DIGITAL OPERATION MANAGEMENT

数字化运维

2022年刊 总第五期

01
聚焦-智能运维
智能运维国家标准解读
中国建设银行智能运维建设实践分享
2020国内智能运维现状调研

前沿观点与技术研究
ITSS 5.0解读
自定义监控采集平台实践
数据中心绿色运维助力碳中和
02

行业洞察
工业互联网平台运维人才培养
攻防演练中运维主动防御实践
03

新华三集团

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

www.h3c.com

Copyright © 2022新华三集团 保留一切权利
免责声明：虽然新华三集团试图在本资料中提供准确的信息，但不保证本资料的内容不含有技术性误差或印刷性错误，
为此新华三集团对本资料中信息的准确性不承担任何责任。新华三集团保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。
CN-223X30-20220429-BR-SD-V1.0

数字化运维
OPERATIONS

主办 新华三集团

出版人
于英涛 / 尤学军 / 毕首文 / 陈孝毅 / 杨　玺
刘新民 / 李劲松 / 王　斌 / 曹东升

策划与监制 汤海华 / 叶璐

主编 陈静

本期编辑 刘岩 / 王萌 / 张晶晶

外部专家
包航宇 / 陈　贺 / 陈宏峰 / 秦明焓

编委会成员
丁　峰 / 方卫国 / 伏三强 / 耿　亮
郭世龙 / 何洪团 / 胡在亮 / 黄　鹏
黄晓容 / 贾　晗 / 蒋三庆 / 李　富
李　光 / 李国宝 / 刘嘉嘉 / 尚琪杰
舒中华 / 铁　婧 / 汪　东 / 汪　宏
汪　军 / 王　磊 / 张利兵 / 赵鸿生
赵俊华 / 郑圆圆 / 钟　果

版权声明

本刊所有文章除注明转载外，版权归新华三所有。欢迎转载，请注明出处。

免责声明

虽然新华三试图在本资料中提供准确的信息，但不保证本资料的内容不含有技术性误差或印刷性错误，为此新华三对本资料中信息的准确性不承担任何责任。

任何意见或建议，欢迎与本刊编辑部联系。

投稿和建议邮箱

NewITOps@h3c.com

PREFACE 卷首语

2021年10月，经过20余次线上线下会议，650余人天的研讨和集中编制，由新华三参与编制的《信息技术服务 智能运维 通用要求》（T/CESA 1172—2021）团体标准正式发布实施。该标准提出了智能运维的能力框架，明确智能运维所需要的组织治理、智能运维场景实现和能力域的通用要求等。今年标准编制小组也将围绕各分主题进一步细化、完善相关的内容，为智能运维国标的发布做好准备，为企业智能运维的能力建设提供进一步的指导。

回首来路，IT运维走过纯手动运维、平台化、自动化的进阶之路，也一直在通过流程化、规范化不断提升运维效率，保障运维质量。但随着数字化业务转型趋势的到来，企业对SLA的要求越来越高， IT规模亦不断扩大，架构复杂度日趋增高，运维仍有“力不从心”的感觉。另一方面IT运维天生拥有海量数据的特质，这为AI+奠定了良好的基础，而如今随着大数据平台、机器学习等关键技术的日臻完善，智能运维势必应运而生，趁风而起，成为运维领域未来一段时间的重点的发展方向。

本期《数字化运维》聚焦智能运维，内容既包含最新标准的解读，也囊括了智能运维相关技术的发展现状和方向，乃至新华三智能运维的观点和实践，力图成为展示智能运维全局的一个浓缩窗口。

当前，智能运维已成千帆竞渡、百舸争流之势。新华三集团身为一家专业的IT运维管理服务商，也一直致力于分享运维实践与国内外理论经验，数次与业界共同开展智能运维相关课题研制，积极推进智能运维国家标准的修订工作；还曾多次获得国际智能运维（AIOps）挑战赛冠亚军和“IT管理和运维产品”等业内大奖，并持续将前沿的智能运维算法和技术落地在统一运维平台U-Center上，用AI技术提升IT运维的风险控制能力和服务效率，推进运维自动化、智能化演进，护航百行百业的数字化转型。

有人曾这样描述“人工智能就像一列火车，它临近时你听到了轰隆隆的声音，你在不断期待着它的到来。它终于到了，一闪而过，随后便远远地把你抛在身后。”智能运维的脚步亦是如此，我们当下能做的就是躬身入局，赶上这趟数字化的时代列车。

毕首文

目录

CONTENTS

01 聚焦–智能运维

智能运维国家标准解读 1
中国建设银行智能运维建设实践分享 7
2020国内智能运维现状调研 12
数智革新引领IT转型升级 15

02 前沿观点与技术研究

ITSS 5.0解读 23
SRE减少琐事的妙方 29
自定义监控采集平台实践 35
数据中心绿色运维助力碳中和 41
RPA技术及在生产制造业的应用 45
即服务 自服务——HPE GreenLake Central 前沿方案概述 53

03 行业洞察

城市商业银行网络运维自动化趋势与实践 59
富国基金统一资产管理平台（CMDB）落地经验 64
如何提供安全的远程运维服务 67
工业互联网平台运维人才培养 72
攻防演练中运维主动防御实践 78
AIO服务助力移动公有云运维质量提升 83
数字化时代如何进行业务故障定位 91
新型医保云容灾最佳实践分享 103

04 最佳实践

VMware vSphere虚拟化平台规划与性能优化最佳实践 109
IT管理外包项目交接维管理实践 114
北京大兴国际机场网络运维创新实践 122
江苏移动，运维在云上 129

05 资讯动态

资讯动态 131

智能运维国家标准解读

文/包航宇

技术应用 日新月异

自2003年谷歌大数据“三驾马车”论文发表至今，大数据技术已历经10余年，得到大规模的普及。机器学习、深度学习、知识图谱、因果推理等算法与模型的应用为从海量数据中挖掘价值提供了更高级的手段。在数据中心，随着微服务、容器的使用，应用朝着小型化、隔离性和动态性方向转变，云、混合云、虚拟化、SDN/SD WAN改变了监控方式和数据获取方式……普惠算力更易获得，AI技术羽翼渐丰，技术的飞速发展为运维场景中的创新应用提供了更为广阔的舞台，数据中心的数智化进入加速发展阶段。

时代强音 催人奋进

《2020年政府工作报告》明确提出“加快5G网络、数据中心等新型基础设施建设，加强人工智能、大数据技术的融合发展”。《2021年政府工作报告》再次重申：“推动产业数字化智能化改造，战略性新兴产业保持快速发展势头”。新发展理念要求以技术创新为驱动，基于信息技术发展为企事业提供数字转型、智能升级、融合创新等服务，这为数据中心转型创造了契机。运维组织必须制定清晰的战略，深入挖掘新基建应用场景，补齐短板、构建新能力、提升用户体验，才能更好地拥抱数字化时代的到来。

运维转型 时不我待

早期的运维工作大部分靠人处理，或者编写脚本执行，属于手工运维。在工具化运维阶段，建设模式基本以烟囱式为主，每个烟囱只为解决单一的运维场景，如主机监控、数据库监控等。随着新技术的不断应用，IT基础设施与架构越来越复杂，非标准化的建设模式难以满足集中式运维的要求，这时ITIL作为最佳实践引入到数据中心，为运维管理提供指导框架，同时以国外厂商主导的各类流程自动化工具大行其道，各项活动变得相对体系化和规范化。但由于IT运维系统的厂商、架构各不相同，彼此之间没有统一的接口可以高效交互，数据规范和格式的差异也给流程和工具的打通造成障碍，为此，运维开始向着平台化、一体化的数字化运维方向演进。随着数字化转型的深入，IT规模急剧膨胀、监控对象和指标快速增长、依赖关系变得错综复杂，大规模、分布式架构的演进也增加了运维的难度。同时，数字化经营的业务比以往更加关注用户体验，监管机构对于安全、业务连续性等方面的要求也日益严格，种种压力都需要数据中心这个底座来承接，迫使运维部门不得不从被动救火式运维向主动运维转型、从问题驱动向价值驱动转型、从制度和流程为主向数据与算法为主的智能运维时代迈进，这不仅仅是技术能力的转型更是运维体系化思路的转型。

图1 运维的发展历程

产学研用 擿埴索途

于是，国内的用户、厂商、高校和研究机构开展了大量的智能运维理论研究和实践，然而由于缺乏统一标准和框架指导，应用效果参差不齐，许多疑惑亟待回答：到底什么才是智能运维？智能运维与传统运维的区别在哪里？……

勠力同心 砥砺奋进

终于，大家盼来了一个重要的里程碑：2020年10月智能运维国标工作组正式成立，来自金融、交通、能源、高校、研究机构和厂商等产学研用各界50多家企业的上百名专家聚到一起，先后召开会议40多次，消化各方意见400多条，累计投入1000多人天，不到一年时间就发布了阶段性成果——3万余字的T/CESA 1172-2021《信息技术服务 智能运维 通用要求》团体标准，填补了国内该领域标准的空白。同月，《信息技术服务 智能运维 第1部分：通用要求》获得了国家标准化管理委员会颁发的国标计划号，比预期快了半年时间。同年12月，国家十个部委联合发布了《“十四五”推动高质量发展的国家标准体系建设规划》，明确指出“推动智能运维等领域重点标准的制定工作”。这一系列成果的背后，是智能运维国标编委们苦思冥想的投入、上下求索的坚持和敢为人先的情怀与抱负。打破了人们心中只有欧美国

家才有能力制定创新领域标准的固有印象，改变了中国人只会具象演绎而不擅长原创性、系统性研究的传统认知，实现了中国“运维人”从跟随到引领的跨越。

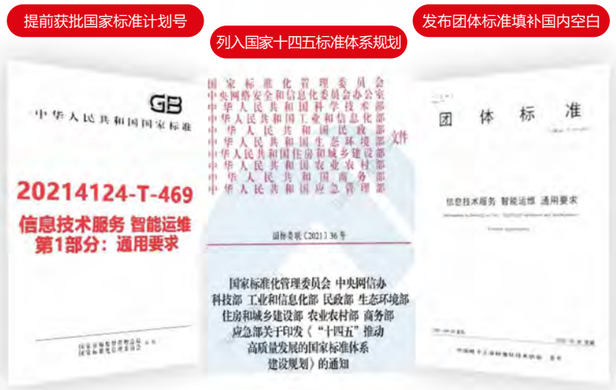


图2 智能运维标准研制成果

学无遗力 功夫始成

一路所思所见所想，凝练成智能运维标准的“三驾马车”框架：以组织治理为引领，以场景实现为中心，以能力域构建为支撑。

智能运维能力框架（如图3所示）包括组织治理、智能特征、智能运维场景实现、能力域和能力要素，其中能力要素是构建智能运维能力的基础。组织在组织治理的指导下，对智能运维场景实现提出能力建设要求，开展智能运维能力规划和建设。组织通过场景分析、场景构建、场景交付和效果评估四个过程，基于数据管理能力域提供的高质量数据，结合分析决策能力域做出合理判断或结论，并根据需要驱动自动控制能力域执行运维操作，使运维场景具备智能特征，提升智能运维水平，实现质量可靠、安全可控、效率提升、成本降低。

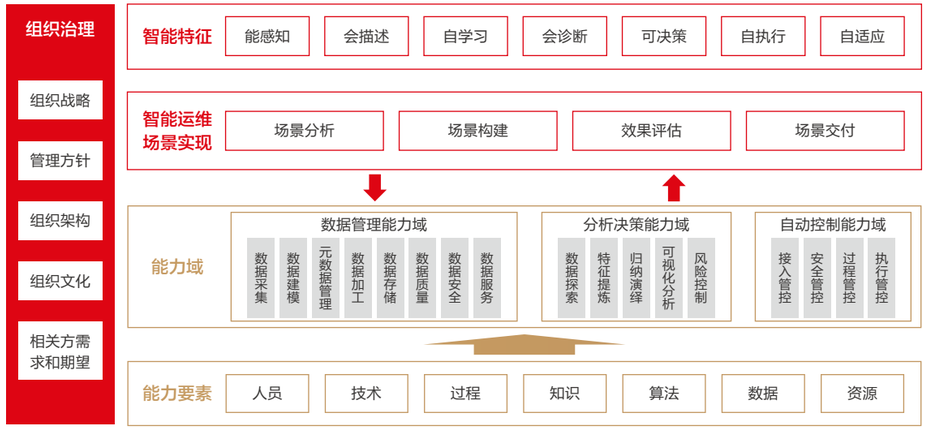


图3 智能运维能力框架

三驾马车之能力构建

不确定性的本质是信息约束条件下人们有限的认知能力，人类社会的发展一直伴随着对确定性的追求，确定性是行为能够被预测的前提，也是我们安全感的来源。化解不确定性首先是理解和认知世界运行的规律，从龟甲占卜到宗教传播，从电灯发明到万物互联，人类在生存、发展的过程中不断理解和认知着事物运行的规律，根据规律进行判断和预测，再将决策付诸于行动，从而把不确定性转化为确定性，感知力、决策力和控制力之间的相互作用构成了人类文明进步的内在动力。智能运维，正是我们在运维领域复杂的数字生态系统中面对不确定性时做出的必然选择。

感知力：在数字化的世界里，我们通过数据的流动和消费来化解不确定性，因此智能运维构建的感知力主要在于采集、处理、存储和共享各种运维数据，相当于运维的“眼睛”；决策力需要以感知到的数据作为输入，以便做出实时的运维决策，以便驱动自动化的操作；控制力根据运维决策执行具体的操作，优化资源配置效率，为工作提质增效。

决策力：需要指出的是，传统运维方式中，数据大多用于单一场景和一次性消费，很多企业对运维数据治理没有给予足够的重视，但随着运维数字化程度的提高，数据质量成为了突出的问题。可以说，运维数据的质量直接决定了运维智能化的水平。一旦有了高质量的运维数据基础，基于运维数据的分析和决策就成了智能运维场景建设面临的新课题。分析决策的能力可以通过基于海量数据的机器学习得到，也可以通过运维专家的经验和知识获得，有了分析决策能力，就能根据需求做出合理的判断或结论，并驱动自动控制能力执行运维操作，它是智能运维的“大脑”。

控制力：要想将从分析决策能力中得到的判断结果与各个工具、流程有效地联动起来，就离不开强大的自动控制能力。自动控制能力是大幅提升运维工作效率的关键，它相当于运维的“手”和“脚”，不仅可以替代人工来执行大量重复性的日常工作，还能促进运维操作的标准化，提高运维流程的可控性，并将运维知识进一步固化和沉淀到数字系统中。

数据管理、分析决策、自动控制这三大能力域支柱，能够很好地满足各种个性化智能运维场景的建设需求。同时，每个能力域中包含了多个能力项，而每个能力项最终又是由人员、技术、过程、数据、算法、资源、知识这七大能力要素组成的。

一个完整的场景建设过程，应该基于数据管理、分析决策、自动控制能力域的充分评估，提前确定待建设的能力项和待提升的能力要素。就是说，在构建智能运维场景前，先要全面梳理从场景到能力域、能力项、能力要素之间的关系，统筹考虑、全局谋划，制定合理且可行的智能运维场景建设方案。在这个过程中，场景是抓手，没有场景的建设方案是不可行的；能力是底座，构建能力项要特别关注其通用性、组合性和可复用性。只有同时兼顾“自上而下的场景驱动”和“自下而上的能力支撑”，才能真正把智能运维场景建设好。同时，智能运维场景的实现与能力域之间是相辅相成的映射关系，场景实现的四个关键过程实际是智能运维能力域能力循环迭代实现的步骤，每一项能力的提升都需要四个过程循环一次，多项能力提升是需要四个过程经过多次迭代循环而完成。

智能运维不是新技术的照搬引入，也不是运维场景的简单堆叠，而是体系化思想的生动显现。如果把数据中心的运维比作一棵树的话，那么地表下面就是数据管理、分析决策和自动控制这三根粗壮的根系，汲取着云计算、大数据、人工智能等新一代信息技术土壤的滋养。正所谓“道生一，一生二，二生三，三生万物”，中国思辨哲学的精髓构成了向上生长的主干，通过业务和技术融合、稳态与敏态融合，将三大能力供给到各种运维场景的枝干中，绽放出具备能感知、会描述、自学习、会诊断、可决策、自执行、自适应等智能特征的花朵，收获质量可靠、安全可控、效率提升、成本降低的运维成果，支撑企业的长久、稳定和繁荣发展。下面，我们就围绕场景构建和融合运用来说一说。

图4 智能运维生命之树

三驾马车之场景实现

所谓运维场景是实现具体运维目标时所需的人员、活动与对象的组合。而对于智能运维来说，其场景无穷无尽，不胜枚举。比如，多个场景可以组合成混合场景，混合场景也可以拆分成多个单一场景分阶段实现。因此，如何以合适的颗粒度拆解场景涉及到的具体活动，就显得非常重要。

首先，需要根据场景复杂度、技术实现难度、数据质量情况、资源支持情况、需求紧迫性等，明确场景构建的阶段和步骤；其次，可采用列举、分析、归纳等方法，识别场景建设的运维角色、运维活动、运维对象、智能特征等；另外，设立可评估或可量化的指标，如故障发现准确率、平均故障修复时间等。

智能运维场景建设可以借鉴，但很难复制。究其原因，是因为大家看到的智能运维场景，只是冰山一角的表象。想要真正建设一个智能运维场景，需要做好大量基础性工作，比如企业架构设计、开发日志规范、运维数据治理、服务流程改进、专业队伍建设。然后通过场景分析、场景构建、场景交付、效果评估四个关键过程，并持续迭代调优，不断提高场景的智能化水平。

三驾马车之组织治理

传统模式下运维工具大多是分散建设，缺乏统一的标准和规范，容易造成信息孤岛和数据烟囱，无法形成合力，最终跨不过质效跃升的门槛，因此必须消除数据的壁垒，打通相关的流程，实现数据在工具间无障碍的流动。同时，随着数据的连接、人机的协同、能力的交融，势必引起流程、组织、职能、标准等方方面面的变化，这已经不是靠单个团队竖井式的管理能够搞得定的了，顶层规划、统筹设计、组织级别的保障是实现智能运维建得牢、用得好的必要条件。

顶层设计：在智能运维的建设过程中，场景和需求会从各个方面涌现出来，如果依赖各自为政的开发模式，没有进行数据的整合、技术的沉淀和能力的共享，就必然会出现大量重复建设并增加后续迭代的复杂度，造成前台“烟囱林立”、后台支撑乏力的困局，激发需求和开发的矛盾，最终落下一个用不好、不好用的差评。因此智能运维应当作为“一把手工程”从组织层面统筹规划和协调。

统筹实施：规划应分为近期、中期和远期，明确各阶段的工作任务、落实责任人、执行计划和评价指标，确保每项任务可执行、可追踪、可验收。场景化的建设方式需要融合应用众多智能运维技术和能力，需要消除数据壁垒、打通流程和工具，因此常态化的架构、需求管控等就特别重要了。确定目标后，就要集中优势力量进行攻坚了，尽快取得成效并迭代优化，利用产品思维做好推广宣传，真正听到和解决用户的反馈。

创新激励：智能运维是“给自己做鞋子”，舒不舒服得问自己，因此需要在组织内部针对智能运维的建设和使用建立起广泛的主人翁意识，譬如：建立柔性工作团队等协作机制，通过开展DEMO设计、创客演说等活动营造创新氛围，发动运维人员参与需求分析、开发测试等活动，通过建立沟通渠道及时获得用户的吐槽、建议及需求，对于贡献突出的人员给予激励等。这正是以人为本、管理和技术并重理念的体现，使运维人员在智能运维建设过程中创造价值、转化角色、提升能力。

风险防范：技术的便利也会带来风险与挑战，随时随地按需接入使得边界更加模糊，集权类系统一旦失控将会造成巨大的危害，因此必须加强风险防范，争取早识别、早预警、早处置，做好智能运维手段失效时的补偿策略和应对方法。同时，科技封锁和技术打压正在不断升级，例如俄乌军事冲突后，西方采取从SWIFT系统中剔除俄罗斯等措施进行制裁和围堵，为我们再次敲响了警钟。因此，我们应当积极响应国家号召，有序开展国产技术的应用，并做好知识产权保护，勤于实践、敢于挑战、勇于创新，筑牢这道护城河。

科技伦理：随着智能化的推进，AI的信任危机不可避免地出现了，对于我们有三个方面需要重视：一是数据，应当正确选取数据的属性和特征用于模型训练，确保数据标注的安全合规，避免产生系统性偏见和信息茧房等问题；二是算法，应当兼顾可解释性和决策有效性，审慎引入模型和算法，加强对黑箱风险的监控和防范，确保正当与公平；三是应用，应在符合认知、道德、伦理、法律的框架下，建立AI技术引入、实施、应用、验证等全流程的风控机制，提供偏离报警、纠错和关停的手段。

大道行思 履践致远

新一轮科技革命和产业变革促使社会结构、价值体系、生产消费方式不断变迁，推动着技术赛道的变更和发展范式的改变，百年变局百年难遇，机遇稍纵即逝，抓不住就有被时代抛弃的危机！习总书记提出“加快发展新一代人工智能是事关我国能否抓住新一轮科技革命和产业变革机遇的战略问题”，智能运维标准的编制，正是对国家战略的积极践行。一方面，它明确了运维智能化建设和运营的要求，填补了这一领域的空白，增强企业在智能运维方面的规范性，起到支撑和引领作用；另一方面，它也促进了运维高端领域的专业性交流，拓展了创新思路，对打造智能运维产业生态、带动上下游企业协同发展产生积极作用，也必将为信息化领域“双循环”格局的构建和中国数字经济的发展做出更大的贡献。

知大势，行致远，我们在智能运维的大道上一起向未来。

中国建设银行智能运维建设实践分享

文/转载自《中国智能运维实践年度报告2020》

2019年起，建设银行运营数据中心践行金融科技战略，以项目群方式启动了智能运维体系建设。我们基于建设银行新一代工程设计理念，以运维数据为基础，以自动化实施、智能数据分析为支撑，打造具备“安全风险管控、快速业务响应、高效运维交付和标准运营支撑”四大能力的全方位数字化运维应用，旨在构建金融行业最佳运维管理能力，为数字化经营保驾护航。

经过两年多的探索与实践，建设银行运营数据中心完成了流程与工具的全面打通，实现了端到端的自动化，投产效率成倍提升；实现了毫秒级采集、1秒级运算能力，监控与预测更加精准；规范了主要系统的配置信息及架构数据，夯实了数字化底座。具备感知力、控制力、决策力的企业级智能运维体系初步建成，有力保障了建设银行信息系统的安全稳定运行和集团业务的稳健发展。建设银行在取得智能运维实践成果的同时，也带动了周边运维生态的发展，在智能运维标准赛道上率先发声，牵头推进智能运维国家标准建设，实现运维能力从跟随到创先的跨越。

未来，我们将秉承自主可控的要求，发挥“企业级”融合统一的特点，对内建设持续进化型智能运维、保障稳健运营，对外拓展开放共享型运维生态、实现创新发展，建设具备安全稳定、自主可控、弹性敏捷、高速连接、绿色智能、融合共享6大特征的新型数据中心。

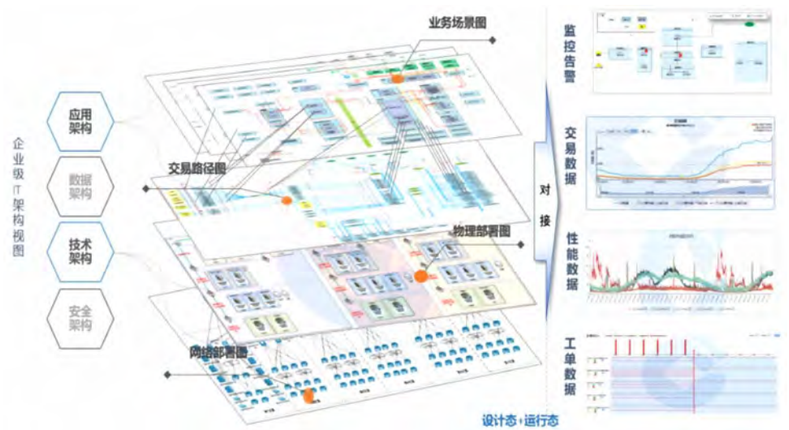
架构视图——打牢数字基座

背景

基于企业级架构，建设银行通过技术和管理创新，突破性地解决了IT架构数字化、可视化及管控能力不足的问题，搭建企业级IT架构数字化管控及展示平台。

解决方案

构建架构数据自动采集解析与人工设计相结合的架构数字化能力；形成一套与IT系统开发、测试、生产相结合的架构常态化管控机制；利用可视化、大数据技术实现IT架构资产以及运行态数据的全景视图展示；串接从业务规划、架构管控、开发设计、测试投产、生产运维全领域应用。



实践成果 / 收益

通过架构视图系统建设，有效提升了建行IT架构数字化水平，保证企业级战略高质量落地实施和可持续性地发展，推动运维模式的改进和效率的提升。主要建设效果如下：

■形成了统一的IT架构视图数字化模型及视图设计标准，构建以监控、配置及流程管控为一体的架构资产数字化能力，打通了业务应用、系统及基础设施的关系，实现架构设计“书同文、车同轨”。

■有效融合架构信息和运维信息，以场景化的模式汇聚系统、工具及基础设施信息进行可视化展示，实现重要应用场景的场景化监控及应急展现。

■构建应用架构的数据治理体系，建立并在全行推广了交易线主动检核及常态化闭环管控方法，完成了上万条交易线的治理，识别慢交易、失败交易，推动架构资产数据质量的提升和精细化整改。

■实现企业级项目总体架构图和作战地图的在线编辑和展示，确保各作战单元提供端到端的协同作战能力，支撑企业级项目的架构设计、分析决策、可视化应急等场景应用，推进企业级架构数字化。

精细化监控能力——识别运行风险

背景

随着银行系统的分布式架构转型和上级监管要求的提高，故障的发现与处置需要更加及时和灵敏，对于监控来说，就必须要提供更精细化、更全面的监控及分析能力，并具备实时的监控能力、快速的告警能力和故障分析能力，以满足重要交易系统早发现早处理的监控要求。

解决方案

建设银行的精细化监控能力，包括以下三个方面：

实时监控能力：具备全面覆盖的秒级指标监控能力，计算能力达到毫秒级采集、一秒级计算，提供能够准确评价系统运行情况的指标体系（每秒交易量、成功率等），并能覆盖各种计算维度（子系统维度、AP维度等），保证全面、快速地发现系统运行异常。

全面告警能力：通过通用与特色相结合的告警规则体系，达到覆盖各种情况的系统异常场景。制定标准化的通用告警套餐，对普通交易运行情况进行监控，在此基础上，针对一些系统的交易特性，提供小样本类型交易累积告警规则、窗口累积类型的告警规则以及告警自适应升降级规则，以满足不同类型的系统对告警策略的个性化需求。

故障分析能力：基于已经采集的交易数据，提供了多种监控查询分析方式，如监控指标视图趋势图、单笔链路跟踪、根因辅助分析等。监控指标趋势图提供全维度多层级的查看能力，帮助用户在发生故障时迅速缩小排查范围；单笔链路跟踪功能提供单笔交易的完整链路追踪能力，除了能查看系统间的调用关系，还能查看系统内的服务间调用关系，能够快速确定故障影响范围以及故障所在节点；根因辅助分析帮助用户迅速确定故障可能发生的根源系统及根源对象，并辅助展示与根源系统有关的软件、硬件等相关设备运行状态，以提升应急过程中的排查效率。

实践成果 / 收益

在提升了监控的精细化水平以后，目前监控系统已经成为建设银行故障发现及问题处置过程中必不可少的工具。

目前监控系统能够为各重要系统提供秒级监控能力，日数据处理能力达到TB级，指标计算时间控制在一秒内，可以更快地为用户提供各维度统计指标数据，并为可视化大屏展示提供了有效的数据支持；提供多种类型的告警策略，支持不同类型系统的个性化告警定制策略，能够快速全面地识别出系统异常场景并通知用户，保证无漏告、少错告、高灵敏告警能力；提供强大的故障分析能力，包括单笔交易的链路追踪能力、监控指标各种视图展示能力及根因分析能力，在应急过程中提供有效的分析及故障定位功能，极大的提高了日常应急效率，降低了故障根源定位所花费的时间。

动态告警定级——提升运维效率

背景

在实际生产环境中，由于在线服务的复杂性和动态性，系统会生成大量告警，亟需一种准确的、自适应的告警定级算法，对告警进行严重性排序，把严重的告警推荐给运维工程师，以便快速发现潜在的故障，缩短修复时间。实现这个目标的挑战有以下几点：

- 告警数量大、种类多
- 数据标注难以获得
- 系统具有复杂性和动态性
- 数据不均衡

解决方案

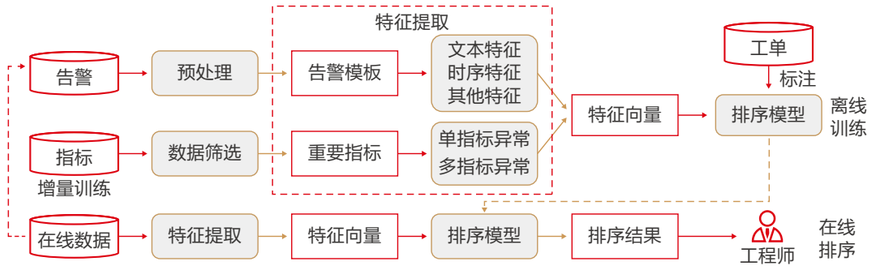
动态告警定级方案分为离线训练和在线排序两个模块，如下图所示。该方案的主要创新点是：

■首次围绕告警动态定级问题提出了基于机器学习的智能运维解决方案；

■利用历史事件工单和告警处置记录，自动给每条历史告警标注严重性分数，有效解决了无法对海量告警——手工标注的问题；

■抓住告警数据的特点，采用数据融合和特征融合的思想，从告警数据和指标数据中提取了一系列可解释的、有物理意义的特征来区分告警的严重性；

■将告警动态定级问题建模成推荐排序的问题，根据模型给出的告警严重性排序，优先为运维工程师推荐严重告警。



实践成果 / 收益

通过历史大规模告警数据的测试，验证该方案可以准确地推荐严重告警，平均准确率和平均召回率分别超过86%和91%。实验证明，该方案中设计的两部分特征（告警特征和指标特征）都是必不可少的，对结果都有较大的贡献：增加告警特征，平均准确率可以提升40%；增加指标特征，平均准确率可以提升约10%。同时，和基于规则的定级方式相比，该方案省去了手工制定和维护规则的时间，并且能够更准确地识别严重告警，减少了处理无效告警而浪费的时间，节约了人力成本，提高了运维效率。

智能运行分析——支持业务发展

背景

近年发生的重大生产事件中，变更实施和容量耗尽引发的问题占比非常高，很多大型故障在发生之前都有潜在的隐患持续发生，但是受当前的监控手段所限，对于持续发生的潜在隐患无法进行有效识别。随着运维体量不断扩大，精细化管理要求不断提高，对运行风险识别能力、扩展风险识别手段等方面提出了更高的要求，需要更有效地识别运行风险，延长系统平均无故障时间。另一方面，随着人工智能技术手段的丰富和对智能运维场景理解的深入，综合各种智能手段去满足智能运行分析的条件也愈加成熟。因此，我行建立了智能运行分析系统，对版本投产后、基础设施变更后的风险、容量瓶颈风险以及特定场景（重大节假日系统容量预测）的风险进行识别，综合保障系统的安全稳定运行。

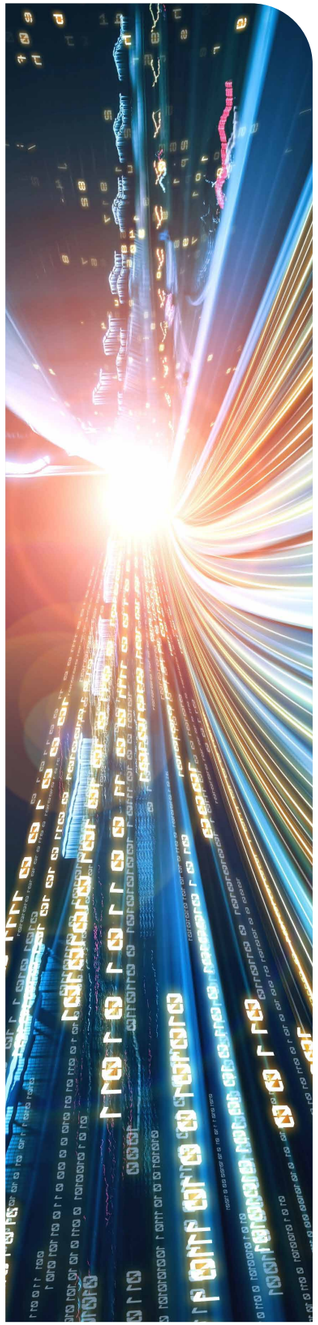
解决方案

由于版本投产、基础设施变更导致的事件占比比较高，所以重点对变更后的风险进行识别。结合智能运行分析手段，针对性地设计版本投产后的风险识别检查组合，在版本投产完成后、版本投产后的几个小时、版本投产后开门前等多个常见故障时间点，进行智能变更风险识别，更早地发现和解决问题，控制问题影响范围，提高版本投产效率。

在变更后的每一个风险识别检查点，对本次变更涉及到的应用和基础设施指标进行预处理和特征描述，提取指标的一些特征信息。数据预处理主要是对指标进行指标内异常点的剔除和指标缺失段的判断与修复。特征描述是通过特征工程提取时间序列的分布、形状、波动和周期性等特征。基于提取的特征，运用多种基于时间序列的智能风险识别手段，如指标比对检测、突变模式识别、离群机器检测和短时高频趋势预测，来对当前的运行风险进行综合诊断和发现。

实践成果 / 收益

我行建立的运行风险识别体系和多种智能运行分析手段，在实践中能够帮助运维人员更早地发现和解决问题，控制问题影响范围，从被动运维转向主动运维。特别是版本投产后的变更风险识别，通过版本投产后进行的指标比对，可以及早地发现交易、基础设施资源指标的显著变化，以及由于配置问题导致的离群机器问题。针对部分网联重大版本投产后的指标和离群比对，最早可以在版本投产后的分钟级内发现隐患。针对业务系统重大节假日的容量风险进行识别，提前发现容量隐患，便于应用管理员提前准备相应扩容方案。目前容量长时预测准确率可达到90%，短时预测准确率可达到96%。

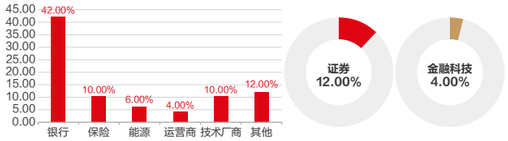


2020国内智能运维现状调研

文/转载自《中国智能运维实践年度报告2020》

本次调研共收集50家单位的智能运维实践现状，调研单位主要分布北京、上海、浙江、广东、云南、四川等地区。

参与调研单位概览

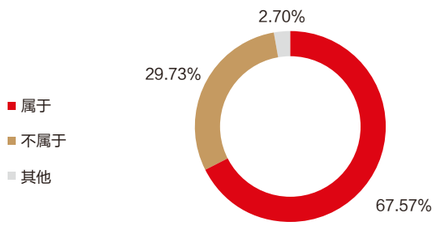


本次调研单位主要来自于银行、保险、券商、金融科技、能源、技术厂商、运营商、政府机关等。

在运维领域，智能运维包含自动化运维的认知在增强。

这是智能化运维内涵逐渐增强，外部环境愈加复杂带来的认知变化。

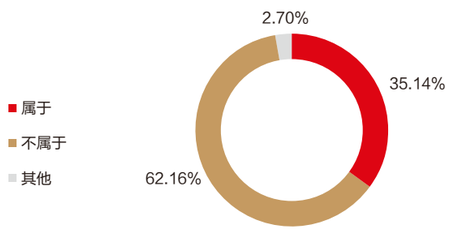
自动化运维是否属于智能运维?



满足智能特征的运维才能被称之为：智能运维。

智能运维并不仅仅是某个或某几个算法的落地。

只有基于AI算法的运维能力才叫智能运维



从各家急需提升的能力来看，智能运维的基础–运维数据治理和传统运维能力首当其冲。

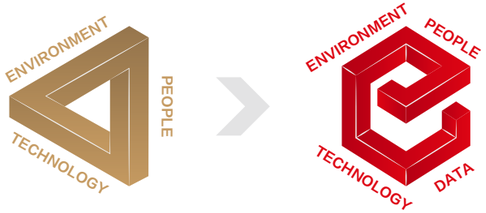
虽然已经实施智能运维场景，并取得一些成绩，但并未解决难度较大的运维数据质量问题。

凡是能用技术解决的都不是问题，很不幸，运维数据质量属于不是靠技术就能解决的问题。

在过去几十年中，运维一直是在解决人、环境与技术之间“三维”彼此影响的问题。

当AI类技术不断引入到环境中来协助人处理问题时，我们才意识到运维到了一个新阶段，然后称之为：智能运维。

当智能运维应用的越来越深，我们发现智能运维要解决的是人、环境、技术和数据之间“四维”彼此影响的问题。

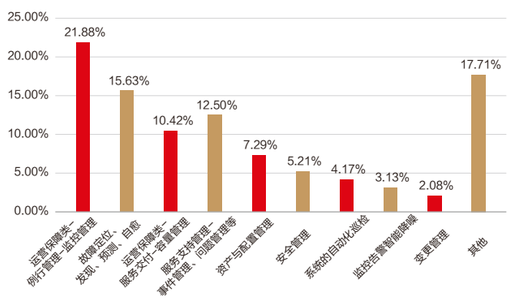


智能运维场景应用当下出现长尾的特点。

监控、容量的常规场景应用依然较多，但也从调查中看到细分场景以散落方式出现，总体数量不少。

未来2–3年会有更多细分场景引入智能运维，但不会改变常规场景占优的局面。

智能运维场景



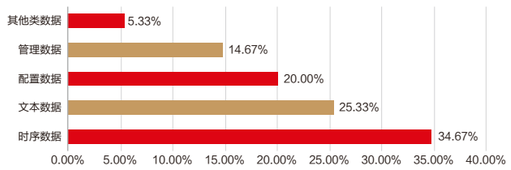
智能运维最不缺的就是算法。

各有千秋，但没有哪一个能够独霸武林，独步江湖！

智能运维平台的分析能力利用算法和模型来支持，然而结果并不总是通用或相似的。

因此，算法价值是有限的。

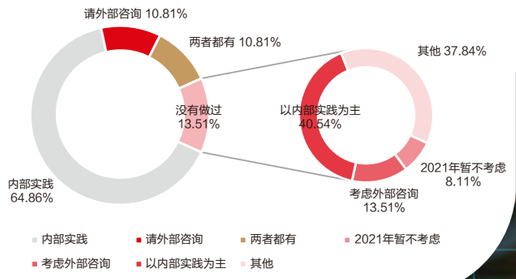
应用AI算法的数据类型



智能运维在复杂的运维数据治理中艰难地前行。

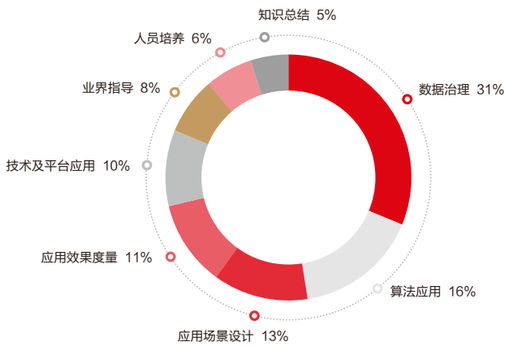
是继续艰难度日，还是借力打牛，如何选择将影响智能运维未来2到3年发展的速度以及持续提升的基础。

运维数据治理

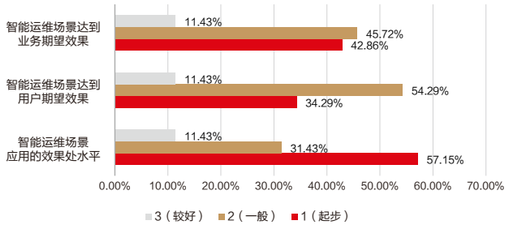


运维数据治理重要，但业界缺少适合的工具平台来支持运维数据治理的价值体现。

智能运维建设难点



目前国内各单位智能运维建设基本处于起步水准。



数智革新
引领IT转型升级

文/李富

形势

世界正在经历百年未有之大变局，国际格局深刻调整。过去的这两年，新冠肺炎疫情全球蔓延，百年变局加速演进。乌卡时代，在我们面临的所有的不确定当中，有一件事是确定无疑的，那就是数字化的趋势没有改变。数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量；数字经济是把握新一轮科技革命和产业变革新机遇的战略选择。

图1 乌卡时代

数字经济已然成为国家战略，《中华人民共和国国民经济和社会发展第十四五规划和2035年远景目标纲要》提出“加快数字化发展，建设数字中国”的目标，激活数据要素潜能，充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业、新业态、新模式，以数字化转型整体驱动生产方式，不断做强、做优、做大我国数字经济。

在面对产业结构调整、资源环境挑战、数字技术与创新带来的行业颠覆与机遇，我国各行业企业逆水行舟，不进则退。在此背景下，对于各行各业来说，数字化转型是企业提升经营效率和竞争力的必然选择，已不再是“选择题”，而是关乎生存和长远发展的“必修课”。

使命

在数字化转型大形势下，企业IT技术部门迎来了一个重大的挑战，不再仅仅作为支撑部门，而是第一次作为生产建设者的身份指导企业未来发展方向。“数据”是IT部门的最强抓手，“技术”是IT部门最大的优势，每个企业的IT领导者，不得不思考的一个问题是企业数字化转型的业务战略是什么？有没有针对企业的业务战略设计与之相对齐的IT战略或数据战略？ IT部门如何利用好这些抓手和优势，制定IT战略为业务赋能，提升企业整体数字化能力?

数据战略源自业务数字化战略并与IT战略保持一致

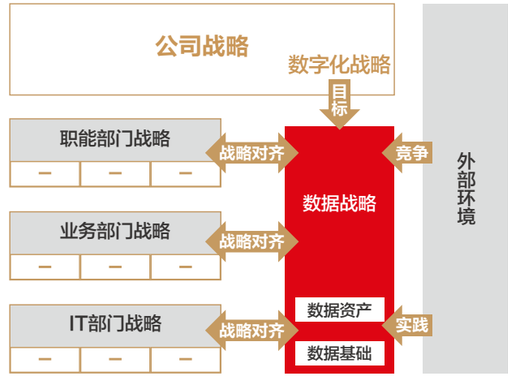


图2 企业数字化战略

幸运的是，挑战与机遇并存，IT领导者可以从思想、行动进行调整，从而改变其IT的运营和管理的模式，帮助企业灵活应对数字化变革带来的各种业务不确定性和挑战。这是时代赋予IT领导者的使命！这一使命决定了IT部门必须要转型，从信息化建设转型为数字化运营，帮助企业降本增效，实现高质量发展。

另外一方面，重大的变革需要一些早期的成功来证明其价值和方法的可行性，数字化转型也是如此。首先是IT技术的升级，其次是数字技术的使用和破局，最后是基于这些技术和平台的业务创新。IT运维工具、平台相对独立可控，数据敏感度较低，变革风险较低。从这些角度来看，IT部门也是数字化转型当仁不让先行先试的引领者。

挑战

IT部门职能业务包括整体统筹规划设计、系统构建部署、投产管控、系统监控感知、服务事件运行管理，以及整体运营能力持续提升的运营管理。运维管理提供了基础设施环境支持，确保业务连续性、可用性、安全性和运营服务支持。

图3 IT价值链

如今IT的环境复杂性越来越高，业务停滞一秒钟都可能带来巨大损失，保证业务可用性和连续性需要有效地减少非计划的业务中断、防范运维操作风险，对于异常的出现能够利用工具量化分析并快速定位、修复，确保业务的连续性。业务部门希望IT部门的运营速度和响应能力具备更高的水准。原来被动救火式、问题驱动式、操作运维、经验运维等特点已不能有效支撑公司业务发展与转型。

爱因斯坦说：某个层次的问题，很难靠这个层次的思考来解决。答案永远比问题高一个维度。当你提升一个维度以后，看问题的角度和视野会完全两样，有更宏观的视野与更清醒的洞察，很多以前无法理解的事情会变得豁然开朗、无法解决的问题可能会迎刃而解。全面的数据化提供了“上帝”视野，可以从全局、深度、高维审视破解这些挑战。

由于历史及组织分工的原因，传统IT系统多采取竖井式的方式、烟囱式的系统架构，各自为政系统建设，导致企业产生了大量的“数据孤岛”。 由于绩效考核机制、部门利益保护等问题，部门之间形成一道无形的“部门墙”。“小数据”普遍存在数据不一致、不准确、不完整等数据质量问题，系统之间数据无法打通、难以融合，企业信息共享困难。打通数据就是打通管理壁垒，数字化转型的基础就是打破数据壁垒和统一数据口径，消灭组织里面的信息不对称。

破局

数字化转型的本质就是尽可能地挖掘和释放“数据”的价值。“战略性”使用数据，改变数据使用的现状，将数据真正作为企业的“生产要素”去管理和使用。

数据是对事实的记录，要发挥数据的价值，就需要将其转化为信息或者知识。从古代的“结绳记事”，到现在的“智能仪表盘”，从数据到信息再到知识的转化过程中，数据分析和可视化是关键。数据分析和可视化不仅让数据看起来直观，更重要的是，使数据更易于理解和解释。

Gartner给出了数据分析的5个层次：

- 描述性分析—发生了什么；
- 诊断性分析—为什么会发生；
- 预测性分析—可能会发生什么；
- 处方性分析—该做些什么；
- 自动化分析—智能自动决策。

这是一个从数据中得到“后见之明”，到从数据中获取“洞察力”，再到给出“远见”的过程，不同层次的分析所需的技术、算法、方法、工具会有所侧重或不同。数据分析、挖掘、可视化的工具有助于提升数据处理、数据分析、数据展现的效率和效果，充分挖掘数据中蕴含的价值。

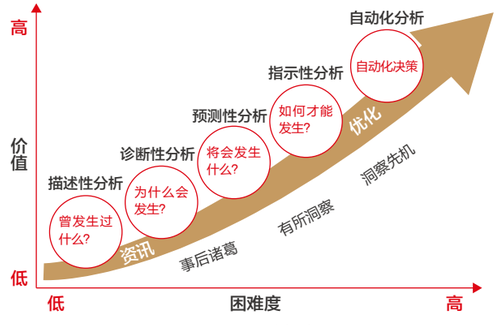


图4 Gartner分析类型

数智化，即数字化+智能化。数智化的核心，是以海量大数据为基础，结合人工智能相关技术，结合场景化去解决问题。也就是说，数智化可以简单理解为是在数字化的基础上的更高诉求。智能化本质是复杂问题需要借助智能化的能力来解决高维问题。

Gartner 在2017年提出了AIOps智能运维概念，以描述使用人工智能应用于IT运维领域的方向。利用大数据、机器学习等技术手段处理运维相关的数据，通过实时、动态、增强等高级分析，使之具备诊断、预测能力，直接或间接提升系统的稳定性、可用性、体验感，实现更高质量、更低成本、更高效的支撑，改善和增强IT运营能力，以提高企业的竞争力。

图5 Gartner 2021年中国新技术发展周期图

Gartner报告显示随着越来越多的业务运营数字化及不断增长的数据量，用户对AIOps平台功能的需求也将不断增长，数字业务转型正在推动AIOps发展。渴望建立数字业务的行业将率先采用AIOps系统。数据量的快速增长和变化的速度不能等待人力获得洞察力，不包括 AIOps的IT运营没有未来。到2024年，将有30%的企业领导者将依靠IT运营（AIOps）平台中的AI获得自动见解来推动与业务相关的决策。

2021年12月14日，国家标准化管理委员会、应急管理部等10部委联合印发《“十四五”推动高质量发展的国家标准体系建设规划》，其中智能运维、大数据治理、数据资产规划、数据服务能力等相关标准均被明确写入。《信息技术服务 智能运维 第1部分：通用要求》作为智能运维的标准，定义了智能运维能力框架，规定了智能运维能力要素和能力实现的过程。以信息技术服务领域智能运维最佳实践为基础，明确了信息技术服务领域运行维护服务智能化建设和运营要求；增强了信息技术服务领域企事业单位在智能运维技术方面的规范性及其运维服务能力。

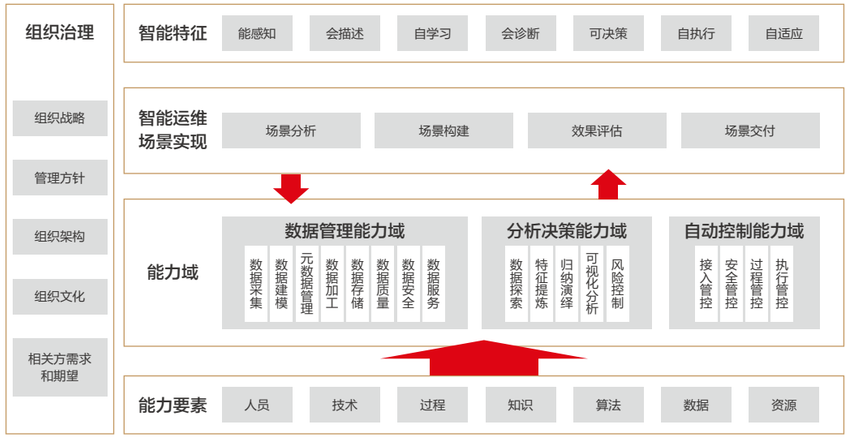


图6 智能运维国标框架图

智能运维能力框架包括组织治理、能力要素和能力实现三部分。智能运维建设需要在组织治理下，进行战略宣贯、组织拉通、总体规划、资源保障及建设管理；运维需求及各种场景应用层出不穷，能力平台是将各类运维场景共同用到的数据和技术加以整合、沉淀，实现能力的共享。运维组织将能力平台提供的数据管理能力、自动控制能力和分析决策能力通过场景分析、能力构建、服务交付和迭代调优等活动，在具体的运维场景中进行融合创新，最终实现具备智能特征的运维能力，从而达到安全风险管控、高效运维交付、快速业务响应、标准运营支撑的运维目标要求。有了标准的指导，有助于构建智能运维产业生态，支撑信息技术服务业持续发展。

实践

数据中心数据化运营体系统建设

某头部金融企业的金融科技战略是以数据为关键生产要素，以科技为核心生产工具，驱动金融创新，按照“综合性、多功能、集约化、创新型、智慧型”方向，实现全方位数字化转型，致力打造“以客户为中心”的最具“智慧”的银行。面对新形势、新挑战，如何构建安全、可靠、自主、创新的金融科技底座，有力支撑企业数字化转型，数据中心从数字化运营、精细化管理、技术运营标准规范这三个主要方面统筹谋划，调整目标，由确保信息系统安全稳定运行的运维目标转变为“安全稳定、高效敏捷、创造价值”的运营目标。通过数据化的工具、技术和方法，对运营过程中的各个环节进行科学的分析，为数据使用者提供专业、准确的行业数据解决方案，持续提升技术运营数字化能力，实现从“技术运维”向“数据运营”转型，达到优化运营效果和效率、降低运营成本、提高效益的目的。

数据中心从运维到运营的转型中由于缺乏有效的数据化运营能力，面临诸多挑战。缺乏数据思维，缺乏数据驱动运营的思想；数据越来越多，但可以有效用来决策支持的数据却很少；分析无从下手，不知道分析什么、如何分析；数据分散在不同的IT系统中，没有集中管理，数据质量参差不齐，治理困难，整合难度很大；零散指标手工统计耗时费力，无法持续跟踪运营工作情况、优化和改进服务质量，时效性和可信度无法保证。同时在“数据运营”转型中，技术运营能力是数据中心的重要标尺，而如何度量、评估、提升运营服务能力，需要一套标准来指导，更需要一套体系来检验。

数据化运营指标体系正是这样的一个抓手，根据数据中心智能运维和数据化运营目标的指导和要求，构建可量化、可导向、可对比的技术运营指标数字化评价体系，对运营数据（管理数据+技术数据）进行分析，揭示与分解各项运营管理活动要素，形成可监测运营效果与衡量发展方向的运营指标。采用自顶向下的设计方法，分层分类进行分解，数据中心运营水平一级关键目标指标，分解“安全运维，高效运营、资源规模、创新发展”关键成功因素二级指标，每个二级指标再次分解为三级关键绩效指标，逐层向下，规划了六百多个指标，目前建设落地了两百多个指标，最终形成灵活可伸缩扩展的指标体系（如图7）。体系中的指标设计为量化指标，基于客观事实数据计算，能够反映真实的运营情况，可实现自身对比以及行业对比，还可以通过高级指标设置以及权重的分配体现关注领域和发展方向，实现导向。每个上级指标可以逐级下钻到下级指标直至事实明细数据，定位异常偏差的指标和事件记录。每一层级的任意指标可以根据具体维度、时间周期、时间跨度范围进行多视角多组合维度的观察分析对比。

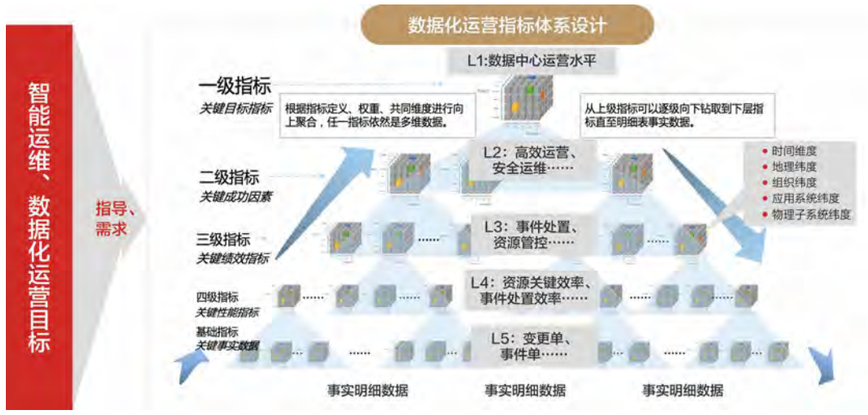


图7 数据中心数据化运营指标体系规划

支撑数据化运营体系的数据基础在于运维大数据资产平台的建设。并不是所有的数据都是数据资产，那些不能给企业带来价值和利益的数据，就只是数据资源。数据资源化是第一步，数据汇聚，打通数据孤岛。拉通流程管理、事件整合、监控平台等各运维管理工具平台，自动化采集技术和管理数据，完成数据质量校验和评估，推动数据治理，提升数据质量。数据资产化是第二步，盘点摸清数据家底，从业务域出发进行数据的梳理，从信息系统出发进行数据盘点。建立数据标准，包括数据资产编码，数据分类分级，数据资产目录。构建运维业务的企业级一致性数据模型，建设基于大数据的运维数据仓库和统一指标模型，实现数据联接；通过数据模型规范整合，形成数据中心优质数据资产。数据价值化是第三步，打造数据资产的运营能力，真正实现让数据为业务赋能。数据服务层提供指标数据得分实时计算、多维度多视角指标分析、运维系统画像、可视化报表、分析挖掘等数据服务，支撑数据化运营指标体系、智能管控、安全态势感知等各种场景数据需求，实现运维数据的统一与共享。场景数据应用的反馈，推动改善了数据质量，进一步提升了数据服务能力。

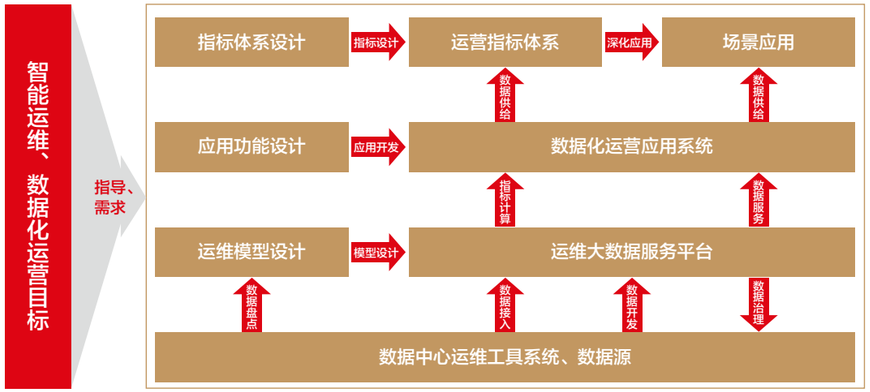


图8 数据中心数据化运营体系构建图

数据中心数据化运营体系的建立，打通了数据孤岛，实现了数据拉通融合，夯实了数据驱动的数字化运营底座。运营指标评价系统的建设，成功地构建了领先的指标模型库，全面涵盖运营数据中心主体业务的工作数据、性能评价、绩效评价、整体评价、整体运营目标等，建立了可量化、可对比、可导向、场景化的运营指标体系，实现了实时观测运营情况，多维度多视角持续评价技术运营能力，跟踪监督运营服务质量，为运营活动提供了精细化科学管理依据和手段，持续改进、提高数据中心运营能力。

数据化运营体系构建是智能运维国标框架的实践案例，积极践行框架中的组织治理、数据管理能力域、分析决策能力域以及智能运维场景标准。数据化运营指标评价体系在数据中心落地实践的摸索，也为数据中心能力评估提供标准依据。智能运维标准的建设和推广应用、数据化运营指标评价体系标准规范化制定，将有助于指引数据中心建设发展。

数据智能赋能运维事件治理

IT中心最显而易见的一大挑战就是运维事件的治理问题，一面是“海量”的告警信息需要处理，一面是故障被动应对，响应处置效率低下，业务部门诟病IT部门支撑不力，影响业务目标。要解决运维的复杂问题、提升运维的价值、引领运维的演进的关键方法，是拉通、整合运维数据，增强数据质量，将可观察性数据和AI更好地结合在一起，并应用多层AI。

数据选择算法消除了数据噪声、冗余的数据项。模式发现算法查找与那些重要数据项相关的模式。因果推理算法能从这些相关模式中识别出哪些实际上是相关性的根源告警。协作算法能够对现在相关且因果分析的重要事件做出反应。最后，自动化算法将执行团队协作计划中产生的计划。

图9 事件智能化治理框架

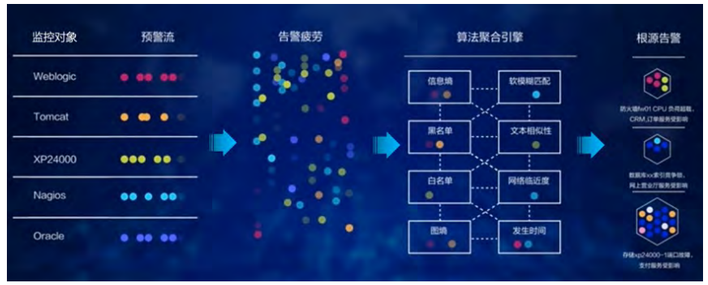


图10 事件智能化处理原理

通过AIOps处理日志、指标，跟踪和告警这些可观察性数据，消除噪声、确定优先级、切实可行地建立相关性，并提供深入的上下文洞察力，聚焦有效事件（如下图，某客户告警整体压缩率达到了99.15%）的高效处理，确定故障根本原因并进行补救，增强了运营的可见性并改善风险管理，这些都与企业目标保持高度一致。

图11 事件智能化过程告警处理统计

笃定

乌卡时代，挑战和机遇并存！总有一些睿智、勇敢的企业和个人，能够把握住时代的脉搏，敢于挑战、勇于挑战，从挑战中发现机会、把握机会、甚至创造机会。他们不仅没有在未知、不确定性的乌卡时代迷失，而是找到了支撑他们不断前进的笃定力量，帮助他们寻找方向，探索未知。这个“笃定力量”，他们称之为“VUCA 2.0”！乌卡2.0代表Vision（愿景）、Understanding（理解）、Courage（勇气）、Adaptability（适应）。如果说， 乌卡是数字化转型的挑战，那乌卡2.0就是数智化引领的方向！道阻且长，行则将至，行而不辍，未来可期！

ITSS 5.0解读

文/陈宏峰

什么是ITSS 5.0？

ITSS是IT Service Standard的缩写，即信息技术服务标准体系，它是动态发展的，与信息技术服务相关的技术和产业发展紧密相关，同时也与标准化工作的目标和定位紧密相关。ITSS不断适应时代发展需求，从2009年ITSS 1.0版本发布至今，ITSS标准体系框架已更新迭代至5.0版本，推动了信息技术服务的高质量发展。在标准研制方面硕果累累，截止2021年9月，ITSS已发布实施64项标准，其中，国家标准37项，行业标准17项，团体标准10项。在标准应用推广方面，截至2021年9月，认定评估机构34家，培养评估师1300余名，有5600余家单位获得ITSS符合性评估证书。在国际标准化方面，持续深化国际标准化合作，贡献中国力量，实质性参与14项国际标准研制工作，并分别担任编辑／联合编辑。

ITSS 5.0标准体系框架，在数字中国建设、产业高质量发展、新发展格局构建以及自主创新的国家战略和市场需求的双轮驱动下，以基础服务标准为底座，以通用标准和保障标准为支柱，以技术创新服务标准和数字化转型服务标准为引领，共同支撑业务融合的实现。

时代背景：百年未有之大变局

当今世界正经历百年未有之大变局，新一轮科技革命和产业变革深入发展，信息技术服务业发展环境日趋复杂，机遇和挑战均有新变化。

一方面，信息技术服务业面临严峻的外部环境。国际环境日趋复杂，经济发展不稳定性、不确定性明显增加，新冠疫情等黑天鹅事件频发，数字化转型下行业分化变革加速，信息技术服务业传统的商业与盈利模式受到严重挑战。另一方面，信息技术服务业面临巨大的发展机遇。国内大循环为主体、国内国际双循环的新发展格局正加速形成，数字经济迅猛发展，数字技术创新日新月异，围绕云、物联网、数据资产等领域不断涌现出新的信息技术服务形态。我国经济的转型和发展以及新业态的出现给信息技术服务业带来了大量新的机会。

认知升级：重识信息技术服务

新形势下，信息技术服务突破了单纯的“信息技术服务提供方”为“需求方”提供服务的限制，服务领域从咨询、设计与开发、集成实施、运维、云服务等基础服务，拓展到智能化服务、数据服务、数字内容服务、区块链服务及数字化转型服务等，充分体现出“融合创新”等特点。其特点主要体现在：一是各行业数字化转型大形势下，信息技术服务与业务深度融合，如融合装修行业与信息技术服务的智能家居、智慧楼宇服务等，融合金融行业与信息技术服务的金融科技服务等；二是IT基础设施建设从分散建设到集约化建设，IT基础设施标准化封装并对外提供服务成为趋势；三是人工智能、大数据等新技术在信息技术服务中创新应用，重构IT服务模式，如以人为主的人工巡检、人工操作等传统运维向自动感知、自主决策、自动操作的智能运维转变等。

ITSS 5.0结合新形势下信息技术服务融合创新特点将信息技术服务的内涵重新界定为：组织为达成用户期望的结果，利用信息技术为用户交付价值的活动。可以理解为组织以信息技术为手段为用户交付的一切有价值的活动都是信息技术服务的范畴，“组织”本身不再强调供方和需方，且不止限于基于IT的服务即开发、应用信息技术的服务，和IT驱动的服务即以信息技术为手段支持需方业务活动的服务，一切以信息技术为手段提供的有价值的活动都属于信息技术服务，丰富了信息技术服务的内涵。

在各行业加速数字化转型的形势下，随着新一代信息技术的快速发展和应用，信息技术服务的外延得到很大的扩展。新形势下，信息技术服务包括基础服务（咨询设计、开发测试、集成实施、运行维护、云计算、数据中心）、技术创新服务（智能化服务、数据服务、数字内容处理服务、区块链服务）、数字化转型服务等。

标准应变：融合创新谋发展

随着信息技术服务内涵和外延的拓展，信息技术服务与业务的边界越来越模糊，“你中有我，我中有你”的业务融合成为信息技术服务发展的新业态。标准体系也需要与时俱进，从行业监管、产业基础发展、技术创新应用、融合业务场景四重视角勾画出信息技术服务标准体系的整体轮廓。

ITSS 5.0标准体系框架（如图1所示），在数字中国建设、产业高质量发展、新发展格局构建以及自主创新的国家战略和市场需求的双轮驱动下，以基础服务标准为底座，以通用标准和保障标准为支柱，以技术创新服务标准和数字化转型服务标准为引领，共同支撑业务融合的实现。

ITSS 5.0主要内容包括：

■ **通用标准**是指适用于所有信息技术服务的共性标准，主要包括信息技术服务的业务分类和服务原理、服务质量评价方法、服务基本要求、服务从业人员能力要求、服务成本度量和服务安全等。

■ **保障标准**是指对信息技术服务提出保障要求的标准，主要包括服务管控标准和外包标准。服务管控标准是指通过对信息技术服务的治理、管理和监理活动和要求，以确保信息技术服务管控的权责分明、经济有效和服务可控；服务外包则对组织通过外包形式获取服务所应采取的业务和管理措施提出要求。

■ **基础服务标准**是指面向信息技术服务基础类服务的标准，包括咨询设计、开发服务、集成实施、运行维护、云服务、数据中心等标准。

■ **技术创新服务标准**是指面向新技术加持下新业态新模式的标准，包含智能化服务、数据服务、数字内容处理服务和区块链服务等标准。

■ **数字化转型服务标准**是支撑和服务组织数字化转型服务开展和创新融合业务发展的标准，包含数字化转型成熟度模型、就绪度评估、效果评估、中小企业指南、数字化监测预警等标准规范和要求。

■ **业务融合标准**是指支撑信息技术服务与各行业融合的标准，包括面向政务、广电、教育、应急、财会等行业建立具有行业特点的信息技术服务相关的标准。

ITSS体系坚持动态发展，与信息技术服务相关的技术、服务和产业发展紧密相关，同时也与标准化建设工作的目标和定位紧密相关。

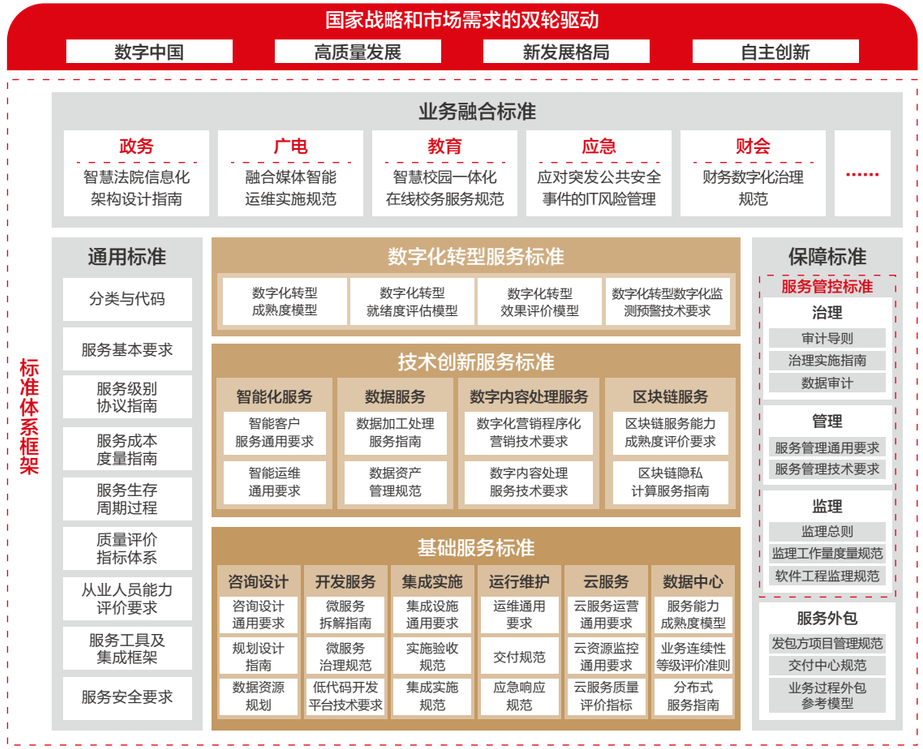


图1 ITSS 5.0体系框架图

注1：因ITSS标准体系包含标准数量较多，在标准体系图中仅标出几项有研制基础或较为重要的标准；

注2：与其他标准化领域有交叉的标准方向，将与相关标准化机构建立联合工作机制共同研制。

生态建设：价值共创向未来

ITSS生态历经10余年的发展，从无到有，已然形成了“政、产、学、研、用”五大生态主体，充分发挥着协同、创新和可持续发展的政策指引、前瞻研制、应用示范、开拓创新的生态体系作用。

信息技术服务标准生态圈（以下简称ITSS生态圈）是指信息技术服务在标准研发、试验验证、成果转化、应用推广和标准改进的周期活动中，政、产、学、研、用等各利益相关方围绕ITSS标准库，共同建立一条标准价值的增值传递链，并赋能在ITSS一体化公共服务平台上。各利益相关方在标准化周期链上各司其职又互相影响，形成有规律的共同体，在产业、技术发展的外部环境下，相互制约、价值共享、互利共存，共同推动信息技术服务标准的健康有序发展，有效提升信息技术服务业的创新活力。ITSS生态圈如图2所示，包括：一个ITSS标准库，政产学研用五主体，标准化周期链和价值化周期链，以及ITSS一体化公共服务平台，可简称为一库、五主体、二链、一平台ITSS生态圈。

图2 ITSS生态图（1521生态图）

十多年来，ITSS标准化成果在国家制定产业政策和规划、构建行业统计制度、提升企业信息技术服务能力、指导服务关键支撑工具和产品研发等方面发挥了重要作用。标准在各个领域呈现越来越多的应用表现形式，应用范围越来越广，应用成果越来越显著。ITSS价值链作为ITSS生态圈的关键组成部分，政产学研用五大主体均可参加ITSS标准研制完成价值创造，并在标准推广应用中实现价值转换、价值传递、价值实现、价值共享和价值反馈活动，具体的价值传递可体现在以下5条线上：人才培养线、行业监管线、能力建设线、业务赋能线、产品研发线，并以标准库为中心通过价值传递新产生6个卫星库包括：人才库、智库、实践库、解决方案库、产品／工具库、赋能案例库。ITSS价值链见图3。

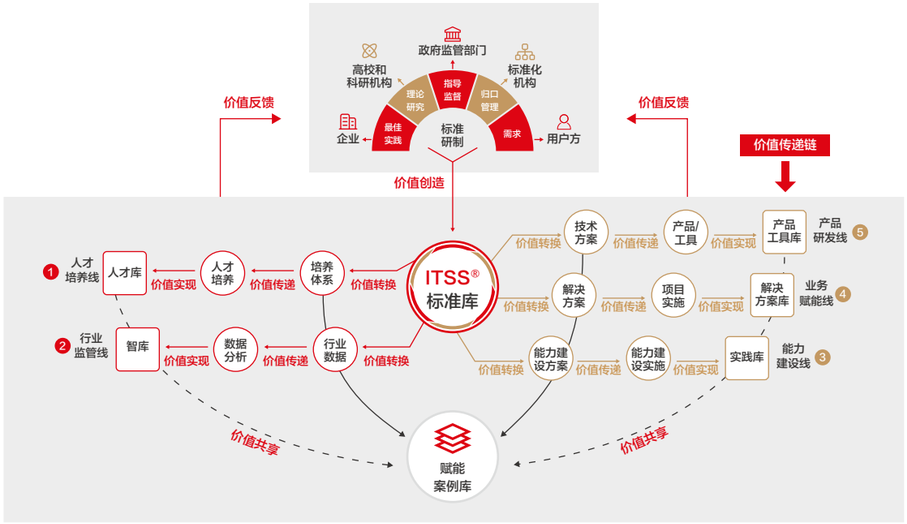


图3 ITSS价值链

ITSS生态的形成和不断丰富加强，将促进ITSS可持续发展，ITSS标准价值将在更多参与主体及价值链各环节上得以体现，同时，吸引或孵化更多主体参与其间，迸发出更多价值实现的创新火花，共创共赢才是未来的大势。

结束语

本文主体内容是摘引自《信息技术服务标准体系建设报告5.0》。ITSS标准人经过不懈的努力，不断探索和实践，从1.0到4.0，持续迭代信息技术服务的这个连接底座。如今，数字经济时代的到来打破了原有“信息技术”与“业务”的边界，“价值导向，融合创新”成为时代的主旋律，而ITSS 5.0将成为奏响这个时代乐章的总指挥。

SRE减少琐事的妙方

文/李光

随着企业数字化转型的深入，企业对IT的依赖越来越强，系统复杂度在增加，部署规模在扩大，传统的运维团队规模与系统负载基本成线性关系，共同增长。单纯靠增加运维人力不仅增加企业的成本，也无法满足数字化业务对敏捷IT的需求。运维团队应该在考虑稳定性的同时，通过开发工具、建设平台提升运维效率保证系统可靠性，使用技术手段优化服务运行成本。SRE就是这样一种运维理念和运维模式，SRE是Site Reliability Engineering的简称，区别于传统运维模式，SRE强调自动化系统，主张通过软件工程方式开发出一些场景化的自动化运维工具来替代重复性的手工操作。与运维服务相关的重复性的、手工的工作，Google用一个专门的词语——琐事（Toil）来进行描述。在Google SRE中，如果运维人员都致力于逐步减少琐事、消除琐事，就可以把工作保持在健康状态，就可以将更多时间投入到有创新性和创造性的工作中去，有助于使整个团队或是整个组织在维持同等人员配备的情况下接手更大或者更多的服务。

SRE中琐事

SRE强调自动化，运维工作的绝大部分是工具自动化完成的。它的核心优势是自动化、可编程性、效率高。典型的SRE活动分为软件工程、系统工程、琐事、流程负担四个部分。四部分工作中有一类工作与日常运维服务直接相关，Google用琐事（Toil）来进行描述，被定义为低效工作。SRE的公开目标是保持每个SRE的工作时间中琐事的比例低于50%。减少琐事和扩大服务规模的工作就是SRE中的E（Engineering），逐步消除琐事的最有效手段是自动化。多做创新，少干琐事是一种最佳的运维状态。实际上，在我们的工作中不可避免的会出现琐事，公司不同、岗位不同，琐事的数量和种类也不尽相同。我们先来看看如何识别运维中的琐事。满足下列一个或多个属性都可以称为琐事：

- 手工操作：手工或者手工运行脚本执行某个任务。
- 重复性：某件事是第一次做，甚至第二次做，都不应该算作琐事。琐事就是不停反复做的工作。
- 可以被自动化：如果计算机可以和人类一样能够很好地完成某个任务，或者通过开发工具代替某项任务执行，这项任务就是琐事。如果某项任务必须人为主观判断，那么很大程度上这项任务不属于琐事。
- 战术性的：琐事是突然出现的、应对式的工作，而非策略驱动和主动安排的工作。处理紧急告警是琐事，我们可能永远无法完全消除这种类型的工作，但我们必须努力减少它。
- 没有持久价值的活动：如果在你完成某项任务之后，服务状态没有改变，这项任务就很可能是琐事。如果这项任务会给服务带来永久性的改进，它就不是琐事。
- 与服务同步线性增长：如果在工作中所涉及的任务与资源数量，服务的大小或用户数量呈线性增长关系，那这项任务可能属于琐事。

例如对服务器硬件巡检，每天手工检查几百台服务器的硬件指标，这就是琐事，分析一下这里有几个琐事属性。这是手工操作；是每天或每周重复做；是可以用定时脚本自动完成的；这事做完后并不能长治久安，所以没有持久价值；最后，随着业务量增加，服务器规模增加，检查工作也会同比增加，所以是线性增长关系。

日常运维中确实存在不少琐事，如清理磁盘空间、监控系统状况、处理常见告警、定位常见问题、统计业务数据、日报、周报等都是琐事，如果对这些琐事不加以管理，有技巧的去处理，运维人员的价值就被这些琐事淹没。长期处理琐事造成工作重点不突出，绩效差，个人能力无提升，长期下去会消耗掉工作激情，对组织来说运维工作效率无法提升。我们应该减少琐事，将更多时间放在创新工作上。减少琐事，构建自动化平台是SRE开出的一个妙方。

自动化系统可以提供一个可扩展的、通用的平台。平台可以将日常运维工作集中化，从而规模化地处理运维工作，也能比人更持续更频繁地运行任务，通过自动化平台固化运维流程，自动化平台与流程管理系统联动，实现自服务化能力输出。通过平台集中运行后的数据分析，可以帮助我们发现以前运维流程中不易察觉的细节，依托数据分析改进运维流程，用数据量化运维服务。自动化会带来效率的提升我们很容易理解。虽然我们经常会听到一个声音“实现一个自动化流程或者场景所花费的时间和精力比原来手工执行的成本要高很多，还不如手工做”，但是我们还应该看到一旦自动化得以实现，将会把某个操作与具体的操作者解耦，通过自动化平台把专家经验变成固化流程，让平台自动完成一些需要专家才可以完成的工作。

运维自动化是运维人员一直追求的目标，自动化水平高低也反映一个公司IT运维的成熟度，初级阶段的运维很多工作需要人工处理，处于“人肉运维”阶段；中级阶段很多工作可以由脚本或者程序来完成，但是还需要人工去执行，处于“机器运维”阶段；高级阶段整个运维系统有充分的监控感知，有智能中心根据感知的数据自行判断执行自动化脚本和程序，处于“智能运维”阶段。在运维的三阶段中，最后的智能运维要求最高、实现最难，但是很多组织完全可以通过努力实现第二阶段的运维，将日常重复的、需要人工处理的工作，逐步的用自动化脚本或者程序来实现。

逐步消除琐事的最有效手段是自动化，一个合格的运维工程师很少做繁琐的重复性的工作，当碰到重复性的工作，肯定会考虑通过自动化运维解决。运维体系建设的越完善，自动化成熟度越高，琐事就越少，运维工程师就胜任更多的工程性工作，组织效率就越高。

SRE消除琐事案例

常见的琐事有：

- 问题解答
- 例行维护，包括日常巡检、清理磁盘空间、安全加固等
- 处理常见告警
- 日报、周报
- 定位常见问题

硬件巡检

硬件巡检任务介绍：

- 巡检要求：每周一次完成所有计费设备巡检，并生成报告。
- 设备多：移动业务的迅猛拓展，计费设备数量多。
- 地理上分散：众多设备分散在多地机房。
- 巡检指标众多：如网络吞吐量、磁盘利用率、CPU使用率等30多项。

随着管理规模增大，硬件巡检任务的工作量显著加剧，需要专人负责此项工作，每周五管理人员需要逐一登录到设备的管理网，查看各项指标并截图，在汇总生成报告，发给相应负责人。

琐事属性识别：

- 手工操作：登录管理网，执行命令获取数据，截图保存。
- 重复性：每周五做一次。
- 可以被自动化：设置定时任务，每周五自动发起巡检。
- 没有持久价值的活动：硬件巡检任务手工执行，下次还需要手工完成，重复性消耗人力，对运维人员自身能力提升没有价值。
- 与服务同步线性增长：2020年一个管理员2小时完成，到2021年要专人半天才能完成，2022年计费设备持续增长，需要更多的人力投入。

硬件巡检，就是琐事，通过自动化在2022年消除该项工作，硬件巡检不需要人工参与。

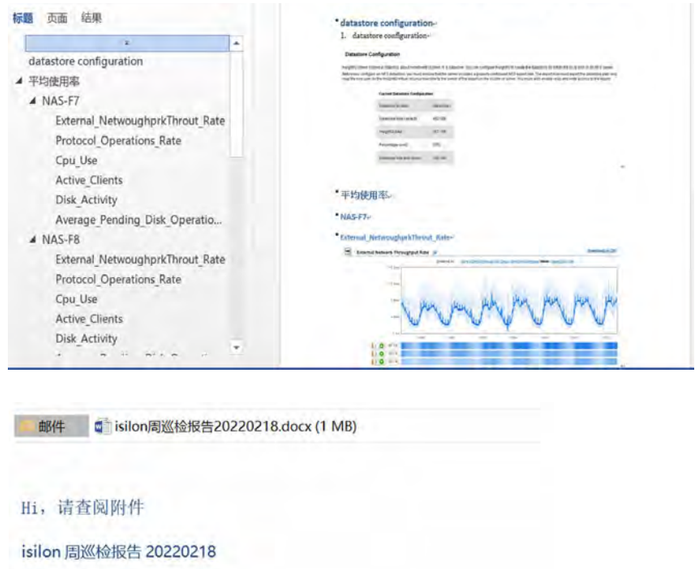
运维工程师通过使用python工具开发一套自动化的硬件巡检工具，根据巡检指标自动完成硬件巡检工作，具备自动截图留存、指标状态分析、报告汇总分析、生成巡检报告，定时任务调度，定时邮件发送报告功能。

通过python工具实现自动化巡检的整体设计思路：

- 借助selenium自动化框架，轮巡设备。
- 使用python图像处理函式库pillow对管理网界面进行裁切，格式转换、数据分析、转存。
- 巡检报告输出，使用docx库自动生成多级标题、正文、图片，发送巡检报告。

效果：

整个架构不限定设备类型，操作系统类型，代码高可用，支持横向扩展。有效避免了重复性劳动，通过定时任务自动执行，提高了生产安全性。



服务器上线加固

服务器上线加固任务描述：

现网有3000+台服务器，每次上线集成都会新增几十台服务器，新集成服务器上线前必须完成20+项安全加固动作，加固后要检查每项指标是否生效，每个动作要重复操作几十次，整体上线过程繁琐复杂、工作量大。目前需要两个维护团队分批次手工完成加固工作才能保障按时上线，而且两个团队之间操作规范不统一，容易出错，而且效率低，进而造成安全隐患。

原团队安全加固工作存在问题：

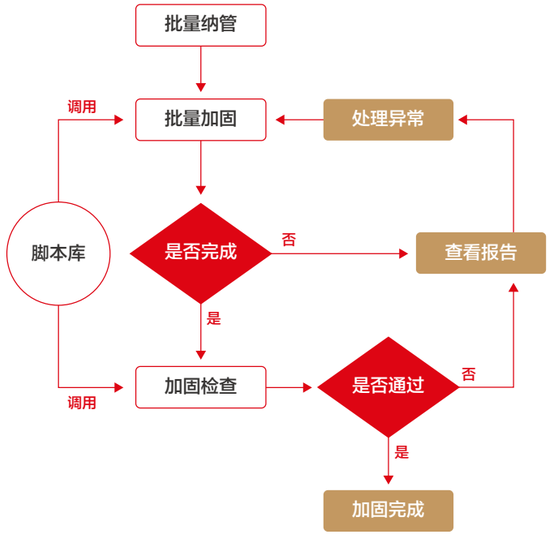
- 逐台设备SSH登录并上传脚本；
- 根据不同的集成应用需求修改加固脚本（加固项有可能变化）；
- 配置出错后需要人工删除错误配置；
- 不能增量加固，需要人工识别增量点；
- 加固动作一旦出错，需要大量时间排错；

- 两个维护团队都有自己的加固方案和加固脚本，实施细节在团队间不共享；
- 人工检查加固结果不可靠。

琐事属性识别：

- 手工操作：人工SSH登录每台服务器，手工执行脚本。
- 重复性：每次上线都要完成加固动作，每周都有上线任务。
- 可以被自动化：自动化和工单联动，上线流程自动触发加固动作。
- 没有持久价值的活动：每次上线都要手工完成加固工作。
- 与服务同步线性增长：上线服务器规模逐年增加，需要团队投入更多人力。

服务器上线加固，就是琐事，通过自动化在2021年消除该项工作，通过流程触发自动化完成加固工作。



效果：

在上线流程中，增加自动化加固动作，效果明显。不需人工参与，能够自动增量加固，自动纠正错误的加固动作，加固标准统一，让整个加固过程更安全、更可靠！

安全加固

加固检查

结束语

从业界的发展历程来看，技术的标准化是一个必然的演进过程，运维自动化其实就是标准化的一种体现。SRE团队构建的第一步，应该从整理和梳理工作职责开始，把需要解决的琐事形成清单，通过自动化手段逐步消除琐事，同时让效率持续提升。这个历程可能会很长，不计成本的平台化，只是光鲜的政绩，并没有有效地解决问题。通过小步迭代，按照实际取得的效果持续改进，最终才能实现企业运维能力的提升。

一切代码化、标准化、自动化

最佳实践代码化	经验标准化
生产环境经过检验的运维场景代码标准化，可以做到快速复用	将经验整理成各种可复用的解决方案
统一入口	**自动化联动**
•统一对资源接口 •统一的运维接口 •统一的监控接口 •统一的日志接口	•关联多个数据源分析系统 •自动化与分析系统联动

支持多种语言的统一SRE服务框架

自动化的最高形式是智能化系统，但是智能化还需要时间积累和技术突破，目前致力于消除琐事的自动化运维更加务实。SRE通过自动化逐渐消除琐事，运维人员拥有更多的时间提升自己的专业技能，才能帮助运维团队履行职责，保障线上服务稳定性，通过工具提升效率、用技术手段控制优化服务运行成本。

自动化运维是一个理想，没有最好，只有更好。运用SRE理论，专注在业务层面，切入实际问题点，总结经验，一次性解决问题。SRE不仅提供了一种方法论，指导我们运维工作的同时，还提供了一些具体的实践来供我们参考，如建立以客户感知为导向的SLA，制定统一的SLO，打造标准化和简单的运维流程，通过全面监控以落实SLO目标，通过自动化提升运维效率。无论企业规模或者IT规模大小，SRE的本质就是提高运维效率。目前还从事传统运维工作（运维工作相对单纯，一般以日常、重复性的工作为主，不涉及开发）的组织和个人应该提升自身研发能力、问题分析能力、项目管理能力。因为为提高运维的效率和质量，SRE会专注于开发各种自动化的运维工具，这对研发能力提出了较高要求；SRE要善于分析问题，从问题中提取用户需求，进而将其沉淀为一个运维工具。最后良好的项目管理能力可以帮助SRE合理安排时间，协调资源投入，保证各项工作的顺利进行。

自定义监控采集平台实践

文/钟果

近年来，随着数据中心、云计算等技术的兴起，企业信息化建设的不断深入发展，各类信息系统越来越庞大复杂，与之对应的，各类信息系统的监控软件也必须不断的进行技术演进，才能适应潮流变化。

监控软件的发展

早期的计算机大部分是单机运行，部署在其上的各类软件也大部分是单机版本。对操作系统和各类软件的监控，操作系统层面提供了相关的工具软件，如Unix/Linux的Top、PS、*stat命令工具，Windows的性能管理器等，一般通过人工巡查，发现问题处理问题，手段较为单一。

而早期的监控系统也主要基于SNMP（简单网络管理协议）的网络监控和系统（主要指操作系统）监控，一般来说，网络设备和操作系统可以提供标准的SNMP服务，虽然一些Web服务器、数据库、中间件也部分支持通过SNMP获取状态，但都不是很完善，所以对它们的监控也存在缺失。这一时期开源监控系统还处于萌芽状态，业界主流还是商业监控系统，如IBM的Tivoli、HP的OpenView、CA的UniCenter等，有很大的市场，但其主要服务的还是大客户，比如银行和运营商等。

随着计算机技术的发展，步入互联网时代，各个行业对业务、服务、应用都逐渐有了较强的监控需求，同时监控对象越来越多，也越来越复杂，业界主流的商业监控系统，也水涨船高，有了更大的市场。同时开源的监控软件也在不停的发展壮大，各类开源软件虽然宣称各种类型的资源均可监控，但侧重点却各有不同，有的侧重于网络监控，有的侧重于系统类监控，有的侧重于云原生监控，目前国内比较流行的开源软件包括Zabbix、Nagios、Prometheus等。

监控软件对于扩展性的挑战

监控软件经过多年的迭代发展，无论是商业软件预置支持的监控能力、还是开源软件社区支持的监控能力或者服务商定制监控能力，各类监控系统的应用水平其实相差不大。但当前互联网技术快速发展，大量的软硬件新产品层出不穷，硬件设备种类、型号多，商业软件升级更新版本、开源软件不断涌现。因此对于监控软件提出了新的挑战：必须具备快速适配的能力，才可以满足企业对于新产品监控的及时性要求。

传统的做法，要么等待商业软件版本迭代支持，要么等待开源软件社区支持或者开源软件服务商收费定制支持。但依赖于厂商或者社区的做法，对新产品一般都会有一个适配期，及时性无法保证，与企业的期待值相差较大。

当然，客户通过自定义的监控来满足及时性的要求，也是一种可行的方法。因此，无论是商业软件或者是开源软件，或多或少提供了一些自定义监控采集的能力，在一定程度上可以应对新软硬件产品的监控采集。但由于当前一般是通过使用各类复杂的配置文件，如XML/YML等，手动下发或者自动化工具下发采集指令来完成自定义采集的实现，对使用者有相当高的要求，而且学习成本非常高，使用极其不便，一般客户很难通过这种方式做到自定义采集。

因此，监控软件提供简单、易用并且通用的自定义监控采集平台至关重要，在这个平台中，从指标定义、指标采集方式、指标处理计算，以及指标界面展示效果等所有自定义采集相关的步骤，都完全可以通过可视化的界面配置来实现。通过可视化的自定义监控采集平台，降低学习门槛，使各种层次的运维人员均可轻松使用，这必将成为监控软件未来发展的重要趋势。

基于低代码思想的自定义监控采集平台设计

一个灵活可扩展的自定义监控采集平台，后端要做到预置支持多种协议的采集适配器，同时也需要提供南向接口，供第三方采集器接入。前端要做到全部的可视化配置，需要从如下方面入手，监控对象的定义可配置、监控指标的定义、监控指标对应的采集指令的定义、监控指标的展示形态的定义等。

其中，对于自定义监控对象指标的阈值配置，如门限阈值和动态阈值等功能，告警管理，如告警过滤、聚合收敛等功能，可以复用监控系统平台本身的能力，自定义监控采集平台的设计只需要按规范适应监控系统的要求即可。

预置采集器

自定义监控采集平台需要预置支持多种协议的采集适配器，包括脚本类采集器、SNMP采集器、WMI采集器、SMI-S采集器、JMX采集器、数据库采集器、Exporter采集器、Python采集器等，来覆盖业界主流管理对象的监控采集方式。

脚本类采集器

脚本类采集器需要支持shell/vbs/bat等业界主流脚本类语言，采集、计算逻辑一般封装在脚本中，采集器执行脚本，规定南向数据接口格式，可要求脚本返回值必须符合数据规范，才能接入到自定义采集平台中。

自定义采集平台可提供多种数据规范，比如支持分隔符方式的数据格式或者Json格式，其中key*表示指标名称；v*表示对应指标的值：

|||分隔符形式

```
key1|||key2|||key3
    v11|||v12|||v13
    v21|||v22|||v23
```

Json格式

```
[{
      "key1": "value1",
      "key2": "value2",
      "key3": "value3"
   }, {
      "key1": "value11",
      "key2": "value22",
      "key3": "value33"
   } ]
```

使用脚本类的采集器，可自定义出基于复杂脚本的指标的采集，如通过ipmitools工具的服务器硬件状态信息，shell脚本实现客户复杂的业务逻辑场景等。

■SNMP采集器

SNMP作为最基本的简单网络管理协议，一般的硬件设备如网络设备、存储设备、服务器等均有实现，SNMP采集器需要支持不同版本协议的采集，同时也需要实现GET和WALK两种采集方式。

使用SNMP采集器，可在监控系统未迭代新设备支持的情况下，根据mib说明快速自定义对新设备本身以及各部件的运行状态和性能指标的监控。

■WMI采集器

WMI（Windows Management Instrumentation），即Windows管理工具，它是Windows操作系统中管理数据和操作的基础模块。WMI采集器可以通过WMI脚本去采集本地或者远程计算机上的资源状态信息和性能数据。

微软公司发布的应用套件，如IIS、Exchange、SharePoint等，均实现并发布了基于WBEM的CIM模型，可由WMI获取到相关的状态和性能计数器。使用WMI采集器，可自定义出Windows系统及微软相关应用软件的性能计数器的采集。

■SMI—S采集器

SMI-S规范（Storage Management Initiative Specification），由众多存储厂商共同参与开发的一种标准管理接口，用来监控和管理来自不同厂商的存储设备，SMI-S采集器主要用于对存储设备指标的监控采集。

大部分存储设备内置了SMI-S Provider对外提供SMI-S接口数据服务，SMI-S采集器可直接连接设备采集。但部分厂商的存储设备未内置此软件，需要单独部署SMI-S Provider软件对存储设备进行管理，单独部署SMI-S Provider可管理多个存储设备，因此在这种情况下，SMI-S采集器需要兼容，能够准确区分通过同一SMI-S Provider管理的多个存储设备的各类采集数据。

■JMX采集器

JMX（Java Management Extensions）用于Java程序扩展监控和管理项。除了JVM预置的Java MBean丰富的管理类，大部分Java开发的系统和软件，也都扩展了很多MBean管理类。使用JMX采集器，可从Java应用系统本身提供的JMX信息获取我们需要的监控项。

■数据库采集器

数据库采集器需要内置业界主流数据库的驱动，在自定义监控时灵活选择对应的数据库类型。同时，还需要预留南向接口，以扩展未预置的小众数据库或者新数据库类型，方便将对应的数据库驱动导入到自定义监控采集平台。

对于客户定制化的业务系统，有很多有用的信息存储在数据库中，使用数据库采集器，可以很方便的将数据库中存储的业务数据作为一个个的监控指标采集出来并可视化展示，同时复用监控系统的告警平台，对业务数据进行监控告警，达到对业务系统监控的目的。

■Exporter采集器

随着云原生应用的发展和普及，大部分开源组件都实现了提供metric接口的服务，让第三方软件通过metric接口获取服务的运行状态和性能监控信息成为了一种趋势，对于自定义监控采集平台来说，这也是必须要实现的基本功能之一。

Exporter采集器一方面要能够正确配置和区分metric的四种数据类型，包括Counter（计数器类型）、Gauge（仪表盘类型）、Histogram（直方图类型）、Summary（摘要类型），以达到不同类型的Metric指标数据的采集。另一方面也需要将四种类型的数据与监控系统当前的指标体系融合为一个整体。

使用Exporter采集器对Metric数据的采集，再加上自定义的指标以及自定义的可视化界面展示，在一定程度上可以替代Prometheus+Grafana的监控开源组合，并且在易用性方面也是大大超出。

■Python采集器

Python作为一种主流的类解释型语言，功能强大，可以对接各种类型的API，如RESTful API、SDK API、网页爬虫、任何类型的数据库查询等，几乎可以实现任何数据的采集。

因此自定义监控采集平台内置Python解释器，对外提供统一的Python采集器执行Python代码，并规定执行结果的数据格式规范，是很有必要的。同时很重要的一点是Python作为运维人员的常用必备技能之一，拥有庞大的用户群，也给运维人员多一种实现自定义采集的方法。

监控对象类型自定义

监控对象类型的自定义，除了定义监控对象的基本信息如名称、默认采集协议外，还包括添加监控时的各种参数定义，如IP地址、端口号、用户名、密码等通用参数，同时也必须支持自定义的采集参数，如数据库的实例名等。

通过这些参数的定义，低代码平台自动生成增加该种类型的监控添加页面。

指标自定义

自定义监控采集平台从指标相关性分类和采集性能的角度出发，引入了指标组的概念，即一个指标组可以包含多个指标，这些指标间具有强相关性，可通过一条命令、一个CIM实体等方式采集。

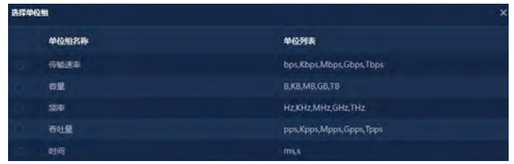
在定义指标组时，需要区分是单实例指标组，还是多实例指标组，可通过指定指标组内某个指标是否是唯一标识来确定。当某个指标定义为唯一标识，则此指标组为多实例指标组，否则为单实例指标组。

如网络接口指标组，包括接口索引、接口名、接口速率等指标，设置接口索引指标为唯一标识，则表明此指标组为多实例指标组，在数据采集时会处理多个接口实例的数据。

对于指标组内的指标自定义，包括对指标定义、指标采集方式的定义（即绑定采集器），采集后各种处理的定义等。

■指标定义

指标定义，包括指标名称、指标数据类型、指标单位等，其中为了在可视化展示时更加的易用，引入了单位组的概念，即在同一单位组内的单位可根据实际的指标值自动置换为合适的单位显示。自定义监控采集平台预置了5类单位组，包括传输速率、容量、频率、吞吐量、时间等类型的单位，具体定义如下图所示。



例如自定义监控Linux的文件大小指标，其单位组选择容量，其原始单位为B。监控了一个Linux的某个文件大小，其采集值为25,000,000，在可视化展示时，会自动转换为23.84MB显示。

■指标采集方式定义

指标采集方式的定义即指定指标的采集协议，后台自动绑定指标与其对应的采集器，同时指定对应的采集指令。不同类型的采集器的采集指令类型不尽相同：

脚本类采集器：指定需要执行的脚本

SNMP采集器：指定指标对应的OID

WMI/SMI-S采集器：指定指标对应的CIM类以及属性

JMX采集器：指定指标对应的MBean类以及属性

数据库采集器：指定需要执行的SQL脚本或者存储过程

Exporter采集器：指定指标对应的metric名称以及类型

Python采集器：指定执行Python的片断

■指标处理定义

指标根据采集定义，采集到值后，可能需要对这些值进行处理，才能符合指标的定义要求，指标处理是可选操作。

自定义监控采集平台可预置多种操作方式和处理逻辑，比如包括：

● 赋值操作

即将采集结果赋值给指标，例如：指标为名称（指标编码为name），采集结果为systemName，则将采集结果systemName赋值给指标（name）。

● 数值类型计算

数值类型计算包括如下几种：

√ 四则运算，加减乘除

例如：(MemTotalReal-MemAvailReal-MemBuffer-MemCached)/MemTotalReal*100

√ 取绝对值

例如：ABS(Size)

√ 三元表达式，()?:

例如：(PageIn > PageIn0)?(PageIn-PageIn0):0

√ 上一次采集结果用于计算，则返回结果属性后加0表示上一次采集结果

例如：(PageIn > PageIn0)?(PageIn-PageIn0):0

● 字符类型计算

对字符类指标的计算包括连接运算和MD5摘要

√ 连接运算符+

例如：LogTime+Message，"ABCD"+"EFGH"，LogTime+"EFGH"

√ MD5摘要

例如：MD5(LogTime+Message)，MD5("ABCD"+"EFGH")，MD5(LogTime+"EFGH")

● 特殊公式计算

特殊公式计算包括如下几种：

√ 求和：SUM_

计算采集值总和，只针对数值类型，例如：SUM_FileSize

√ 计数：COUNT_

计算采集值个数，数值字符类型都可，例如：COUNT_Handle

√ 取最大值：MAX_

计算采集值的最大值，只针对数值类型，例如：MAX_FileSize

√ 取最小值：MIN_

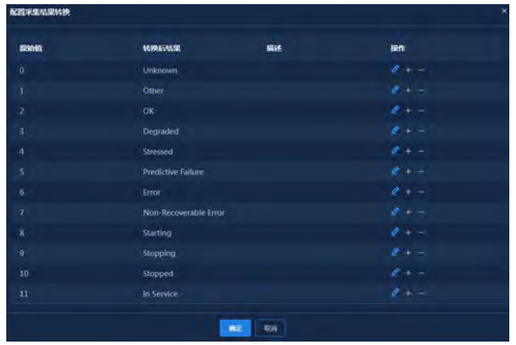
计算采集值的最小值，只针对数值类型，例如：MIN_FileSize

√ 取平均值：AVG_

计算采集值的平均值，只针对数值类型，例如：AVG_FileSize

● 采集结果转换

可根据采集结果的不同值，转换为有意义的描述信息。如CIM schema模型定义中，对OperationalStatus属性定义的采集值均为无意义的数字，需要额外做对应的映射转换。如下图所示：



展现形式自定义

自定义监控采集平台内置了低代码平台，可灵活定义自定义监控对象的展现形态，在画布上自由布局、绘制Widget，在Widget中配置采集指标，可以自定义丰富的展现形式，并实时显示配置效果，做到真正的所见即所得。

低代码平台通过Widget的方式，对指标的展现形式提供多种配置，包括：

■ 图形配置：可分别对每个数值型的指标配置各自的展示图形，包括趋势图、柱状图、饼图、仪表盘等。

■ 表格配置：预置多种表格样式供选择，并可配置表格数据过滤方式，包括基于某个指标的排序字段、排序方式、TopN等参数。

结束语

基于低代码思想的自定义监控采集平台，提供全套自定义采集过程的可视化配置工具，是监控软件系统未来的一个重要演进方向和发展趋势。沿着这条路线持续前进，不仅能降低自定义指标采集的学习和使用门槛，也可以使运维人员进一步减轻工作压力，提高对新产品的适配效率，充分发挥运维人员的能动性，体现运维人员的价值。同时，这也是商业化的监控软件与时俱进，提高差异化竞争力的重要手段。

自定义监控采集可视化平台涉及面很广，平台的设计还可以继续优化和完善，欢迎大家共同探讨提升。

数据中心绿色运维助力碳中和

文/汪宏

低碳运维——大势所趋

“双碳”战略成为我国经济发展长期目标。数据中心作为一种新型基础设施上升为数字经济时代区域和国家竞争力的核心战略资源。数据中心在双碳背景下正在追求绿色高质量可持续发展。

数据中心的全生命周期包括规划、设计、实施、验证、运维五大阶段。

数据中心全生命周期各阶段对能耗都有影响，其中运维、设计对能耗的影响最大，设计决定了数据中心的基因，运维决定了数据中心的效果，运维可以占到能耗影响因子的40%，而且有逐年上升的趋势。

基础设施运维经历了从人工运维、流程化运维到自动化运维，发展至今随着巨型数据中心的增长，数据中心运维管理工作的难度和复杂度越来越大。此时智能化运维应运而生。

智能化运维实际就是一个高度自动化的产物。利用人工智能对数据中心的运行数据进行分析，从而提高运维水平。当业务量处于波谷时降低设备运行功率，实现能源合理高效利用，从而实现低碳运维的终极目标。这个趋势和数据中心的可持续发展是相吻合的。

运维的理念贯穿于数据中心的整个生命周期，它在实现数据中心规划、设计和建设过程中所追求的可靠性、能碳双效目标方面发挥着重要的作用。低碳运维，势在必行。

数据中心运维面临新挑战

降低PUE，不仅能降低数据中心年运营成本，现在更是企业的社会责任。国家监管部门不断出台政策，对电能利用效率有着越来越严苛的规定，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，国家枢纽节点绿色节能示范进一步降到1.15，这对自然条件没有优势的地区都是巨大的挑战。

运维方式需要从粗放式运维管理向精细化运维管理转变。

现有数据中心的监控系统不完善，能耗计量不完备，无法准确地掌握数据中心的总体能耗情况。大中型数据中心系统复杂，参数繁多，需要进行优化设置。对于已建成的大型数据中心来说，影响能效的参数，可能有成百上千个，互相制约，相互影响，如何进行优化设置？运维团队无从下手。如何在保障数据中心可靠的基础上进行节能优化，运维改造方案对我们数据中心的可靠性影响有多大？是否对我们未来的运维工作带来安全风险隐患？面对更少的预算、有限的资源和环保要求，能耗过高的数据中心变成了问题的焦点。

事实上任何数据中心都可以持续提高能源使用效率，甚至采取低成本或无成本的措施就可以实现。

低碳运维之道

降低PUE是运维工作中的重点。PUE和我们数据中心的地点、等级规模、负载率等都有很直接的关系，特别是国内建成多年的数据中心，从设计规划之初，为了保障可靠性，对节能的要求不高，能耗指标普遍都是不符合目前监管要求的，运维团队如何在运维工作中，持续地优化，实现低碳运维呢？

主要包括两方面，一方面是技术措施，一方面是管理措施。

那么在技术措施上面，从以下几点入手：

能效评估

深入了解数据中心的能耗水平，发掘节能潜力。我们数据中心的能耗结构如何？我们的设备、系统，它的损耗是否在合理的范围之内？特别是对于老旧数据中心，由于设备本身的运行老化问题，或者是本身的一些性能指标设置，它的能耗已经非常高了，甚至远超同类设备的水平了，有没有必要进行换新？

暖通节能措施

- 根据机房负荷制定蓄冷罐充放冷运行策略；
- 探索热回收技术，可通过热泵机组及蓄热技术提供其它区域热源；
- 小流量，大温差，提高冷冻水供回水温度，充分利用自然冷源；
- 自然冷却，提高能效的核心是不用机械制冷或少用机械制冷，充分利用自然冷源；
- 设备升级、比如磁悬浮压缩机等；
- 合理参数治理，气流组织优化。

电气节能措施

- 提升负载率，根据末端负荷所需，动态调整；关停“超支冗余设备”；
- 关闭/调节不需要的照明，按需分区，控制启停灯具数量；
- 淘汰老式电机，更换为节能型电动机，并合理选型，提高负载率；或采用变频器控制，降低转速节能；
- 无功自动补偿，降低线损，节约电能；

■设置UPS的ECO模式和HVDC模式；

■简化架构，在保证可靠性的前提下从电气架构上做减法，从2N，到DR\RR的应用，从2路UPS到一路市电一路高压直流，都可以减少损耗，提高能效；

■直流电网，用储一体。

BMS优化

许多数据中心有最可靠的电力系统和空调系统，但是缺乏足够可靠及智能化的BMS系统。现实中自动控制设计往往居于次要地位，不良的BMS系统往往给数据中心的运维带来风险。国内外数据中心的运维经验表明：超过50%以上的故障原因直接与人为活动或者人力运维行动相关。BMS可以提供在不同的内部、外部负荷及室外气象条件下，严格控制空间环境的状况，自动替换故障组件和故障系统；减少运维人员的失误，能源效率最大化，以及确保数据中心可靠性。

IT节能降耗

■应用优化，通过架构优化，应用代码前后台优化，提升应用的效率；

■架构优化，综合考虑计算/存储/网络/备份等不同类型资源能源消耗占比；

■使用云/SDN，增加硬件设备的复用，使用容器，减少平台能源消耗；对容灾环境资源合理利用；

■使用低耗能/绿色/环保的硬件设备如液冷设备，使用低耗能的平台。

在管理措施上面，可以从以下几点入手：

积极开展运维评估

开展运维评估，就是要找出数据中心当下的运维水平和高成熟度的差距。通过差距分析来新建或者是优化管理制度或者流程，实现精细化运维，全面提升运维管理水平。

健全数据中心的能耗管理制度

运维团队要定期进行一些专项培训，提升团队的节能减排意识，同时也需要建立域名能效考核评定，进行能效考核的奖惩。从政策上激励员工节能积极性；从制度上来约束和强化节能意识。

建立电机的专项管理制度和流程

电机的专项管理制度在很多数据中心也是比较容易被忽略的一项，因为电机效率，随着长时间的运行，以及设备的老化，或者是维护的不当，它的效率是逐渐下降的。电机的专项管理制度是需要对电机这块进行一个全生命周期的建档制度的管理，对效率以及震动等等很多重要参数，进行建档分析，电机的制度相当于是做主动式运维。主动式运维的核心就是趋势分析。在问题发现之前，由运营团队发现这种故障趋势，而进行前期的干涉和处理。

提升自动化的管理水平

减少运维管理对人员的依赖性。通过智能的运维平台，提高运维管理水平，积极从传统运维向智能运维转型。

新华三运维服务

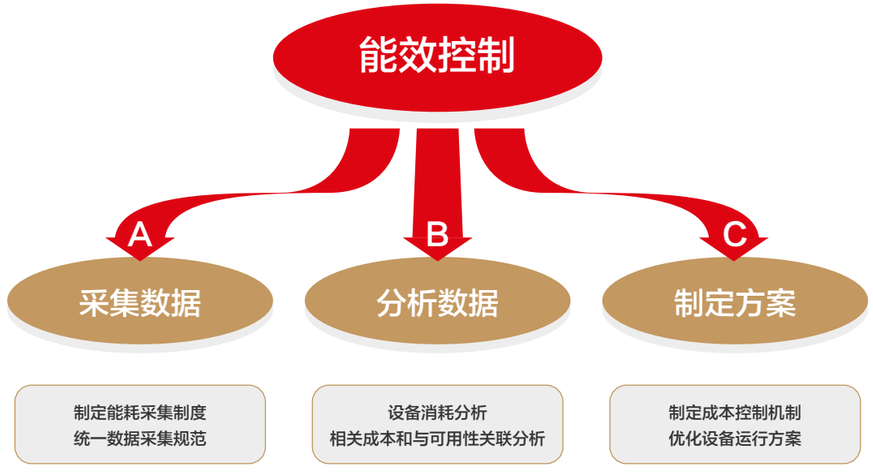
新华三提供数据中心全生命周期服务，包括数据中心的规划、咨询、工艺设计、集成总包以及验证测试和数据中心的运维，并且提供全过程的项目管理服务。在运维阶段具有大数据中心自底至顶的统一运维能力，融合全面AI的数字基础设施、云平台、云服务的统一运维体系，并具备持续优化能力。

在运维阶段，我们主要提供以下这四类服务。包括运维体系搭建服务，运维体系评估服务，设施运维服务，运维能效评估提升服务，其中运维能效评估深入分析数据中心的各设备、各系统的能源效率。根据我们的测算结果，提出合理化的数据中心能效优化建议和改进措施。

通过运维提高数据中心能碳效率是一个多步骤的过程：通过了解哪里可以节省以及能节省多少、了解成本、对需要改变的地方进行规划，所有这些都可以通过运维专家服务获得。

新华三数据中心能碳双效管理体系就是从数据中心全生命周期的全过程出发，遵循系统管理原则，通过实施一套完整的标准、规范和大量的项目实践经验，建立起一个完整有效的能碳双效评估体系。

通过例行节能监测、能源审计、能效对标、组织能耗计量与测试、组织能量平衡统计、节能技改等措施，不断提高数据中心能效管理体系持续改进的有效性，实现能效管理方针，达到预期的能源消耗或使用目标。



它可以帮助数据中心更好地利用数据中心现有空间；减少能源使用，提高数据中心效率；降低数据中心运营费用和碳足迹。

新华三结合了丰富的数据中心的运维最佳实践，建立了一套完备的数据中心运维管理体系。为客户提供覆盖全生命周期的运维服务。保证我们数据中心的低碳、安全、稳定、可靠的运行。

RPA技术及在生产制造业的应用

文/耿亮

前言

随着大数据、云计算、物联网、人工智能等新技术的不断涌现，以及国务院《中国制造2025》的战略推动下，数字化转型已经成为传统生产制造业实现质量变革、效率变革、动力变革的重要途径。

如何借助日新月异的新技术实现数字化转型，进而提高企业生产效率，增强企业核心竞争力，开始成为很多传统生产制造企业探索实践的新方向。

当下，传统生产制造企业面临着许许多多、各式各样的问题。

■ 逐渐增加的人力成本，高昂的自动化设备更换成本；

■ 车间员工逐渐流失，新老交替困难；

■ 信息化较为落后。大部分中小型生产制造企业依然在采用Word、Excel 、Email等原始方式进行信息管理和沟通，无法做到信息的实时共享反馈；

■ 业务系统集成难。大多数生产制造企业使用大大小小各类业务系统，而且大部分是采购第三方提供的信息系统。各个系统间极易形成信息孤岛，致使业务流程难以闭环，数据无法互通，进而无法实现数据反哺并驱动业务；

■ 技术更新迭代快。传统制造业如何选择适合的技术，更快速的实现数字化，成为一个难题。目前大多数中小型制造企业是以回报优先作为数字化转型的优先策略。

那么如何在现有的条件下，通过RPA快速帮助传统生产制造业实现比较切合实际的数字化转型，将是本文需要探讨的话题。

何为RPA？

为了在全球经济中保持竞争力，降本增效和提高生产力，已成为制造业的普遍共识。以工业机器人和智能制造设备为代表的智能装备，正为传统生产制造业带来全新的变革。流水线、设备自动化改造与升级，工业机器人为企业带来了生产高度自动化，可控的成本以及丰厚的利润。那么企业的业务管理系统也同样需要实现业务流程自动化。

RPA（Robotic Process Automation），译为流程自动化机器人，又可以称为数字化劳动力（Digital Labor），是一种智能化软件，通过预先设置好的流程、规则，模拟人工在各类应用软件中进行点击、输入等操作，以协助员工完成“规则较固定、频率高、重复性较强”的工作。

Robotic 机器人	Process 业务流程	Automation 自动化
为企业构建虚拟劳动力，引入OCR、NLP、语音识别等人工智能技术，提升速度、准确性、合规性、可审计性及可扩展性，助力现代企业数字化与智能化转型	通过训练之后，能够像人类一样通过用户界面(GUI)模拟人的操作来驱动应用。机器人可灵活的在各个系统之间，执行操作并自动触发下游活动，完成一个完整的业务流	数字化与智能化，7×24h运行

RPA特点

■ 高效率、高准确率，提高追溯性

可减少人为错误，提高可追溯性，因为机器人自动化执行过程中的每一步操作都会进行日志记录，甚至是截图，这样可以更快速的排查问题。

■ 降本增效

机器人速度非常快，且可不中断地进行7×24小时工作，相较于员工每天工作八小时，可大大提高生产力，降低人力以及时间成本。

■ 投资回报周期较短

例如系统集成，通过使用机器人，模拟人工操作，可快速实现系统数据互通，投资回报周期远比传统的软件开发短。

■ 自动操作，非浸入式

像人工一样，操作各种系统，就可以对企业业务系统进行外挂式集成，而系统本身没有任何修改，风险很低。

RPA擅长做哪些工作?

数据密集性工作
大量数据检索、搜索、导出、整理、录入，按照既定业务逻辑进行数据处理、分析等工作

高度重复
业务流程标准化程度高，工作量大，重复度高，现在是以大量人工来完成的

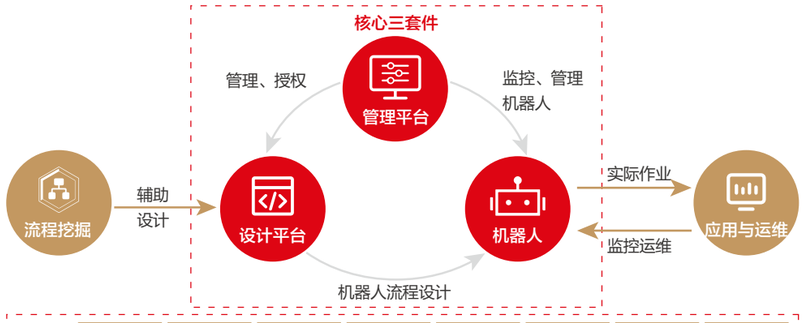
大量文本操作
从海量的文本中检索、分类、查找对应的文件、文本信息，进行语音分析处理等

信息私密敏感
操作的数据或信息，属于涉密或隐私文件，人工操作泄密风险高

高出错率
大量人工操作，容易导致高出错率，高离职率，极大的影响业务的稳定性和持续性

IT系统复杂
需要跨系统、跨平台操作数据和业务流程串联，现有系统复杂度高，改造工作量大、风险大

RPA产品全流程与技术



管理平台
实现对设计平台的管理、授权等功能，提高设计平台安全性。
用来集中调度、监控、管理机器人运行。包括机器人集群管理、流程任务分发、定时计划，提高了机器人的利用率。

设计平台
自动化流程编排工具。依据业务流程，利用可视化界面，以低代码/零代码的方式设计各种自动化业务流程。内置丰富的预构活动模板，融合NLP、CV/OCR、Ops等多种前沿技术，并支持多种编程语言作为脚本，以实现对机器人的流程设计。

机器人
机器人负责执行设计平台设置好的流程。
运行方式有无人值守和有人值守2种，无人值守可在包括虚拟环境的多种环境下运行；有人值守需人来控制流程开关。

流程挖掘
通过录屏、大数据、AI等技术，对用户行为进行分析，挖掘出以流程为核心的业务，辅助用户，快速构建机器人流程，降低RPA实施成本。

应用运维
机器人执行预设流程，进行全链路性监控。提升对机器人的运维能力，为实现智能调度提供数据依据。

生产制造业应用

RPA在生产制造中的应用场景

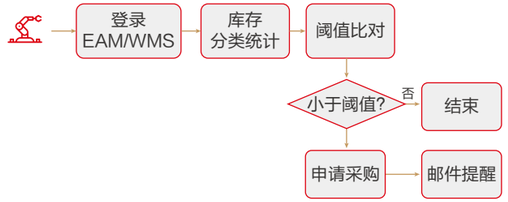
生产制造业中存在很多与RPA高度适配的业务，且技术ROI表现良好。传统生产制造业系统种类繁多，大致包含ERP、制造执行系统（MES）、高级计划与排程系统（APS）、设备资产管理系统（EAM）、仓库管理系统（WMS）、过程质量控制系统（PQC）以及一些常规的OA系统等等。随着智能制造的兴起，企业数字化转型的推动，又引入了物联网平台、机床设备数据采集系统（MDC）、分布式数控管理系统（DNC）等相关系统，加强了生产设备的监控与管理。其中RPA可适配的业务包含常规的统计报表、邮件服务、系统集成、数据迁移等等。

系统整合机器人

工厂会部署多项ERP子系统，包括财务管理、生产制造执行系统、设备管理系统等等。员工经常需要从一个系统跳到另一个系统中，以实现数据的交换共享。RPA可以整合ERP、MES等系统，代替人工、以低/零代码方式实现各系统间的交互。还可以推动MES等运营管理平台与其他管理系统之间的交互操作，有效增加运营的灵活性和透明度，例如离散型MES生产订单与过程质量管理系统PQC正反向信息同步。

原材料 / 设备备件库存预警机器人

在修理设备时用来更换磨损和老化零件的零件叫做配件。为了缩短设备修理停歇时间，在备件库内经常保存一定数量的配件，叫做备件。当备件库存数量低于维修人员设置的阈值，就需要采购备件。



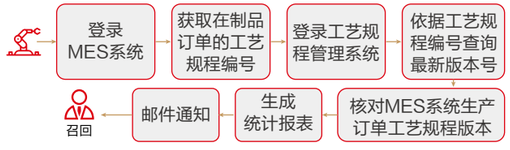
BOM信息同步及核对机器人

BOM信息是生产制造企业的核心数据，同时被多个IT系统使用，其准确性和及时性是确保企业正常开展生产业务的重要基础。XX汽车制造企业需要从Excel/Word/PDF文件中汇总BOM基本数据，再以传统的手工方式录入SAP，效率低、易出错、时效性差。

引入RPA后，由机器人自动完成各类文件的解析和汇总，基于SAP GUI自动完成信息录入，并与初始数据进行数据比对，确保数据准确性，1000条BOM数据10分钟即可完成整个流程。

工艺规程升版提醒机器人

在离散制造行业中，工艺规程复杂多变，经常会出现生产订单初始采用的工艺规程为最新版，但是在生产过程中，该工艺规程进行了升版。此时，工艺人员通过电话联系文件管理部咨询确定哪些生产订单在使用旧版工艺规程，再联系生产车间召回正在使用的旧版，改为采用最新版本继续生产。首先需要确定涉及到哪些订单，其次追回旧版比较耗时。



引入工艺规程升版预提醒机器人后，可更快速的发现哪些在制品生产订单的工艺规程存在升版的情况，方便工艺人员、文件管理部、生产车间及时更换。

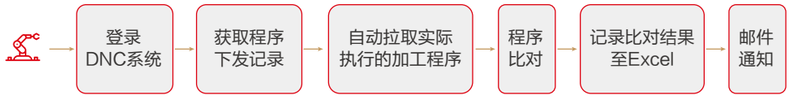
设备故障检测机器人

员工手动抄录生产设备上的各种传感器数据，难免有所疏漏，统计分析错误的数据信息，还可能导致潜在问题迟迟未被发现。一旦设备出现故障，必将影响生产。智能制造中所涉及到的MDC数据采集系统（Manufacturing Data Collection & Status Management）主要用于采集数控机床和其他生产设备的工作和运行状态数据，实现对设备的监视与控制，并对采集的数据进行分析处理，也可为MES和ERP等其他软件提供数据支持。

RPA机器人可7×24小时不间断工作，一旦发现MDC采集数据出现故障类异常信息立即通过邮件发送给负责人。不但将员工从重复单调的抄录统计中解放出来，还可提高检测频率和准确性，防范故障隐患。

数控加工程序比对机器人

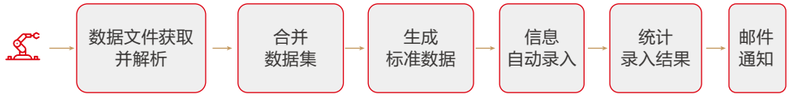
数控编程工艺员，编写完成数控加工程序后，通过DNC分布式数控管理系统，将程序下发至生产设备工作站，待生产车间员工对程序进行调整后，再执行数控加工。加工完成后，数控加工程序会被生产车间工人回传到DNC系统中。最后，数控编程工艺员会对该程序进行比对、调优。



引用数控加工程序比对机器人后，使得数控编程工艺员仅需处理程序比对结果，无需人工点击比对操作，而生产车间工人亦不用手动回传数控程序。既降低了人力成本，又提高了流程效率。

数据迁移机器人

很多中小型传统生产制造企业，信息化程度较差，依然采用Excel、Word、PDF等方式进行信息记录、共享。当某天企业启用新的业务模板或采购新的业务系统后，迁移费时费力。

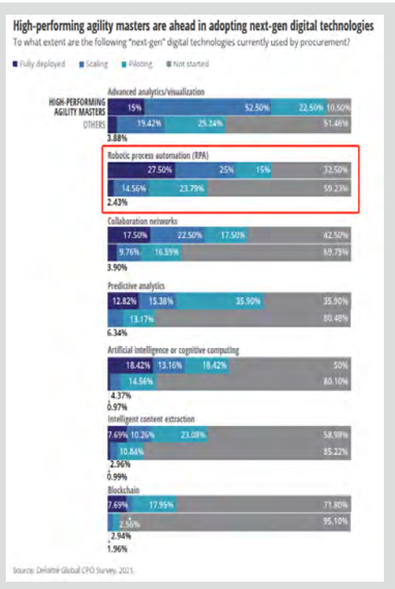


使用数据迁移机器人，可7×24小时无人值守，不仅可以降低人工迁移成本和减少人为出错率，还可以零代码进行迁移并提升迁移速度。

行业现状

自2011年开始，德勤每年都会发布《全球首席采购官（CPO）调查报告》，通过采购官们对创新技术的采购意向、标准，了解企业业务流程中面临的挑战和机遇。今年，德勤对40多个国家/地区的400多位大型组织的首席采购官进行了调查，技术采购标准基于投资回报率、运营效率、易用性、敏捷性和人工节省等。

运营效率和数字化转型成为采购技术的最重要的两个标准，直接关系到组织的业务可持续性发展。



调查报告显示，在创新技术采购领域中，RPA成为了首席采购官们的采购重点。

据统计相较于2019年RPA采购率2.4%，2021年暴涨至27.5%，采购率超10倍。

行业前景

根据全球知名咨询调查机构Gartner的最新预测，到2022年，全球支持超级自动化的技术市场将达到5966亿美元，高于2020年的4816亿美元和今年预计的5324亿美元。到2024年，组织将超级自动化技术与经过重新设计的运营流程相结合使用，可以降低30%的运营成本。

Gartner研究副总裁Fabrizio Biscotti表示，由于COVID-19（新冠）的出现，组织对超级自动化的态度已从“选择”变成了“必须”。尤其是那些迫于数字化转型的组织，急需将更多的数字化业务流程和IT工作实现自动化。

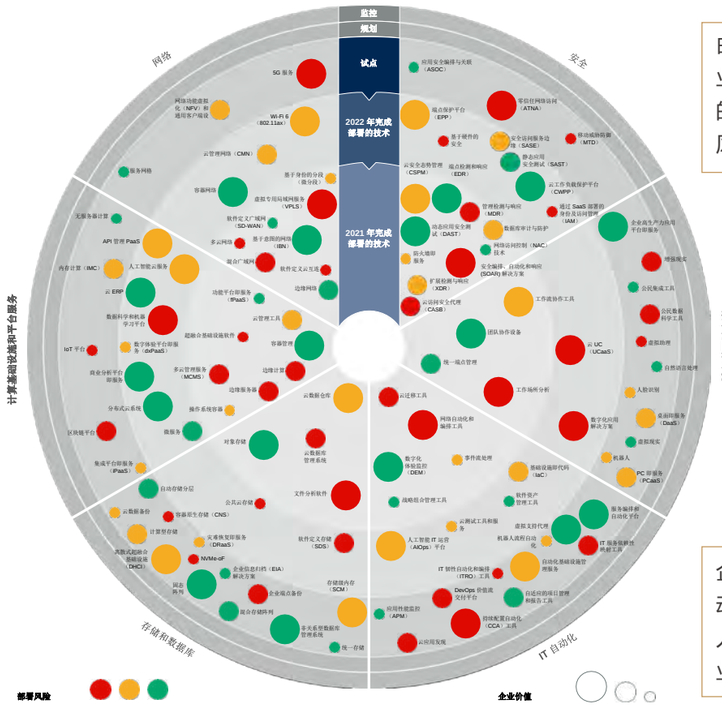
Gartner研究副总裁Cathy Tornbohm表示，卓越的运营效率和成本的大量节省，是全球组织使用超级自动化的根本原因。很多组织正在从低效自动化技术过度到更加紧密、功能强大的超级自动化技术。所以，为了满足用户需求，很多厂商开始将RPA、LCAP、AI等技术集成在一起使用。

Table 1:Worldwide Forecast for Hyperautomation-Enabling Technologies（Millions of U.S.Dollars）

	2020	2021	2022
Process-Agnostic Software That Enables Hyperautomation	19,604	25,108	30,184
Other Software That Enables Hyperautomation	462,030	507,316	566,433
Total	**481,635**	**532,424**	**596,616**

Source:Gartner(April 2021)

Gartner，2021-2023大型企业新型技术路线图



由437家企业机构的IT专业人士共同对111项技术的使用计划、预期价值和风险进行基准测试。

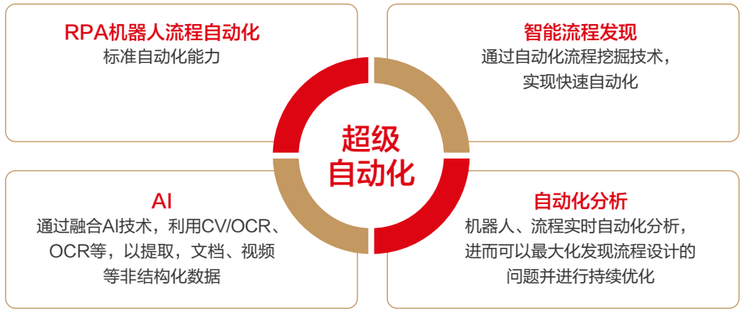
由于对疫情应对日趋成熟，与2020年相比， 2021年对全新数字化工作场所的技术需求达到高峰，该技术对新冠疫情的反应已经十分成熟。很多企业试点了机器人 。

企业更有选择性地采用自动化相关技术。其中机器人流程自动化成为很多企业首选试点技术。

展望

10月19日，Gartner发布了《2022年12大技术趋势》报告。超级自动化已连续3年入选，成为入选次数最多的技术之一。充分说明超级自动化在全球数字化转型浪潮中将继续担任重要角色，超级自动化市场将继续保持高速增长趋势。超级自动化曾在《2020年10大技术趋势》报告中有Gartner首次提出且位居首位，并在《2021年9大技术趋势》报告中再次入选。

超级自动化以业务驱动，可识别、审查和自动执行尽可能多的业务和IT流程，需要协调使用多种技术工具和平台，包括机器人流程自动化（RPA）、低代码平台和流程挖掘工具。



目前各大RPA厂商基本战略都是超级自动化。产品能力拓展主要以“AI深度融合”、“智能流程挖掘”、“流程执行”、“效能分析”、“运维管控”为探索方向，旨在通过对业务流程进行有效的挖掘来快速构建自动化流程，对机器人执行过程进行实时分析，进而发现问题优化自动化流程，对机器人进行360°监视管控。

AI融合

标配：非结构化数据提取

探索：智能自动化，智能捕获、智能编排，促使这位“数字同事”与公司员工之间能更智能的协作办公

流程构建

标配：录屏功能，这是建立在已知的业务流程上，用以快速构建自动化流程

探索：智能流程挖掘，通过对第三方系统操作日志进行智能分析，构建流程

执行效能分析

标配：机器人流程执行记录、看板

探索：机器人执行自动化流程过程时，实时分析，从中发现自动化流程问题，持续优化

运维管控

标配：实时显示机器人状态、流程状态，简单的启停控制

探索：Ops运维管控，“数字员工”像公司员工一样有组织有纪律

即服务 自服务——HPE GreenLake Central前沿方案概述

文/秦明焓

HPE重新定义数字化转型

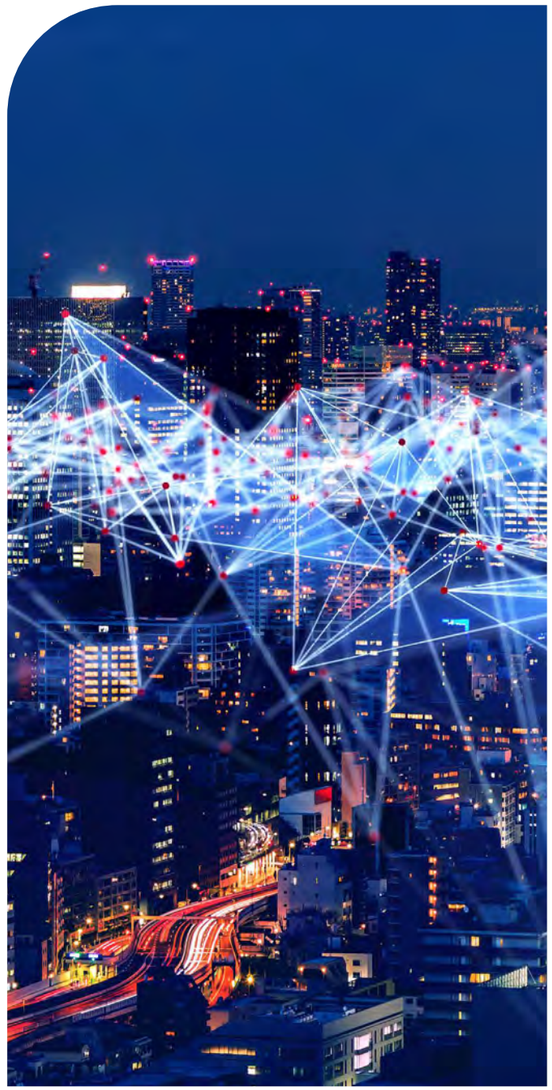
麦肯锡早在2016年发布的企业数字化转型研报中就指出，高达70%的数字化转型项目最终失败，原因在于缺乏相关经验、无效执行以及企业文化不配合。过去几年，尽管数字化转型的呼声很高，但各大技术厂商只是从推广自家产品角度发声，企业真正需要的高效、快速、低成本落地的数字化转型整体方案寥寥无几。

刚刚第三次蝉联Gartner年度供应商评估“优级”的HPE，对于成功的数字化转型有着自己的定义：将自动化与敏捷实践带入企业IT，交付敏捷且灵活的业务，以适应并在任何市场环境中获得成功。

HPE首席数字化转型专家Steve Fatigante与HPE企业服务副总裁Alexey Gerasimov联合撰文指出：要实现成功的数字化转型，需要关注四大关键点：安全、企业架构、基础设施和应用开发。首先是安全，整体方案建设初期就要将安全设为首要目标；其次是企业架构，采用业界标准架构意味着能加速推出业务成果；第三是基础设施，企业往往都有遗留IT系统，而全盘托管并以即服务形式交付，能让企业轻装上阵；第四是应用开发，通过与开发团队的合作，了解敏捷开发方式下对于工作负载的需求、每个工作负载所需的交付方式、对工作负载进行云原生重构，从而优化整个过程。

HPE GREENLAKE一切即服务

在2017年，HPE推出了面向“即服务”商业模式的全新品牌GreenLake，在本地及托管环境为企业全面提供数字化转型咨询及开发、基础设施按用付费及生命周期全托管服务。自HPE GreenLake品牌发布后，HPE就不断将该品牌扩展到自有的软件、硬件和服务产品中，并可跨企业本地、托管数据中心以及公有云，提供一整套完整的云管理体验。上市以来，HPE GreenLake就不断整合HPE及合作伙伴的产品与方案，典型组合包括：



■ HPE GreenLake for VDI云服务在疫情期间受到了极大的欢迎，为了帮助更多的企业和机构，HPE GreenLake for VDI拓展了合作伙伴方案组合，收录了Citrix、VMware和微软的VDI方案以及NVIDIA vGPU等，甚至还囊括了合作伙伴Wipro和Accenture的工作场所服务。

■ SAP HANA内存数据库及SAP S/4 HANA ERP套件是很多企业的基础性软件，HPE GreenLake为了SAP HANA而设计了优化的方案，采用按使用付费模式以及可满足苛刻关键任务所需的性能、安全性和控制。与其它云产品（提供商决定客户何时更新和运行何种版本）不同，适用于SAP HANA的HPE GreenLake允许用户控制特定的应用程序升级。此外，企业还可以选择由SAP提供、HPE GreenLake支撑的SAP HANA企业云（客户版）。

■ HPC高性能计算对于很多企业R&D特别是数据密集型分析、AI、ML任务来说越来越具有战略价值，HPE一直是HPC领域的领导厂商，也发布了HPE GreenLake Cloud Services for HPC服务“超级计算即服务”，为数据科学家、企业科研人员和数据分析师等提供了易用的HPC能力，而无需考虑复杂的HPC互连配置等IT问题，这对于中小企业来说特别具有普及超算的价值。

■ 在边缘计算方面，HPE SimpliVity是面向企业边缘场景优化的HCI方案，最新支持Kubernetes的Container Storage Interface（CSI），从而在边缘节点运行基于容器的工作负载。HPE SimpliVity同时支持CSI以及持久化卷（PV），这样就可以同时运行VM虚机和容器工作负载，推动云原生应用向边缘的扩展。

■ 在计算实例方面，HPE GreenLake最新推出了裸金属服务器，让企业可以直接在服务器上运行工作负载；HPE GreenLake的虚机服务则推出了最小100VM起步以及4、8、12、16节点的配置，为企业提供了丰富的选择。

■ 在合作伙伴方面，HPE GreenLake继续进入到大型分销商的云市场，现在超过10万家合作伙伴可以通过分销商为企业和机构提供HPE GreenLake。而对于那些需要托管数据中心模式的客户，HPE GreenLake也加强了与CyrusOne、Equinix的合作，企业和机构现在可以通过一张合同和一份发票就在CyrusOne和Equinix的数据中心运行HPE GreenLake。

与HPE GreenLake相配合，HPE PointNext Services提供售前咨询及开发服务，HPE GreenLake Managed Services提供全球IT运营离岸外包服务。如今HPE GreenLake已成为一个年订单额超过52亿美元的庞大业务，在50个国家拥有1200多家客户。

GreenLake发布以来，HPE不仅持续将其扩展到更多产品线及相关服务，而且在2019年推出了GreenLake Central管理平台，形成横跨企业本地及托管环境IT基础设施，且提供一致性云化IT管理体验的完整解决方案。企业IT基础设施的运营和治理，包括成本管理、IT运行部署、性能优化、合规策略等，都可通过GreenLake Central实现。

HPE GREENLAKE CENTRAL概览

HPE GreenLake Central是一个实现即服务的在线门户和操作平台，企业可以由此轻松地访问、操作及部署GreenLake管理的各地IT基础设施及其服务，它还可以进行消费分析，计算出该客户使用了多少GreenLake基础设施，并追踪可用容量，由此，客户通过一个门户就可以获得统一的云管理体验。

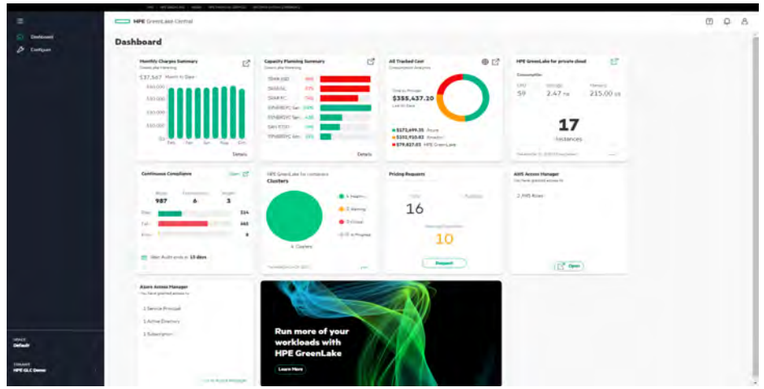
由HPE GreenLake Central实现的各项服务中，有一款服务是专为虚拟云环境打造的：

■ 硬件和软件将由HPE的工厂进行预集成，运至您的托管设施或数据中心，然后由HPE（中国市场是新华三）负责安装、配置和优化。

■ GreenLake Central自助式门户除了提供基于角色的访问策略，还通过广泛的API赋能快速完成VM虚机的配置，并提供一套丰富的能力和自动化功能来编排和管理应用生命周期。

■ 方案交付转运营后可由HPE全托管，HPE将实时监控并管理用量和性能，在需要时及时扩展容量，同时负责基础设施的运维、容灾、合规等事务。

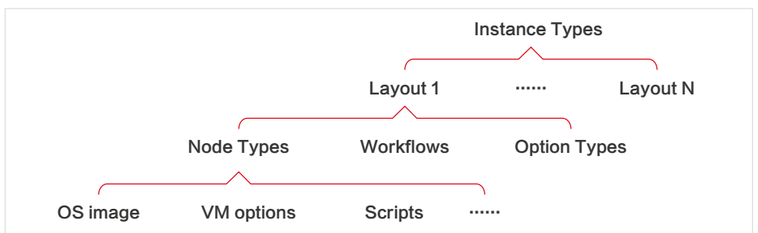
此外，GreenLake Central还拥有一系列丰富的能力，包括实例类型、蓝图、自动化脚本集成和工作流等，不仅能以即服务的形式交付虚拟机基础设施，还能以轻松、灵活和可靠的方式创建并部署应用。下面将简单介绍GreenLake Central如何发挥这些功能和最佳实践。



实例

云应用管理具备多种能力，Instances（实例）功能就是其中之一。在包括AWS在内的很多云管理平台中，Instance代表了虚拟机等单一对象。GreenLake Central中，实例可以是一个安装了基础操作系统的虚拟机，也可以是在一个或多个虚拟机上运行的应用服务。比如，实例可以是运行CentOS OS的虚拟机，也可以是运行在一个虚拟机上的MariaDB数据库服务，或是运行在三个虚拟机上的MariaDB数据库服务。

■实例类型

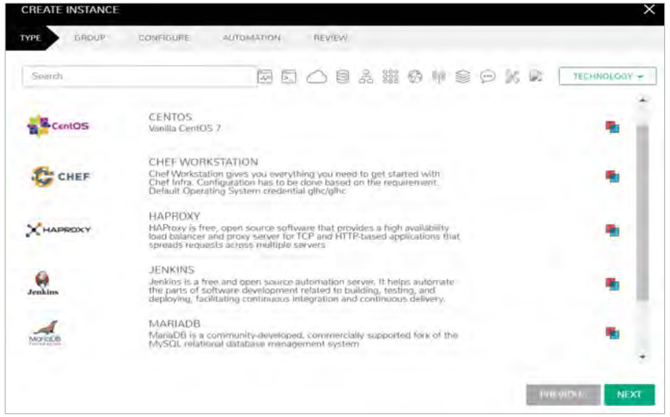


上图展示的是实例类型的层级式设计。一个实例类型包含有一个基础操作系统映像，以及大量其它的配置选项，例如脚本、工作流和选项类型等。

■创建实例

当您搭建好了自己的实例类型，并将它添加到实例类型目录中之后，您就可以利用实例创建引导程序来创建实例。

在GreenLake Central控制面板中，在主菜单中点击Provisioning标签页，选择 Instances，点击绿色的+ADD图标来添加新的实例。在CREATE INSTANCE引导程序中，TYPE标签页会显示实例类型目录中有哪些实例是可用的。下图显示的是范例截图。



默认情况下，GreenLake Central提供一些预置的实例类型，例如CentOS和Apache，用户也可自定义实例类型，例如Chef、HAProxy、Jenkins和MariaDB。我们建议您遵循最佳实践来创建应用实例类型和实例。

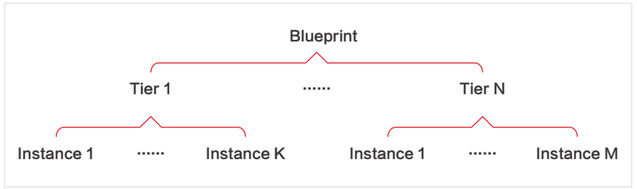
■实例最佳实践

我们之前已经提到过，GreenLake Central的优势之一是为终端用户提供了简单易用的自助式门户。为了给客户提供更有效的服务，公司的IT部门可以根据公司的标准和业务需求，搭建一系列的黄金镜像，例如一系列最新的guest操作系统（Windows、CentOS、Ubuntu、SLES、Red Hat®Enterprise Linux®[RHEL]等）的主要版本；或是要满足网络、安全性、NIC等方面的具体要求；再或者需要一些基础应用服务器，例如Apache Web Server。之后，IT部门将这些黄金镜像上传至GreenLake Central的虚拟映像商店。利用GreenLake的自助式门户，应用开发者可以使用同样的黄金OS镜像来创建自己的应用实例类型，例如，数据库开发者创建MariaDB实例类型，DevOps开发者创建Chef Workstation实例类型，或HAProxy负载均衡器及proxy服务器实例图像，或Jenkins实例类型等。利用此最佳实践，公司的IT团队仅需要维护黄金镜像；应用开发者也获得了极大的灵活性，能够快速、敏捷地搭建他们自己的应用实例，同时减少了对公司IT部门的依赖。

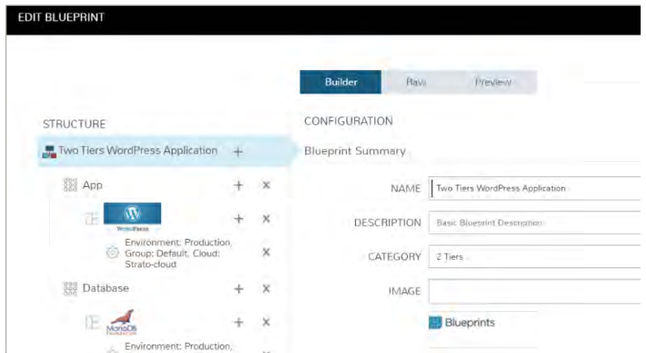
蓝图和应用

GreenLake Central的另一个强大功能是蓝图功能。利用蓝图功能，您可以快速、可靠地完成应用的实例化。

蓝图层级



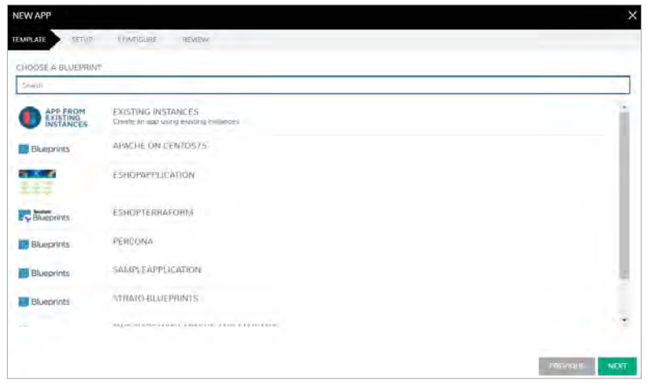
上图展示了蓝图的层次设计。简单说，蓝图是一个应用模板，它定义了应用的结构。应用程序可以是单层或多层的，例如连接在一起以提供服务的web层、应用层和数据库层。层级和实例类型决定了蓝图的结构。一个蓝图可以有多个层级，例如web、应用、数据库、缓存、通信等等。一个层级可能包含有一个实例类型或一组实例类型。层级可以被标记成互联状态，并依此来恰当地定义网络通信层级。这些层级也可以根据应用的要求来设定启动顺序，一个应用就是一个蓝图的实例化。



上图显示的是两层级的WordPress应用蓝图范例，在应用层级利用WordPress实例类型，在数据库层级利用MariaDB实例类型。蓝图以YAML或JSON代码输出，利用API和CLI创建。GreenLake Central在构建了自己的蓝图之后，就能够轻松地输出蓝图，并将它交付给另一个GreenLake Central环境。

蓝图最佳实践

了解了什么是蓝图后，就可以来看看如何利用蓝图功能快速创建并部署应用。正如我们在“实例”一章中所讲的那样，应用开发者已经获得了灵活而丰富的配置选项，可以根据应用的要求，利用黄金OS镜像来构建实例类别。蓝图功能赋能应用开发者利用不同的实例类型，轻松搭建多层级的蓝图。在完成了应用蓝图之后，您就可以将它存入蓝图目录。之后，您可以进入Provisioning > Apps，点击绿色+ADD，然后再依循NEW APP引导程序，从目录中选择相应的蓝图来快速配置应用。



上图所显示的就是在NEW APP引导程序中的蓝图目录范例。基于蓝图功能，我们就可以轻松创建并部署具有复制能力的应用。

自动化工具集成

GreenLake Central还具有丰富的自动化功能，例如，任务、工作流，以及与各行业的多种自动化工具集成的能力，包括Puppet、Chef、Ansible和Ansible Towe等。任务是单独的自动化元素（例如，单独的手册或脚本）。工作流包括一个或多个任务。任务及工作流可以在Pre Provision、Provision或Post Provision阶段与实例、蓝图相集成。

结束语

HPE GreenLake Central具有一系列丰富的能力，实例、蓝图、自动化脚本、Ansible手册、任务和工作流等，不仅能够以即服务的形式提供VM基础设施，还能在其基础上，助您轻松、灵活地创建并部署可靠的应用，是一款强大的云应用管理平台。HPE作为一家传承了80余年经验和历史的企业IT服务巨头，在众说纷“云”时代为企业数字化转型找到了一条全新的路径，这就是打破对“云”的迷思、抓住云原生和企业需求的本质，为企业重新组装适应数字化新业务的IT基础设施。2020在疫情的催化作用下全球数字化转型进程提速了至少2-3年，有的行业甚至是5年。HPE GreenLake的“总装”模式，让企业和机构可以在本地数据中心快速获得云式IT服务，无疑将规模化激发后疫情时代的下一站数字化创新。

城市商业银行网络运维自动化趋势与实践

文/黄鹏

随着云计算、大数据、人工智能、区块链和5G技术的快速发展，全球金融机构的科技变革进程加快，银行业网络由传统网络向SDN网络演进，城市商业银行也紧跟时代步伐开始采用SDN网络，其网络虚拟化技术经历了传统的堆叠技术、大二层技术、NVO3技术（NvGRE、VxLAN、STT）的不断演进，到现在SD-WAN技术的应用。城市商业银行网络的高拓展性、伸缩性得到提升，但同时导致云化网络与传统网络并存，存在网络巡检难、故障感知难、问题定位难等网络运维难题，因此其网络运维自动化势在必行。

网络运维自动化趋势

网络运维难点

■统一管理难

城市商业银行大多存在多个厂商设备和运维工具，设备种类、品牌繁多，软件架构、版本各异。各运维工具之间缺乏协同、功能交错，不具备统一的网络资源管理平台形成全局网络可视化，导致整体效率低下。

■网络精细化管理难

网络监控颗粒度不足、告警信息不智能、链路和流量分析不全面。网络运维问题的发现往往依赖于用户、业务人员投诉等事件驱动，而基于静态阈值告警则极易造成问题误报和漏报，又不具备全面的链路和流量分析，因此难以及时发现问题、快速定位网络故障。

再加上SDN、云计算等新技术大大增加了应用系统以及基础网络的复杂度，云网融合环境出现的问题原因难以定位。例如，业务超时原因分析，需要追溯到任意一个历史时刻的网络、设备、链路、流量和业务状态，分析是中断、丢包、拥塞还是其他异常，导致的关联影响有哪些。

■网络风险把控难

缺乏完整的电子化运维流程和自动化手段，在日常变更工作中经常走线下审批流程，运维人员存在操作不规范情况，可能导致业务故障风险。

■网络配线维护难

由于城市商业银行网络分区固化造成跨机房的复杂布线、网络配线错综复杂，传统表格无法直观表达线路空间位置和分布情况，难以阅读理解，要查找关键信息较为困难。例如，发生通讯中断故障时，难以定位故障点，不利于故障分析处理；新增设备时，无法及时掌握端口占用情况，需要花费大量人力查找，运维效率低。

■运维效率提升难

随着网络规模日益庞大、业务架构日趋复杂、运维人员职责范围日渐扩大，解决网络运维问题需要更高的技术水平和更长的时间。而且一个业务牵涉诸多设备、策略和路由。例如，针对业务系统的网络访问权限策略、域间访问关系、网络设备配置和应用系统安全，其中的任何一个环节出现安全风险，都会影响整个业务系统。

当前网络设备配置，防火墙策略下发，访问关系梳理等工作很多通过人工完成，比如银行运维工作中经常碰到服务器ACL规则配置，大多都是人工完成。但是数据中心中服务器的数量非常庞大，需要大量人力部署海量的ACL规则和梳理出应用之间的访问关系，维护效率低且容易造成操作失误。因此银行需要一套高效率、自动化、准确性高的网络自动化运维平台。

网络运维自动化发展趋势

在当前云网融合的大环境下，银行业的云化网络与传统网络并存，网络运维场景由单一场景到复杂场景，从单数据中心到跨数据中心，从传统灾备到云多活灾备。随着网络技术域扩展，对网络运维提出了更高要求，网络运维也逐渐向自动化方向发展。

■由“独立运维”向“集中式运维”转变

随着银行业网络规模不断扩大，运维趋向集中，由以前各自为战的独立运维方式向集中式运维方式转变。

■由“集中式运维”向“标准化运维”转变

由于银行网络规模和复杂度的持续增加，如果缺少必要的操作标准和流程机制，运维工作会难以进行。运维团队开始逐渐使用运维工具和运维流程进行标准化运维，以此提高运行维护效率和网络运行质量，并保证包括软件版本数据、网络资源数据、网络运行质量数据、设备性能数据的一致性。

■由“标准化运维”向“自动化运维”转变

当业务规模达到一定程度后，银行对于运维效率和误操作率有了更高的要求，网络运维自动化势在必行。各大银行开始建设运维自动化平台，通过大数据和人工智能等技术实现自动化操作，进而解放人力，提高运维质量。

城市商业银行网络运维自动化实践

建设思路及目标

针对城市商业银行网络架构的复杂性和运维问题，建议从流程、工具、技术升级三方面进行思考和建设。首先需要构建标准的运维流程，通过标准化的人工操作来实现标准化运维。其次，结合网络自动化运维工具，将简单的运维工作自动化，提高运维效率。最后，随着技术的不断发展，结合SDN、容器、大数据和人工智能等技术，完善网络运维自动化能力。

主要建设目标：

■资源梳理要清晰。构建全行视角资源管理，梳理资源间关联关系；

■网络监控要全面。实现所有设备所有端口监控；

■故障告警要及时。要在业务受影响前发现问题；

■ 故障分析要智能。保证故障告警准确性的同时，进行故障关联分析，准确分析出故障根因及故障影响的业务范围；

■设备基线要准确。建立设备基线阀值，网络流量基线、网络切换时间基线必须准确；

■变更操作要自动。实现自动化配置检查、变更下发及验证；

■运维效率要提升。把日常运维操作固化到自动化脚本，降低人为操作失误，提高运维效率；

■ 网络技术要先进。通过INT、Telemetry Stream等流量分析技术，实现毫秒级网络运行指标监控，并结合自动化服务编排实现部分故障场景的自动恢复。

建设方案

针对银行网络运维的复杂问题，新华三U-Center 2.0统一运维平台，实现网络数字化、管理精细化、流程标准化、配线可视化、运维自动化和智能化。以先进的技术和大量的银行网络运维自动化实践经验，为客户建立统一的网络监管体系。

■网络数字化，构建统一的网络资源管理

目前很多城市商业银行都缺乏完善的CMDB，而数据中心设备种类、品牌繁多，架构、版本各异，运维人员要花大量的时间整理和维护这些资源信息，每次查找设备、资产盘点工作都非常繁杂，而且设备软硬件变更后的配置管理也不能自动更新。

新华三统一运维平台通过构建统一的配置管理CMDB，建立统一的资源管理和监控，构建全行视角资源管理，梳理资源间关联关系，加强网络资源集中化管理能力。

通过对资源关联关系进行建模和资源全生命周期信息管理，完成数据的自动化收集，建设集中、完整、统一、实时的资源配置管理数据库。记录、存储资源的应用系统信息、关联信息、软硬件基本信息、维护信息。为事件管理、问题管理、变更管理提供查询、诊断的基础，同时也为资产管理提供记录、查询、汇总、统计、分析基础。

解决银行实际网络资源管理中设备名称、型号、IP地址、SN、版本、维护人、项目名称、集成商、品牌、维保时间、所在数据中心、所在分区、所在机柜、报废信息、在网运行等信息不清晰的问题。并且可以实现网络设备板卡的品牌、型号、序列号及所在设备的管理。

■管理精细化，建设完善的资源监控体系

通过构建混合架构全域资源管理，实现业务系统、逻辑网络和物理网络三层互视。精细化监控全网所有设备的所有端口、网络链路以及链路健康状态展示，借助动态阈值等领先技术智能收敛海量告警，辅助故障根因定位，准确分析网络故障所影响的IP地址和业务范围，实现业务质量可视可控，持续优化业务可用性。

通过自动化运维平台实现全域设备纳管，设备监控管理不再需要手工一台台添加，可以通过自动探测添加设备监控并更新拓扑图，根据预设规则自动关联设备的配置备份、巡检、合规等策略。

日常运维工作中，运维人员可以通过自动化运维平台实时监控并记录全网设备硬件状态、接口流量和链路状态等情况，提高运维效率，并为网络性能分析、设备扩容提供数据支撑。

当故障发生时，平台会自动发送告警。运维人员可以通过平台进行IP端到端路径分析，查看源IP、目的IP端到端的二三层整体网络路径拓扑，回溯各端口流量变化情况、设备日志、设备配置变化情况等，快速定位故障原因。

在日常变更、主备切换、业务上线时，运维人员可以通过平台实时状态监控和自定义性能数据对比，将设备接口流量等参数放在一起监控，以便监控变更操作前后网络状态变化，保障网络变更顺利进行。

■流程标准化，强化网络运维风险把控能力

建立电子化的IT服务管理流程，执行运维操作线上审批流程，所有运维工作中的故障/问题处理、变更操作需要线上进行方案记录和流程审批，杜绝操作不规范情况，降低业务故障风险。

将IT服务管理流程与监控、自动化、CMDB融合，实现监、管、控的一体化，实现自动化配置下发和配置项修改，可以在变更工单中制定配置项变更计划，计划中可以展示变更前的配置项（CI）属性值和变更后的配置项（CI）属性值，并展现变更影响分析，变更完成后，自动更新CMDB。

新华三有着15年以上金融、证券等行业的运维咨询经验和方法论沉淀，希望通过ITSM帮助客户更好的支撑业务发展和创新，促进IT价值创造，输出更稳定和可衡量的服务，建立更规范的日常运维工作模式，更好的展示运维绩效指标。

■配线可视化，提高配线维护准确率

通过3D技术实现全面的数据中心配线可视化，直观展示机房场景和网络链路情况，包括设备前后面板展示，设备端口类型区分（光口/电口），线缆类型区分，光纤永久链路可视化，链路告警提醒，机房容量管理，摆脱表格管理的困扰。使复杂的配线关系变得易于表达、理解和传播，从而消除运维过程中不同角色之间的认知偏差和监管盲区，实现管理的透明化，更进而有效提升配线的管理效率和准确率，解决银行网络分区固化造成的跨机房布线难题，提高配线维护准确率。

运维人员在设备接线特别是跨机房配线操作前，可以通过平台的3D可视化展示，查看机房的机柜摆放情况和每个机柜内设备连线信息，对漏水线、配线、光纤、铜缆等不同类型配线采用不同的3D展示效果。点击需要连线的设备端口可以查看端口状态，还可以在平台内增加跳线链路并自动估算出跳线的长度，辅助运维人员进行实际布线操作。

■运维自动化，提升网络运维自服务能力

通过自动化操作平台实现网络设备巡检自动化、配置合规自动化、IP地址管理自动化和网络排障自动化等。采用强大的企业级服务编排引擎，把繁杂的手工运维场景变为便捷高效的自动化任务。在新一代网络智能化管理领域，在巡检、合规、IP地址管理、智能排障等场景化能力之上，依托丰富的知识库，实现网络运维工作的自动化。

在银行实际网络运维中可以实现：

- 网络设备巡检自动化。能够实时和周期性巡检网络设备状态并输出巡检报告，在巡检报告中反映出网络变化，所监控参数异常或超阈值等信息。运维人员每天上班时通过巡检报告就可以了解全网设备状态和变化情况，通过巡检报告也可以直观的向领导进行汇报；

- 配置合规管理自动化。基于丰富而详实的合规报告为客户提供专业的合规修复建议，实现网络配置规范性核查的自动化、例行化及持续化。可以实时和定期检查设备配置是否符合行内网络和安全规范；

- IP地址管理自动化。银行数据中心的IP地址数量至少上万个，如果通过人工进行IP地址分配或者故障设备信息查询会非常繁琐，而且无法保证数据的准确性，容易造成IP地址冲突和业务中断。而通过自动化运维平台可以实现IP地址全生命周期监控管理。通过实时和定时扫描在网IP，展示所有设备上的IP地址情况（包括NAT地址），高亮展示IP地址、MAC、VLAN、接口与基线变化情况，并支持设备IP地址与MAC/端口/VLAN/关联网络设备绑定关系变化告警，展示IP冲突、非法绑定等告警信息。

- 网络排障自动化。将日常网络故障排查操作固化到排障流程和脚本中，降低手工排障失误率，提高运维效率。

■运维智能化，打造网络维护的“人工+智能”

运用人工智能技术打造智能运维分析系统，基于Telemetry技术实现毫秒级监控数据采集，将采集的设备指标状态、设备转发表项、网络流量数据等实时推送到系统进行分析，相比传统的SNMP采集、NETCONF、CLI等方式更加高效。同时引入AI技术和大数据分析技术。对于网络/设备/协议/Overlay四大类常见故障，可实现分钟级别发现故障，定位根因并给出处理建议。

随着移动互联网、SDN、云计算、大数据和人工智能的逐步成熟，我们已经可以将运维管理中的工作自动化，用自动化操作替代了过去手工执行的操作，用大数据拟合动态基线替代静态阈值实现系统运行态监控，用人工智能实现了智能分析与排障。

未来网络运维将更加智能，实现网络部署、网络运维的智能化。网络的资源管理和分配将不再采用手工方式进行，而是通过软件定义实现整个网络的自动化管理、自动调度和故障自愈，依托算法和微分段技术实现更加精细化管理，并且通过AI和大数据分析应用分布、网络延时和数据传输效率，实现流量预测和故障预判，智能化提前调度网络以规避链路拥塞和故障发生。

新华三U-Center统一运维平台将继续以客户需求为导向，以技术创新为引擎，为客户数字化转型保驾护航。

富国基金统一资产管理平台（CMDB）落地经验

文/转载自“富国金融科技之路”公众号

CMDB的概念

CMDB，Configuration Management DataBase，配置管理数据库，是与IT系统所有组件相关的信息库，它包含IT基础架构配置项的详细信息。

这是一个相对宽泛的描述，并不具备可落地的指导意义。同时，CMDB是与每个企业具体的IT软硬件环境、组织架构和流程强相关的，这就决定了CMDB一定是高度定制化的体系。虽然我们都知道它不仅仅是一个存储信息的数据库那么简单，但是它的具体形态是什么样子的，并没有统一的标准。

富国基金第一代CMDB的实施经验

富国基金于2016年搬迁万国数据新机房时，构建了整套的ITSM-CMDB体系。ITIL流程在当时更多的被当做流程规范使用，CMDB则是本着应入尽入的原则搭建。基本替代了大家手头的EXCEL表格。

但是理想是美好的，现实是骨感的。和广大行业同仁遇到了同样的问题，由于没有自动化采集能力，没有对CI（配置项）更新的强约束，这个“线上EXCEL”中的庞大数据很快就遭遇了更新不及时，数据没人消费的问题；而这些问题又反过来导致使用者逐渐抛弃这个“线上EXCEL”，恶性循环就此产生。

经历了一段不美好的回忆后，新华三也开展了复盘行动，总结项目收益不如预期的原因：

■信息固化不是目的，也没有价值，只有信息动态流转起来才有价值（跟货币一样），那么进入CMDB的数据并不应是大而全的，而是应该先设计消费场景，再反过来去寻找数据来源并进行入库。

那需要配套设计的工作有：

●基于这些信息进行流程规范的建设，比如服务器的上线、下线、维修、装机等流程。同时，流程过程中状态的变更要同步管理起来；

●拓扑关系的可视化和动态展示，比如应用与服务器之间的级联关系、状态（正常 or 故障）的展示等，这样可以很直观地关注到资源节点的状态。

■需要将更多的精力放在应用及更上层的数据上，发挥数据的价值，而非聚焦于底层的硬件，基础设施；

●如果仅仅基于CMDB的资源信息作自动化，最多只能做出自动化的硬件资源采集、自动化装机、网络-硬件拓扑关系生成等资源层面的工具，这些工具只会在运维层面产生价值，离业务还很远。

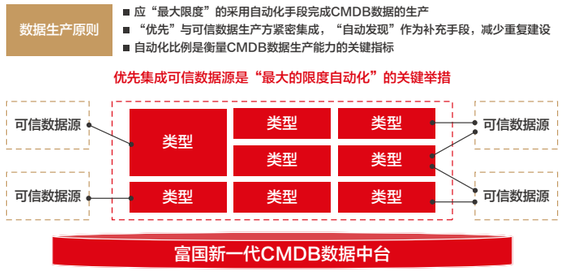
富国基金新一代CMDB扬帆起航

2020年，在完成充分的总结和规划后，新华三启动了新一代富国基金统一资产管理平台的重建并取得了阶段性成果。

目前项目实现了以下既定目标：

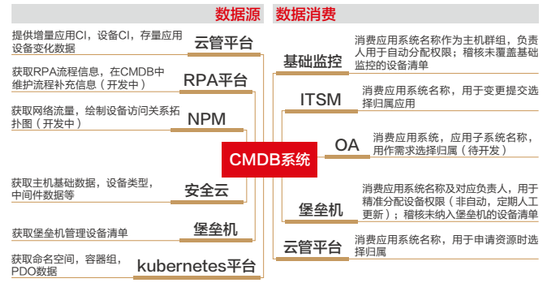
■面向场景重构CMDB模型，提高数据的可消费性和可采集性；

■完成第一阶段CMDB自动同步、自动发现、自动关联体系（CI自动化采集比率80.67%）；



■完成第一阶段CMDB数据治理（关键数据缺失率降至0，通过IP扫活确保不会存在设备遗漏，信息补足依靠后置稽核措施补全）；

■完成第一阶段多个消费场景：运维相关工具平台完成了以CMDB作为核心数据源，实现了告警负责人，变更归属，运维人员堡垒机权限控制等消费场景。



数据流

数据使用率及自动化采集率

应用-子应用、应用-支撑设备拓扑图

展望

由于新华三基础设施架构开始倾向于混合云，应用架构也逐步微服务化、容器化，新一代资产管理平台还需要进一步适配云原生时代的信息资产管理需求，以下问题和消费场景需求亟需解决。

■在传统架构下通过CMDB做资产管理，云原生架构下最小管理单元不再是物理机和CVM，变成pod和容器，安全扫描、安全修复和安全应急都依赖资产信息（节点IP、容器名、容器id、负责人等），资产信息不全可能会导致安全事件无法排查原因和修复。故CMDB需完成多k8s集群对接，application-namespace-service-pod模型构建等工作；

■根据NPM流量镜像绘制应用间访问关系拓扑图（设定规则过滤非关注网段，暨噪音），用于进行变更影响关系分析；

■建立应用等级，高可用要求及现状模型，用于年度切换演练及总结场景消费；

■物理机等目前无数据源硬件资产的信息丰富工作，计划采取带外、SNMP、IPMI、Redfish、SSH等手段。

云原生时代的基础设施与传统运维已发生了剧烈变化，对应的运维工具（监控，CMDB）等均需匹配需求的变化，顺应云原生时代的架构，提升可观测性，保证资产的可管理性。为实现企业数智化转型，信息科技能力发展奠定扎实基础。

如何提供安全的远程运维服务

文/赵鸿生

远程运维的必要性

远程运维，在互联网诞生之时，就已经有了相关场景，大型公司拥有分支机构，跨国公司拥有海外机构，各业务系统的维护往往需要总部的支持。而在地域空间上的距离，也因为互联网与通信技术的支持，得到了缩短，运维人员使用相关通信协议，利用互联网特性，在异地对各业务系统进行远程维护，但因为世纪初的行业规模还不算大，远程运维的模式并没有得到广泛认可，一般还是应用在大型公司与跨国公司，但其必要性已经得到了显现，跨空间支持与整体管控都有远程运维的用武之地。

随着中国一线城市的虹吸效应越来越明显，IT互联网领域内的主要技术人才都集中在了各中心城市，二三线城市的IT互联网人才招聘补充变得越来越困难，寻求外部技术支持的需求变得越来越迫切。

而在全球经济飞速发展的今天，跨国组织越来越多，云计算服务的出现更是推动了远程运维服务的普遍应用，以远程登录的形式来进行支持的远程运维方式也得到了普遍认可，变得更有必要。

国内外远程运维的实践

近十年来，随着互联网规模不断扩大，万物互联概念的提出，相关技术也有了长足的发展，远程运维的场景也越来越丰富，数据中心、云计算资源、业务系统、手机移动端、物流等场景都有应用。

由于员工出差及客户访问内部系统等场景的需要，使得近几年远程服务的热度不断提高。一些远程访问工具，也纷纷面世。如电子邮件、FTP、远程桌面等工具为出差在外的企业员工，提供了访问企业内部资源的网络渠道。很多公司基于相关条件及自身的需求，开通了远程服务，随之衍生出了大规模的远程运维需求 。

在云计算领域，使用公有云资源的客户与提供云服务的供应商之间的交互，就是在远程场景下完成的，做为一种共享经济的体现，云计算的基础设施必然与客户存在非常大的空间距离。而在实际的业务场景中，即使供应商可以基于地域提供多个访问的节点，但是实际上用户还是很难接触到基础设施的设备，整体的服务内容以一种互联网的交互方式来进行，对于云上资源的维护，亚马逊、微软、阿里等3A厂商走在世界的前列，其形式仍然是远程运维服务。而云厂商对于基础设施资源的维护，实质上也分为两部分，机房环境里由专业的人员进行动力环境及IaaS资源的运维，硬件资源之上的PaaS层，更多的还是运维人员在远端进行维护，而SaaS层的应用同样基本也是以远程服务的方式提供给最终用户，这类场景在云计算领域内可以默认为行业标准，应用得非常普遍，多租户的管理概念即是云计算的业务体现。就像大家知道的，云运维是云服务商对于自己云服务的保障，它们都是在远程的环境下进行的。

很多大型公司或者跨国公司，在实际的业务管理上，出于集团对各子公司或组织机构的管控需求，远程的服务对接也成了必选项，多数情况下业务应用的架构都采用分布式或者C/S架构。同样的在这一过程中，为了保证这类业务应用有足够高的稳定性，它们的运维也是需要考虑的重点，像制造类企业，生产工厂可能会配备一名运维专家，但不会配备一个专家组，出现问题的时候，运维专家保证基础数据安全与初始化的排障，最终还是要通过总部的专家团队配合来进行系统的维护或是代码的修改发布，而这种团队的配置，更多的还是出于运营成本的考虑，一中心多机构的运维团队也就应运而生，这也是多组织机构运维的经典场景。

远程运维的安全问题屡见不鲜

随着远程服务与运维的使用场景越来越普遍，对应的一种声音也在逐渐变大，就是远程运维的安全问题。

2019年，某汽车制造厂商关键系统数据被勒索病毒锁定，经过一番紧急处理，虽然挽回了一定的经济损失，但总体上还是丢失了部分业务数据。安全事故之后，该公司投入巨大成本用于整体的安全水平提升，安全事故的原因也随即公之于众，公司内部为了方便整体支持，采用了远程运维的服务方式，而黑客抓住了公司内部的远程运维安全漏洞，利用IT部门对于权限管理的漏洞，通过某些默认不设口令的中间件服务，反向爆破了运维管理工具，从而下发了勒索病毒，最终导致该安全事件。

同期另一家汽车制造厂商，也受到了挖矿病毒的攻击，整体生产受到了很大影响，好在是春节假期刚过，影响不是很大，而黑客的攻击方式与第一种几乎相同。

在互联网上，各类安全事故频发，各类攻击手段层出不穷，安全事故案例屡见不鲜，那么安全事故的原因是否有一些共性或是人们没有了解到的原因呢，经过对多个案例的分析对比，最终得到这样一个结论，这种安全事故，绝大部分都是由于远程运维的方式引起的，只有很少一部分是在密闭的内网环境下出现的，而内网环境出现问题多数是由于USB接口滥用，未得到控制造成的。远程运维服务引起的安全故障有非常多的相同点，例如行业特征，技术域特征等，就像上边举的两个例子，两家汽车制造商，相同的行业，相同的问题。那么在远程运维的安全风险如此之高的情况下，为什么还要选择远程运维服务?

为什么有如此大的安全风险依然需要远程服务运维

远程运维的依托实际上是远程服务，在远程服务依然被需要的今天，远程运维必然有它存在的理由。

而安全事故的问题也并不是发生在远程运维的服务方式上，更多的是相关IT部门为了提供远程运维，没有对支撑远程运维的配套设施与环境做好安全管控，如上面提到的勒索病毒案例，黑客通过基础的用户口令爆破，再通过一些默认不设口令的中间件软件来达到他们的最终目的，这里面有三个漏洞点。

其一，远程运维发布在互联网上，即默认为所有获取到访问地址并有权限的用户就可以访问，而用户的口令被爆破有如下两种原因：首先，客户自己的办公电脑有安全风险，被黑客利用木马的形式获取了登录权限；其次，该公司对于需要访问业务的所有客户，在登录场景下没有安全管控，导致后期排障难度加大。

其二，对于构成应用服务的中间件，一律采用默认部署，没有对端口，口令等内容提出更换或加密请求，导致黑客轻而易举的反向爆破了运维管理系统，从而发生了安全事故。

结合案例过程来看，其根本问题在于安全意识的淡薄，而不是远程运维的方式，远程运维更多来讲，只是给黑客提供了一个契机，但如果后端的安全防控与加固防护做好，这类安全事故也就不会发生了。

同样的案例情况，如果你仔细去剖析就会发现，几乎都是同样的问题，不设限的安全防护，相当于对黑客大开城门，而远程运维很多时候只是无辜的承担了所有过错。

多租户的云计算场景或多组织机构的跨国公司场景下，在没有一种成本效率能够完全替代远程运维时，其存在依然是必须的，实际上来说这种方式永远是先进的，只是使用它的成本在逐渐降低，远程运维的方式永远不会过时。运维管理可以通过流程化与标准化的管理手段，来提升人力效率，也可以通过自动化、智能化的手段来做到人力成本的极致压缩，但是在上面的场景中，运维方式依然还是要依靠远程运维。

远程运维拉近了空间的距离，可以让运维团队在不同的地域对整体服务进行支撑，它天然就是一种容灾手段，团队的地域合理分配可以让运维服务轻松的覆盖到7×24。

远程运维可以做到资源共用，特别是使专家资源的共用成为了可能，当组织内有一名技术域专家，某种程度上组织内的各机构也就相当于具备了专家能力。

远程运维是一种低成本运营的方式，它的形式可以在低人力成本地区去组建团队，来完成对于高人力成本地区的服务运维支撑。

远程运维也是一种管控手段，各机构与租户的业务行为可以在总部或中心形成有效的日志，方便组织内部进行审计与核查。

新华三的远程运维

新华三作为一家硬件厂商，在业界提供了非常多的服务案例给到各行各业的客户。而新华三的远程运维服务，同样也服务了非常多的客户，新华三为超过500个客户提供过远程服务，行业包括医疗、教育、政务、互联网、企业等等，在持续多年的服务过程中，整体的安全事件为0，新华三是如何保证高规格的安全防护呢？新华三在整体的服务规划过程中，信息安全的重要性得到了十足的体现。

在新华三的远程运维服务中，整体的远程方案设计有一个大前提-安全加固，内部流程的管理和优化也充分的吸收了ISO27001与等级保护协定的管理要求，并且内部交付团队也通过了ISO27001与等级保护的认证。对于平台、人员、数据的整体防护是新华三打造远程运维服务的基础，其中远程运维配套设备与平台安全防护是远程服务工作的重中之重：

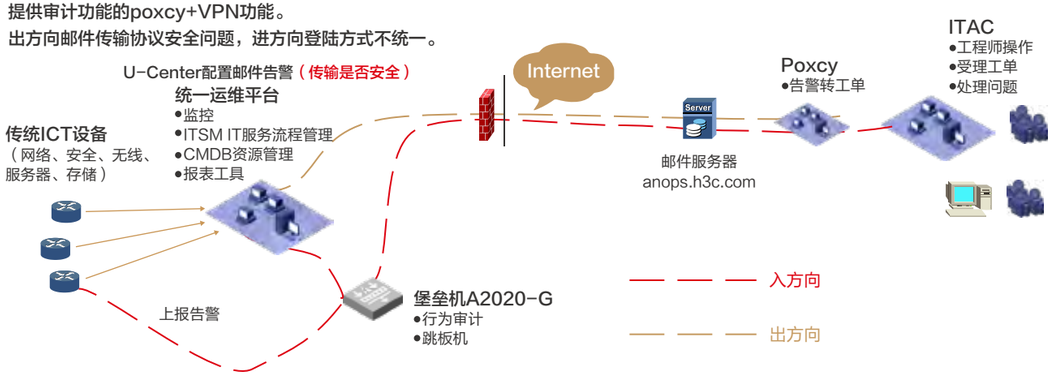
■平台开发侧重安全防护，针对口令管理、安全基线、防病毒、行为等内容，构建了专有的工具模块，而整体平台的构建，也充分的考虑了安全性的需求；

■整体交付团队的分布明确提出了容灾的需求，整个团队分布在多个区域，可以7×24小时保障对用户服务的支持；

■而在整个远程运维过程中，对于数据安全的保护也是新华三平台开发的一个重点能力；

■整体的团队管理有专门的工具，来保障团队与客户达成的SLA。变更评估依赖于专业的巩固，将造成的影响降到最低；

■交付团队的整体管理也具备专门的审计团队，对流程处理，员工操作进行不定期的工具或人力抽检，定期组织员工进行安全规范的学习以及反面案例的分享。



整体的远程运维服务特性如下：

■以ITAC平台做为运维支撑平台，对现有的端口、口令、补丁等关键信息做了加固动作；

■同时数据统一存储在客户侧，以图形化界面的形式进行运维支持，避免了数据信息泄露；

■以ITSM与CMDB系统来做为运维管理平台；

■以流程处理各环节的管控来强调员工操作的合规；

■以配置项管理系统的信息集成产出业务拓扑，保证变更方案制定的严谨性；

■事后定期进行随机审计抽取，提供审计报告。

在操作审计上，配置堡垒机设备

■对所有的远程做登录认证；

■对所有的权限做统一的授权管理；

■账号申请统一纳管，根据实际需求进行小权限授权；

■所有的远程登录操作，必须接受审计；

■整个交付体系已经跟随新华三公司通过了ISO27001与等保的体系认证。

整体上按照基础有保障，过程有检测，事后有审计的原则来进行远程服务的交付，持续不断的优化。从整体部署架构以及管理手段上同时出发，保证客户的远程运维服务时刻处在最高等级的安全防护下，为客户的运维业务添砖加瓦，保驾护航。

工业互联网平台运维人才培养

文/陈贺

引言

工业互联网是工业全要素、全产业链、全价值链的全面连接，是人、机、物、工厂互联互通的新型工业生产制造服务体系，是互联网从消费领域向生产领域、从虚拟经济向实体经济拓展的核心载体。当前企业普遍反映：“工业互联网最大的挑战不是技术，也不是资金，而是人才。”工业互联网人才的缺乏已经成为制约我国工业互联网创新发展的重要因素，对我国工业转型升级和保障经济高质量发展带来较大挑战。工业互联网的核心是工业云平台，由于平台的重要性与其相关的岗位更显得格外稀缺，尤其是具备综合运维能力的专业技术人员。

工业互联网平台人员能力要求

工业互联网平台体系架构

工业互联网平台是工业云平台的延伸发展，其本质是在传统云平台的基础上叠加物联网、大数据、人工智能等新兴技术，构建更精准、实时、高效的数据采集体系，建设包括存储、集成、访问、分析、管理功能的使能平台，实现工业技术、经验、知识模型化、软件化、复用化，以工业APP的形式为制造企业各类创新应用，最终形成资源富集、多方参与、合作共赢、协同演进的制造业生态。

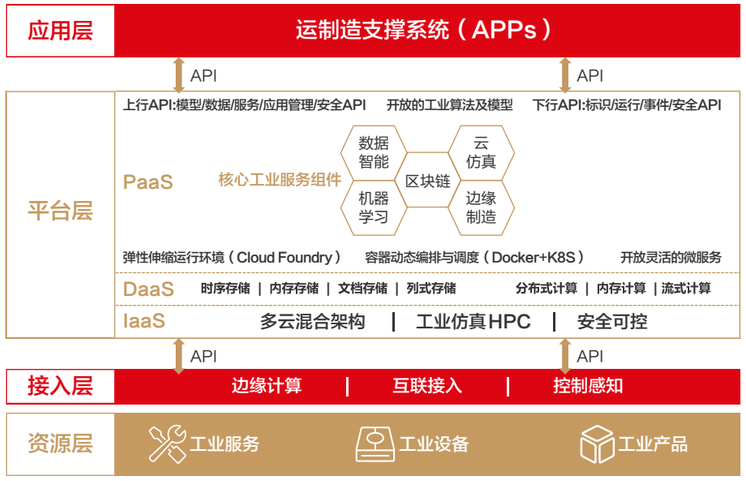


图1 工业互联网平台运维工程师能力框架

如图1所示，第一层是资源层，涵盖大量的工业服务、工业设备和工业产品，例如：智能传感器、工业机器人、智能仪表等。

第二层是接入层，通过大范围、深层次的数据采集，以及异构数据的协议转换与边缘处理，构建工业互联网平台的数据基础。

第三层是平台，包含IaaS基础设施、DaaS大数据服务、和PaaS平台，基于PaaS叠加大数据处理、工业数据分析、工业微服务等创新功能，构建可扩展的开放式云操作系统。

第四层是应用，形成满足不同行业、不同场景的工业SaaS和工业App，形成工业互联网平台的最终价值。

工业互联网平台相关岗位

基于工业互联网平台体系架构的理解，如图2所示，可以识别出应涉及以下岗位：平台架构工程师、平台研发工程师、平台测试工程师、平台运维工程师、工业APP开发工程师、工业APP产品化工程师。

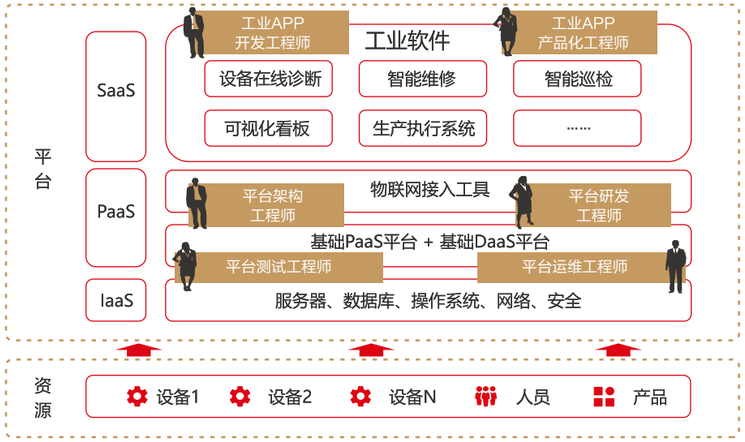


图2 工业互联网平台相关岗位

- 平台架构工程师：负责工业互联网平台建设方案制定和架构设计；
- 平台开发工程师：负责工业互联网平台系统建设研发；
- 平台测试工程师：负责工业互联网平台系统功能、性能及接口测试；
- 平台运维工程师：负责工业互联网平台系统运维部署、管理及优化；
- 工业APP开发工程师：负责工业APP的功能设计、开发、测试、部署与运维；
- 工业APP产品化工程师：负责工业APP的市场调研、需求挖掘、开发指导、成本估算，以及产品推广等职责。

平台从业人员职业发展路径

职业发展路径描述了一名从业人员，从入行到成长为专业人士的职业生涯过程，每个行业都有自身的发展路径，大多会呈金字塔状。工业互联网平台人员的发展路径如图3所示，通常入行人员会经过2至3年的磨练逐渐成长为一名具备一定工作经验的技术骨干，根据岗位职责可以分为产品、开发、运维等方向。随着技术能力成长和工作经验积累，会转型到不同的分支，偏向管理的分支可以逐渐成长为项目经理、部门经理、直到公司领导，偏向技术的分支可以逐渐成长为架构师、技术专家、直到技术总监。

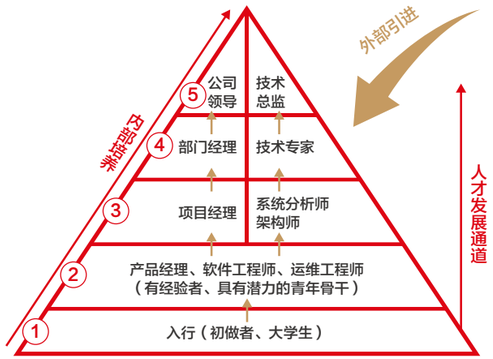


图3 工业互联网平台人员职业发展路径

运维工程师能力分解

根据市场调研，企业用人需求集中在平台使用、工业网络维护、智能产线操作等方面，由此可见具备一定操作能力的运维工程人员是当前的核心需求。依据工信部岗位能力测评标准，应按照综合能力、专业知识、技术技能、工程实践四个维度进行评价，平台运维工程师的能力分解如表1所示。

维度	要素	说明
综合能力	软能力	●掌握工业互联网体系架构及其发展趋势 ●熟悉1-2个工业互联网典型业务场景，及其相应的业务逻辑 ●熟悉工业互联网平台内外部网络的运维、管理及优化
专业知识	基础知识	●掌握现行工业互联网平台运维相关标准内容 ●熟悉工业互联网平台各环节技术规范与运维流程
	专业知识	●熟悉网络通信、计算机、云计算运维相关专业知识 ●熟悉物理及虚拟网络架构的相关技术，保障云计算的网络性能和稳定性
技术技能	基本技能	●掌握Linux/Unix平台系统运维主流技术，熟悉Linux系统及开发环境，熟悉Shell、Python、Perl、Go等其中一种或多种脚本语言 ●熟悉使用Linux命令，对于服务器服务的配置安装、服务器安全、备份及恢复和日志分析具有一定经验 ●熟悉Tomcat、Nginx等的基本原理、故障处理，熟悉常用的互联网技术，包括DNS、HTTP、Proxy、Load banlancing、CDN等，掌握QOS、MPLS、VRF、VLAN等网络技术 ●熟悉Oracle/MySQL数据库原理、部署、备份恢复、迁移、故障处理
	专业技能	●掌握 SDN 及网络虚拟化技术，精通交换、路由协议原理，熟悉常用路由协议（OSPF、BGP 等），能够规划与设计中大型网络结构和路由策略 ●具备交换机、路由器及防火墙等安装、配置、管理及运维能力
工程实践	经验	●具备自动化运维系统的建设、运维等能力，具备云计算运维优化相关经验 ●具备服务器、网络、交换机、路由器、防火墙等的选型和配置管理能力，具有信息安全领域经验，具备工业互联网平台的实际运维经验

表1 工业互联网平台运维工程师能力框架

工业互联网平台人员能力实训

实训环境方案

工业互联网涵盖云计算、物联网、工业控制、工业大数据等多项技术，是信息化与智能制造的深度融合，需要将IT产品和工业仿真产品有机结合才能达到培训效果。因此需要一个真实的培训环境，用于构建基于用户、设备、模型等不同元素的业务生态体系，包含设备上云、建模分析、APP开发、运维分析等，可满足工程技术人员对工业互联网的应用、理解和认知。工业互联网实训环境架构方案如图4所示：

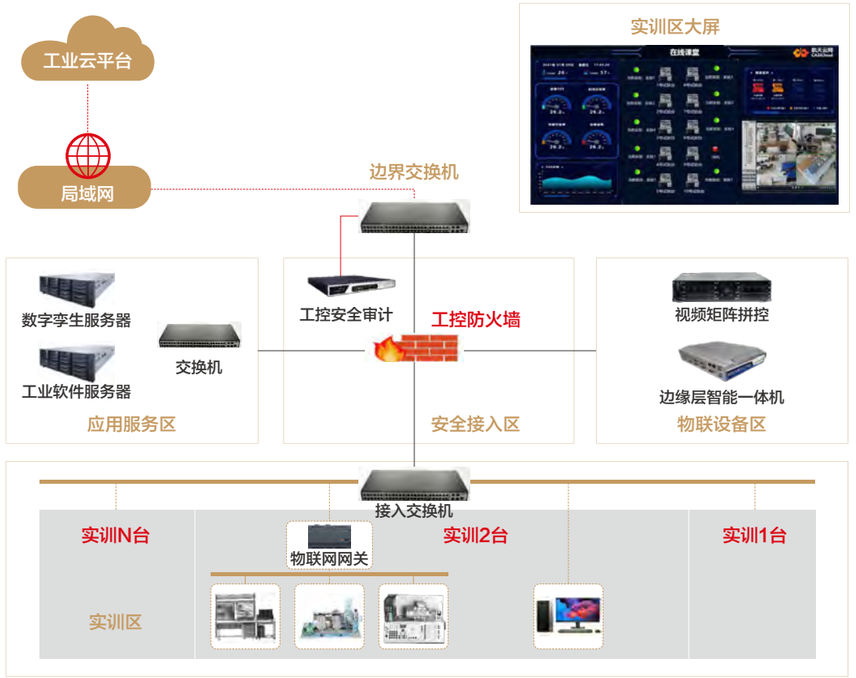


图4 工业互联网实训平台

- 工业互联网实训环境架构可分为5层，包含资源层、边缘层、平台层、应用层、安全层：
- 资源层：提供实验操作试验台，实现工业场景的仿真模拟；
- 边缘层：提供数据采集和在线教室的应用，实现了试验台数据接入和授课教室实时掌握每个实验台的实验进展状态；
- 平台层：包含数据存储服务、数据分析服务、开发工具服务、以及数据查询接口服务；
- 应用层：提供了App开发的在线应用、平台管理应用及其他应用。
- 安全层：提供工业互联网的访问控制和工控安全审计。

实训课程方案

基于工业互联网实训平台，可进行与工业互联网相关岗位的培训内容规划、设计、培训和考试，通过理论和实践相结合的方式完成教学。

课程名称	课程简述	岗位角色
工业互联网概论	●工业互联网发展历程；工业互联网技术体系 ●网络体系、平台体系、安全体系、应用体系 ●工业互联网标识解析体系架构 ●边缘计算发展和应用领域、关键技术	所有岗位
工业互联网网络技术	●工业互联网网络体系架构 ●工业网络技术协议、各种网络传输介质 ●工业网络组建方法 ●工业以太网（PROFINET等）和现场总线的基本概念、组成与连接	与网络相关的架构、研发、运维
工业互联网平台技术	●工业智能网关配置、平台用户创建、设备配置、网关绑定、采点配置、数据可视化、云计算、云组态、工单管理、工业APP发布 ●工业生产协调管理与应用 ●工业智能管控一体化 ●可视化看板组态与应用	与平台相关的产品、架构、研发、运维
工业互联网安全技术	●工业互联网安全体系架构 ●防火墙、网闸等常规安全设备 ●安全策略 ●虚拟专用网络 ●安全漏洞识别和防范 ●安全加固技术 ●入侵检测、入侵防御知识 ●安全审计等	与安全相关的架构、研发、运维

表2 工业互联网实训课程

结束语

2020年国家发改委明确将“工业互联网”作为“新基建”的信息基础设施，由此更加剧了“新岗位、新职业”的人才短缺。与此同时，社会各界也正在加快推进工业互联网人才培养的研究与探索工作，相关人才教育涵盖了企业管理人员、领军人才、专业技术人才、产业工人、高校教师等各类型、各层次，其中，具备基础运维能力的专业技术人才的赋能是当前人才培养的重要方向。

攻防演练中运维主动防御实践

文/李国宝

前言

电报、固话、互联网、手机、物联网，每一项技术都在把社会一步步推向数字化社会的奇点。初始组网并不复杂，都是以能实现信息传输为第一目的，通了就行！有一次旁听了某运营商专家给北邮研一的新生做演讲，互动环节有学生提问：

“为什么三大运营商这么强大的网络资源，却没有一个能做出BAT类似的业务模式？”

答：“因为运营商考虑的永远是通信的问题，而不是互联网应用的问题；

在1G的时代考虑的是如何能增大信号覆盖面积，让更多的人能实现通话；

在2G时代考虑的是如何通过数字通信技术，让用户能够更清晰的通话；

在3G时代考虑的是如何通过3G技术，让用户能够实现视频通话；

在4G时代考虑的是如何通过高速带宽，让用户能够实现高清视频通话……”

我在想是不是在5G时代，他们想的是如何让用户能够实现多方高清视频通话。

在数字化的大背景下，每个行业、每个单位、每个人的需求都在推动着信息系统传输速度更快、数据存储空间更大、计算能力更强、互联更便捷、应用更丰富，伴随而来的是系统越来越复杂，组织的业务运营越来越依赖信息资产。如此一来信息系统及其管理体系脆弱性的增加，导致信息系统的安全风险也在逐步加大。

网络安全形势分析

“勒索”这个词近些年不是出现在港片中了，而是更多的出现在了互联网行业，并逐渐出圈被各行各业所熟知，令人切身体会，甚至咬牙切齿、捶胸顿足。

当你打开电脑，发现屏幕上的图标都不能点开了，点击任何一个都会弹出对话框，告诉你电脑已经被锁定，需要向一个比特币地址汇款才会帮你解锁。或者告诉你，你的数据库已经被拷贝走了，请在某日之前交纳赎金，如果没有收到，就会在暗网上拍卖这些数据。

以前这种勒索行为对操作者有着极高的技术要求。干这些勾当还能全身而退的人，凭他们的才华，即便从事正当的网络安全职业，收益也不会比干勒索低。于是在利益的驱使下，从前的网络勒索行为，甚至还带着一些挑战自我的意味，不为赚钱，只为了秀一把。

现在，随着产业的数字化、虚拟币的发达、新冠疫情后全球货币的滥发，这三个条件导致网络勒索数量暴涨，成为了一个和真实世界里的毒品、偷渡、走私类似的黑色产业，并且规模快速扩大，从个人的黑客行为发展成了一个灰色产业链。

只要稍稍关注就会发现，网络勒索者眼中不少国家的政府部门成了一只只“肥羊”，这和传统犯罪的风险评估完全不一样。传统犯罪，瞄准谁也不会瞄准政府，那相当于自取灭亡。

但令人悲观的现状是，只要被盯上了，就没有特别有效的方法防住网络勒索。我们只能期待底层加密技术的进步，以此加强防守能力。

除了勒索，系统被破坏、内容被篡改、信息被泄露、系统被控制等各式各样的攻击手段层出不穷，只要利益的诱惑足够大，攻击的技术就会不断的演进。

现在信息系统和网络系统在建设的时候，都应考虑怎样才能够减少脆弱性，降低风险。但风险是不可能被完全消除的，漏洞永远存在，风险也会永远存在，正视风险，做好防御才是当务之急。

攻守两端分析攻防演练

新技术催生新的攻击手段，万物互联打破了安全固有边界，数据资源被攫取风险增加。所有的信息系统都不可能等待着网络发生问题，造成了损失再去修补漏洞。主动找出问题，增加防御手段才能提高抵御风险的能力。

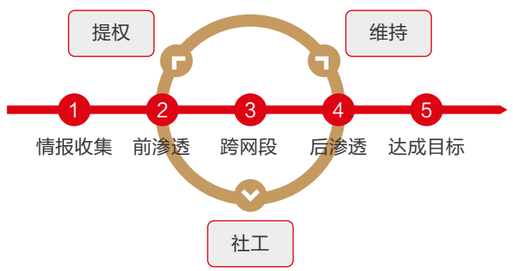
由国家公安机关主导，组织全国网络安全精英力量，针对一些重要单位的信息系统，在可控的、合法合理的范围内发起攻击的攻防演练活动应运而生；目的就是主动发现信息系统的安全隐患，检验各单位的安全监测、防护等能力，提升应对真正网络攻击时各部门协同的应急处理防御能力。

攻防演练从开始只有每年公安部组织的2个星期，渐渐的发展为国家级、省级、市级、纵向行业级、集团单位内部演练，参与范围不断扩大，攻击手段不断翻新。不同层级，不同时间段的攻防演练逐渐发展为常态化的安全活动。

安全是一把手工程，如果没防住，单位一把手可能会被约谈，作为运维岗位的IT工作者则可能需要承受随之而来的狂风暴雨。当然完全防住攻击，甚至还能抓住攻击者，同样也是可以引以为荣的事。

下面我们来看看通常攻防演练是如何实施的：

攻方



■四步走

●情报收集：互联网发布过的信息，无意被泄露到互联网的信息都可能被利用；

●查找短板、突破边界：通过VPN、邮件、边缘系统，比如论坛、职工家园、XX项目管理系统突破到内网；

●内网进行横向移动：扩大攻击面，能够更多的占领系统，进行多点潜伏，同时设置免杀；

●拿下目标，清除痕迹：通过不断的横向移动，逐渐接触到域控、堡垒机、核心生产系统等，最终拿到核心目标数据后，清除攻击痕迹。

■三板斧

●弱口令暴力破解：最简单的方法最常用，保不准就有用123456做系统密码的漏网之鱼；

●漏洞利用：先拿常规漏洞尝试攻击，检测系统漏洞补丁是否及时更新了，不行就使用0day，时间短任务重；

（0day漏洞就是厂商还没有发现。但是已经被黑客或其他人发现，并且已经利用的漏洞。厂商没有发现这个漏洞，就意味着没有修复这个漏洞的补丁和方法，如果被黑客利用就会造成非常大的安全影响。所以，0day被称为网络攻击的核武器。之所以叫0day就是当天被公布当天就可被利用，不需要再探索方法。）

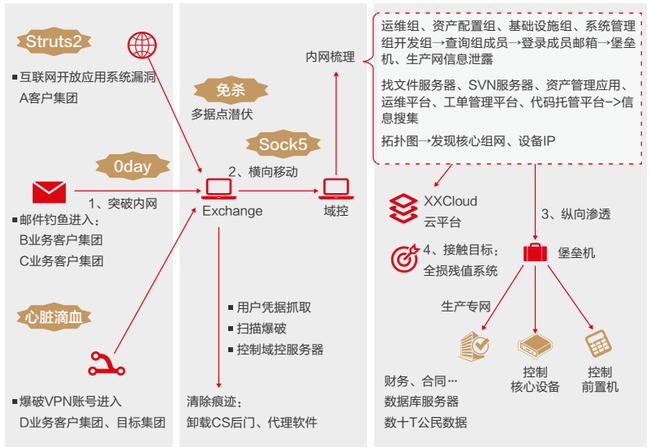
●社会工程学：钓鱼邮件、伪装成客户、色诱工程师……攻击方也是被逼的，谁让传统手段不那么有效了呢，利用心理学漏洞直接攻破人性可能更容易。

目标信息系统的内部信息不方便找到，如果知道系统运维人员是谁，就可以通过喝顿酒来发展关系，一顿搞不定，就喝两顿，实在不行再找点其它娱乐活动，可能就可以从他嘴里套出更多信息。这就是社会工程学的攻击手段。

■攻击趋势

工具先行，节省人力、多源低频绕过，避免被态势行为分析盯上、上来直接用0day，手里有大杀器，时不我待，多拿分才是重点。

■攻击案例



我们来看一个真实的攻击案例：

首先通过三个手段突破了边界：第一个通过目标集团的A客户的Struts2漏洞进入；第二，通过钓鱼邮件进入了B客户和C客户，进而通过0day突破内网；第三通过heartbleed这个多年前就已经披露的SSL漏洞，暴力破解了VPN账号进入系统。

以上三个途径中只有一个途径是直接攻击了目标系统的，也就是说，在攻防演练期间很多攻击过程并不是直接面向目标系统发起攻击。目标系统防御能力非常的严密，直接对目标系统攻击就不那么容易，这个时候攻击者就会通过可关联的供应链、第三方的测试开发商、合作伙伴等等不同的系统，俗称“钻下水道”迂回进入到核心业务系统里面，进而在内网多据点潜伏、设置免杀、进行横向移动，拿下域控，并对内网进行梳理，找到文件服务器、拓扑图等重要信息。

再进一步拿下堡垒机，所有核心应用的账号管理权限都有了，最终接触到核心目标，找到了它的核心生产网，包括财务、合同、数据库等，还有数T的公民信息。

守方

被攻击方也不是干等着被打，也一定会防，这样就能验证现有的防御手段是不是奏效，真的出现了攻击者的时候，能防御到什么程度，即使没防住也知道问题出在哪里。

既然知道了攻击的四步走、三板斧，就来看看防守方需要解决哪些共性问题，提升防御能力。

在攻防演练中，道高一尺魔高一丈，防不住也是情有可原的，但是不能犯非常低级的错误，这些低级的错误最常见的共性问题，我们来说一说：

■**第一个**就是弱口令攻击。弱口令是什么？就是用了123456、纯数字、纯小写字母等等，没用多种组合和符合长度的密码。

123456 a123456 123456a 5201314 111111 woaini1314 qq123456 123123 000000 1qaz2wsx 1q2w3e4r qwe123 7758521 123qwe a123123 123456aa woaini520 woaini 100200 1314520 woaini123 123321 q123456 123456789 123456789a 5211314 asd123 a123456789 z123456 asd123456 a5201314 aa123456 zhang123 aptx4869 123123a 1q2w3e4r5t 1qazxsw2 5201314a 1q2w3e aini1314 31415926 q1w2e3r4 123456qq woaini521 1234qwer a111111 520520 iloveyou abc123 110110 111111a 123456abc w123456 7758258 123qweasd 159753 qwer1234 a000000 qq123123 zxc123 123654 abc123456 123456q qq5201314 12345678 000000a 456852 as123456 1314521 112233 521521 qazwsx123 zxc123456 abcd1234 asdasd 666666 love1314 QAZ123 aaa123 q1w2e3 aaaaaa a123321 123000 11111111 12qwaszx 5845201314 s123456 nihao123 caonima123 zxcvbnm123 wang123 159357 1A2B3C4D asdasd123 584520 753951 147258 1123581321 110120 qq1314520

Top100弱口令

整改建议：加强系统的口令检查，增加多因子认证。

■**第二个**就是老旧资产成为跳板。很多企业并不知道自己有些老旧资产已经停用了，但他们仍旧在网络中存在，这些没有下线的老旧资产可能就成为攻击者的一个跳板。

整改建议：需要完善系统下线流程，以及针对在网资产进行定期的探测，准确地掌握在网设备使用情况。

■**第三个**就是暴露面过大。互联网和内网的敏感信息泄露，比如说技术方案、管理帐号、邮箱信息、手机APP、微信公众号等等，可能都跟内网存在关联。

整改建议：在互联网上对敏感信息进行搜集和检查，尽量清除掉暴露在互联网上的企业内部信息。

■**第四个**就是网络缺乏细颗粒度的隔离措施。也就是网络规划不合理，分区分域之间的策略粗放，比如区域之间的策略放通整个C段地址，或者B段地址。

整改建议：合理规划网络架构，精细化区域策略。

■**第五个**是漏洞修复不及时。系统、应用软件已经公开的漏洞没有及时打补丁。

整改建议：跟随厂家及时对系统和应用打补丁。

■**第六个**也是技术上的最后一道防线。如果网络边界各种防御都失效的时候，最后一道防线就是终端安全。服务器系统、办公电脑的审计和杀毒软件是否在最后时刻有效发挥防御作用非常关键，如果终端都防御不住了，那就彻底失效了。

整改建议：部署终端安全防护。

■**最后一个，**缺乏完善的安全管理制度。比如内网专网的违规外联、员工私接WiFi连接互联网等等。

整改建议：寻求专业的安全咨询团队，采用专用的工具对整个信息系统进行风险评估、对网络规划和策略进行梳理，实现科学的管理，参考ISO27001等标准健全管理制度，在公司内部也要进行制度宣传，安全工作需要从人员意识、管理体系、技术和工具多方面常态化建设和优化才能持续发挥作用。

对于在攻防演练中参与防守的运维人员来说一定要有一个整体防守的解决方案：

■**第一步，准备协调：**要把相关部门的团队协调起来，明确工作职责，细化工作流程，寻求一把手支持，让公司各个团队能够充分配合起来。

进行整体防守方案的制定，包括防守工作方案、预演方案、应急方案等等，把防守预案和工作要求对参与人员进行安全培训，除了对安全专业人员实战化的防护能力培训，也要面向全员进行信息安全意识培训。

■**第二步，自查整改：**包括资产梳理。把老旧资产和互联网暴露面尽可能地收窄，做到资产充分有数。进行风险排查，包括高危漏洞、弱口令，进行渗透测试、基线核查、主机安全的检查、应用系统的检查、终端的检查等等进行风险评估。

把发现的风险和漏洞，该修的修，该补的补，缺失的防御防护措施及时补上，包括安全设备与工具的部署、安全策略的优化等，进行全面整改。

■**第三步，预演：**组建一个演练团队，包括明确的组织架构与决策职能、清晰的演练流程、充分的演练应急机制和处置手段。找到外部专业团队在可控的情况下模拟发起攻击，对内网进行攻防演练，充分验证安全监测的手段是否有效。

预演结束要进行复盘，优化现有的设备及策略。持续的进行日常监测，处理预演的遗漏问题。

■**第四步，防守阶段：**正式进入攻防演练阶段，对告警进行7×24小时监控，把能用的设备、平台全部都用起来，包括态势感知、日志分析、流量分析、主机安全等。

发现攻击行为，一定要知道应急处置该怎么做，攻防演练过程中不允许大段的阻断IP，不允许拔网线，需要精确的封堵攻击源。当真正有黑客攻击的时候，发现数据已经开始向外传输了，这个时候拔掉网线可能是最快速最有效的方式。

通过安全专家研判后进行应急处置，利用工具还原攻击路径，分析脆弱点，实时的优化加固，如果能找到攻击者进行溯源，把他揪出来，那防守端就能拿到更高的分数了。

■**第五步，复盘总结：**整个攻防演练结束之后，要把攻防成果进行复盘，根据演练的结果来总结当前的状况，包括安全问题的根源分析、安全技术的提升、安全管理制度的完善、提升安全意识、增补需要的安全设备等。自有人员技术水平不满足，就需要采购专业的安全技术服务。

运维团队防守总结

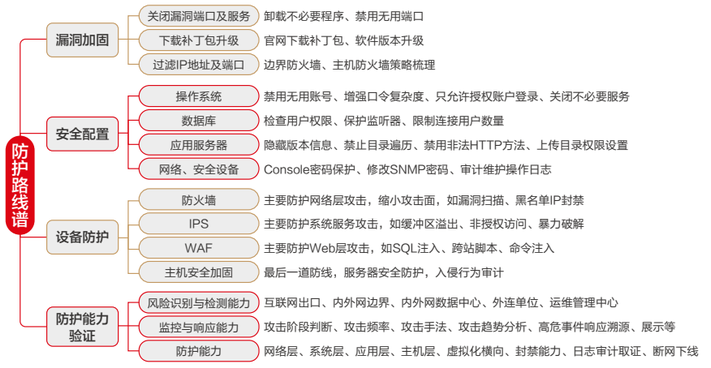
针对运维团队来说，有些工作是可以自己做的，有些工作需要请外援。比如老旧资产的排查、资产梳理、互联网暴露面的排查等，这些肯定是自身运维团队就能做的。

但比如安全工具、分析工具的使用，应急处置和攻击的研判等，就需要外援的介入。

在攻防演练的防守期间，各种防守工具也要充分的利用起来，包括安全检测设备、安全分析设备、安全防护设备、应急处置设备，如果要进行溯源，可再增加欺骗诱捕的工具或手段。

着重强调的是，在攻防演练前，一定要有明确的组织及人员规划，领导小组一定要一把手授权，在攻防演练过程中，一定要得到高层领导重视，没有强力的支持，光靠一个运维团队是没有办法把全部系统都防住的，这需要各个部门充分配合。

如果没有办法请外援，只能通过运营团队自身的能力来完成攻防演练的话，那再送给大家一张完整攻防演练要点路线图，按图索骥可以保证你的工作不会出大的纰漏。



按照防护路线图做成Checklist，对每一个完成项✅，能做到基本防守不出问题。

最最后再次强调：

■弱口令必须改！

■防范社会工程学，防钓鱼、防欺骗、防伪装！

■全员进行安全意识培训！

■宁可错封，不可漏封！

当然，找到新华三专业团队，可以事半功倍！

AIO服务助力移动公有云运维质量提升

文/贾晗

公有云及其市场简介

随着信息技术的不断发展，云计算技术已经逐渐进入到大众的视野中，其中包括了私有云、公有云、混合云等。云计算带动了各个行业的变革。公有云是指第三方提供商通过互联网为企业或个人提供计算、存储、网络等资源，提供所能使用的云服务，公有云的核心属性是共享资源服务。

目前搭建信息系统主要有三种方式：一是自建机房，自购设备，自己维护；二是租用运营商的机房，各自存放设备，各自维护；三是直接租用运营商的设备或者第三方的设备来使用，几种方式都要在IT方面投入较多的人力物力。公有云出现之后，情况有所不同，大家更聚焦自己的业务，将底层IT设施和运维都交给第三方来做，少花钱多办事，中小企业尤其需要公有云，而且公有云还可以提供很多可以二次开发的平台，在公有云上就可以完成应用的开发和部署，极大节省了中小企业在IT方面的费用支出，这促进了公有云市场蓬勃发展。以往那种只租机房或设备的IT服务形式已无法适应新的应用需求。

根据相关统计，2020年全球公有云服务整体市场规模（IaaS/PaaS/SaaS）达到3,124.2亿美元，同比增长24.1%，中国公有云服务整体市场规模达到193.8亿美元，同比增长49.7%。虽然国内公有云市场规模还比较小，但增长是非常迅速的，未来前景不可限量。在我们的工作和生活中都离不开网络，离不开数据中心，而这些都是公有云必备的要素。公有云竞争的关键要素就是规模、成本、技术、产品、服务和行业理解，这其中，规模是第一位，除了资金和规模，公有云对于技术和生态建设的壁垒都比较高，这必然将造成只有具备资源优势，在IT领域技术积累比较强的企业才能进入到公有云的竞争中。公有云当前的市场现状，依靠雄厚的资金，不计成本的投入扩张，强大的产品功能，优质的技术和服务，加上一系列的优惠政策，吸引了更多的用户进来使用，渐渐地增加与用户的粘合度。

移动公有云类业务是满足集团客户业务云化需求，拉动全业务增长的战略型产品，是中国移动政企市场的重要组成部分。移动云在2021年保持着强劲的增长，成为发展最快的云供应商之一。截止到2021年9月份，移动云已经进入了百亿营收的行列，同比增长了110%。公有云上增速第一，市场份额行业第八，其中IaaS+PaaS份额较2020年底提升3名，行业提升最快；在政务云上排名行业前3，在私有云上排名前5，保持行业领先地位。成立中国移动云能力中心，发布并建设“移动云”品牌，负责移动云N+31+X的规划、建设、运维、运营、支撑、研发一体化职责，资源池的整个计算资源达到了500万，产品的丰富度以及综合实力位居行业前三。

随着云网协同工作的持续深入，移动公有云目前面临着三大挑战，即行业解决方案落地的挑战、业务平滑上云的挑战和运维质量提升的挑战。

行业解决方案落地的挑战（售前）

■面向行业领域、技术领域的解决方案落地难；存在售前行业领域、技术领域技能缺乏的问题，政企、医疗、能源、交通、教育等主流行业领域特点了解不足，公有云产品的技术体系掌握不足，不能够很好的进行结合，导致方案难以落地。

■各方协同运营，与客户、第三方的协同，内部各部门间的协同难；各部门之间职责划分不明确，导致沟通效率低。

业务平滑上云的挑战（售中）

■云化业务的上云合理性、架构先进性、部署合规性管控难；前期售前与用户讨论方案时往往技术运维团队参与度不够，导致上云的合理性、架构的先进性、部署的合规性评估不够，后期实施困难重重。

■外部租户在上云时专业技术团队支撑与服务交付的人员配备不足，支撑力度不够。

运维质量提升的挑战（售后）

■运维故障现象复杂多变，情况多种多样，需要梳理运维边界，构建智慧数据驱动能力来保障业务连续性。

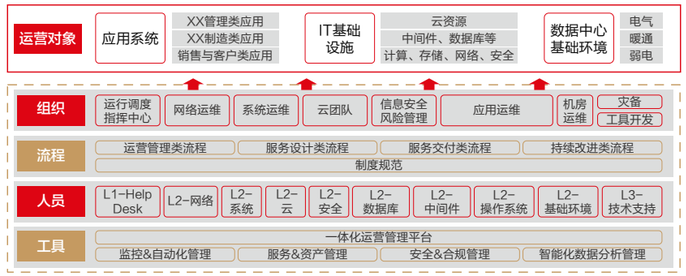
■海量设备海量业务环境下，涉及的产品和业务较多，跨越不同的技术栈，开展问题快速定位应急排障难。

■跨团队协同分析处置优化难；各部门之间职责划分不明确，工单处理流程存在缺陷，部分问题无工单流程处理，导致问题处理效率低。

AIO助力移动公有云服务质量提升

H3C AIO Service一站式运维服务，从组织、流程、人员、工具整体实现统一运维服务交付，与移动公有云运营运维团队共同对其服务的SLA负责，为移动公有云高可用性提供重要保障。

All In One，“AIO Service”



AIO一站式运维管理服务内容主要包括以下几个部分：

■运维工具平台：提供运维工具辅助现场运维，运维平台体系搭建，平台模块化搭建。

■现场运维服务：以SLA为导向，与移动公有云运维团队共担运维责任，共同保障业务正常运行。

■远程运维服务：远程监控与管理，协助现场运维。

■专项创新服务：担当移动公有云基础架构的顾问、运维咨询顾问，提供架构优化、性能分析与优化、流程等专项服务。

公有云业务的服务质量和业务水平是影响用户体验的核心要素，新华三AIO（All In One Service）一站式服务为移动公有云用户满意度提供专业保障。针对移动面临的三大挑战，对于重点用户制定专属“上云”相应机制。

■上云前：协同上云团队，清晰业务架构模型，明确平台业务指标，梳理风险点，量身定制上云网络方案。

■上云中：联合测试，上云前搭建测试环境，联合客户验证，保障方案可落地，杜绝上云后的性能劣化；快速开通，前后端协同，各环节监控，快速开通云网业务。

■上云后：健康巡检，根据客户要求频率，开展资源深度巡检，掌握资源健康状态；分析资源健康程度，提前预警风险；客户业务优化，根据客户业务实际运行情况，结合移动云平台特点，提出客户业务架构优化建议，共同提升业务可用性；应急响应和处理，故障发生10分钟内响应和处理，故障恢复后72小时内提供故障报告，完善各类应急预案。

加强运营运维能力建设

AIO一站式运维团队与移动团队从基础运维、自动化运维、云网融合等方面对售前、售中、售后全方位进行赋能，提升系统业务连续性、缩短故障定位时间、降低运营运维成本。

资源池基础运维赋能

■资源池运维规范和流程培训；

■资源池硬件、网络运维技能培训；

■结合移动云、合营云硬件集成，开展硬件、网络运维实操。

资源池自动化运维赋能

■通过监控工具和各类硬件巡检脚本，确保监控无死角；

■通过工具，自动输出数据库、核心设备、云平台性能分析报告。

售前售中售后支撑赋能

■售前行业解决方案的支撑；

■售中资源管理、业务部署、迁移服务等上云支撑；

■售后运营分析、容量管理、工具优化提供优云提升，云平台、云服务和云安全的护云保障。

云网融合支撑赋能

■参与云网PE合设试点测试；

■参与云网专区组网方案设计和测试方案建设；

■搭建云网实验室。

加强运维服务体系建设

AIO一站式运维团队与移动团队共同建立完善的运维服务体系，加强流程与规范建设、信息安全建设，缩短业务开通时间，厘清故障排查思路，加强各方面合作，为移动公有云的顺利开通和稳定运行提供重要保障。

日常运维

■制定完善的入网、上线、割接等方案，制定应急措施和验收测试方案；

■对移动公有云基础架构、云资源池的运行状况进行检查和分析；

■加强对移动公有云基础架构的可用性管理、变更管理、配置管理；

■对公有云平台集中监控，对现网设备进行定期巡检，对发生的事件进行统计分析。

流程与规范

■针对移动公有云平台制定和优化现网流程，包括入网管理流程、事件管理流程、配置管理流程、变更管理流程、应急流程、日常运维流程等，对个别环节进行优化，协助移动公有云团队建立标准化运营运维流程体系；

■制定服务团队管理机制，包括运营运维保障职责、绩效管理、值班计划、值班守则、人员培训计划等；

■针对移动公有云售中阶段的上云新建和上云迁移流程进行梳理和优化，加强二线三线的技术团队加入到售前方案的制定和评审中，并保障后期实施的顺利落地；

■针对移动公有云售后阶段的故障处理流程进行梳理和优化，重点关注客户满意度，希望达成用户满意度100%的最终目标，加强工单系统建设，打通一二三线支撑团队的沟通，保障问题处理流程更为顺畅，有效缩短问题处理时长；

■以SLA为导向，做到问题及时响应，及时通报，先恢复再排查的原则。

信息安全建设

■对于网络、云平台各操作系统层面的信息安全问题，提供分析风险、规避风险、解决漏洞及配置的能力；

■提供安全漏洞补丁加固能力，能够准确分析出加固风险。

项目实施配合

■对配套的基础资源平台的咨询、规划和技术进行支持；

■对系统平台的新技术方向，系统平台的技术架构部署、性能趋势、扩容方案提供咨询建议，并对重点技术方案进行针对性课题研究。

加强运维质量管控

分层运维规建工作输出了各类标准，是运维质量管控中各模块的需求来源、依据和标准，制定了分级标准、集成和入网标准、监控标准、验收标准等。

质量管控各模块在发布和实践管理时，总结更新出新的标准，输出分层运维体系，更新完善标准，制定了入网管理、应急管理、隐患管理、需求管理、性能容量管理、版本管理、高可用管理、备份管理等。其中入网管理、隐患管理、应急管理，是稳态管理总线的基本要素。

运维质量管控——入网管理

■职能说明：入网管理的目的是定制和更新工程入网验收检查规范，包括基础检查、可用性检查和容量检查等部分。同时，倒推更新基础规范，使集成团队严格按照新集成规范，建设符合入网标准的工程。

■总体目标

●更新集成规范指导手册；

●更新入网验收检查标准；

●严格执行新工程入网检查；

●优化入网验收检查规范。

■重点工作

●组织各专业组，完成更新工程集成规范，包括命令规范、硬件配置要求和逻辑配置要求、组网架构等内容，文档发布给集成组，指导工程集成规范实施；

●完成入网验收检查规范更新，重点完成各专业基础检查、可用性检查、容量检查等细则的制定；

●依据工程入网验收检查规范，对工程阶段设备开展入网检查，通报检查结果、推动和完成优化入网验收检查规范。

运维质量管控——隐患管理

■职能说明：隐患管理适用于云平台各类IaaS基础设施，以确保现网隐患处置工作有章可循、有序开展，保障各类云平台和独立业务平台的稳定运行。

■总体目标

●完善并落实隐患管理细则中相关内容，完成对云平台运行部内部宣贯；

●形成完整的隐患录入、处置、评审、闭环体系；

●最终达到各专业隐患处置工作有序开展，保障业务平台健康稳定运行。

■重点工作：设计并发布标准、流程、角色和分工、隐患管理清单、管理细则、考核标准等。

运维质量管控——应急管理

■职能说明：应急管理的目的是提高应对紧急事件的管理水平和应急处理能力，减少系统故障对生产业务造成的影响，确保系统运行的连续性。从“人”、“流程”、“工具”三方面增强服务台和二线技术团队的应急能力。

■总体目标

●增强服务台总控能力，前15分钟完成响应和组织；

●增强二线技术团队应急处置能力，30分钟内完成定界和处置。

■重点工作

●完成服务台总控能力的调研和提升，重点是提交工具需求，熟练使用总控过程中的各类表单和问答清单，熟悉应急过程中的各个关键步骤和标准动作；

●完成二线技术团队的应急处置能力的调研和提升，重点完成各专业应急手段和应急预案的制定；

●完成若干次故障推演和故障演练，重点在锻炼服务台的总控能力和二线技术团队的应急处置能力。

服务内容、职责梳理优化

为更好的服务移动公有云业务，项目团队梳理了移动售前、售中、售后的服务内容，明确了各岗位的工作内容及职责划分，加强了各部门间的紧密合作，提高了移动公有云运营运维效率。

售前服务内容

■受理所有用户和客户经理的咨询请求，并对咨询请求进行初步解决和分派；

■业务拓展技术支持，宣讲布道，完成移动云客户上云需求调研、售前方案设计、资源规划、技术评估等；

■进行移动云重要咨询请求解答，对行业咨询需求进行分析、研究、处理等；

■关注国内外行业竞品及发展趋势，负责移动云产品的竞争性分析、对标分析、趋势分析等。

售前服务内容	任务	售前团队	售前经理	二线	三线
咨询宣传类	咨询请求分派与解决	R	A	C	C
	云平台宣讲布道	R	A	C	C
业务开拓类	业务拓展支持	R	A	C	C
	上云需求调研	R	A	C	C
方案设计类	售前方案设计	R	A	C	C
	上云新建\迁移方案评审	R	A	C	C
前瞻类	发展趋势分析	R	A	C	C
	行业竞品分析	R	A	C	C

备注：

1、谁负责（R = Responsible），即负责执行任务的角色，他/她具体负责操控项目、解决问题。

2、谁批准（A = Accountable），即对任务负全责的角色，只有经他/她同意或签署之后，项目才能得以进行。

3、咨询谁（C = Consulted），拥有完成项目所需的信息或能力的人员。

4、通知谁（I = Informed），即拥有特权、应及时被通知结果的人员，却不必向他/她咨询、征求意见。

售中服务内容

■负责支撑售前团队完成客户上云需求调研、方案制定、方案设计、资源规划和其他相关售前工作；

■负责非标准资源的开通、发放、变更、撤销等资源配置管理及实施工作；

■协助客户完成业务的上云迁移、上云保障工作，并配合客户进行相关业务的上线割接等技术支持。

售中服务内容	任务	客服	一线	二线	三线
产品类	产品上线	I	R	A	C
	产品变更	I	R	A	C
	产品下线	I	R	A	C
业务类	业务开通	R	A	C	C
	业务 / 账号暂停	R	A	C	C
	业务变更	R	A	C	C
	业务 / 账号恢复	R	A	C	C
	业务退订	R	A	C	C
	业务系统联调	R	A	C	C
资源类	ICP/IP 备案	I	R	A	C
	资源开通	R	A	C	C
上云迁移类	云上基础设施迁云实施	I	R	A	C
	在线业务应用迁移实施	I	R	A	C
	在线业务存储迁移实施	I	R	A	C
	在线业务数据库迁移实施	I	R	A	C
培训	云产品运维培训	I	I	R	A

售后服务内容

■负责云平台运行的定期巡检、故障处理、问题处理、变更实施和其它日常维护工作，负责云平台软硬件设备相关厂商的协调和管理工作；

■负责云服务运行的定期巡检、故障处理、问题处理、变更实施和其它日常维护工作；

■负责移动云相关安全工作的日常维护，安全设备的运维管理工作，安全设备的备件更换保修工作，以及协助省公司安全部门完成移动云的重大安全故障处理。

售后服务内容	任务	客服	一线	二线	三线
事件管理	日常巡检	I	R	A	C
	投诉处理	R	A	C	C
	工单处理	R	A	C	C
故障管理	故障处理	I	R	A	C
	应急保障	I	R	A	C
变更管理	变更处理	I	R	A	C
	信息通告服务	I	R	A	C
服务资产和配置管理	平台交接维	I	I	R	A
	平台资源优化	I	I	R	A
	配置稽查	I	I	R	A
	备份管理	I	I	R	A
服务级别管理	运维手段提升	I	I	R	A
	告警监控优化	I	I	R	A
	性能优化	I	I	R	A
	高可用演练	I	I	R	A

结束语

AIO（All In One Service）是新华三面向ICT基础架构提供的一站式运维管理外包服务，通过完善服务管理体系，从人员招聘、流程优化、质量管控、统计分析、自动化运维等，确保移动公有云的SLA目标达成，也为移动公有云的运维带来了极大的便利和保障，带动移动公有云全面提升整体服务管理水平，厘清故障排查思路，明确各岗位职责，加强各方面合作，提升运营运维效率，确保系统业务连续性，缩短故障定位时间，降低运营运维成本。同时整合了新华三在运维领域的资源与解决方案，在服务管理咨询、运维平台与工具、智能远程运维、技术运维，以及英雄联盟多厂商服务等方面，为移动公有云提供整体运维能力输出，并根据移动业务特点和行业特性，为其提供定制化服务。AIO服务助力移动公有云运维质量提升，为移动公有云的飞速发展保驾护航。

数字化时代
如何进行业务故障定位

文/何洪团

数字化转型改变IT部门对业务运维认识

中国数字经济蓬勃发展，极大的提升了IT业务系统对各行各业的重要性，也改变了企业管理人员和IT部门对业务运维的理解。现在已经很少有人认为“只监控IT基础架构就可以保障业务系统正常运行”。IT部门对业务运维及业务故障定位认知也发生了变化：

- 运维的目标不是保障设备正常运行，而是为最终用户使用业务系统提供良好的用户体验；
- 除了传统的IT基础设施监控（ITIM），UEM（用户体验管理）/NPM（网络性能管理）/APM（应用性能管理）等新的监控手段对于保障最终用户使用业务系统的良好体验、业务故障快速定位非常重要；
- 业务故障定位需要依赖CMDB；
- AIOps 可以提升业务故障定位效率。

业务故障定位认知误区

我们走访了大量客户，发现很多运维人员对于如何进行业务故障定位存在一些认知误区：

- 对CMDB在业务故障中定位有误解，认为CMDB应该提供各种业务故障分析能力。

运维人员能够认识到CMDB对业务故障的价值是一个可喜的提升，但是也不应夸大CMDB在业务故障定位中的作用。CMDB是管理CI属性和CI之间关系的一个数据库，提供数据给监控/ITSM/自动化/业务分析等运维组件消费。CMDB可以为业务故障定位提供“主线索”，但是CMDB本身并不提供业务故障定位功能。业务故障定位是其他运维组件的功能。我们可以认为在业务故障定位中CMDB只是一个“骨架”，只有其他运维组件给骨架添加“肌肉”以后，业务故障定位才能灵活的运转起来。

业务故障定位时经常要用到的CMDB数据包括：资源配置信息、业务间逻辑拓扑、分层业务拓扑、业务变更信息等。

- 没有意识到业务故障定位是分场景的，期望用一个手段解决所有的业务故障定位需求。

很多运维人员认为业务故障定位属于ITIL事件管理流程，指业务发生故障后快速进行故障分析并恢复业务。但是广义的故障定位范围更宽，包括：

- 事前业务故障预防：比如变更评估、容量管理等；
- 事中业务故障恢复：属于ITIL事件管理流程范畴；
- 事后故障根源分析：分析历史故障，找出问题根源，避免问题重复发生，这些属于ITIL问题管理范畴。

事中故障分析也分很多类型，比如服务器硬件损坏引起的业务故障、网络不通引起的业务故障、应用程序异常引起的业务故障等。

所以，用一种手段解决所有的业务故障定位需求是不现实的，需要按场景进行业务故障定位功能设计。

- 在进行业务故障定位时，缺乏对运维数据分层次、分专业进行管理的认识，把各种运维数据堆砌在一起反而影响业务故障定位效率。

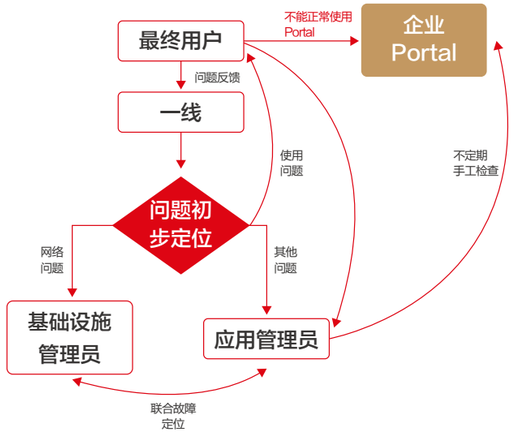
不管运维部门组织架构如何，业务故障定位都会涉及到一线/二线/三线、应用管理员/主机管理员/网络管理员/DBA等不同角色，只是不同的组织这些角色可能由同一部分人承担。所以，业务故障定位一定涉及到不同角色分工协作。但是部分客户在规划业务故障定位功能时，经常把所有运维信息都堆砌在一起，期望让一个人看懂所有运维信息，完成整个业务故障定位过程。这样反而无法让“正确的人看到正确的信息”，影响业务故障定位效率。

比如对于一线运维人员，他们并不具备很强的故障定位技术能力，他们只需要初步对故障进行责任划分，把工单分派给正确的人。如果把所有运维细粒度数据（比如应用程序代码级运行数据）都展示给一线，反而让他们手足无措。

数字化时代如何进行业务故障定位

某客户业务故障发现和定位过程分析

下图是某客户Portal系统故障定位过程，具有一定的代表性：



当前业务故障定位存在的问题：

■问题发现

●一个人管多个业务系统，靠定期手动检查，很难主动发现问题；

●业务故障主要靠客户反馈被动发现；

●部分客户跳过一线直接联系二线（ITSM流程问题）。

■一线分派

●网络问题可以判断；

●简单的系统使用问题可以判断；

●其他问题不能准确分派，一般都派给应用管理员。

■二线故障定位

●应用管理员在定位故障过程中主要靠查看主机资源消耗和应用日志；

●应用管理员在定位过程中看不到完整设备运行信息和性能趋势，需要协调基础设施技术组一起定位，定位沟通效率低。

如何实现完整业务故障定位

我们认为一个完整的业务故障定位方案应该包含三个层次：

■完备的业务端到端监控数据：是业务故障定位的“肌肉”；

■CMDB业务模型：是业务故障定位的“骨架”；

■场景化业务故障分析手段：通过把“肌肉”和“骨架”结合，形成一个可以灵活运动的“人体”，最终实现业务故障定位。

完备的业务端到端监控是业务故障定位的基础

中医讲究“望闻问切”、西医依靠各种检查指标。业务故障定位也是类似，如果没有完备的监控数据，运维人员无法主动发现业务故障。即使业务故障被最终用户发现并上报，运维人员也很难进行定位分析。所以，完备的业务端到端监控数据就是业务故障定位的基础，相当于人体的“肉”。

业务端到端监控应该包括三个层次：

■用户体验监控：应具备的功能包括

●用户体验概览：展示单个业务体验趋势、区域体验分析、TOPn慢页面等

●监控页面：列表展示被监控页面点击信息、性能信息

●页面分析：单个页面点击、响应时间趋势分析

●区域分析：分析访问用户来源区域及不同区域体验

●JS错误分析：分析页面产生的JS错误

●AJAX分析：分析页面AJAX请求和性能

●热力图分析：分析页面中被点击的热点区域

- VIP用户保障：分析重点客户访问业务详情和体验度，保障重点用户体验

- 浏览器分析：分析不同浏览器访问业务次数和性能差异，判断用户体验异常是否与其使用的浏览器有关

■ 应用性能监控：应具备的功能包括

- 情报汇总：展示所有应用程序得分、响应时间、错误率等指标

- 应用拓扑：展示自动发现的应用拓扑

- 外部访问：分析当前应用对其他服务调用的情况

- 异常&错误：分析应用程序产生的异常和错误信息

- 后台任务：分析后台任务（不是由前台请求发起的任务）执行情况

- 数据库/NOSQL：响应时间、总耗时、吞吐率等TOPn数据库访问分析

- 事务：响应时间、总耗时、吞吐率等TOPn事务分析

■ IT基础架构监控

监控支撑业务系统的基础软硬件，包括机房、服务器、网络、存储、操作系统、数据库、中间件、云平台、大数据平台等。

CMDB业务模型是故障定位的主线索

如果没有CMDB，支撑业务的组件（基础软硬件、应用程序、业务服务等）就是一盘散沙，业务故障定位就像大海捞针一样。CMDB是业务系统故障定位的主线索，相当于人体的“骨架”。故障定位可以按照CMDB提供的线索顺藤摸瓜。

■ 业务故障定位经常用到的CMDB功能包括

- 业务间逻辑拓扑：分析某个业务系统跟周边业务系统的关联影响关系。业务故障是否由周边业务系统故障引起、业务故障会影响到哪些周边系统?

- 分层业务拓扑：用于不同运维角色对业务系统有一个整体、全局认识，是他们之间进行业务故障定位沟通协调的“统一语言”。不同运维角色可以看到自己运维组件运行情况，也可以看到其他关联组件基础属性和运行情况。

- 业务变更记录：常用于分析变更对业务系统的影响情况，评估变更是否达到预期、变更是否引入业务稳定性风险。

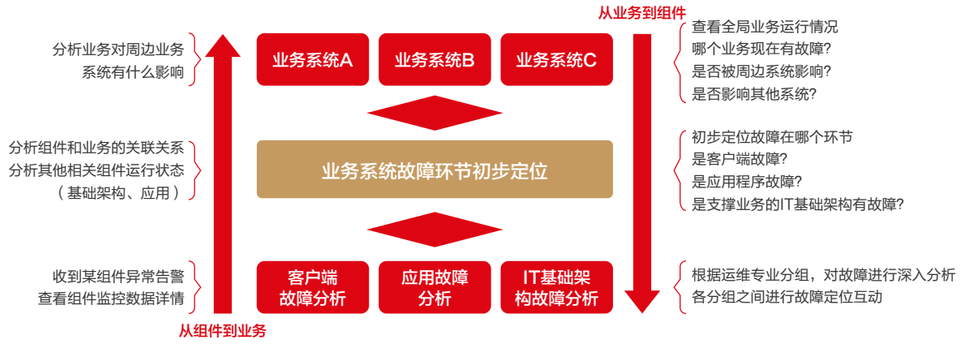
双向闭环业务故障定位

业务故障定位就是基于应用场景，实现监控数据（肌肉）和CMDB（骨架）的有机结合（人体）。部分场景还包含ITSM工单数据。

常用的业务故障定位一般分两种情况：

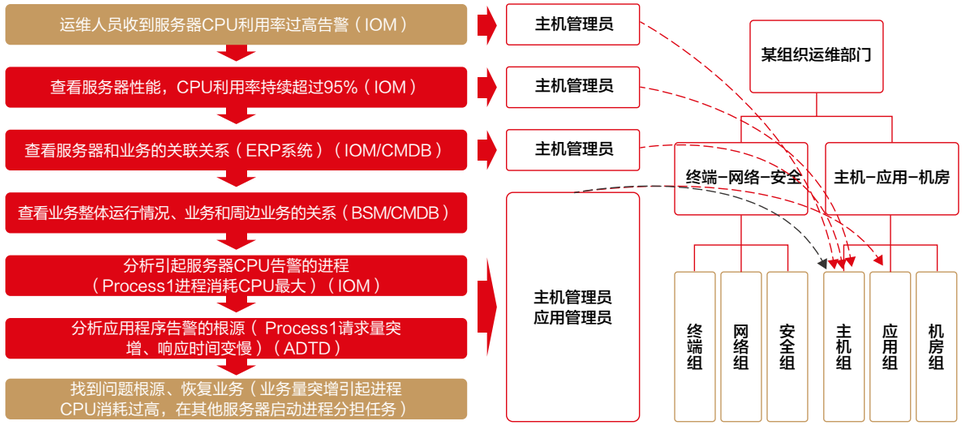
■从业务到组件（基础软硬件、应用程序、业务服务等）：比如一线收到客户投诉某个业务系统访问变慢，需要定位到具体哪个组件是业务故障的根本原因。

■从组件到业务：比如运维人员收到一个服务器CPU告警，需要分析该告警对业务的影响情况，并定位到故障根本原因。



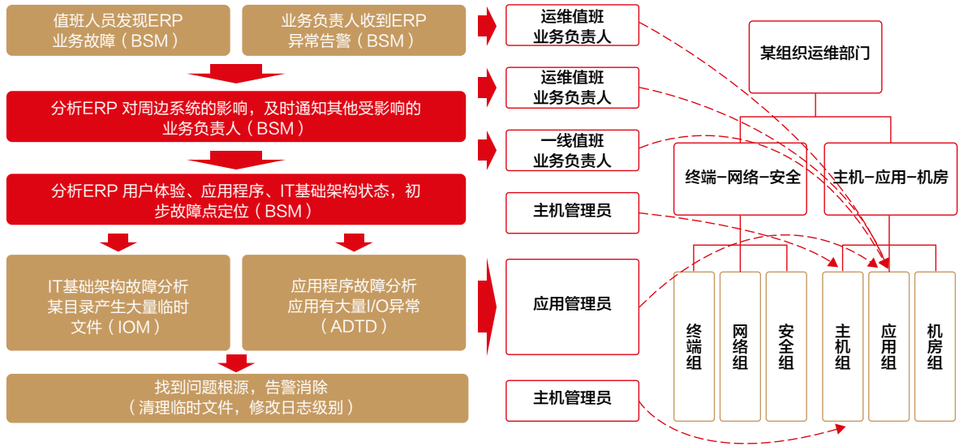
■“从组件到业务”故障定位过程示例

运维人员收到一个设备告警，故障定位线索为：收到设备告警➡找到设备支撑的业务系统➡分析该业务系统和周边业务之间关系➡确定是哪个业务系统有问题➡确定是业务系统内部什么组件有问题➡找到故障根源、恢复业务。



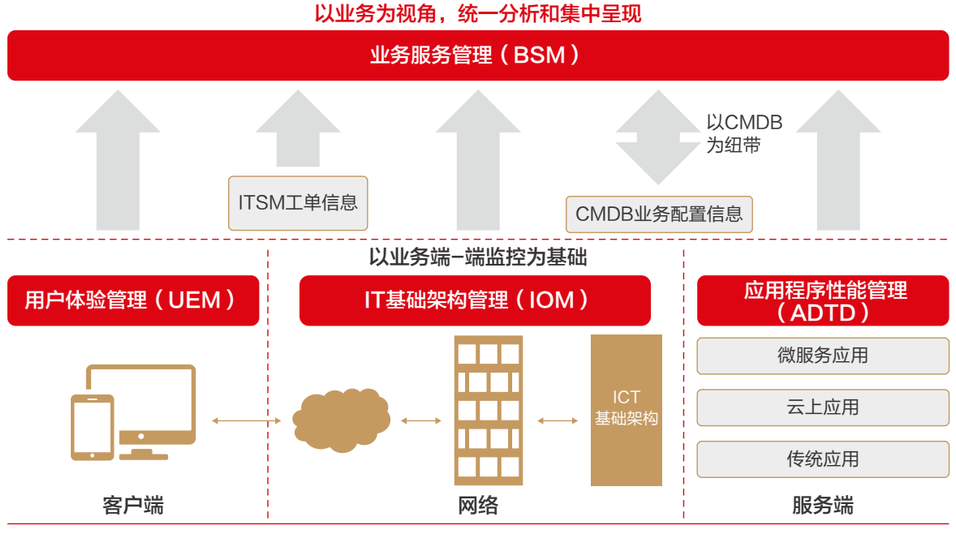
■“从业务到组件”故障定位过程示例

运维值班人员（一线）收到业务故障告警或者最终用户业务投诉后，故障定位主线为：发现业务故障➡分析该业务系统和周边业务之间关系➡确定是业务系统内什么组件有问题➡找到故障根源、恢复业务。



业务故障定位实践

BSM（业务服务管理）是基于U-Center统一运维平台的业务故障定位解决方案，BSM是业务监控和分析平台，该方案以业务为视角、以CMDB为纽带、以业务端-端监控为基础，实现业务运维数据统一分析和集中呈现，最终实现业务故障主动发现、快速分析、快速恢复，把运维部门的业务价值呈现出来。

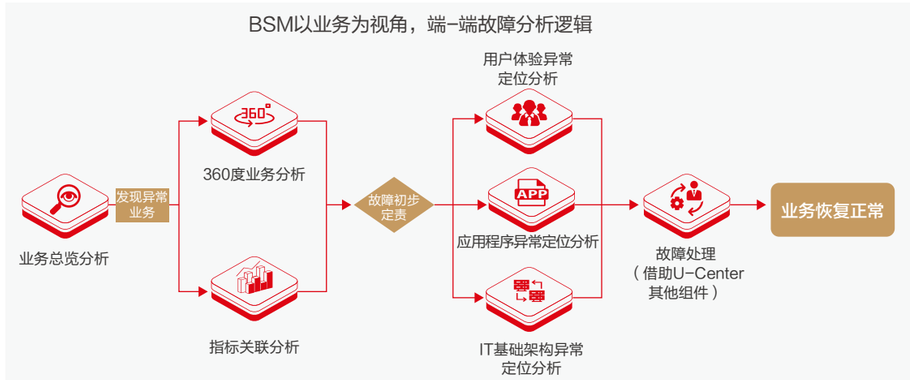


BSM为运维人员提供从业务到组件、从组件到业务双向闭环故障定位能力，系统预置多种场景化故障分析手段，用户也可以基于BSM自定义故障定位模板。

BSM数据来源说明

BSM实现业务运维数据综合分析，数据来源主要包括3个方面：

- 业务端-端监控数据，包括：UEM真实用户体验监控、ADTD应用程序监控、IOM支撑业务的ICT基础架构监控。数据类型包括状态数据、性能数据、告警数据；
- CMDB业务配置信息，包括：业务相关资源配置信息、分层业务拓扑、业务间关系拓扑、CMDB业务变更信息等；
- ITSM业务相关工单信息。



业务故障示例一：从组件到业务故障定位

BSM通过CMDB打通各种监控数据，可以实现从组件告警到业务故障定位分析过程。

下图示例：Tomcat_10.153.49.26无法连接，严重告警➡Tomcat_10.153.49.26监控详情➡支撑CRM系统➡CRM业务详情。

- 查看告警详情：发现tomcat_10.153.49.26无法连接。
- 从告警关联到设备详情：了解该设备所有告警信息、监控指标详情、设备配置信息。发现URL_10.153.49.26访问失败。说明这是一个严重问题。

- 从设备关联到业务系统：通过“关联资源”可以了解到该tomcat支撑了CRM业务系统。

- 分析tomcat告警对CRM业务系统的影响
  - 业务整体健康状态：不健康；
  - IT基础架构层得分：0分，说明有核心组件不可用（该组件不可用，将直接引起业务不可用）；
  - 业务拓扑：可以看出因为tomcat 故障影响了CRM前台页面（URL）不可访问。

用户体验和应用程序得分是100分，是因为已经没有用户能访问业务系统，UEM/ADTD都没有采集到数据。

分析结论：tomcat故障引起CRM系统不可用， 并且CRM系统的tomcat 存在单点故障风险。

业务故障示例二：变更影响分析

企业为了快速响应市场变化，需要频繁对业务进行调整，经常需要对业务系统进行升级改造等变更。变更常常影响业务系统正常运维，据统计约40%的业务故障跟变更有关。

变更影响分析是BSM/CMDB/监控数据/ITSM工单关联分析典型应用场景，分析流程如下：

- 查看某时间范围业务系统相关变更、ITSM工单信息；
- 选择某一次变更（ITSM工单逻辑一样），查看该次变更详细信息；
- 对比变更时间点前后一段时间业务系统关键性能指标趋势，分析业务系统性能是否有突变；
- 进行变更影响评估，如果变更是对业务系统进行扩容和性能优化，变更后性能提升是否达到预期；如果变更是对业务系统进行功能改造，变更后性能是否降低。

业务故障示例三：告警回溯分析

通过BSM对业务系统历史告警进行“复盘”，找出引起业务告警突增的根本原因，并对告警规则、业务系统本身进行优化。

应用场景： 业务系统过去一周告警频繁发生，运维人员对问题根源进行分析。

场景举例： CRM系统昨晚产生大量告警，通过告警趋势分析发现主要是服务器A CPU利用率过高告警，应用程序B响应时间慢告警，并且通过业务拓扑发现A、B之间的关联关系，结合应用程序请求量分析，运维人员最终定位出CRM系统故障根源是应用并发突增。

分析流程说明

- 查看某时间范围业务系统告警趋势；
- 重点分析告警峰值，查看告警详细信息；
- 通过时序分析查看告警发生的时间顺序；
- 点击告警在业务拓扑图上查看这些告警资源之间的关联关系；
- 最终定位出引起告警突然增加的根本原因。

总之，完备的业务端到端监控是业务故障定位的基础（肌肉），准确的CMDB业务模型是业务故障定位的主线索（骨架）。业务故障定位需要基于场景和算法，实现监控数据、CMDB数据、ITSM工单数据有机结合（人体）。

新型医保云容灾最佳实践分享

文/赵俊华

前言

自2018年国家医疗保障局（以下简称国家医保局）成立以来，就开始进行全国医保云建设的统一规划，陆续出台了多项医疗保障信息平台建设的指导意见和标准规范，指导和规范各省级医保云建设。

根据国家医保局发布的《医疗保障信息平台云计算平台规范》要求各省实现医保信息化统一技术架构标准目标，为业务子系统提供技术架构标准所要求的基础功能软件产品和服务。数据中心采用分布式云架构，封装核心云支撑服务适配接口，用于实现云产品解耦设计，为上层的HSAF（Healthcare Security Application Framework）框架及应用系统提供标准化支撑。HSAF适配框架适配分布式微服务、分布式消息队列、分布式缓存、分布式数据库中间件和分布式非结构存储等。在应用架构方面，如定义了14个业务子系统+业务中台+数据中台，规范了应用的技术架构HSAF，统一了应用系统的UI界面，提出了各厂商云平台需具备的能力需求。

在医保数据方面，实行两级集中模式，制订了相关数据治理和管理规范，实行国家和省级数据的大集中。在网络方面，实行全面覆盖，核心业务区网络统一规划、分级管理，纵向与国家、省、市、县、乡互联互通，横向与人社、卫计、民政、财政、税务、公安以及医院、药房、银行和保险公司互联互通。

在2019年6月国家医保局提出的《医疗保障信息平台建设指南》中，对容灾总体能力提出了要求，其不能低于《信息系统灾难恢复规范》中定义的第5等级的实施方案，生产灾备双中心必须实现数据层、业务应用层和网络访问层的平稳切换，实现多中心、并行运行、互为容灾的目标。医保云的容灾主要针对数据和应用两大类，根据提供基本的数据保护和提供不间断的应用服务来区分，一般情况下容灾类型可以分成数据级容灾、应用级容灾和业务级容灾三个级别。整体容灾技术指标要求核心关键数据（数据库、Redis、Kafka等）RPO约为0，文件影像数据（对象存储）RPO 3分钟， RTO 30分钟。

医保云架构

医保云平台在功能方面划分为公共服务区和核心业务区，在技术层面分为云基础设施、IaaS平台、DaaS平台、PaaS平台、适配框架、业务中台、业务前台。应用系统是基于HSAF框架开发，在业务支撑中提供各种服务接口。云支撑服务层基于云基础设施，为应用层提供通用的技术支撑服务，包括分布式服务、分布式缓存、分布式数据访问、日志服务、非结构化存储和消息队列等。云基础设施层采用云架构，在物理设备基础上，实现计算资源、存储资源、网络资源的动态管理和资源调配。

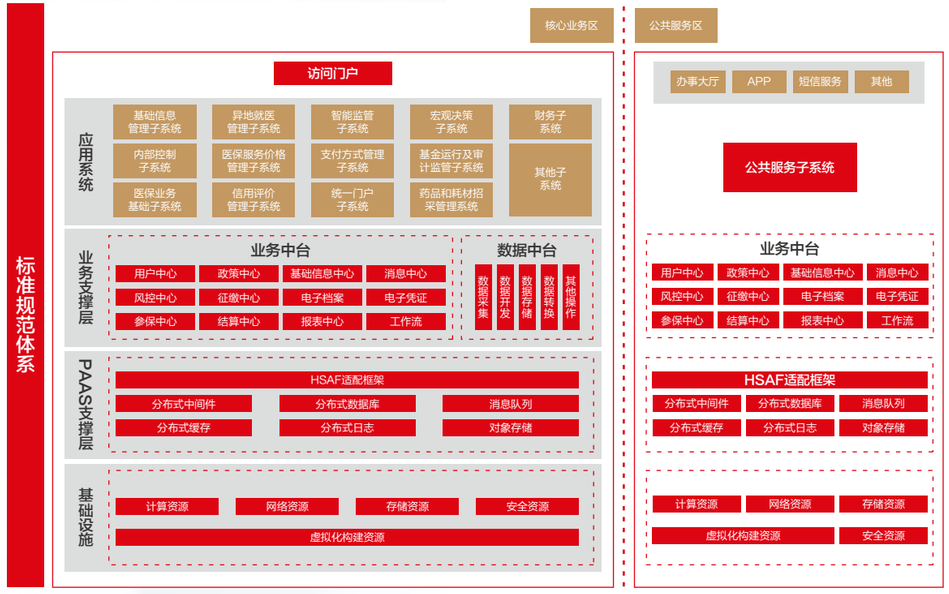


图1 总体架构 来源参考《医疗保障信息平台建设指南》《医疗保障信息平台云计算平台规范》

生产和灾备中心是业务边界清晰、定位明确的两个中心，生产中心可以闭环承载全部生产业务，灾备中心双活运行并实时复制数据。生产和灾备中心间没有业务互访流量。在生产中心出现重大灾难性故障时，灾备中心可以自动化一键切换关键业务到灾备中心运行。同时灾备中心又作为生产中心核心生产业务数据的异地备份中心。生产中心与灾备中心采用完全相同网络和安全架构，中心按照1:1的处理能力配置计算资源，支撑各应用系统实时在线运行。生产中心与灾备中心之间通过万兆光纤网络直连，实现数据高速同步与复制。

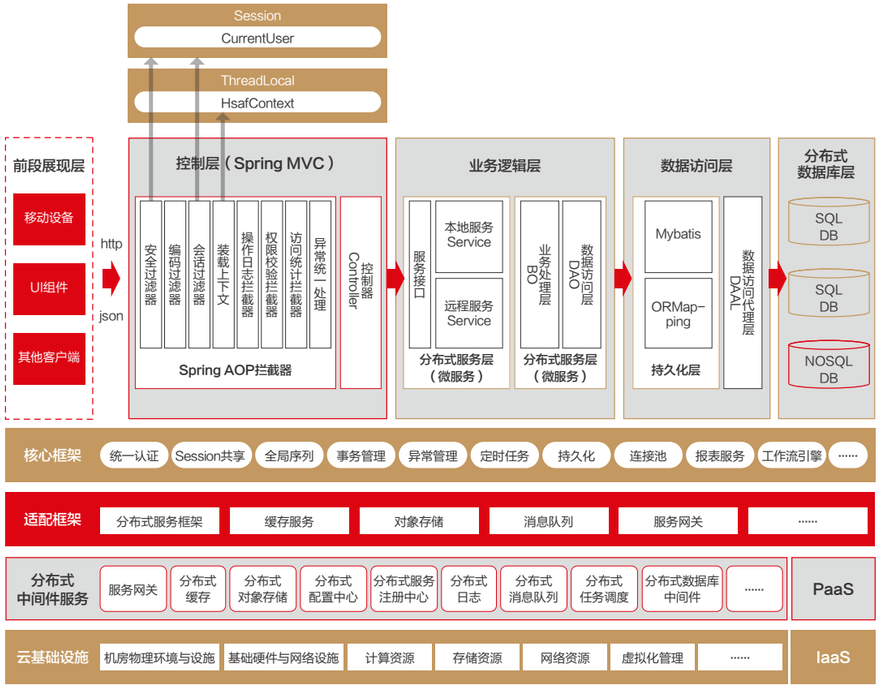


图2 应用技术架构 来源于《医疗保障信息平台应用系统技术架构规范》

常见的方案包括如集群整体切换方案，即“两朵云”架构，主备机房独立运行，PaaS数据层之间通过专线进行数据复制同步，当主机房应用或数据服务发生故障时，通过DNS域名或GSLB快速切换到备机房来接管业务。另外一种方案就是，单集群跨数据中心部署，在数据层，将不同数据的主副复本分散在不同的机房，当某个数据的主复本所在机房出现故障时，可以在另一个机房将副复本设置为主复本。鉴于“两朵云”架构最为常见，在接下来的阐述中，如无特殊说明，都将以这种架构为基础，来介绍医保云容灾演练实践。

演练实践

容灾方案是否能够满足业务持续性要求，容灾建设目标是否成功实现，都需要容灾演练来检验。

演练原则与策略

■ 演练有效性和安全性

找出存在的问题，找出不足并加以改进和完善是演练的目标之一，包括系统、预案和资源等方面。

既要保证演练的有效性，又要保证演练过程的安全，而安全性和很多特性是相冲突的，如安全与易用性，安全与有效性等，而我们需要找到一个平衡点。常用的方法就是分解，将一个大的容灾演练流程分解成小的子流程，先演练小的流程，再组合成大的、复杂的流程。至于哪些云平台组件或场景先演练，需要我们从全局推进并根据实际情况进行决策，一般建议先局部后整体，先简单后复杂，先手工后自动的原则进行容灾演练。如一些常用的子流程，DNS域名切换子流程、PaaS层组件自动启停、应用自动重启子流程可以先进行测试。

■ 数据一致性策略

在医保云信息系统中，各云平台厂商提供了各自的分布式PaaS层数据组件服务，如缓存Redis，消息中间件Kafka，对象存储OSS，分布式数据库DRDS，而国家医保局提供的应用技术框架HSAF，通过适配层来匹配各云厂商提供的PaaS层数据服务。在应用层，采用的是无状态的设计模式，所有用户Session通过共享Redis集群的方式来进行共享存储，所以应用层的数据一致性又由PaaS层数据服务Redis来保障。

事前准备工作

根据国家医保局提出的总体容灾能力要求，容灾工作涉及应用层、数据层和网络层等方面的平滑切换。每一层又都涉及众多供应商提供的产品和服务，比如不同的应用子系统可能是由不同的应用厂商独立开发的。网络方面，包括安全设备、GSLB或DNS，骨干网，数据中心核心网络、第三方横向接入等。数据层涉及Redis、Kafka、OSS和DRDS等组件，都可能采用不同厂家的产品或技术。各家技术人员侧重于自身产品特点，而容灾意识或容灾认知水平存在较大差异，在容灾演练前，需要做好容灾知识的宣贯以及容灾方案的简要描述，让各参与方明白自己的职责。

凡事预则立，不预则废。从容灾建设方案来看，似乎很容易理解各层次的容灾切换，但从实际容灾演练的经验来看，出现问题的情况颇多，其中很多因素都可以在事前避免，所以充足和全面的准备工作是非常必要的。

演练预案设计

预案的设计，要切合总体容灾目标。在常用的容灾预案场景收集中，已经抛弃了过去从故障原因角度进行收集，而是以IT组件视角，以结果为导向，只要组件发生了故障，不能正常提供服务，在规定的时间内不能恢复，用同样的解决方案就可以归为一类。

一旦确定好了预案场景，就要开始设计预案执行步骤了，预案执行步骤的设计影响预案执行的效率、有效性和安全性。虽然在事前做了相关准备，尽量减少可预见的问题影响容灾演练，但是实际中问题出现的多样性，以及我们也不可能不计成本地去预防可能出现的所有问题。

容灾工具

工欲善其事必先利其器。处于建设期的医保云系统，更需要一些好的工具来发现、定位和解决问题。在满足指南和标准要求的前提下，容灾演练工具应从预案维护的专业全面，到任务流转的高效协作，再到预案执行时全局监控，实现信息沟通智能化、响应过程自动化、执行过程可视化、资源调度合理化、通讯互联一体化。通过科学、现代、高效的应对危机事件和常态化的演练提升应急管理能力，提高容灾和风险预防及应对能力，保障业务服务水平和关键业务持续。

在突发事件面前，通过平台进行快速切换，缩短灾难恢复时间，其本身需要具备如下能力：

- 具有灵活的任务流程编排能力，根据需求灵活自定义任务，如与云平台，或DNS等组件，能够自动获取相关任务配置信息；
- 具有可视化能力，全方位展示预案流程执行的过程；
- 具有自动化切换能力，通过一键切换功能，降低RTO；
- 具有高效的沟通协同能力，指挥整体演练流程；
- 具有切换过程可记录、追溯和审计能力。

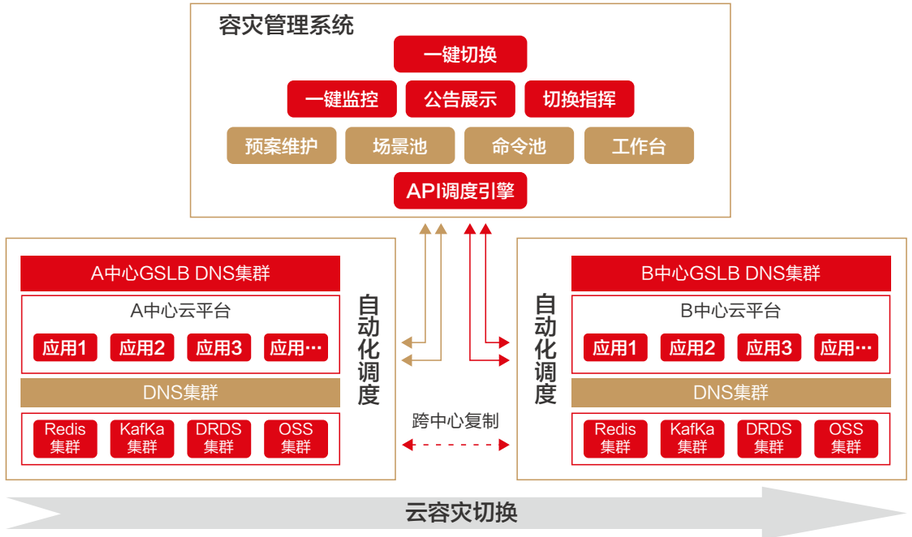


图3 容灾切换架构 来源于云容灾项目实践

以AB中心的云容灾架构为基础，通过容灾管理平台与其进行对接，如DNS设备，云平台应用，数据组件（Redis, KafKa, DRDS, OSS)等。在突发故障时，能够自动实现网络流量、业务应用和数据服务在AB中心的按需切换，提高切换效率和成功率。

应急人员组织

医保云系统在建设期就需要考虑灾难应急恢复组织架构的建立，前面分析到，由于众多供应商进行承建，更需要一套应急恢复处置组织架构来处理面对可能的突发灾难事件。可以与运维组织建立一起考虑，同一套人员在日常运维与应急处置时分别承担不同的角色。主要包括建立灾难恢复决策指挥领导组角色，技术恢复保障组和业务应用验证组等角色，其主要职责包括如下：

- 决策指挥领导组角色：负责日常容灾体系的建设，以及在突发事件发生时的决策指挥、内外部门沟通协同和资源保障与调度。
- 技术恢复保障组角色：包括云平台、网络、存储、安全和物理设备等恢复，在突发事件发生时，收集评估受到影响的应用、损失程度和范围，以及预计恢复时间，供决策指挥领导组决策是否启动切换。在切换时，执行指挥决策领导小组下发的具体容灾切换指令，汇报恢复进度；在事件完成后，提出和完成改进建议。
- 业务应用验证组：医保云的各应用子系统一般由多家厂商进行开发，其主要负责应用故障的排查，以及容灾切换后的业务验证，同时保持与相关经办机构、定点医院和指挥决策领导小组的沟通，反馈问题原因和恢复进展。

演练验证

确定了容灾场景，准备了演练预案，做好了事前准备工作，就要按计划进行容灾演练。通过容灾演练来检验我们容灾恢复预案的完整性、可操作性和有效性，检验应急人员之间的协作与沟通，检验我们容灾切换效率和数据一致性是否满足RTO和RPO目标。

在演练过程中，由演练总指挥进行整体指挥和调度，正常情况下通过容灾管理系统进行调度推进，以可视化的方式展现切换进程，如出现自动化切换失败时，需自动转为人工任务进行处理。在演练过程中，各参与人员各司其职，可以通过容灾演练群等方式，及时反馈重要步骤的执行结果，让所有人了解当前的状态。如在演练过程中，出现了不可预见的情况，继续演练将可能带来更大的损失，演练总指挥需根据事先准备的应急预案进行回退。

演练总结

只有通过持续的容灾演练，找出薄弱环节，加以改进，才能满足国家医保局的容灾验收条件。除前面讨论的一些实践经验外，在这里对于一些非技术方面的重要经验进行分享：

- 容灾演练事前准备很重要，可以避免很多问题，节约容灾演练时间；
- 演练过程中出现的问题，要进行总结分析，及时跟踪和处理，同样的问题不能重复出现；
- 演练的目的是发现问题，不能为了演练而演练；
- 演练沟通会要提前开，做好人员动员，沟通容灾演练大致步骤、开始时间，明确好相关人员职责，跟踪事前准备项工作完成情况；
- 演练中，配合协同很重要，出现问题，不要推诿；
- 演练报告中，要体现发现的演练问题，明确责任人及建议的改进措施和完成时间。

结束语

医保云的容灾体系建设，并非一蹴而就，也不是一成不变，是一个动态、持续改进的过程。医保云从建设期过渡到成熟期的过程中，虽然会遇到各种各样的挑战，如业务模式的变化、信息系统的动态变化、人员的变动及不同类型的突发事件导致的业务中断，但只要我们坚持驾驭好了三驾马车，人员、流程和工具，积极完善容灾体系建设，不断的更新预案、坚持持续容灾演练，让容灾意识融入到组织文化中，让应急人员都具备相关容灾技能，即使突发事件发生时，也能快速、有效的进行业务恢复和验证，逐步提高组织面对突发事件的综合处置能力。只有这样，才能让 “互联网+医保”真正发挥其更大的作用，真正成为老百姓满意的高品质医保服务。

VMware vSphere虚拟化平台规划与性能优化最佳实践

文/汪东

概述

VMware vSphere服务器虚拟化产品到现在已经发展得越来越成熟，功能也越来越完善。结合现代CPU和服务器主板提供的硬件辅助虚拟化技术，vSphere ESXi服务器所支持的物理配置不断提升，单台虚拟机的处理能力也持续增强。在搭建vSphere虚拟化平台时，事先做好充分的需求调研，制定合理的容量和性能规划，实施过程中遵循一些基本的配置原则和最佳实践，运行中一般很少会出现性能问题。缺省参数配置下，ESXi宿主机和虚拟机在性能方面可以满足大多数应用场景需求。但在某些特殊场景，例如高IO、低时延场景下可能需要进行额外规划和优化才能达到效果。本文将主要从ESXi宿主机和VM两个层面给出一些规划与部署的最佳实践，以及性能优化的方法。

vSphere ESXi宿主机相关最佳实践

与vSphere ESXi宿主机相关的最佳实践主要包含服务器、存储和网络三个方面：

ESXi 服务器

■使用支持硬件辅助虚拟化(hardware-assisted virtualization)服务器

■服务器相关硬件必须满足VMware官方兼容性要求

兼容性匹配是指服务器硬件，包括服务器型号、CPU规格、BIOS版本、网卡和HBA卡（型号、驱动、FW）等等，必须满足特定ESXi版本的兼容性要求。

■服务器BIOS设置最佳实践

●启用CPU超线程（Hyper-threading）。

●禁用node interleaving/启用NUMA node。

●启用hardware-assisted virtualization设置，包括CPU(Intel VT-x/AMD-V)、内存(Intel EPT/AMD RVI)和I/O(Intel VT-d/AMD-Vi)。

●电源管理：禁用电源管理，或者设置为“OS Controlled Mode”。

●禁用不必要的硬件设备，如串口、USB等。

Datastore存储

虚拟机和数据存储在Datastore上，存储空间由后端存储阵列或者vSAN提供。因此，后端存储阵列的选型、连接方式等都会影响虚拟机性能。同样，后端存储系统也需满足VMware官方兼容性要求，包括存储型号、FW版本、连接方式等。

■选择合适的后端存储系统

根据业务需求：性能、容量、可靠性和可扩展性要求等指标来选择合适的存储产品和型号。

■选用支持VMware vStorage APIs for Array Integration (VAAI)功能的存储系统

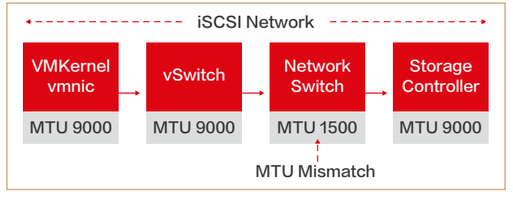
■iSCSI和NFS后端存储优化建议

使用专用的物理网卡访问存储，并使存储访问网络与业务网络隔离（物理或VLAN隔离）。

●使用独立硬件iscsi适配器，且支持TOE功能。

●至少使用万兆速率网卡，并配置多网卡绑定，以提高带宽和可用性。

●使用巨型帧(Jumbo frames)，例如设置MTU为9000。启用巨型帧，要求在整个数据访问链路的各个环节，包括iSCSI网卡、物理交换机、vmkernel端口、后端存储端口等等，都要启用巨型帧，并配置合适的MTU值。通常，物理交换机端口的MTU设置要大于9000，例如设置为至少9198或者9216，具体设置需咨询交换机厂商。如果链路上MTU设置不匹配，常见的问题就是，虽然存储挂载成功，但是读写IO会失败。



●配置多路径，启用Round Robin Path Policy。

■FC SAN后端存储优化建议

●保持SAN网络端到端速率一致，包括HBA速率、SAN Switch端口速率、存储端口速率等。如果不一致，建议使用强制固定速率进行匹配。

●根据HBA卡速率，选择合适的服务器PCIe插槽。例如单端口的32Gb/s光纤卡，如果要充分使用其带宽，则至少需要PCIe 2.0 X8（8通道）槽位来适配，或者PCIe 3.0 X4（4通道）槽位来适配。PCIe 2.0单通道速率为4Gb/s，PCIe 3.0单通道速率为8Gb/s。

●配置多路径，并根据SATP(Storage Array Types)设置合适的PSP(Path Selection Policy)。

■本地存储优化建议

●使用硬件RAID卡保护。

●HDD磁盘建议启用RAID卡write-back模式，SSD磁盘可使用write-through或者write-back模式。

宿主机网络建议

■选择企业级网卡。建议网卡本身支持一些高级功能/特性，例如：Checksum offload、TCP segmentation offload (TSO)、Jumbo frames (JF)、Large receive offload (LRO)、Receive Side Scaling (RSS)、NetQueue、Support 64-bit DMA addresses等。

■确保网络架构无瓶颈。从网络源端到目的端无网络瓶颈，包括网卡速率、交换机端口速率、网线等。

■对不同功能的网络创建独立的vSwitch，例如业务网络、vmkernel、vMotion等，并为vSwitch配置多个物理网卡。

■vSwitch上联端口配置多网卡teaming或者EtherChannel /LACP（需要上联交换机支持）。

虚拟机相关最佳实践

一般场景

■选择较新版本的VM操作系统。RHEL 6/Windows 2008 R2及以后的操作系统针对虚拟化环境运行进行了大量的优化，大大降低了guest OS本身对虚拟化平台资源的消耗。

■安装并运行VMware tools。VMware Tools 中包含一系列驱动和服务，能够优化虚拟机性能和提升可管理性。

■合理配置虚拟机vCPU和内存。实际上，并不总是虚拟机vCPU和内存配置越多越好。大体上需要综合以下几方面情况来综合考量：

●虚拟机应用和guest OS的实际情况，例如应用本身是否支持多线程，guest OS是否存在CPU/MEM数量限制，或者应用程序运行和数据量是否需要大量内存等。

●虚拟平台宿主机的配置情况，物理CPU槽位数和核数，NUMA节点的内存配置等。

●虚拟资源池的资源利用率情况等。

总的原则就是：保持一定的guest OS资源利用率下满足业务需求。过多的虚拟机资源分配，尤其是vCPU配置，某些情况下反而会影响虚拟机性能，例如增加虚拟机vCPU调度的%RDY和%CSTP时间。

■合理配置虚拟机资源预留、限制和份额。份额表示虚拟机相对于同级其他虚拟机可占用资源的优先级。虚拟机具有的份额越多，当存在资源竞争时所获得资源分配的机会就越多。

■关于虚拟机硬件的建议

●使用与宿主机兼容的最新虚拟机硬件版本。

●推荐使用VMXNET 3虚拟网卡。VMXNET 3 vNIC在Guest OS中支持offload、RSS等高级特性且占用较少vCPU资源，以及其他功能。

●推荐使用PVSCSI(VMware Paravirtual SCSI)或者Virtual NVMe虚拟磁盘控制器，vNVMe控制器要求虚拟机硬件版本13及以上。每PVSCSI控制器仅支持一个queue，最大queue depth为1024。对于IO密集型VM，一方面可增加多个PVSCSI控制器（最多4个），使VMDKs尽可能使用单独的控制器以避免共享控制器queue；另一方面可适当增加queue depth(缺省为254，需与宿主机HBA卡和后端存储端口所支持的queue depth范围适配)。而每vNVMe控制器支持多达64 queues，每个队列的queue depth为最大64K。

低时延 (Latency Sensitivity) 场景

■配置虚拟机NUMA节点affinity。为了获得最佳的虚拟机性能，虚拟机vCPU和内存最好每次都被调度在同一NUMA节点上，因为NUMA节点上的所有Core会共享LLC(Last Level Cache)。为了实现这一点，可以将虚拟机固定调度到特定的NUMA节点。在虚拟机配置->高级选项中增加numa.nodeAffinity参数，值为0或1…（NUMA节点编号）。需要注意的是，该设置并不意味着虚拟机会独享NUMA节点，因为其他未设置该参数的VM依然会被调度到该节点，且虚拟机vCPU共享LLC的效果并不能保证。另外，启用node affinity可能会导致宿主机物理CPU负载不均衡。

■优化UNMA scheduler

●设置numa.vcpu.min = N。vNUMA功能使虚拟机能够感知宿主机的NUMA节点，并自动将虚拟机vCPU和内存调度到同一NUMA节点。但vNUMA设置缺省配置下只在vCPU数量大于8，或者大于node节点的物理CPU core数时启用。当vCPU数量少于等于8时，如果也要启用vNUMA特性，需设置numa.vcpu.min参数，其中N为vCPU数量，例如4颗。

●设置numa.vcpu.preferHT = TRUE。启用Hyper-threading后单个物理CPU Core上的两颗Logical processors会共享该Core的L1和L2 cache，这种共享cache和内存的机制会提升某些虚拟机应用的性能，例如应用本身使用大量进程间交互。但缺省配置下，NUMA scheduler仅根据NUMA节点上的物理CPU Core数量来判断和调度VM，而忽略Logical processors。此时，可以设置numa.vcpu.preferHT参数为TRUE，使NUMA scheduler根据Logical processors数量来判断和调度VM。注意，该设置如果经测试未提高性能，建议使用缺省配置。

●设置numa.consolidate = FALSE。当单个NUMA node不能满足VM的内存需求但能够满足该VM的vCPU需求时，缺省配置下，NUMA scheduler会将VM的vCPU调度到一个NUMA node，而从其他Remote NUMA node分配剩余的内存。在某些Guest OS和应用场景下这种状态会影响性能，可以设置虚拟机参数numa.consolidate = FALSE使vCPU和Memory尽可能平均地调到所有NUMA node。注意，该参数的优化效果取决于Guest OS和应用本身对于NUMA架构的优化，应进行充分的评估与测试。

■设置虚拟机Rx/Tx 使用多进程。缺省配置下，即使VM配置有多个vNICs，每台虚拟机仅各使用一个world来处理VM network IO的接收(Rx)和发送(Tx)，每个world占用一个vCPU资源。针对Rx流量，可以启用宿主机pNIC NetQueue功能（需物理网卡和驱动支持）。结合CPU的VMDq(VM Device Queues)功能和pNIC NetQueue多队列，虚拟机会根据需要分配额外的world来处理Rx流量；针对Tx流量，可以增加虚拟机高级参数ethernetX.ctxPerDev = 1，为虚拟机分配额外的world

来处理Tx流量。该参数可针对每个vNIC单独配置，其中X为vNIC号。

■禁用Interrupt Throttling和Interrupt Coalescing。Interrupt Throttling和Interrupt Coalescing功能都是通过限制或者减少发送到ESXi和Guest OS的Interrupt数量来降低网络IO对CPU的消耗，但可能会增加latency sensitive应用的时延。

■设置虚拟机Latency-Sensitivity为High。从ESXi5.5开始，虚拟机支持Latency-Sensitivity设置，有“低、正常、高”3个选项。缺省为正常，将Latency-Sensitivity设置为高，则意味着要求100%的vCPU和内存预留。

■宿主机禁用电源管理。在BIOS中将电源模式设置为：static high或者Maximum Performance，禁用处理器P-States和C-States/C1E，并在VMware Host Client中将宿主机vSphere Power Management Policy设置为High Performance。

■启用Turbo Boost（睿频加速）。当开启睿频加速之后，CPU会根据当前的任务量自动调整主频，从而提高业务高峰时的处理能力，通常在低时延场景下建议开启。但睿频加速技术也带来了性能和时延上的抖动，如果业务系统要求有稳定的性能与时延，则建议在BIOS中关闭该功能。

■使用Pass-through（直通）模式网卡和HBA卡。ESXi支持两种类型的直通模式，分别是：DirectPath I/O和SR-IOV。区别在于DirectPath I/O模式下一块物理网卡只能被一台虚拟机使用，而SR-IOV模式允许多台虚拟机共享一个物理设备。虽然直通模式下虚拟机能够直接访问物理IO设备，使得虚拟机的网络性能达到最优，但也存在与vSphere虚拟化核心功能不兼容的问题，例如使用DirectPath IO和SR-IOV网卡的虚拟机不支持vMotion、HA、FT等等，也不支持虚拟机快照、挂起和恢复等操作。因此，需要结合实际情况评估是否采用直通技术。

■使用NetIOC(network I/O control)为虚拟机预留带宽。当业务场景既要保留虚拟机vMotion和高可用等功能而不能使用直通技术，又需要保证低时延性能时，可以采用Network I/O Control来实现。NetIOC v3支持系统流量和虚拟机业务流量分别采用不同的模式进行控制。NetIOC v3将网络带宽也视为资源，与vCPU和内存一样使用预留、限制和份额这三个参数为系统和虚拟机分配带宽资源。

结束语

VMware vSphere虚拟化平台的规划与优化不仅仅局限于文中提到的内容，针对不同的应用类型、业务场景可能还有其他需要特别注意和优化的地方。另外，文中的建议并不一定适用于所有场景和应用，尤其是一些高级参数设置，在生产环境中实施前应进行充分的测试与验证。

在虚拟化平台运行过程中，如果由于业务量的增加、特殊业务场景的应用上线等等原因导致性能问题时，需通过合适的工具获取虚拟机、宿主机、资源池、物理网络、后端存储系统等各个层面的相关性能指标，结合性能基线，综合判断性能瓶颈所在。

IT管理外包项目交接维管理实践

文/郑圆圆

基于新华三在IT服务管理外包项目中积累多年的交付实践经验，下面，我们以真实案例为素材，分享一个典型的IT服务管理外包项目交接维交付过程的实践案例。通过该实践了解交接维管理是如何保障运维工作安全、稳定的从客户方或其他服务商转移到新华三运维团队，并进行相应运维服务能力的提升，以最终满足并达成合同中约定的服务条款内容，确保新华三接维团队所提供的运维服务标准化、规范化，为后续提供持续性日常运维服务交付打下坚实基础。

项目背景

客户方用于信息化的设备总数约3000台，业务系统总数约113套（200多个子应用系统），这些系统存储大量敏感信息，保障数据安全，确保系统安全、稳定、可靠运行至关重要，这就要求该单位需采购专业的运维服务来保障各类信息化系统的平稳运行和数据的安全可靠。

项目目标

本IT服务管理外包项目的核心内容是基于ISO20000和GB/T28827标准规范建立科学的运维服务体系，为本项目组建专职的运维服务团队，对单位的基础设施、基础软硬件平台、网络、安全系统、各类应用系统提供统一的运行维护服务，保证数据的完整性，保证系统的高可用性，并根据运行维护服务对象实际运行状态，提供优化改进方案及其他相关咨询服务，确保实现“网络不断，系统不瘫，数据不丢”的整体目标。

而运维服务交接工作则要确保交接期间的运行维护质量不下降、不发生安全事故或群体事件，实现“平稳过渡”的主要目标；通过交接维管理工作，使IT服务管理外包项目顺利接维，高效达到稳定运行状态。

什么是IT服务管理外包？此类项目交付过程中的交接维管理如何定义？

关键词定义

■IT服务管理外包：是指用户在规定的服务水平基础上，将信息系统业务通过合同委托给第三方组织，通过支付费用，在一段时间内，由第三方组织管理并提供用户所需的信息技术服务。这些服务包括：软硬件维修和维护、技术培训、数据中心托管、服务器、网络、桌面系统运营和管理、应用开发等。

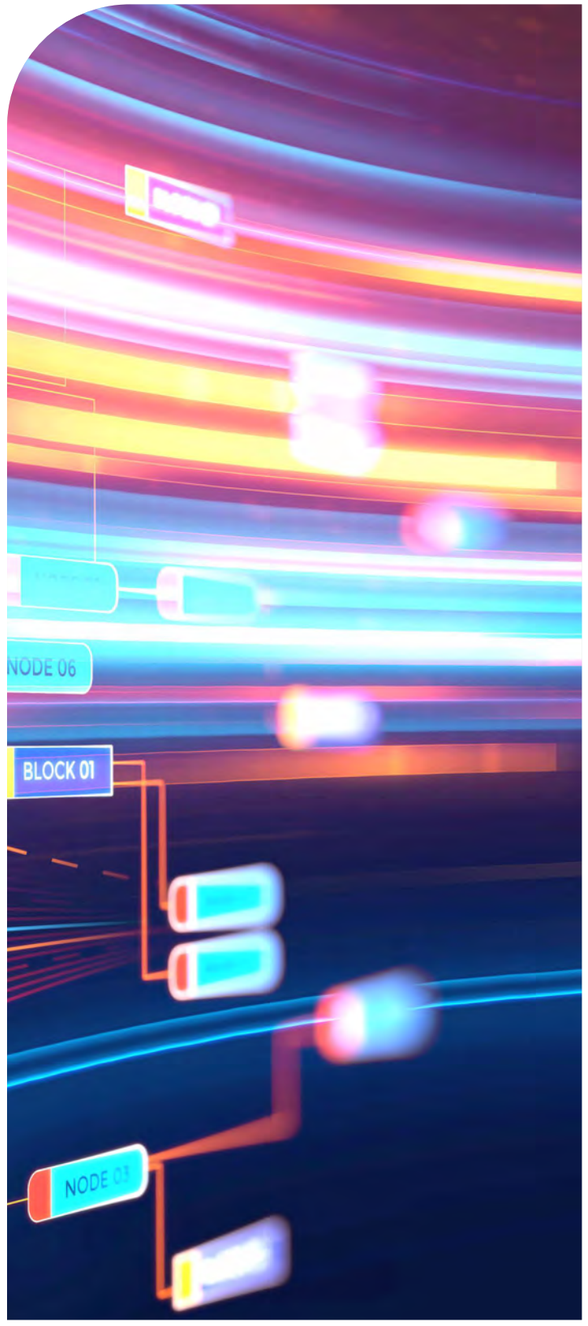
■交接维管理：为运维服务团队顺利从前一个运维服务商转换到现有服务商，所经历的服务迁移和转型的管理活动，确保提供的服务安全与稳定，并在此基础上，针对服务支持与交付过程进行优化，从而保证服务SLA目标达成。

为什么要做交接维？

总结起来有以下几点：

■为了有效开展项目的管理交付工作，保障IT服务管理外包业务在客户的运维服务商之间平稳、高效过渡，接维服务商可以快速提供高质量的服务；

■帮助接维团队快速熟悉客户现场运行维护情况，发掘客户的业务需求及痛点，寻找可能的改进提升机会；



■让接维驻场工程师快速明确工作职责、工作对象和内容，甲乙双方对运维边界达成一致，圈定运维边界；

■保证原有知识体系不缺漏，原知识体系是接维工作的重要输入，通过技术管理助力客户运维服务的转型升级；

■在交接维过程中，体现接维服务商的专业性，取得客户信任，增强客户粘性，提升与客户方的业务及合作紧密度，为后续客户所有信息化项目的开展提供帮助与支持。

交接维管理工作中有哪些是重点关注、必须要做的关键活动？具体如何开展？

交接维管理工作中的关键活动

下图为交接维管理工作整体框架，其中标红色内容则为交接维管理过程中的关键活动，即为在交接维期间应重点开展的管理活动。

输入 · 调研记录 · 与客户初步沟通纪要 · 项目招投标材料 · 合同文档 · 客户运维现状情况：客户组织架构和运维流程、工具等现状情况 · 客户运维需求	**输入** · 项目招投标材料及合同文档 · 一、二线等人员/岗位职责要求 · 客户运维目标和需求 · 客户现场的规范要求	**输入** · 日常运维数据：监控数据、服务工单数据 · 交接维管理计划 · 客户服务转型和提升需求 · 风险清单
具体活动 · 调研及与客户初步沟通 · 识别关键干系人 · 制定IT服务管理外包项目交接维计划 · 制定IT服务管理外包项目交接维详细进度计划 · Kick-Off启动会议 · IT服务管理外包项目运维组织架构制定	**具体活动** · 确认项目交付范围和目标 · 人员招聘管理 · 团队建设及管理 · 现状调研和尽职调查 · 知识转移 · 技术管理和风险管理 · 技术规范梳理、SOP等作业指导制定 · 制定人员考核要求和绩效管理制度 · 值班管理和重大活动保障管理 · ITIL导入培训 · 监控管理规范、操作指南、手册收集梳理 · 建立标准规范的运维管理体系 · 维保服务管理 · 项目预算及成本核算管理	**具体活动** · 运维服务报告(月报、季报、周报、年报) · 性能分析和优化 · 高阶服务流程管理 · 完善各领域的技术类规范文档 · 相关运维管理文档、SOP完善及标准化或自动化 · 团队建设及培养计划 · 定期进行IT运维能力成熟度评估/AHC评估 · 统一标准的质量管控机制
输出 ·《IT服务管理外包项目交接维管理计划》 ·《IT服务管理外包项目交接维详细进度计划》 ·《项目kick-off启动会议PPT》 ·《IT服务管理外包项目运维组织架构》	**输出** ·《SLA服务级别协议》和《项目验收和付款方案》 ·《项目组员工管理规范》 ·《尽职调查收集表》和《系统维护手册》 ·《人员考核要求和绩效管理制度》 ·《风险清单表》和《问题跟踪表》等	**输出** ·《运维服务报告》 ·《性能分析和优化报告》 ·《高阶服务流程管理二、三、四级文档》 ·《IT运维能力成熟度评估/AHC评估报告》 ·《改进计划》

■确认项目交付范围和目标

在IT服务管理外包项目运作前期，就需要明确项目目标范围、分解项目工作说明书（SOW）、根据项目目标及工作内容细化服务项及明确验收标准及付款条件。

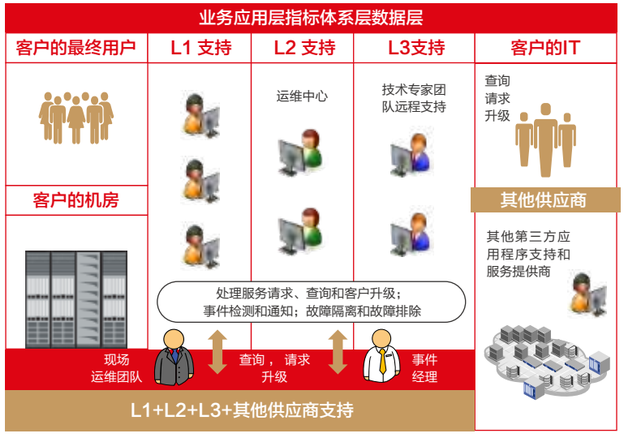
●明确工作说明书：准确描述项目的交付范围、交付工作内容，减少招标文件与投标文件间差距，作为合同的附件约束项目交付，在IT服务管理外包项目投标前期需要制定该文档；关键内容包含：项目目标、交付范围、工作内容、人员数量及资质要求、甲乙双方职责、验收标准等。

●服务级别管理细化：根据客户的招标文件、合同及考核要求，明确各运维对象服务级别及运维服务水平；细化服务级别——明确服务对象（梳理相关应用系统）、定义应用系统重要程度、根据重要程度制定支持方式及业务恢复时长等，量化服务质量——定义故障级别、明确扣分项、定义考核规则等。

●明确验收标准及付款条件：梳理验收交付清单——根据合同工作项及工作内容梳理8类服务，共计123类交付文档；验收标准及付款计划——验收标准会根据驻场团队的实际服务质量进行定期考核。

■团队建设及管理

需要考虑合理设计驻场团队组织架构、明确职责分工、结合客户要求招聘组建团队，在合同签署前完成团队建设。



●设计组织架构：设立适应运维服务管理要求的组织机构，是确保运维管理体系正常运行的基础条件和组织保障，根据运维服务管理体系建设要求，结合实际情况和需要进行设置。

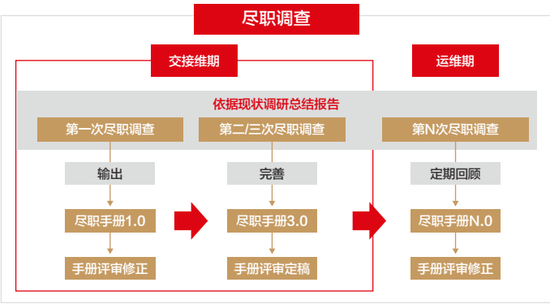
●明确职责分工：为了提供良好的运维服务、及时的响应，在运维服务管理人员配置上应尽可能做到分工明确，职责分明，实现客户运维服务要求时限的规定，提高运维服务质量和客户满意度。

●人员招聘管理：根据招标文件中对于岗位工程师的岗位职责和技能要求，梳理招聘岗位JD，快速有效组建团队，结合组织架构设计合理安排一线、二线人员分配，整体把控人员成本。

●量化绩效考核：结合驻场工程师的岗位职责和能力要求对日常运维工作进行量化考核，确保和促进运维服务质量的提升。

■现状调研和尽职调查

在项目交接维过程中，需要提前明确现场环境与合同要求差异点，从而识别风险及时制定风险规避措施并同客户达成一致。



●对内尽职调查：让运维工程师快速明确自己的工作职责、工作对象和内容，将工作目标准确传递给运维工程师；尽职手册的不断更新和完善，形成知识积累，为后续人员更换交接提供支持；通过对自身能力与服务内容的对比，识别当前运维风险点。

●客户现状调研：识别客户运维现状与标准规范的差距，作为后续体系建设与工具引入的参考；发现客户的业务需求及痛点，寻找可能的改进机会；结合合同正确引导客户期望。

●获得客户确认：通过客户现状调研及对内尽职调查结果，结合SLA、SOW、验收条款等内容，识别现场运维环境与合同目标差异点及风险点，形成并输出应对方案和交接维确认单，最终促使甲乙双方对运维边界达成一致，圈定运维边界。

■知识转移

在项目交接维培训及过渡过程中，需要对交维团队知识框架及内容进行分析鉴别，对于不准确或缺失的部分需要求交维方整改并补充。

●知识框架梳理：现场各岗位的专业技术经理针对运维工作，根据自身经验能力借助公司总部IT服务管理外包的知识体系，快速梳理运维工作所需知识框架，最终通过公司总部专家团队对梳理出的知识框架做最终

评审；各岗位的专业技术经理依据SOW、SLA、验收条款等结合接收到的交接文档清单，梳理得出后续日常运维所需与目前所接收的文档资料存在的差异点。

●知识转移与培训：根据知识框架对交维团队提出对应的资料清单申请，组织现场接维团队参加知识转移培训，认真阅读学习知识转移文档，结合现场情况进行实践对照；在资料移交、培训及交接维整个过程中，需要各运维工程师认真对比所接收的文档内容，识别错误、缺失部分的信息，向交维团队提出整改要求，最终形成知识库。

运维服务转移 交接维计划 知识转移计划 交接维清单 交接维日志 资产清单 运维服务SOW	**运维服务支持** 三线专家支撑管理 内部升级管理 客户满意度调研 沟通与汇报机制	**人员与团队管理** 工程师岗位职责 人员技能矩阵 员工管理手册 人员考勤管理 值班管理与排班表 人员绩效考核管理 培训与职业规划 团队建设 人员交接管理	**运维管理流程与规范** 监控事件管理规范 故障处理规范 问题管理规范 变更管理规范 资产管理规范 配置管理规范 服务台管理规范 服务请求管理规范 巡检管理规范 作业计划管理规范 知识管理规范 应急管理规范 质量管理规范 重大活动服务保障规范 升级与沟通管理规范 安全管理规范 维保管理规范
运维服务报告 运维日报、周报、月报 年度服务计划 服务总结报告 服务验收报告	**运维技能与文档** 操作手册 维护手册 应急预案 运维对象清单 配置信息 运维脚本 运维记录模板 运维方案模板		
运维服务管理体系			

专业技术经理需要系统的梳理技术规范文档、技术维护手册、SOP文档等，并建立匹配的一、二线技术人员支撑体系。

●制定统一技术管理规范：各领域专业技术经理根据现场运维情况梳理出接维团队在未来日常运维工作中所需的技术规范、技术维护手册、SOP作业指导书等技术文档清单。

●技术风险识别及制定应对策略：在尽职调查过程中，交接维经理与各领域专业技术经理共同识别出现存的技术风险，梳理技术风险清单，根据风险偏好、风险管理策略及更新的风险登记册对所识别出的风险项进行风险因素和影响分析，并根据相关技术经验及风险管理预算输出风险应对控制及对应策略，从而达到将风险降至最低或转移风险的目的。

●构建总部专家技术支持体系：为驻场的一、二线团队搭建总部专家技术支持体系，规范总部专家团队技术资源申请流程，提供12大类、27个技术领域、近50名专家资源池，为项目建立一、二、三线提供整体技术支撑。

■建立标准规范的运维管理体系

在交接维管理过程中，交接维经理需要根据客户运维实际情况及管理需求建立标准规范的运维管理体系，并依靠管理工具有效落地执行，来保障驻场运维团队的服务质量。

●流程体系建立：交接维经理结合现场运维实际情况及在现状调研过程中收集到客户提出的运维需求，输出12大类74份IT服务管理外包项目交接维标准化文档，规范驻场工程师的日常工作和行为，提升运维服务水平，提高客户满意度。

●运维工具支撑：根据客户实际情况设计的各管理流程，与运维管理工具进行适配；工具辅助管理体系落地执行，过程闭环管理，降低操作风险；工具可定期采取各种展示形式统计、分析运维数据及趋势；帮助项目服务交付经理快速掌握各项管理流程指标（SLA）的达成情况。

■统一标准的质量管控机制

在项目交接维过程中，就需重视运维质量管理，对日常运维工作质量进行监控，明确日常运维服务管理报告的要求及模板；否则，只在付款时关注SLA，运维质量无法保障，将存在扣款风险。

●交接维期的质控管理：根据现状调研结果结合SLA、SOW要求，识别出项目运维服务质量考核的内容，并与客户制定相互认可的标准，定期输出相关的服务报告模板（周度、月度、季度及年度）。

●正式运维期的质控管理：运维团队管理组对服务报告内容持续改进，并要按时、准确记录服务结果，严格对结果进行审核，第一时间发现问题，立刻整改，确保SLA及服务质量可控，通过完善的定期质量检查，建立起有效的运维服务管理体系的检查、控制及改进质量管控过程，有效保障运维服务管理体系的运行，并推动现场运维服务质量持续不断的提升和完善。

结束语

通过对本IT服务管理外包项目交接维管理活动的执行，帮助新华三接维团队顺利平稳的进入运维交付阶段，确保提供的服务质量满足合同所约定的服务要求；成功帮助客户建立起统一运维管理流程体系和统一运维管理平台，使得运维保障能力得以提升，辅助客户打造核心业务能力并达成提升运维总体效能的目标。

但交接维只是开始，进入运维交付阶段，新华三运维服务团队将与客户长期并肩作战，将日常维护优化、关键时刻保障、工具高效辅助等工作内容常规化、标准化，为客户提供智简、至暖、致远的IT运维服务，新华三努力创新从而实现运维服务的最大价值，取得信赖从而为客户数字化发展保驾护航。

北京大兴国际机场网络运维优化与创新

文/胡在亮

项目背景

北京大兴国际机场定位为大型国际枢纽机场，是国家发展一个新的动力源，支撑雄安新区建设的京津冀区域综合交通枢纽；按2025年旅客吞吐量7200万人次、货邮吞吐量200万吨、飞机起降量62万架次的目标设计。大兴国际机场网络包括内部网络系统、旅客无线接入网络系统以及配套的安全管理系统。其中，内部网络系统承载着所有大兴国际机场的关键业务，一旦出现严重的网络问题，将可能是全局性的影响，导致大兴国际机场业务运行降效或停滞。为保证网络平台运行稳定、提供可靠连续的业务支撑，大兴国际机场网络运维团队由网络一线和网络二线两个团队协同工作，网络一线运维团队负责日常运维工单和简单故障处理，网络二线为网络一线运维提供技术支持并负责复杂故障、运维规范、网络优化、承接运维需求以及运维创新等方面的工作。新华三运维团队作为网络二线团队的重要组成部分，人员比例达到70%，在大兴国际机场网络二线技术支持工作中也发挥出至关重要的作用。

新华三运维团队按照AIO（All In One）“智简、至暖、致远”的运维管理外包服务模式，满足客户高效统一运维需求，帮助客户以更低的运营成本与更快的业务变革速度顺利推进数字化转型。

需求挑战

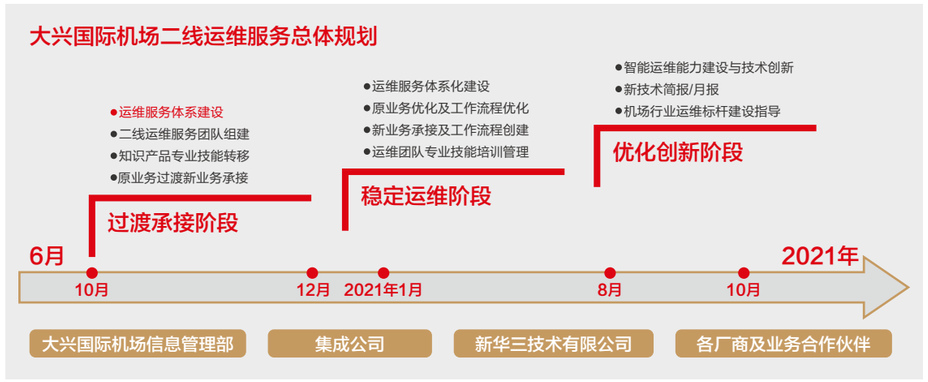
大兴国际机场是一座超大型国际枢纽机场，在投入运行初期网络运维存在如下挑战：

- 需对网络资源、运维文档等台账进行完善和补充；
- 需对多驻场团队和设备厂商进行统一管理；
- 需建立完善有效的网络运维体系，提高运维管理质量；
- 需对网络运行中存在未知隐患进行优化；
- 需对全网制定切换演练方案，验证网络运行的可靠性。

大兴国际机场运维方案

大兴国际机场二线运维服务针对当前存在的挑战，将网络运维按照不同阶段进行分解，遵守每个阶段工作有重点、有目标、有计划的原则，对大兴国际机场网络运维进行优化，从而提升网络运维服务的整体质量。

- 过渡承接期：整合各运维团队和设备厂商资源进行统一管理，并建立完善的网络台账、运维知识库、运维管理制度，降低运维管理复杂度提高运维工作效率。
- 稳定运维期：以平台体系建设为重点，同时稳定开展业务流程、现场工程师管理规范、考勤管理、培训计划等其他运维服务工作。
- 运维优化期：使用自动化脚本、运维自动化工具对网络进行深度巡检，发现网络运行隐患并优化，同时逐步实现运维自动化，再向AIOps运维智能化过渡。



运维服务优化

大兴国际机场运维团队通过网络巡检和切换演练解决网络运行中的隐患的同时，也不断从日常运维中吸取总结运维经验和管理流程，形成管理规范文档，以方便后期的运维工作参考。

设备信息台账优化

工欲善其事必先利其器，对于网络运维工作而言，拥有一本完整台账和一个有效的网管监控平台是一切运维工作的良好开端。在日常的运维工作中设备信息和资产信息也是动态变化的，如何能够同步保持台账和网管监控平台的实时更新显得尤为重要。我们通过对全网设备进行全面摸排和梳理完善了网络台账和网管监控信息，达到全网设备资产均在册，在册资产均受监管的目标，为日常运维提供极大的便利性。

AIO运维服务管理

大兴国际机场网络二线运维团队以新华三AIO运维服务的核心理念进行运维团队管理，以提高大兴国际机场网络运维服务整体质量为目标，对不同远程运维团队、不同厂商设备资源进行整合，统一规范和集中管理，建立有效的沟通矩阵，协助大兴国际机场解决网络运维中多服务商、多厂商管理难度高的问题，提升网络运维的整体管理水平。

运维体系建设

在运维工作中，运维团队通过处理故障、网络隐患优化、网络切换演练和需求处理等工作积累了大量的规范要求和经验知识，如何将这些规范要求和经验知识整理成册变成有形资产以提高网络整体的运维规范性和技术水平显得尤为重要。通过对日常故障处理、实施方案等知识进行总结归档完成知识库SOP、MOP、EOP共计70篇、编写运维流程规范共计20篇，并通过在网络二线团队和网络一线团队之间组织37次培训考试、46次每周团队内部专题讨论，并设置专职审核岗位进行日常工作审核，在向每一位工程贯彻管理规范的同时提高每位工程师技术能力。

网络深度巡检

网络故障发生了能够快速解决固然重要，但是如果能通过网络巡检和梳理发现网络中运行的隐患并防患于未然更加重要。我们在梳理分析历史巡检内容和管理流程后，通过优化网络日常巡检模板和巡检制度使网络一线的日常巡检工作更加完善和有效。同时借助新华三以及其他自动化巡检工具，网络二线运维团队针对核心、汇聚和骨干设备的运行配置、协议状态和版本补丁等方面进行深度巡检，共输出66篇巡检报告，并针对巡检报告问题进行分析并编写方案进行优化解决。

切换演练

网络建设按照设备冗余和链路冗余的原则进行设计，但是通过梳理和分析发现部分设备的配置缺失导致设备或者链路冗余并不能达到预期的效果，我们通过梳理全网的配置进行分析，针对不满足冗余条件的场景提出优化方案，在进行大量的配置优化操作后按计划进行了关键设备切换演练且均到达理想效果，在很大程度上减少了单机设备故障引起业务中断的风险。

主动式服务

为保障节假日和重大时刻机场网络能够稳定运行和快速响应故障，除了日常运维工作的开展，新华三运维团队从全局出发在新华三集团资源的支持下提供主动运维服务，如备件先行、版本评估、版本升级等。

主动运维防患于未然-“扫雷”服务

新华三主动规划的特色“扫雷行动”，针对重要客户、重要局点、关键产品和解决方案的高危版本进行全面梳理和排查，提升客户对我司产品和解决方案的体验感、客户满意度，避免客户在网设备因已知问题引起重大事故，提前进行风险排查和防范。针对“扫雷”中发现的问题进行风险评估后制定设备版本升级计划和后期设备入网的版本统一原则。

无线春风护航”服务

新华三2021年无线产品春风护航行动，针对大兴国际机场无线网络进行梳理，从软件版本、设备配置和信号测试等方面入手重点排查在网设备的潜在风险及隐患，向客户提出预警和修改方案，并对隐患进行整改，提升服务质量，提高客户满意度和旅客无线网络体验。

重大时刻保障

过去的一年里，新华三在每一个重大节日和关键时刻都不遗余力，由新华三行业/产品技术专家、一线人员、总部市场/服务领导等组成大兴国际机场服务保障小组，通过现场备件及时到位、后端技术专家随时待命、现场技术工程师轮班值守三管齐下，保障了元旦、春运、国庆等节假日和两会、建党百年等关键时刻网络系统稳定运行，让每名旅客“乘兴而来，尽兴而归”。

方案亮点

近年来在各种运维大会上AIOps成了高频词汇，不同行业、不同企业的运维现状也不尽相同，对AIOps和未来的建设计划也不尽相同。AIOps与其说是产品，不如说是一种理念和策略，通过以数据为基础、算法为支撑、场景为导向的AIOps平台，为企业现有运维管理工具和管理体系赋予统一数据管控能力和智能化数据分析能力，全面提升运维管理效率。如何优化现有的运维模式，提高网络运维效率是大兴国际机场甲方团队和新华三网络运维团队一直探索的方向。

新技术简报

大兴国际机场甲方团队和新华三网络运维团队成立技术创新小组制定运维创新计划，研究行业前沿智慧机场解决方案、物联网技术、网络安全、软件定义网络、Wi-Fi 6、5G、云计算和大数据等专业技术，共输出13篇《新技术简报》。

网络自动化运维

日常网络运维中不乏一些需要经常性重复、难度较低的工作，但是开展这些工作所花费的时间较多且会因人员变化导致效果差别较大；如每日对汇聚及以上两百台左右设备的数十项巡检指标进行巡检，定期梳理两千台左右的网络设备信息，定期统计两千台左右设备的端口表使用信息，分析关键链路带宽使用情况等。我们通过提炼工作内容和工作要求，制定标准化的方法和输出方式，使用python编程语言开发对应自动化运维系统，在提高运维工作效率的同时加强标准化的管理。

自动化巡检子系统

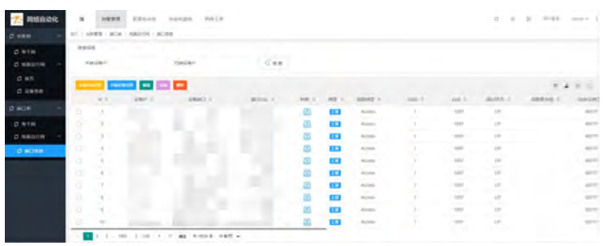
针对日常巡检工作量大、频率高、人工巡检比较费时费力的问题，运维团队开发了自动化巡检脚本。按照大兴国际机场巡检管理规范输出巡检文件，效率从原来每次4-5小时的巡检工作提升至每次1小时左右。

设备信息台账子系统

将设备上线后需要手动收集设备的软件版本、补丁版、设备系统名称等信息的工作，通过编写自动采集脚本来完成，提高了信息收集的效率和有效性。

设备端口表子系统

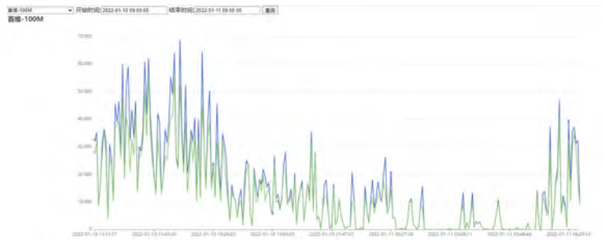
定期收集网络设备的端口使用情况，自动生成设备端口表，效率提升至1小时/张网。



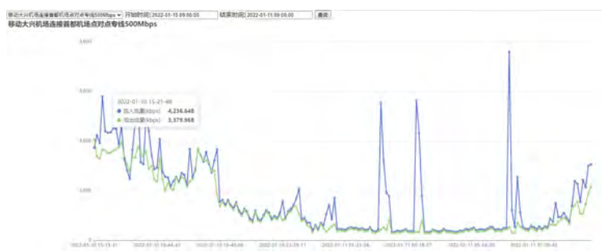
网络带宽监控子系统

针对当前网管无法针对防火墙的每一条带宽策略进行监控，使用网管平台分析专线带宽利用率峰值时步骤繁琐、耗时较长，且需要定期对网络带宽进行统计分析的场景，我们开发了网络带宽监控子系统，按照指定时间范围自动生成防火墙带宽策略流量分析图、大兴国际机场自用专线带宽流量分析图，使运维工程师分析工作效率大幅提升。

防火墙策略带宽监控



大兴机场自用专线带宽监控



网络运维工作台账管理系统

开发工作台账管理系统，进行二线团队工作的录入、更新和导出，提高二线工作的跟踪和分析的效率。

客户受益

大兴国际机场网络二线运维团队在一年多的运维服务中，陪伴客户左右共同进步、共同成长，取得了不错的成绩。

- 保质保量完成日常故障处理，日常运维需求对接等日常基础网络运维工作；
- 通过梳理日常运维工作流程优化了网络运维管理规范、补充完善了网络运维体系；
- 通过网络深度巡检发现并优化网络运行隐患，制定切换演练方案保证了网络的可靠性；
- 参考AIOps的运维理念，开发自动化运维工具提高运维的工作效率，为未来网络运维自动化、智能化打下了一定的基础。

江苏移动运维在云上！

文/转载

自中国移动宣布启动“云改”战略已有三年。当前，中国移动核心系统全部云化、容器化，并按照云原生的开发和运维模式，实现敏捷开发和智能运维。

云网融合的理想，正逐步照耀进现实。尤其是随着移动云苏锡中心四千台节点投入与运营，中国移动集团网络事业部、中国移动云能力中心、江苏移动三方通力合作，为实现云、边、端算力协同做出的诸多努力已初见成效。作为备受江苏移动信赖的运维合作伙伴，新华三集团助其在规模化运维、标准化运维、协同化运维、智慧化运维四方面焕新升级，营造云上运维新体验。

规模：基于“资源整合”下的庞大投入

作为IT技术的集大成者，云计算是诸如虚拟化、分布式存储、分布式计算、多租户等技术自然发展、精心优化与组合的结果。

相对于传统电信运维，原本单一、物理的设备变为了动态、虚拟的资源，海量的告警、日志、性能参数扑面而来，从指数级增长的网元设备管理和租户管理要求到多数据中心管理带来的风险管控和应急开销，云运维“规模巨大”，需要以更加灵活、自如的方式去管理虚拟的计算节点、存储和网络等资源。

仅以加固动作为例，江苏云资源池上当前已经有3000+设备，每次集成都会新增几十台设备，新集成设备上线前必须完成20+项安全加固动作，维护人员需要逐台设备SSH登录并上传脚本，并要针对不同的集成应用需要多次修改脚本，一旦设备加固出错，需要先人工删除错误配置，时间成本成倍增加，整体流程繁琐复杂，且多个维护团队之间操作规范不统一，带来潜在的安全隐患。江苏移动开展大规模运维应用实践刻不容缓，以自动化平台作为作业中心的执行平台和执行通道恰逢其时。围绕安全建设、执行通道、服务编排能力、全栈接入能力、多数据中心管理五大议题，江苏移动利用自动化平台完成入网验收、日常巡检、告警预处理、统一运维等运维工作。针对安全加固工作量大，效率低下的问题，新华三集团AOM上线后，原有的手工安全加固操作升级为全面自动化过程，对加固操作脚本化、标准化、流程化、参数化，并实现异常步骤重复执行，整体上提升了安全加固效率，保证加固结果的一致性和准确性。诸多努力下，安全加固工作改善效果明显，所需时间较原来缩短5倍，更规避了操作过程中的异常错误，让整个加固过程更安全、更可靠。从原始人肉运维升级到工具融合协同的平台化运维，运维效率获得指数级提升！

标准：寻找最优解的落地实践

运维走向运营，并向服务化、标准化演进是云运维的必然趋势。这主要是因为，云运维具有被管网元同质化的特质，即由每台设备的部署参数，诸如系统版本、部署目录、配置参数、部署工具统一等带来的运维工作基本一致，大量重复性、批量级的运维任务使运维标准化至关重要。以此为基础，通过对“运维最佳实践”的归纳和总结，进而对“最佳实践”进行统一规范和执行的“运维服务标准化”有助于降低维护难度、能耗需求及运维成本，并提高运维效率、资源效率与服务质量。而在中国移动的运维实践中，由于标准迥异、交付体系未统一等因素造成的运维能力不足仍制约着运维的效果。例如，因属地运维工作对工作内容及标准界定模糊，运维人员对告警的故障点定界不足，漏查了其中一端；又如，由于售前、售中、售后等环节的服务交付体系未统一，致使预期的全周期服务交付在服务组织、客户响应、适配需求、故障投诉支撑等方面尚存欠缺。

于此而言，制定标准化的运营流程，严控验收环节，搭建标准化运维服务体系，形成快速交付能力已成为影响租户满意度的关键举措。在新华三集团的帮助下，江苏移动围绕“服务、运营、验收、建设、设备”五个维度搭建起标准化运维服务体系，并将日常巡检、较低风险变更、故障通报等标准化相对较高的工作抽离出来，组成服务台团队成为内外部门信息交互的唯一接口，总体控制事件、问题、故障、变更的流程运转，全面感知云平台运维状态，以自动化支撑手段持续提升运维标准化和自动化。

协同：拒绝“一盘散沙”，建设“一支队伍”

纵横交织、流程冗长，是移动云资源池运维工作面临的最主要困境。一方面，云运维工作横向涉及网络事业部、云能、政企、客户，纵向涉及省公司各专业、IT维保商，分工界面纵横交织，切分存在困难。另一方面，运维流程长，一个普通的投诉都会涉及多达13个环节，因个别环节设计不合理导致效率低下的事情时有发生，需要扁平化的流程和精准的故障定界能力来保证处置效率。

牵一发而动全身，一子落而满盘活。系统性问题，当通过机制建设来解决。依托新华三集团丰富的运维经验，一套能够持续优化的运维质量管理体系得以迅速搭建。通过定期对基础运维指标、运维性能容量指标、专项团队管理指标的集合衡量，围绕“人员、服务、平台、流程、事务”等关键要素对云资源池运维整体管理和技术水平进行评估，并不断强化弱指标来提高整体运维质量。运维服务依托人来展开。在搭建运维质量管理体系后，新华三集团凭借丰沛的运维人才资源助江苏移动在内部开展全网云运维培训、赋能工作，详细介绍“云计算、云存储、云专网、云安全”等前沿技术演进趋势，并对云运维所涉及的工具、制度、流程做统一梳理，最大化发挥江苏移动内部运维人员价值，全力保障业务的平稳推进。

智慧：立足当下，放眼未来

预测未来的最好方式，是创造未来。回头看，经过多年的研发、测试、部署及运行，运营商系统内部积累了大量的运维经验。但两类情况仍是事故高发区，一是由于升级后的某些隐患未能及时发现而造成的事故；二是由于事故的发生很突然，不能快速定界，贻误时机，酿成大事故。向前望，智能运维是运维发展的大势所趋，数字化技术通过规避故障与计划性例行维护成为传统电信系统提升运维效率、降低运维成本的重要手段。在可预见的未来，对业务的深层理解，丰富的运维经验，基于数字化技术的智能运维，将构成驱动运维效率的三驾马车。

作为赢得未来的关键一步，新华三集团助其构建“2+5+N”框架下的智慧化运维，围绕“预测-感知-诊断-决策-控制-执行”5大领域的应用，进行智能引擎设计，并建立端到端的故障处理协同流程，实现从云到网的“一步响应、协同处理”，整合碎片化的数据、知识和AI能力，快速构建可灵活复用的智慧能力模型，牵引运维智能化水平提升，有效帮助企业将风险系数与业务需求进行匹配，并在日常运维中对故障做到主动感知，最大化降低企业运维风险。在数字化转型大潮下，传统运维面临的挑战不容忽视，仅确保IT设备安全稳定运行已无法满足企业的需求，为企业及业务创造价值已成为更深层的诉求，这要求云资源池运维工作朝更深度与更前沿的方向发力。在与江苏移动深度合作的征程中，新华三集团将通过数智化运维助江苏移动打造优异的运维能力，加快推进运营商数智化运维转型进程！

资讯动态 Consulting trends

07

“数智变革 共创未来”新华三服务合作伙伴大会在京召开

10月13日-14日，“数智变革 共创未来”新华三服务合作伙伴大会在京召开。作为新华三集团服务生态建设的重要组成部分，来自全国各地的服务合作伙伴相聚一堂，新华三集团副总裁、技术服务部总裁陈孝毅，技术服务部副总裁曹东升，技术服务部服务合作部总监陈斌等人出席会议，总结过往优秀经验，展望未来革新动向，携手合作伙伴统一“以客户为中心，深化技术服务数字化战略”目标，赋能客户体验全方位升级。众多合作伙伴也在现场分享了自身优秀的运营经验。

02

凝心聚力汇聚共识 新华三承办智能运维国标2021年闭门讨论会

2021年4月25日-4月29日，智能运维国标2021年第二次闭门讨论会在杭州召开，新华三集团、中国建设银行、中国电子技术标准化研究院等15家单位34位专家参加了本次会议，本次会议由新华三集团承办。作为智能运维国家标准编制组主要参编单位之一，新华三集团积极推进智能运维国家标准的制定及落地。此次会议再次集合产业届与学术届各家力量，旨在凝聚产、学、研、用多方共识，促进业务实践向行业应用标准的转化，将对智能运维的深刻认知反哺于运维实践工作中，帮助客户实现从基础运维到自动运维、再到智能运维的转变升级。

03

《中国智能运维实践年度报告（2020）》出炉 新华三助推智能运维新发展

2021年6月5日，双态数据基础设施建设峰会暨央企和金融数字化转型对话峰会在京召开，300余位数字技术与信息技术领域专家齐聚古北水镇进行跨行业的深入交流。会上，中国电子技术标准化研究院、中国建设银行、光大银行及新华三集团等智能运维国家标准编制组核心单位共同发布《中国智能运维实践年度报告（2020）》，新华三以丰富业务实践引领行业发展的“领航者”地位得到更广泛认可。

04

新华三架构认证体系重磅发布

这是一项自主创新的架构师级别认证体系，也是新华三认证体系的一次全新升级。新华三架构认证体系与新华三技术认证体系、新华三专题认证体系共同组成新华三的3大认证体系，其内容涵盖了ICT基础架构规划、业务连续性规划的顶级认证；带领学员深入理解行业应用，从而具备解决方案级的架构能力，满足企业和个人数字化转型的培养需求。

06

新华三IT外包服务斩获行业第二

国际数据公司（IDC）发布了最新的《2021上半年中国IT服务市场跟踪报告》。报告显示，2021年上半年，中国IT外包服务市场份额较为分散，新华三集团以4.74%的市场份额占比位居中国第二，首次在IT外包服务领域闯入行业前三。此前4月，新华三整合运维领域资源与解决方案，发布AIO（All In One）一站式运维管理外包服务，正式进军外包服务市场。在经历充分的市场竞争检验与优胜劣汰洗礼后，新华三“智简、至暖、致远”的AIO外包服务已获得各方认可。

01

“AIO一站式运维管理外包服务”重磅发布

秉承“智简、至暖、致远”的服务理念；AIO服务生态体系签约10余家服务商，构建IT服务人才供应链；与9家院校进行校企战略合作，携手打造探索校企合作新模式、新方法的“星空计划”，目前在培青年运维人才253人，服务客户140位。

05

新华三集团与无锡机电高等职业技术学校举行校企合作签约仪式

2021年9月29日，作为进一步完善IT运维服务人才供应链的关键举措，新华三集团与无锡机电高等职业技术学校校企合作签约仪式在新华三杭州基地举行，携手打造旨在探索校企合作新模式、新方法的“星空计划”。

资讯动态 Consulting trends

10月14日，以“拥抱数字化 · 服务启未来”为主题的“2021新华三服务中国行”于上海正式启航。横跨上海、杭州、广州、深圳、郑州、合肥、苏州7城市，累计参会人数近千人。在“数字中国”建设全面推进的当下，新华三集团将基于“云智原生”战略和“数字大脑2021”，以满足客户需求为导向，秉持“更温暖 更专业 更智能”的服务理念，用极致服务与专业精神温暖客户，带动客户全面提升IT系统成熟度，为数字经济有序发展保驾护航。

08 “拥抱数字化 · 服务启未来” 2021新华三服务中国行

09 《信息技术服务 智能运维 通用要求》团体标准正式发布

由中国建设银行股份有限公司、平安科技（深圳）有限公司、中国光大银行股份有限公司、新华三集团、中国电子技术标准化研究院、清华大学等多家单位共同参与起草的《信息技术服务 智能运维 通用要求》（T/CESA 1172—2021）团体标准，于2021年9月30日发布，并于2021年10月30日正式实施。该标准基于行业发展及组织实践，提出智能运维的能力框架，描述智能运维的特征，明确智能运维所需要的组织治理、智能运维场景实现和能力域的通用要求，通过场景分析、场景构建、场景交付和效果评估的过程，实现运维场景所预定的目标，为智能运维的能力建设提供指导。

10 S+新一代网络自动化运维平台2.0发布

在2021年新华三集团主办的“新华三U-Center AOM自动化运维筑牢智能运维基石”活动上，S+新一代网络自动化运维平台2.0发布，这是“全域融合、开放架构、功能深化、云图排障”的新一代网络自动化平台，通过开放、易用、准确的“S+ 2.0云图排障”工具为网络工程师排忧解难。

国际数据公司（IDC）发布了最新的《IDC中国统一运维软件市场半年跟踪报告（2021H1）》。报告显示，2021年上半年，新华三集团在中国IT统一运维软件市场中以13.3%的业务占比排名行业第一。在细分领域，新华三以28.2%的份额连续四年半在中国网络管理软件市场蝉联行业第一；在中国IT基础设施管理软件市场，新华三以11.2%的市场份额占比排名第一，在激烈的市场竞争中持续扩大自身优势。

11 新华三统一运维软件 蝉联市场份额冠军

12 新华三亮相CDCC年度盛会，开启数据中心“绿色低碳”全生命周期之旅

2021年11月24日-25日，CDCC第九届数据中心标准峰会在上海拉开帷幕。新华三集团开设“智行——低碳数据中心技术专场”，与海内外数据中心行业的专家、学者、企业代表共同探讨新一代绿色数据中心的建设之道。

“中国IT用户满意度大会暨信息技术应用生态伙伴大会”于2021年12月在北京成功举办。会上，《2021中国IT用户满意度报告》年度评选结果正式揭晓。新华三集团凭借自身在IT服务领域30余年的丰富经验，在业界赢得了广泛赞誉，一举揽下“IP通信领域满意度第一”、“运维管理软件用户满意度第一”及“运维管理外包服务满意度第一”三项殊荣。该会议是目前国内IT领域持续时间最久、规模最大、最具权威性和影响力的用户满意度调研活动，已连续举办20年。

13 新华三斩获“2021中国IT用户满意度大会”三项大奖

iService服务数字中枢搭载“金手指”系统重磅升级，构建ICT产品全生命周期智能化工具集，打造数字化运维新模式，为10000+客户提供涉及60000+设备的公告预警。

14 iService服务数字中枢搭载“金手指”系统重磅升级