
6.6 其他风险与去 IOE 化	130
第 7 章 大型商业银行电子银行系统的运维实践	132
7.1 电子银行业务构成	133
7.2 电子银行架构体系	136

7.3 电子银行运维管理体系	139
7.3.1 监控全面化	141
7.3.2 任务流程化	142
7.3.3 运维主动化	148
7.3.4 过程自动化	151
7.3.5 团队管理科学化	152
7.4 应急风险管理和风险防范	154
7.4.1 电子银行风险分类	155
7.4.2 电子银行应急风险管理实践	156
7.4.3 电子银行风险管理实践	158
7.5 电子银行运维实践小结	162
第 8 章 研究总结和展望	164
8.1 研究总结	164
8.2 前景展望	165
8.2.1 互联网金融	166
8.2.2 大数据时代	167
参考文献	170
索引	175

第 1 章

引 言

1.1 研究背景

银行业是我国最早将信息技术引入业务管理的行业之一。从 20 世纪 70 年代末开始,银行的储蓄、对公业务等逐渐以计算机处理代替手工操作,标志着银行信息化的开始。进入 80 年代,我国开始大规模引进计算机技术,银行业率先广泛使用计算机系统,大大提高了业务处理水平。90 年代以后,银行业建立起一批网络系统,实现了全国范围的计算机联网,通过数据中心处理业务数据,人们切身感受到通存通兑带来的方便快捷。

银行业信息化建设在过去几十年中取得了巨大的成绩,目前各商业银行拥有世界先进水平的大型计算机、小型计算机、PC 服务器和刀片服务器等各类计算机,建立了覆盖全国的网络通信系统,开发了包括综合业务系统、经营管理系统等在内的应用系统,形成了比较完整的金融信息基础设施体系,国内上市银行基本实现了全行数据的集中管理和维护,提高了信息系统的整合应用能力,为业务发展提供了有力的支撑。

1.1.1 银行业信息化现状

当前,我国商业银行的信息化主要是基于核心业务处理的信息化,因此,信

息化对银行变革最大的作用在于推动了银行经营方式的变革,同时引入一些较为先进的经营理念来适应经营方式的变革。首先,满足客户需求的经营理念。客户需求是推动信息化发展的根本动力。其次,需要给客户提供多样化的服务和产品。新一代综合应用系统平台的建立使大规模的产品开发成为可能。银行产品由传统的柜台负债业务和贷款业务向综合性、多样化的产品转变,产生了代理国债、代理基金、代缴费、银行卡、托管资金、现金管理等多种中间业务产品,极大地改变了银行的经营方式。最后,银行作为服务行业,所有的工作都是围绕服务来进行的,如何开拓多元化的服务渠道,使服务水平高效化是银行信息化的首要目标。

(1) 银行信息化拓展了银行的服务渠道。由传统的柜面服务延伸到网上银行、电话银行、手机银行、银行卡、POS、ATM 等多种服务渠道,改变了银行的经营方式。银行信息化打破了区域、行际和时间限制,使得同城、异地、跨行存取款不再受到限制,资金能够实现实时到账,加强了服务效率。而在服务功能上,信息化又使得银行在提高了传统的存取款功能以外,还增加了多渠道的快捷查询、转账、对账、透支、综合账户、综合理财、外币兑换等多种功能,极大地扩大了服务范围,提高了服务质量。

(2) 科技创新水平成为商业银行的核心竞争力之一。科技创新帮助大型商业银行完成了业务流程再造、管理模式再造以及风险内控等。同时,通过科技创新,银行改变了过去以产品为中心的经营管理方式,全面转向了以客户需求为导向的发展模式。通过遍布全球的数万家营业机构、数十万台 ATM 和自助终端、几十万台 POS 机,以及强大的电子银行系统,大型商业银行可以在全球范围内为客户提供全天候、全方位的金融服务。同时,依托综合信息网络和强大的科技研发能力,大型商业银行正为客户提供越来越多样化的产品,进一步满足客户多元化的金融产品需求。特别是上市银行,科技创新水平与其市场地位是直接相关的。

(3) 信息化带来的潜在科技风险不可忽视。目前,国内主要商业银行均实现了全行数据的大集中,数据的集中也带来了风险的集中。银行机构运营的稳

健性和安全性,已不仅仅关系其作为一个法人组织的经济收益、股东权益和组织生命力的问题,更是一个关系着整个国家金融安全和社会秩序稳定与否的重大国计民生问题,牵动着整个国家和社会运行的每一根神经。一旦出现业务运营中断,将可能导致银行系统内部全国网点的业务停顿。这不仅会给银行机构带来直接的财务流失,还会对其多年树立起来的品牌效应和公信力造成恶劣的影响,更甚者将面临经济赔偿责任和法律制裁。为此银监会等监管部门出台了《商业银行业务连续性监管指引》等制度规范。银行的开放平台系统作为科技系统的重要载体,如何科学维护稳定运行,提高开放平台系统的运维效率,有效地防范科技风险,成为大型商业银行面临的新任务。

1.1.2 开放平台系统在银行业的发展与变迁

银行开放平台通常指除具有数据存储功能的大型主机之外的科技信息系统。随着银行信息化的推进,开放平台技术在银行业逐步得到广泛使用。开放平台技术在银行业的应用最早可以追溯到 20 世纪 80 年代,当时国内银行信息化还处于起步阶段,利用计算机将银行传统的手工工作电子化,实现柜台服务自动化,进而升级为基于服务器的中型联网,实现同城通存通兑。由于全国各地电信网络基础设施还不够完善,各家商业银行以省分行为单位建立了内部的信息系统,此类信息系统中开始有一部分搭建在开放平台系统上。之后,在网络技术的推动下,银行业逐步实施全行的数据集中,各商业银行将原先由各分行维护的业务数据系统上收到总行数据中心集中管理,实现了实时的通存通兑,并且做到全行业务的统一管理。

在这一阶段,股份制商业银行、城市商业银行、农信社等金融机构,由于其业务量相对较小,而大型主机系统费用昂贵,中小银行往往完全基于开放平台搭建所有的信息系统,核心银行账务均交由开放平台处理。以国有四大行为代表的大型商业银行在信息基础设施上采用大型主机与开放平台系统相结合的技术方案,大型主机系统负责核心银行账务处理,开放平台系统负责其他业务逻辑的处理。