文章编号：1007－5399（2018）06－0014－02

中国邮政储蓄银行推进运维自动化的探索与实践

张 帝，李庆华，胡学勇

（中国邮政储蓄银行数据中心，北京 100166）

摘 要：文章从数据中心所面对的监管要求、技术发展、内部治理和日常运维等方面出发，设计了整体性运维体系框架，对中国邮政储蓄银行推进运维自动化进行了探索，并指出了未来工作方向。

关键词：运维；自动化；灾备；风险；认证；权限

中图分类号：F61 **文献标识码**：A

中国邮政储蓄银行（以下简称“邮储银行”）数据中心承担着全行储蓄、信贷等近200套计算机系统，以及小型机、PC服务器、存储、网络等数万台设备的运行维护工作，存储着海量的数据资产，支撑着5亿客户、数万亿元的资金流和信息流运转，肩负着一线运营支撑保障，是邮储银行业务运行的中枢，也是邮储银行的生命线。信息系统的安全性、可靠性和有效性不仅是一家银行赖以生存和发展的重要基础，还关系到整个银行业的安全和国家金融体系的稳定。

1 实用性需求分析

1.1 遵从监管需要

依据银监会《商业银行数据中心监管指引》《商业银行信息科技风险管理指引》等文件精神，数据中心对于日常运维操作需要遵从最小授权原则，对操作人员、操作指令要做到可信，对所有操作尤其是变更类操作需要留痕等。为了将监管要求落到实处，数据中心需要从技术上对操作权限、操作指令、操作复核等环节进行限制，通过技术方式保障合规性和安全性，守住不发生系统性风险的底线。

1.2 适应开源技术广泛应用的需要

伴随国家“双创”战略的实施和互联网金融的快速发展，银行业传统的应用架构面临着高频交易、大并发的挑战。为了响应国家数据安全战略，需要对原有封闭的被国外公司垄断的IOE产品重新进行更替，兼顾银行业“十三五”规划中的云考核要求，邮储银行新建和改建的系统中大量应用开源产品，云计算、大数据等节点数量成倍增加。在运维人员保持不变的情况下，为了保证已有的运行维护质量，快速访问维护数量剧增的服务器，强烈要求运维手段自动化，以适应新技术在金融生产网中应用所带来的现实与潜在挑战。

1.3 跟进数据中心流程化治理的需要

目前，邮储银行数据中心正在积极推进ISO20000认证工作，需要对变更管理、权限管理等进行记录。虽然数据中心已建成运维管理平台、安全管理平台等系统，但这些系统相互之间彼此独立，数据信息无法交互，尤其对于各业务系统中自动执行作业的灰色地带，数据中心需要进一步融合现有资源，实现无死角全覆盖管理。

1.4 满足日常运维工作合规便捷处理的需要

数据中心运维人员的工作有着鲜明的特点。一是运维工作立足一线，要求快速处理事件单、问题单及变更单。处理共性的事件单需要频繁使用相同的工具，对工具执行效率和执行质量提出了更高的要求。二是计划内的工作远远多于计划外的工作事项，即使对于事件单，也基本上符合“二八”定律。基于上述两点，如果将80%的工作所需要的工具进行实例化，需要利用平台编制、审核、测试与执行，满足日常工作中的高频操作要求，同时兼顾平台自身的合规性及操作执行上的便捷性。

2 全局性应用架构设计

为把邮储银行建设成为一家资本充足、内控严密、营运安全、功能齐全、竞争力强的大型零售商业银行，2014版IT规划的IT愿景提出，将业务变革诉求与技术手段深度融合，通过科技引领实现弯道超车，为邮储银行打造体验和智慧并重的智慧型银行。邮储银行数据中心积极面对新需求与新挑战，借鉴业内成熟做法，完美融入中心内部操作流程和控制制度，全面衔接现有的运维管理平台、安全管理平台、灾备管理平台功能，打通信息交互通道，在现有运维体系支撑下全局性地设计和实现了运维自动化应用架构，见图1。

数据中心的核心运维体系包括灾备管理平台、安全管理平台、运维管理平台、综合监控平台和运维自动化系统5个组成部分，其中，安全管理平台、运维管理平台、综合监控平台在邮储银行数据中心已经使用多年，持续为生产系统的安全运行保驾护航。

2.1 灾备管理平台

主要实现生产系统应急流程管理和编排、应急演练排期与应急演练结果处理、人员管理等功能。它不直接与生产系统产生交互，是静态输入记录型系统，完成记录与报表处理等功能。在整个运维体系中，灾备管理平台充当着“指挥

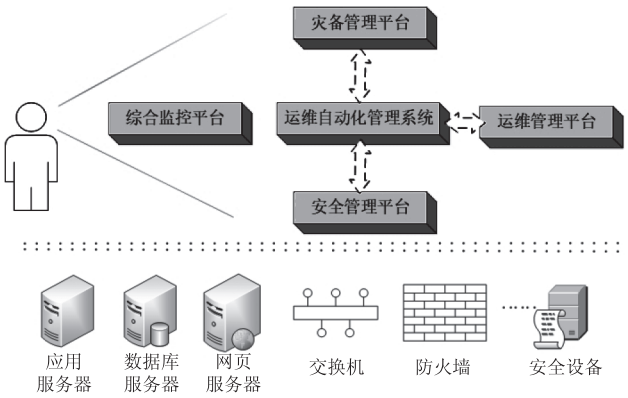

图1　数据中心运维体系全局性应用架构

中枢”的角色，向下指挥运维自动操作，充分发挥其编排功能；向上为指挥和监管服务，提供在线流程进度查阅和操作结果排查。

2.2　安全管理平台

这是数据中心所有生产系统用户的认证中心。操作系统级用户、数据库级用户和中间件级用户的认证工作都由安全管理平台负责管理。同时，安全管理平台是登录生产系统的唯一门户，负责登录会话管理与安全审计管理。在整个运维体系中，安全管理平台充当“千里眼”的角色，负责所有用户认证的工作，并具有第二道防火墙的功能，即只有安全管理平台配置范围内的权限，才可启动运维自动化管理系统中的调度任务。

2.3　运维管理平台

这是数据中心投产最早的运维管理、流程管控类系统，负责事件单记录、流程处理、变更审批等。在整个运维体系中，运维管理平台的“审批师”角色不变。站在运维管理平台的视角看，运维自动化也是一个类生产系统，给运维自动化管理系统增删改工具，相当于一次变更操作，需要执行完整的变更流程，在运维管理平台中进行详实的记录。除此之外，高风险级的自动化操作，相当于一次变更，如计划内的批量修改参数类操作，也需要在运维管理平台中进行记录，以保障运维管理平台中的变更记录全面、真实。

2.4　运维自动化

运维系统既包含任务设定、文件管理、作业编辑、工具箱维护、系统日常检查、运维操作等自动化操作功能，又具备操作行为审计、细粒度权限管理和报表供给等功能。它是整体运维体系中的自动化执行臂，既可完成周期性的定制化工作任务，又可对接灾备管理平台提供流程化的操作服务，打通自动化操作“最后一公里”。

3　运维自动化探索

伴随运维自动化的试用探索，数据中心整体运维体系实现数据流通和信息共享，已有平台与新建系统相互融合，展现出更加强大的功效性。

3.1　作业执行自动化，实现灾备管理平台一键式功能落地

运维自动化管理系统实现了灾备管理平台一键式切换功能的落地工作。运维自动化管理系统位于灾备管理平台与各业务系统之间，对上接收灾备管理平台下发的粗粒度操作流程指令，反馈执行进度，屏蔽各生产系统操作平台的差异性；对下将粗粒度调度指令具体化，保证操作指令有序执行。

3.2　认证处理集中化，化解因系统密码而引入的自动化短板

运维自动化管理系统与安全管理平台进行对接，实现登录环节的认证操作自动化处理，屏蔽操作系统用户密码、数据库用户密码等变更事项，在满足监控要求的情况下实现执行整体的自动化。

3.3　维护工具标准化，降低人为因素引入的运维操作风险

数据中心大量运维人员24小时不间断地维护着各业务系统稳定运行。日常运维工作中，基本上每个系统都有日常检查、故障排查等同类功能的工具。运维自动化管理系统可将这些通用工具进行汇总和共享，既提升了整体运维技能和工作效率，又降低了运维工作中人为因素引入的操作风险。

3.4　日常事项定制化，将运维经验有机纳入自动化巡检范畴

伴随业务的快速增长，系统数量急速增加，而运维日常检查的事项急剧上升。运维自动化管理系统具有定制化的特性，非常适用于日常检查事项不断完善、不断细化的场景。

3.5　脚本管理集中化，化解版本管理难题

脚本质量是工具安全执行的前提。运维自动化管理从脚本编辑开始进行脚本单一性管理，每一次执行向多台服务器发出的指令，其源文本有且仅有一套，强化了脚本质量及流程管理控制，提升了操作的安全性。

3.6　权限管理细粒化，实现各系统在工具级层面最小授权

权限约束了工具的执行人员、可见系统和执行影响的范围。为了将监管要求的最小授权落地，运行中每新增一个工具，都要在系统、人员、操作、风险和可见通道层级进行约定，保障用最小权限操作最适合的工具，实现风险控制。

4　结语

邮储银行在自动化运维阶段，将在技术与流程上同向发力、共同推动，进一步提升运维工作的合规性和时效性，解决技术进步给运维工作带来的新问题、新烦恼，满足新环境下运维工作的新需求。自动化不仅是工具执行的自动化，还有管理流程的自动化、数据流动的自动化等。数据中心将继续遵循行业最佳实践，继续跟踪技术最新发展趋势，在运维工作中夯实自动化的基础工作，助力银行数字化转型。

收稿日期：2018-05-08

作者简介：张帝（1978～），男，内蒙古赤峰人，博士，主要从事运维管理、数通网络、数据相似性等方面研究；李庆华（1959～），男，天津人，硕士，高级工程师，主要从事数据中心规划、治理、建设和运行维护管理研究；胡学勇（1971～），男，山东诸城人，硕士，主要从事数据中心系统、网络、动力规划建设及运维管理研究。