

没有银弹，但有飞轮 运维治理与AI的协同演进

嘉为蓝鲸智能运维产品团队 | 2026年

引言

Agentic Ops实践中一个规律越来越清晰：AI在运维场景的落地效果，根本上取决于运维数据、流程和知识体系的治理质量。没有扎实的运维治理底座，AI能力只能停留在“理想很美好”阶段。

但这并不意味着「先把治理做好，再来建AI」。我们观察到一个更有价值的模式：治理与AI可以协同演进，相互加速——扎实的治理让AI落地更可靠，而AI本身也可以成为持续提升治理质量的有力工具。配置数据质量运营Agent可以替代人工月度核查，监控运营Agent可以持续分析告警规则优化空间，知识库运营Agent可以将故障案例沉淀从「依赖主动填写」变为「自动提取确认」……

核心观点

AI不是运维治理的替代品，也不需要等待治理「完美」才能引入。治理是AI落地的基础，AI是治理持续改善的加速器。两者协同演进，是Agentic Ops落地最优路径。

嘉为科技

广州嘉为科技有限公司（简称“嘉为科技”）成立于2001年，依托自主研发的“嘉为蓝鲸”一体化平台，构建覆盖IT研发、运维、运营全领域的产品与解决方案，全面支撑政企客户数字化转型！

嘉为蓝鲸，是中国一体化智能研发与运维解决方案领先品牌，深度融合AI原生能力与蓝鲸PaaS架构，结合嘉为科技20余年研运经验，打造出智能化程度持续提升的一体化数智运维解决方案AIOps、一体化智能运维订阅服务WeOps、一站式研发效能解决方案DevOps三大产品系列，并朝着AI驱动的运维自治方向持续迈进。

声明

本刊物所载分享内容均来自嘉为蓝鲸官方公众号发布原创内容。

本刊物所载企业案例中涉及数据均已脱敏处理。

本刊物由©广州嘉为科技有限公司所有，未经书面许可，不得擅自修改、删减、改编、用于商业用途或进行二次出版。

CONTENTS

目录

01 智能体典型场景落地

故障诊断智能体	02
ITSM流程数字人智能体	03
自动化巡检智能体	04
智能问答与查询智能体	05
场景与治理依赖速览	06

02 智能体需要什么样的一体化运维基建

嘉为蓝鲸Agentic Ops四层架构：从基建到生态	09
MCP：标准化接入，让Agent驱动一体化运维	10
Skills：封装运维最佳实践，沉淀可复用原子能力	11
Agent的构成要素：从能力组件到可信执行	12
知识层：让Agent成为业务专家	13

03 运维治理：AI落地的关键

CMDB配置治理	15
可观测性治理	15
ITSM流程治理	16
知识治理	17
自动化能力治理	18
发布投产治理	18
灾备应急治理	19
资源与容量治理	20

04 治理路径与实践方法

第一阶段：基础夯实	22
第二阶段：深化融合	23
第三阶段：智能运营	24
度量体系：让治理投入可见	25
AI技术就绪度：MCP与工具生态治理	25

05 AI加速运维治理：飞轮的另一面

配置数据质量运营智能体	28
监控运营智能体	29
知识库运营智能体	30
ITSM流程质量运营智能体	30
自动化覆盖运营智能体	31
AI辅助治理的整体价值	32

06 客户案例实践

案例：某大型组织——从0到30+运维数字员工	34
------------------------	----

PART-1

智能体典型场景落地

在进入治理讨论之前，我们先梳理当前Agentic Ops最具代表性的落地场景。正是因为有了这些场景的目标，我们才能回溯每个场景对治理底座的具体依赖。

1.1 故障诊断智能体

1. 场景描述

故障诊断是Agentic Ops最核心、也最具挑战性的场景。统一故障入口（告警/事件单/故障单等多源信号）触发主智能体，经过Agentic编排（已知/未知双通道）、故障识别（问题理解与分派）、假设推理（多假设并行验证）、结论裁判（证据汇总与输出）四个主流程，协同六类专项分析子智能体并行执行，同时调用排障知识库（历史故障库/运维手册库/应急预案库）和场景小模型（时序异常检测、知识图谱RCA、维度下钻、告警降噪聚合）进行诊断分析，最终输出置信度排序的根因结论与可执行处置建议。

2. 核心工具链与子智能体

组件	职责	核心依赖数据
告警分析Agent	告警聚合、降噪、分级，识别有效告警信号	告警规则库、历史告警记录、事件关联规则
指标分析Agent	指标趋势分析、基线偏差检测、容量瓶颈识别	指标时序数据、动态基线、黄金指标体系
日志分析Agent	日志聚类、异常模式识别、错误链路提取	日志采集覆盖率、结构化日志规范
调用链分析Agent	分布式链路追踪分析、接口延迟定位、调用异常识别	Trace数据完整性、服务接口拓扑
拓扑与变更Agent	服务依赖关系遍历、近期变更关联分析	CMDB拓扑准确性、变更记录完整性
知识与历史Agent	历史相似故障检索、SOP推荐、经验复用	历史故障知识库、运维手册库、应急预案库

3. 治理核心依赖

可观测拓扑完整性

CMDB服务依赖关系准确性决定影响面评估的可靠性；监控覆盖率决定根因链路是否存在盲区。

多维数据可关联性

指标-日志-Trace的关联能力是多模态根因推断的基础，数据孤立则推断片面。

历史案例结构化程度

知识与历史Agent的能力上限由故障案例库的覆盖率和结构化程度决定。

告警质量

大量噪音告警会严重干扰告警分析Agent的信号识别，有效率不足时诊断结论失真。



关键论断

没有完整的可观测性拓扑关系和高质量的监控数据，就不可能构建可靠的故障诊断智能体。这条链路上任何一个节点的数据质量不达标，都会导致根因推断偏差，进而让运维人员失去对Agent的信任。

1.2 ITSM流程数字人智能体

1. 场景描述

流程数字人（AI员工）是面向特定任务场景的智能执行单元，打破传统AI场景封闭模式，构建可无限拓展的智能服务体系。核心理念是：不是角色，是任务执行人——AI员工是具体任务的执行者，不再仅限于问答。整体架构由调度中心（意图识别/LLM分析/AI员工调度）、AI员工本体（职责/目标/行动计划/工具集）、知识中心（按职责限定知识范围）、员工中心（界面化零代码配置与全生命周期管理）、工具中心（通用工具注册与内置MCP服务）五个模块构成；触发方式支持用户对话、例行任务（周期性）、流程引擎（AI节点驱动）多路并行。

2. 核心工具链与子智能体

组件	职责	核心依赖数据
调度中心	接收用户请求，完成意图识别、LLM分析，调度对应AI员工	明确的员工职责、分级意图路由规则
AI员工本体	按职责定义执行任务，包含工作目标、行动计划，以及配套的知识集和工具集	SOP文档库、操作权限配置、ITSM流程规则
知识中心	按员工职责限定知识访问范围，提供专域知识支撑	结构化知识库、FAQ库、操作手册
工具中心	提供通用工具注册与内置MCP服务，AI员工通过工具中心调用运维操作能力	MCP工具注册表、APIGateway接口

3. 治理核心依赖

ITSM流程数字化程度

事件/变更/请求管理流程必须足够标准化，且深度打通运维工具能力，形成数字化的流程，Agent才能更好驱动流程推进。

SOP覆盖率与可执行性

AI员工可自主执行的操作范围严格受限于已文档化的SOP，SOP越精确、覆盖越广，AI员工能力上限越高。

工单分类体系准确性

通过结构化的工单表单设计，形成工单分类体系，有助于AI员工持续沉淀经验，作为后续执行任务的参考，持续提升AI准确性。

权限管控机制

操作权限必须按职责最小化配置，高风险操作由AI员工给出审批建议，强制HITL审批，缺乏权限边界的AI员工存在较大安全风险。



关键论断

流程数字人的能力天花板由SOP覆盖范围和ITSM流程数字化程度决定。未文档化的操作只能转交人工，未数字化的流程无法被Agent驱动。知识治理和流程治理的深度，决定了流程数字人规模化的边界。

1.3 自动化巡检智能体

1. 场景描述

运维团队每日需手动查看监控和告警、执行脚本获取服务器/中间件/数据库/网络设备运行状态、手动点击页面检查业务健康度，耗时费力且依赖个人经验，覆盖不全面。

巡检智能体实现全链路分层自动巡检（服务器/网络设备→中间件/数据库→应用进程→系统页面），经过多维分析流程，包含异常深度分析、时序对比分析、拓扑分层分析，生成标准化结构化智能化报告，并针对巡检异常自动转工单/告警。

2. 核心工具链与子智能体

组件	职责	核心依赖数据
分层巡检执行Agent	按照服务器/网络设备、中间件/数据库、应用进程、系统页面等层级拆解巡检任务，调度对应Skill执行检查，并汇总各层原始结果	CMDB巡检对象清单、巡检计划配置、各类对象巡检脚本库、各类对象巡检指标库
时序对比分析Skill	对比当前巡检与历史巡检结果，识别持续异常、周期性异常、突发异常、恶化趋势和恢复趋势	历史巡检报告、历史异常明细
深度巡检分析Skill	针对已识别异常项进行2-3轮递进排查，从表层异常下钻到具体对象和原因，形成可解释的根因线索与处置建议	异常项清单、自动化执行MCP、运维知识库
CMDB拓扑查询Skill	查询业务、应用、模块、主机、实例、数据库、中间件、网络设备及上下游依赖关系，可视化展示巡检异常项的影响范围和关联关系	CMDB各资源对象拓扑关系
巡检结果分析Skill	对各层巡检结果进行结构化解析、异常识别、规则匹配、等级判定和健康度评分，输出可进入深度分析的异常清单	巡检原始结果、指标阈值、健康度评分规则
PDF/EXCEL报告生成Skill	将结构化巡检结论渲染为标准报告，支持PDF汇报版和EXCEL明细版导出，并按渠道推送	报告模板库、推送渠道配置

3. 治理核心依赖

◆ 巡检指标库和脚本库

巡检的全面性直接取决于巡检指标库和巡检脚本的覆盖范围，从主机，到网络/存储/安全设备，到中间件/数据库，到应用/URL/页面，整体的覆盖面。

◆ CMDB对象完整性

巡检对象范围由CMDB中的资产记录决定，异常项的影响范围和关联，也依赖CMDB的关联关系，CMDB缺漏即意味着巡检遗漏。

◆ 报告模板标准化

巡检报告需有统一结构化模板，才能形成跨周期可比较的健康度趋势。



关键论断

巡检智能体的价值在于「用一致的标准持续扫描全栈IT对象」，而非「偶尔深度分析」。巡检覆盖率和CMDB对象完整性是巡检智能体能否做到「无死角」的硬性前提。

1.4 智能问答与查询智能体

1. 场景描述

运维人员在日常工作中频繁面临两类需求：一是知识检索（如查询故障处置方法、操作规范），依赖关键词匹配检索和个人经验总结，效率低、门槛高；二是数据查询（如统计指定版本的CMDB模型实例数量、查询资产关联关系），依赖对CMDB接口参数的熟悉程度，有一定学习成本。智能问答与查询智能体通过自然语言交互，将这两类需求统一承接，实现知识问答与数据查询的双轨覆盖。

2. 核心工具链与子智能体

组件	职责	核心依赖数据
查询分析Agent	理解用户自然语言意图，拆解为知识检索或数据查询任务并路由执行	意图识别模型、查询历史记录
知识库RAG Skill	向量语义检索，LLM上下文问答，含引用溯源与不确定性声明	结构化知识库（故障案例/操作手册/架构文档/FAQ/应急预案）
CMDB查询MCP	模型筛选、关联查询、全文检索等多模式数据查询，支持ChatBI图表生成	CMDB数据准确率、字段定义标准化、数据实时性
数据理解分析Skill	对查询结果进行二次分析、摘要提炼、可视化展示	数据分析模板、图表渲染能力

3. 治理核心依赖

知识库覆盖率与结构化程度

知识库覆盖范围决定问答的有效率；知识必须结构化（而非纯文档），RAG检索才能准确命中。

知识时效性

过期的知识比没有知识更危险，架构变更时相关知识必须同步更新，否则Agent会给出错误答案。

CMDB数据准确率与字段标准化

CMDB查询结果的可信度完全取决于数据准确率，字段口径不统一会导致查询结果产生歧义。

数据关联关系完整性

关联查询（如「该IP运行了什么软件，归属哪个系统」）依赖CMDB中完整的CI关系模型。



关键论断

知识问答的「幻觉」风险本质上是知识治理问题：知识库不完整导致Agent依赖模型参数知识进行猜测；知识过期导致Agent给出已失效的操作建议。解决幻觉的核心手段是提升知识库的覆盖率、结构化程度和时效性。

1.5 场景与治理依赖速览

可以看看这几个典型场景的Agent落地和基础设施的关系：

智能体场景	最关键的治理依赖	治理缺失的典型后果
故障诊断Agent	可观测拓扑+监控覆盖率+历史案例库+CMDB服务依赖	误判率高，运维人员失去信任，退回人工模式
ITSM流程数字人	SOP覆盖率+ITSM流程数字化+知识结构化+权限管控	大量请求转人工，覆盖范围无法扩大，价值难以体现
巡检Agent	巡检覆盖率+CMDB对象完整性	巡检存在盲区，报告失真，管理层对结果不信任
问答与查询Agent	知识库覆盖率与时效性+CMDB准确率+数据字段标准化	答案不准确，幻觉率高，用户放弃使用

而更多智能体建设则需要更为完善的基础设施：

业务领域	智能体名称	能力描述	预期核心价值
监控管理	告警辅助分析Agent	多源告警接入，意图识别，知识库检索，MCP生成，生成决策建议	提升告警分析效率和准确率
日志管理	日志智能解析Agent	划词分析即可快速理解复杂日志含义，减少跨系统查阅成本，根据实际环境解析日志	提升日志解析效率
故障诊断	故障诊断Agent (A2A)	多智能体协同，专项分析智能体，可观测MCP调用，根因分析诊断	提升故障根因定位效率和准确率
ITSM	IT流程数字人Agent	工单录入时：合规性审核+字段智能补全； 工单提交后：智能分类+委派推荐； 处理过程中：AI辅助助手（按需，侧边栏）； 工单解决时：解决方案总结+知识库转化； 工单关闭后：复盘分析+问题管理推送	提升流程运转效率
变更管理	变更风险评估Agent	LLM方案完整性检查+CMDB影响分析+冲突检测	提升变更质量
巡检管理	业务巡检与分析Agent	分层巡检（基础设施→平台→应用→业务），日/周/月计划自动执行，结构化报告	提升巡检覆盖度和效率

业务领域	智能体名称	能力描述	预期核心价值
运维开发	脚本生成与安全审查Agent	自然语言→运维脚本（Shell/Python），同步安全审查（危险命令/边界条件/幂等性）	提升脚本安全
自动化操作	标准操作数字人Agent	低风险标准操作自动化响应	提升自动化响应效率
运维技术对象	SQL风险识别Agent	高危SQL识别、语法性能诊断	提升SQL风险识别能力
配置管理	自然语言查询Agent	自然语言CMDB查询和导出	提升CMDB查询效率
配置管理	数据运营检查Agent	根据数据运营指标进行数据质量巡检	提升CMDB数据质量运营效率
知识库	智能知识问答Agent	自然语言语义检索（向量）+LLM上下文问答+引用溯源+不确定性声明	提升问题回答效应效率
运营分析	运维报表生成Agent	基于数据聚合的报表生成，实现日常运维巡检、指标分析、工作分析报告	提升报表、报告的生成效率
容量管理	容量预测与规划Agent	根据历史容量数据，结合预测模型实现30/60/90天的容量趋势预测	帮助容量瓶颈风险的提前识别
资源管理	成本治理Agent	闲置识别（CPUP95<5%）→通知回收+过配降配建议	提升资源利用率
.....			

PART-2

智能体需要什么样的一体化运维基建

一体化运维平台是Agentic Ops的「上下文和触手」：AI的感知能力来自可观测数据，行动能力来自自动化工具，认知能力来自CMDB和知识库。没有丰富、准确、标准化的一体化运维基建，Agent只是一个无法落地的逻辑框架。

2.1 嘉为蓝鲸Agentic Ops四层架构：从基建到生态

Agentic Ops的整体架构由四个层次构成，自底向上层层依赖：



层次（自底向上）	核心组成	与智能体的关系
第一层： 一体化运维基建	CMDB、ITSM、可观测（指标/日志/Trace）、自动化运维、应用发布、灾备应急、云管CMP、知识库等17+产品模块	提供智能体感知环境、执行操作的原始能力；基建质量决定智能体的数据上限和操作可靠性
第二层： 大模型网关及大模型	LLMGateway（屏蔽模型差异，提供统一OpenAI协议API）；支持DeepSeek、Qwen、Hunyuan、GPT等各类通用/私有大模型；SRE领域大模型（增量预训练+微调+RLHF）；ML小模型（时序预测、异常检测、告警聚合、日志聚类等）	提供智能体的推理内核；大模型网关负责权限、审计、监控、配额限流；大小模型协同满足精确性与效率的双重要求
第三层： 智能体开发平台（AIDEV）	Agent开发框架（单Agent+基于Graph的多Agent编排）、MCP管理、Skills管理、RAG知识库、提示词管理、LLMAdaptor适配层迭代的各类单/多Agent应用	提供智能体研发、编排、部署、管理的统一底座；平台化使新场景快速复用已有组件，避免重复建设
第四层： 智能体生态	自动巡检智能体、IT流程数字人、标准操作数字人、故障分析智能体，以及持续迭代的各类单/多Agent应用	面向具体运维场景的智能化能力交付；智能体生态的丰富程度体现Agentic Ops的整体成熟度

这四层并非独立模块，而是严格的依赖关系：智能体生态（第四层）的可靠性由开发平台（第三层）的完善度、大模型（第二层）的能力边界、以及一体化基建（第一层）的治理质量共同决定。基建层的任何数据质量问题，都会沿依赖链向上传导，最终体现为智能体的误判或失效。

2.2 MCP：标准化接入，让Agent驱动一体化运维

MCP（模型上下文协议）是智能体调用运维操作能力的标准化接口层。通过复用API网关，将原有一体化运维平台API快速转化为LLM可调用的MCP接口，实现智能体对运维系统的标准化、安全化调用。



统一规范

统一MCP Server的发布规范，集中管控，支持各开源/私有大型模型的集成对接。



安全认证

与权限体系融合，解决MCP协议本身无安全与认证的问题；集中管控、会话保持、日志审计、MCP路由。



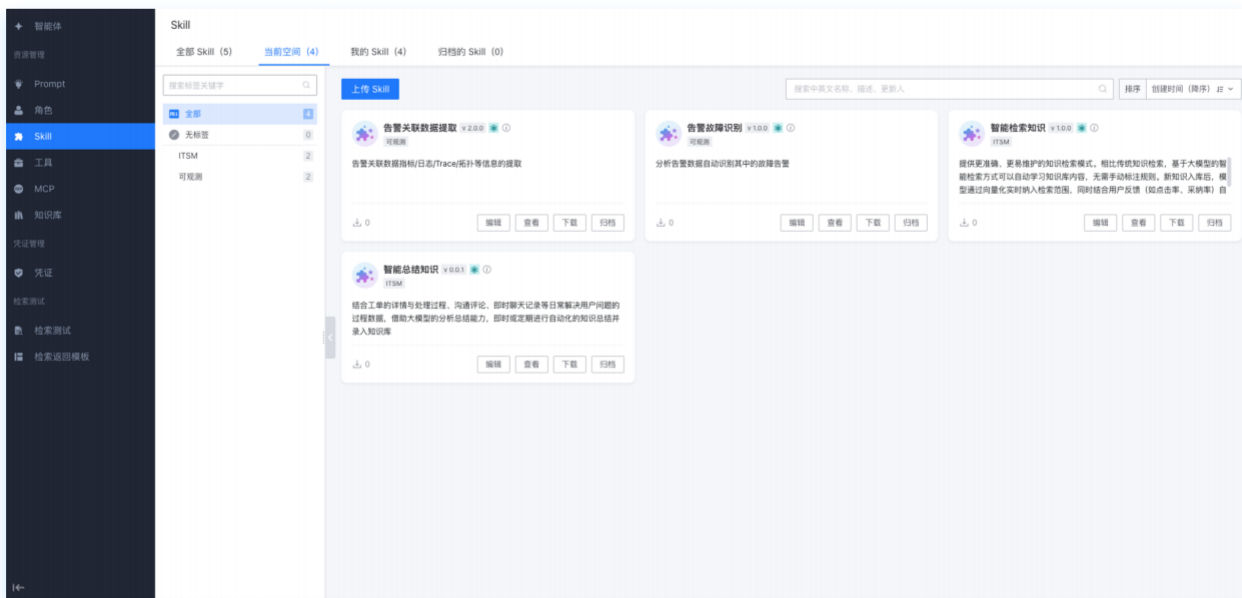
能力复用

与API Gateway集成，复用权限、限流、熔断等能力，API网关支持一键发布至MCP市场。

当前已覆盖的MCP能力：配置平台MCP（CMDB读写）、可观测中心MCP（指标/日志/Trace查询）、自动化运维中心MCP（作业执行）、IT服务管理MCP（工单操作）、应用发布中心MCP（发布触发）等核心模块。

2.3 Skills：封装运维最佳实践，沉淀可复用原子能力

Skills是将反复使用的原子操作封装为标准化技能单元，供多个Agent复用，是运维最佳实践的代码化体现。平台提供Skill托管和分享功能，支持开源Skill包兼容，提供开发工具包支持快速生成和调试。



典型Skills类型：



数据处理类

告警聚合Skill、日志聚类Skill、指标异常识别Skill、数据脱敏Skill。



推理分析类

根因分析Skill（RCA排序）、影响面评估Skill、RunBook匹配Skill、风险评分Skill。



操作执行类

标准重启Skill、配置下发Skill、流量切换Skill、回滚执行Skill。

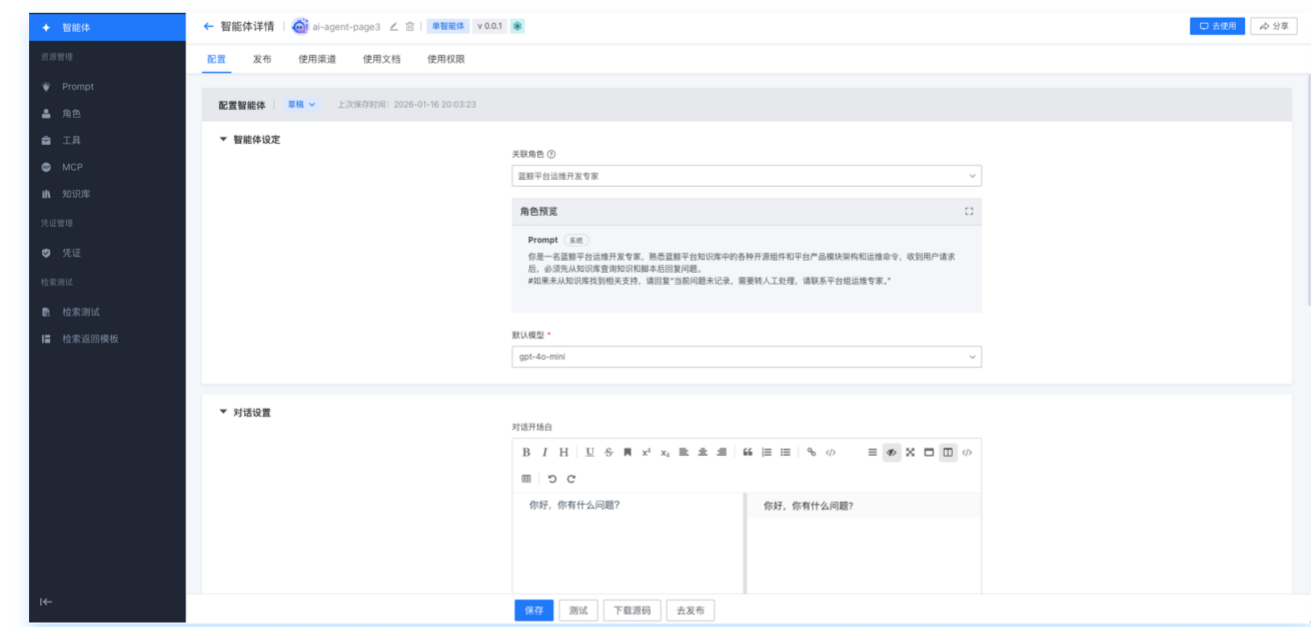


输出生成类

报告生成Skill、通知推送Skill、图表渲染Skill。

2.4 Agent的构成要素：从能力组件到可信执行

除MCP和Skills外，一个生产可用的Agent还依赖以下关键要素共同构成：



构成要素	说明	对治理的依赖
提示词工程 (Prompt)	定义Agent的角色、行为边界、输出格式和推理策略；支持在线调试和版本管理	Prompt质量直接影响Agent推理准确性；需随业务变化持续优化
RAG知识检索	运维历史事件、操作手册、架构文档全量向量化；Agent推理时通过语义检索获取精准上下文，显著降低幻觉率	知识库的覆盖率、结构化程度和时效性决定RAG检索质量
Context Engineering	为Agent提供任务相关的背景信息和记忆（上下文/跨会话记忆/持久知识三层）；使Agent理解当前环境和历史状态	CMDB、监控快照、变更记录等实时数据的准确性决定上下文质量
Human-in-The-Loop (HITL)	在高风险操作节点强制插入人工审批卡点；AI越自主的地方，管控越要精确；支持界面化配置每类操作的审批策略	操作风险分级需清晰定义；审批流程需与ITSM流程集成
操作日志与审计	所有Agent操作写入不可篡改的操作日志，满足等保合规要求；支持回溯Agent的每一个决策依据	审计体系是建立组织信任的基础设施；是Agent权限逐步扩大的信用基础
多Agent编排 (A2A)	主Agent分解任务，子Agent并行执行，通过A2A协议实现标准化通信和结果汇总	多Agent对数据一致性要求更高；不同Agent访问同一资产状态必须保持同步

2.5 知识层：让Agent成为业务专家

知识层解决Agent的「长期记忆」问题，分三个层次管理：



知识层次	定义	典型内容	生效范围
上下文 (Context)	本次对话中Agent需要看到的即时信息	当前告警详情、实时指标快照、本次变更方案	单次Session，对话结束后释放
记忆 (Memory)	跨越会话存在的业务特征信息	某服务的上下游依赖、某团队的操作习惯、上次故障的处置方式	跨会话持久，按CI或服务维度存储
知识 (Knowledge)	持久化的领域知识，供所有相关Agent共享检索	历史故障根因库、操作手册、应急预案、架构文档	长期持久，分通用/业务线/专项三层管理

PART-3

运维治理：AI落地的关键

Agentic Ops的落地效果，根本上取决于各运维治理领域的成熟度。每个领域围绕「最佳实践建设维度+核心建设内容+持续运营机制」三个维度展开。

3.1 CMDB配置治理

CMDB是Agent的「认知地图」，服务依赖关系、资产归属、环境配置都在这里。CMDB不准确，意味着Agent对整个IT环境的认知是失真的。

最佳实践维度	核心建设内容	持续运营机制
统一建模	建立标准化CI（配置项）模型，覆盖主机、容器、应用、服务、数据库等各类型；定义CI之间的关系模型（运行、依赖、归属等）；关系模型是故障影响面分析的数据基础	模型版本管理，随架构演进定期评审更新；新CI类型上线前完成建模评审
自动采集	通过自动发现工具持续采集物理/虚拟/容器资源，与API Gateway集成实现多云、多平台资产自动纳管；自动发现覆盖已知属性，服务依赖等逻辑属性辅以人工维护	采集覆盖率纳入KPI，定期扫描采集盲区；新资产入网自动触发采集任务
流程驱动更新	所有变更（新增/下线/配置修改）必须触发CMDB记录联动更新，变更审批与CMDB更新强绑定；杜绝「变更不入库」，确保CMDB与真实环境的动态一致性	变更闭环率作为考核指标，异常变更（未同步CMDB）自动告警；月度变更与CMDB差异核查
数据消费建设	将CMDB数据开放给监控、ITSM、自动化、发布等各平台消费，建立数据消费场景；CMDB数据被消费越多，维护动力越强，形成正向循环	通过消费量和消费准确率反向衡量CMDB数据质量与价值；消费方反馈的数据问题纳入治理工单
数据运营	定期（月度）执行CMDB数据核查，对比自动发现与手工维护数据的差异；设立「CMDB数据准确率」核心指标，核心业务系统目标>85%，全量目标>75%	数据质量看板持续可视化，异常数据自动推送责任人处理；准确率低于阈值触发专项治理

治理关键点

CMDB的准确性不是一次建设可以解决的问题，而是持续运营的结果。范围聚焦原则：优先治理核心业务系统（30%的系统覆盖80%的价值），逐步扩展。变更驱动是保持准确性的核心机制，定期核查是兜底手段。

3.2 可观测性治理

可观测性是故障诊断Agent的「感知神经系统」。指标、日志、Trace三支柱缺一不可，拓扑关联是多维数据发挥价值的关键。

最佳实践维度	核心建设内容	持续运营机制
统一对象建模	以CI为锚点统一监控对象，确保监控数据与CMDB资产一一对应，实现「监控找到资产，资产找到监控」；新资产上线自动触发监控配置，资产下线自动清理	新资产接入标准化流程，含监控配置验收；监控对象与CMDBCI的映射关系定期核查
指标体系建设	建立分层指标体系（基础设施→中间件→应用→业务）；对每类对象定义统一指标分级规则（生死指标、告警指标、分析指标）；	指标标准化覆盖率纳入KPI；新服务类型上线前完成指标定义评审
告警治理	建立告警分级机制（致命、预警、提醒）正确反馈对象的运行状态；持续提升告警覆盖率，引入智能基线检测，降低漏告，告警覆盖度提升至95%以上；持续清理噪声告警，优化告警策略，降低误告，告警有效率提升至80%以上	月度告警质量回顾；有效率低于阈值触发专项治理；新增告警规则上线前评审
观测数据关联	打通指标-日志-Trace的数据关联（通过InstanceID、ServiceID、TraceID串联）；构建应用横向、资源纵向关联融合拓扑；实现metric/trace/log三维融合，为故障诊断Agent提供全链路证据	数据关联覆盖率持续追踪；断点（无法关联的链路段）告警通知负责人修复
监控覆盖管理	以应用为单位定义监控覆盖率，识别监控盲区（重点补齐容器、进程级监控盲区）；目标监控覆盖率>95%，Trace覆盖核心微服务>90%	覆盖率看板持续可视化；未覆盖资产定期推送应用负责人；覆盖率纳入应用上线验收标准



治理关键点

告警降噪是可观测性治理最直接的价值产出：大量噪音告警会让故障诊断Agent的信号识别能力大幅下降。建议将「告警有效率」作为可观测性治理的核心KPI，持续追踪改善。

3.3 ITSM流程治理

ITSM流程是流程数字人的「行为规则集」。流程的数字化程度决定了Agent能够自主执行的范围边界；未数字化的流程，即使逻辑设计合理，Agent也无法驱动执行。

最佳实践维度	核心建设内容	持续运营机制
流程数字化建设	将事件管理、变更管理、问题管理、请求管理等核心流程完整数字化，包括分类体系、分级规则、审批矩阵、执行窗口、SLA定义；流程节点与Agent行为直接映射	新流程上线前评估AI自动化可行性；流程变更时同步评估对Agent行为的影响
AI员工职责分级体系	创建AI员工，职责定义需要清晰、工作目标需要明确，以便AI员工稳定运行，确保意图调度的准确性；业务变化后，需审视AI员工团队职责，同步更新	定期统计调度准确率，低准确率（<80%）AI员工触发优化；新业务场景及时补充新的AI员工
变更流程规范化	变更类型三级分级（标准/常规/紧急），审批矩阵结构化存储；每类变更必须有经过验证的回滚方案和明确的执行窗口；变更成功率和回滚率纳入质量指标	变更成功率与回滚率月度分析；回滚失败案例专项复盘；执行窗口合规性监控
SLA治理	为各类工单和事件定义清晰的SLA目标（MTTD、MTTR、首次响应时间等），为Agent的优先级决策提供量化依据；SLA目标随业务重要性分级差异化设定	SLA达标率月度分析；持续改善低达标场景；SLA变更需经过评审

3.4 知识治理

知识是Agent推理的「经验记忆」。知识的结构化程度和时效性，直接决定了知识问答Agent的准确性和故障诊断Agent的历史参照能力。

最佳实践维度	核心建设内容	持续运营机制
知识分类与建模	建立运维知识分类体系：故障案例库、运维手册库、应急预案库、架构文档库、FAQ库；定义各类知识的结构化模板，非结构化知识拒绝入库	新知识按模板录入；模板定期评审迭代；非标准知识单独审批流程
故障案例沉淀	故障处理结束后，将处置过程结构化记录（根因/影响/处置步骤/预防措施）；通过Agent自动提取草稿，人工审核后入库；故障沉淀率纳入团队KPI	月度统计故障沉淀覆盖情况；相似故障重复出现时检查知识库是否已录入
SOP可执行化	SOP必须达到「机器可执行」的精确程度：明确操作步骤、前置条件、执行命令、预期输出和异常处理；模糊的自然语言描述无法被Agent执行，可执行性是SOP质量的核心标准	SOP可执行性评分定期统计；低评分SOP触发专家评审更新；新操作上线前完成SOP编写
知识时效管理	建立知识版本管理机制；技术架构变更时同步触发相关知识的审核更新；设置知识有效期，超期自动触发复核流程；过期知识自动下线或标注失效	知识有效率看板持续可视化；架构变更单关联触发知识更新任务；知识负责人定期收到复核提醒

3.5 自动化能力治理

自动化是Agent的「手脚」。Agent的自主执行能力完全依赖自动化工具层的覆盖范围和可靠性；自动化能力薄弱，Agent只能「出谋划策」而无法「亲自执行」。

最佳实践维度	核心建设内容	持续运营机制
自动化通道覆盖	围绕全栈IT对象建立统一的自动化接入通道，覆盖操作系统、网络设备、存储设备、安全设备、数据库、中间件、应用进场、容器平台、系统URL和UI和内部API等对象，而不是只停留在孤立的主机脚本自动化	持续扩展自动化通道对全量IT对象的覆盖范围，按对象类型、产品型号、版本和厂商能力维护覆盖矩阵，将新增对象接入、老旧对象适配和通道下线纳入生命周期治理
操作标准化封装	将主机、网络设备、SQL、RPA等执行通道统一封装为标准的MCPTool，明确输入参数、输出结构、前置校验、超时重试、幂等要求和失败处理，支持Agent高效稳定安全的调用；高风险命令内置拦截和灵活分批执行机制，保证Agent调用结果可解释、可追踪	持续监控工具调用成功率、平均耗时和失败原因；失败率超阈值自动告警并触发工具治理，支持提升agent调用标准自动化MCP的成功率和稳定性
自动化场景覆盖	围绕典型运维场景构建端到端闭环自动化能力，而不是只建设零散脚本或单点编排流程。以巡检场景为例，应打通巡检对象、指标库、巡检脚本、任务编排、结果分析、智能下钻、报告生成、异常转工单/告警闭环。	深入调研日常自动化操作，对不同自动化操作进行逻辑抽象和场景归类，识别其是否形成完整闭环；建立自动化场景生命周期管理机制，覆盖创建、执行、分析、反馈的闭环机制
权限最小化原则	按照业务系统、IT对象、脚本/工具和操作类型进行严格权限划分，Agent或用户没有授权则无法查看、选择或执行对应脚本；建立“对象级授权+执行前审批复核+高危命令拦截”三层权限安全管控，确保查询、执行、变更、回滚等动作都在授权范围内完成	建立业务系统、IT对象、脚本工具、用户/Agent身份之间的权限矩阵，并随组织、系统和资产变化持续更新

3.6 发布投产治理

发布变更是运维风险最集中的场景，也是变更执行Agent落地的核心依托。发布流程的规范化程度，直接决定了AI能否安全介入发布决策。

最佳实践维度	核心建设内容	持续运营机制
统一发布标准	以应用为核心建立统一发布模型，将CMDB拓扑、制品/介质、审批、发布执行、验证、回滚纳入同一框架，统一管理主机、容器、SQL和配置变更	用一套标准和工具入口管理发布变更，持续提升业务系统和发布类型覆盖率；定期治理绕行发布、线下变更和标准缺失场景
测试生产CI/CD联动	打通测试到生产的晋级链路，确保同一应用、同一制品、同一配置基线和同一发布模板进入生产，并将测试结果作为生产准入条件	持续复盘生产变更失败是否源于测试缺失、环境差异或准入不足，并将问题回流到测试用例、环境基线和流水线模板
统一配置变更	将应用的静态配置和动态配置纳入统一配置管理，区分环境配置和业务配置匹配不同策略，支持版本、差异比对、审批、发布、回滚	持续核查配置漂移、线下改配和测试生产差异；配置变更故障必须复盘，并回流到配置模板、审批规则和验证脚本
发布稳定和效率度量	建立发布质量与效率指标体系，覆盖发布成功率、发布执行耗时、发布次数等度量指标，并按业务维度治理	按月分析指标趋势和瓶颈环节；对高失败率、高耗时发布专项优化

3.7 灾备应急治理

灾备应急治理决定了Agent在故障高压场景下是否敢用、能用。核心不是准备几份预案，而是把应急/灾备预案演练、故障分级、应急指挥协同、故障排查分析、故障复盘沉淀做成可检索、可执行、可度量的闭环。

最佳实践维度	核心建设内容	持续运营机制
应急预案数字化	按业务系统、故障类型和影响范围沉淀应急预案，将应急预案从Word文档转化为结构化、可检索的数字化格式，覆盖P0/P1级别故障的处置流程	预案有效性年度评审；架构变更触发相关预案同步更新；预案覆盖率纳入治理指标
灾备演练常态化	定期执行灾备切换演练（包含混沌工程故障注入），验证预案的实际有效性；演练结果结构化记录并沉淀为知识；基于演练数据持续优化预案	演练频率：核心系统季度演练，全量系统年度演练；演练报告纳入知识库
应急演练常态化	开展桌面推演、故障注入和应急切换演练，验证监控告警、人员协同、应急预案、通知机制和恢复验证是否有效	核心系统季度演练，全量系统年度演练；演练问题进入整改闭环，并沉淀为知识和自动化改进项
故障复盘与知识回流	对重大故障结构化记录时间线、根因、影响、决策、处置动作和预防措施，形成可被Agent复用的故障知识	P0/P1故障复盘率100%；复盘结论落实到应急预案、协同流程中

3.8 资源与容量治理

资源容量治理是容量规划Agent和FinOpsAgent的数据基础。资源数据的准确性和口径一致性，直接决定了预测模型的置信度和成本优化决策的可靠性。

最佳实践维度	核心建设内容	持续运营机制
资源标签完整性和准确性	多云资源统一纳管，并建立资源的全生命周期管理流程和标签规范，确保资源业务归属信息的完整性和准确性	定期统计与改进：资源标签完整性和准确性的定期统计和异常告警，推动资源管理者持续完善
度量指标一致性	基于数仓分层最佳实践，建立原始数据、指标明细标准、场景化运营指标，并将异构数据进行统一接入	消费驱动的运营理念：通过容量分析、成本分析等场景反向推导所需业务指标及其标准化建设
业务基线动态管理	建设容量预测所依赖的业务流量基线，基线随业务迭代持续更新；支持节假日、大促等特殊时期的差异化容量预测模型	基线更新频率：常规季度，大型活动前专项更新；预测准确率持续回验
成本数据整合	将财务成本数据与技术资源数据打通，实现业务成本结算；闲置资源识别标准（CPUP95<5%为闲置基准）；过配降配建议基于量化数据支撑	周期性FinOps报告：闲置资源清单、过配资源建议、成本优化执行情况；回收率纳入KPI



治理领域全览（不限于）

CMDB配置治理



统一建模·自动采集·流程驱动·数据消费·数据运营

可观测性治理



统一对象建模·指标体系·告警治理·观测数据关联·覆盖管理

ITSM流程治理



流程数字化·工单分类·变更规范·SLA治理

知识治理



分类建模·故障沉淀·SOP可执行化·时效管理·显性化

自动化能力治理



场景覆盖·操作标准化·权限最小化·回滚能力

发布投产治理



统一标准·策略规范化·风险量化·质量复盘

灾备应急治理



预案数字化·可执行化·演练常态化·RTO/RPO量化

资源与容量治理



映射完整·口径统一·基线动态·成本整合

PART-4

治理路径与实践方法

运维治理不是一次性的技术改造，而是以业务价值为导向、以数据驱动为核心、以支撑AI效果落地的系统性变革工程。

4.1 第一阶段：基础夯实

1. 核心定位

解决“数据孤岛、标准缺失、操作混乱”的基础问题，为AI建立可信的数据输入和可靠的执行通道，实现从“人工被动救火”到“标准化主动运维”的转变。

本阶段是整个治理体系的基石，其质量直接决定了后续AI能力的上限。没有准确、完整、实时的数据，任何AI算法都只能产生不可信的结果。建立统一的数据底座和操作规范，使AI具备基本的感知和执行能力。

建设主题	核心内容	交付标准
统一配置	构建全栈自动采集体系，覆盖物理机、虚拟机、容器、网络、中间件、应用全维度；建立“业务线-应用-服务-资源”四层映射关系；定义数据质量标准和生命周期管理流程；构建面向运维全场景的数据消费接口	核心业务系统CMDB准确率≥80%
统一监控	监控覆盖补齐容器/进程监控盲区，建立企业级指标标准体系，统一指标命名、采集频率和存储周期；基于历史数据构建动态基线；建立P0-P3四级告警分级标准和升级机制	监控覆盖率≥80%，告警有效率≥60%
统一日志	构建“采集-清洗-结构化-存储-检索-分析”全链路日志能力；支持多源日志统一接入；实现日志与指标、链路的关联查询；预置常见异常日志模式库	核心应用日志100%全采集；日志结构化率≥70%；全文检索响应时间≤3秒
统一链路	构建分布式调用链追踪体系，实现服务间、接口间调用关系可视化；采集接口响应时间、成功率、调用量等核心性能指标；支持慢调用和异常调用自动标记	核心微服务Trace覆盖率≥70%
统一告警与事件	实现所有监控系统告警统一接入、统一展示、统一通知；建立事件全生命周期管理流程（发现-分派-处理-复盘-关闭）；实现告警与事件的自动关联	告警统一接入，事件P0-P3分级清晰
统一操作	梳理高频运维操作场景，将巡检、补丁安装、基线检查、服务启停、应急处置等标准化操作转化为自动化脚本；构建统一的自动化执行平台和权限管控体系	高频操作自动化率≥50%
统一服务	ITSM核心流程（服务/事件/变更/问题）数字化，工单自动分配，与CMDB/监控/自动化打通	核心ITSM流程数字化，工单路由准确率≥80%

第一阶段可解锁的AI能力：告警降噪与智能归并、日志异常分析、知识问答（基础）、CMDB辅助查询、巡检报告自动生成。

4.2 第二阶段：深化融合

1. 目标

打通各领域数据壁垒，实现"指标-日志-链路-事件-配置"多维数据融合，构建全局运维视图，使AI具备推理和辅助决策能力，实现从"标准化运维"到"智能化运维"的转变，解锁Lv.2→Lv.3（人机协同）的AI能力。

建设主题	核心内容	交付标准
统一观测	构建实体和数据模型，数据治理融合，构建应用/资源两层拓扑，实现metric/trace/log三维融合	跨系统故障可关联诊断，根因定位准确率≥85%
统一发布	构建标准化的CI/CD流水线，应用发布时间缩短，发布成功率提升，支持蓝绿/灰度等高级策略，发布风险量化评分	高风险发布识别率≥90%，回滚成功率≥95%
统一操作	自动化率提升至70%，覆盖发布、变更、网络策略等核心场景，减少人工操作	核心运维场景自动化率≥70%
统一灾备应急	实现灾备演练、应急处置一体化，预案可执行化，与周边系统联动打通	预案可执行化率≥80%，演练RTO达标
统一资源管理	提升资源生命周期管理，加速资源交付；闲置资源识别与回收机制建立	资源利用率提升，闲置资源识别准确率≥85%

第二阶段可解锁的AI能力：故障诊断Agent（辅助模式）、ITSM流程数字人（标准场景）、SQL风险排查Agent、CMDB智能查询、发布风险评估Agent。

4.3 第三阶段：智能运营

1. 目标

实现全链路智能自治，构建“感知-决策-执行-优化”的闭环运维体系，使AI具备自主决策和执行能力，实现全链路智能自治，向「无人值守运维闭环」演进。

建设主题	核心内容	交付标准
统一可用性管理	实现「1-10-30」故障响应目标（1分钟发现/10分钟定位/30分钟恢复），构建根因分析融合场景	P1故障平均定位时间<10分钟，根因准确率≥85%
服务台智能化	升级流程数字人能力，支持复杂问题的多轮对话和跨系统协同处理；构建用户意图识别模型；实现工单自动分类、自动分派和自动闭环流程数字人解决70%+一线咨询，用户满意度提升，工单处理时效大幅压缩	一线咨询自动解决率≥70%，满意度≥95%
统一FinOps	构建可度量的资源成本中心，实现按业务线、应用、环境的多维度成本核算；建立成本优化模型和智能推荐机制；实现资源成本的动态管控和优化	年化云成本降低20%+，资源利用率提升30%+
统一运维分析	构建面向管理层的运维数据驾驶舱；提供业务健康度分析、用户体验分析、SLA趋势分析、运维效能分析等核心报表；实现运维数据对业务决策的赋能	管理层运维数据报表自动化率≥90%
持续自动化与智能化	持续扩展Agent能力覆盖范围；构建多Agent协同框架，实现跨域自治运维；建立Agent能力评估和持续学习机制；逐步完善运维数字员工生态	覆盖场景数持续增长，Agent自主完成率稳步提升

第三阶段可解锁的AI能力：故障诊断Agent（自主模式）、变更执行Agent、容量规划Agent、自愈Agent、多Agent协同。

4.4 度量体系：让治理投入可见

运维治理最容易陷入“投入可见，产出不可见”的困境。建立科学、全面的度量体系，是证明治理价值、争取持续资源投入、推动治理工作不断深化的关键。我们建议分阶段建立以下四类度量指标

度量类型	典型指标	适用阶段
治理质量指标	CMDB准确率、监控覆盖率、告警有效率、SOP可执行化率、自动化覆盖率	第一阶段起持续追踪
Agent效能指标	Agent执行次数、任务成功率、处理时长（BeforevsAfter）、人工干预率	每个Agent上线后即追踪
Agent质量指标	决策准确率、误操作率、SLA达标率、人力替代比例	第二/三阶段，需3-6个月数据积累
业务价值指标	MTTD/MTTR改善、一线咨询自动解决率、资源成本降低比例、管理层满意度	阶段性评估，用于向管理层汇报ROI

度量关键原则

每个Agent上线前，必须建立价值基线（Before数据）；上线后，定期回顾数据对比。没有Before，就没有After，场景就永远是Demo。治理指标的持续改善，是AI能力持续提升的前提。

4.5 AI技术就绪度：MCP与工具生态治理

运维治理的成熟度决定了AI能力的的数据上限，而AI技术本身的就绪度决定了这些数据能否被Agent有效利用。在实践中，我们发现一类容易被忽视的瓶颈：运维数据已经足够好，但Agent调用工具时频繁出错——根本原因不在数据，而在MCP工具本身的质量。从API到可靠MCP工具，这条路径同样需要系统性治理。

治理维度	核心治理内容	常见问题与影响
API规范治理	统一API命名规范（动词+资源：listHosts/restartService）、参数命名、返回格式（统一JSONSchema）、错误码体系；API文档必须包含完整的参数说明、调用示例和边界条件说明	LLM依赖API description理解工具能力，描述模糊或缺失会导致Agent调用错误参数，产生难以排查的随机性错误
MCP工具粒度设计	工具粒度需在「原子性」和「可用性」之间平衡：粒度太粗（如「执行任意运维脚本」）导致Agent调用权限失控；粒度太细（如每个操作拆成独立工具）导致Agent编排链路过长、上下文消耗过大；建议以「单一职责+明确边界」为设计原则	粒度不合理会直接影响Agent的调用成功率和Token消耗效率，高频调用场景中影响尤为显著
MCP工具描述质量	每个MCP Tool的description字段是LLM选择工具的核心依据，必须精确描述：工具的功能边界、适用场景、关键参数含义、典型调用示例、不适用场景（negative-examples）；description需纳入版本管理，随工具能力变化同步更新	description质量是Agent工具选择准确率的决定因素，模糊的描述会导致Agent频繁调用错误工具，严重时引发误操作
MCP工具测试与验证	MCP工具需建立独立的测试机制：单元测试（参数边界、异常处理）、集成测试（与下游系统的真实调用）、幂等性验证（同一调用多次不产生副作用）、回归测试（工具更新后自动回归）；工具测试覆盖率纳入发布门禁	缺乏测试的MCP工具在Agent自主调用时风险极高：Agent会在各种组合场景下调用工具，覆盖范围远超人工测试预期
Prompt工程治理	Agent Prompt需纳入版本管理（Git托管，变更可追溯）；建立Prompt效果评估机制（离线评估集+线上A/B测试）；Prompt变更需经过评审，防止随意修改引入回归；支持按业务场景差异化配置Prompt模板	Prompt质量直接决定Agent推理准确性，无版本管理的随意修改是Agent行为突然退化的常见原因
大模型接入治理	LLM Gateway统一管理模型接入：配额管理（按Agent/场景分配Token配额）、审计日志（记录每次模型调用的输入输出）、模型切换机制（主模型故障时快速Fallback）、成本监控（按场景统计模型调用费用）	无Gateway直接接入大模型，在Agent规模增长后会面临成本失控、无法审计、无法限流等管理问题

工程实践教训

我们在某客户的实践中发现：CMDB数据准确率已达85%，但CMDB查询MCP的description中对「服务」和「应用」两个概念的描述混用，导致Agent在查询服务依赖关系时约30%的概率调用了错误的查询接口。修复description后，调用准确率从70%提升至95%。

这说明MCP工具的质量问题有时比数据质量问题更隐蔽，却同样致命。建议将MCP工具质量（description完整性、测试覆盖率、调用成功率）纳入AI技术就绪度的常规评估指标。

PART-5

AI加速运维治理： 飞轮的另一面

至此，我们已经充分讨论了「治理如何支撑AI落地」。但飞轮的转动是双向的——AI同样可以反过来加速运维治理本身。治理工作长期面临一个核心困境：数据核查靠人工、问题发现靠巡查、执行监督靠规范。这些工作耗时、低效，且难以持续坚持。

AI治理智能体的价值在于：将原本依赖人工周期性执行的治理动作，转变为持续自动运行的治理闭环。治理的持续运营质量提升，反过来进一步扩大AI落地的空间，形成加速飞轮。

飞轮逻辑

治理夯实数据基础→AI落地效果提升→AI辅助治理运营→治理质量持续改善→AI可覆盖更多场景→.....

关键转折点：当AI开始辅助治理本身，治理不再是纯粹的「人工负担」，而成为一个可持续自运转的质量保障体系。

5.1 配置数据质量运营智能体

1. 解决的核心问题

CMDB数据准确率的持续维护是运维治理中最耗时的工作之一：人工核查覆盖面有限、问题发现滞后、责任人推送依赖手工统计。配置数据质量运营Agent将这个过程自动化。

2. 核心能力



数据质量巡检

定期对CMDB数据执行多维度质量检查：字段完整性（必填项缺失）、数据一致性（自动发现与手工维护的差异）、关系合理性（孤立CI、断裂的依赖链）、时效性（长期未更新的资产记录）。



异常自动识别

基于规则引擎+LLM辅助推断，识别可疑数据：IP地址冲突、资产状态与监控数据不符、人工录入拼写错误修正、服务依赖关系与实际调用链路不匹配等。



责任人智能推送

将识别出的数据问题按CI责任人自动分发，生成结构化的问题清单和修复建议，支持直接在IM或工单系统中处理。



修复效果追踪

持续追踪问题修复进度，对超期未处理的问题自动升级，数据准确率趋势可视化。

3. 治理价值

将CMDB数据准确率的维护从「月度人工核查」转变为「持续自动监控+精准推送」，异常发现时效从月级压缩至天级，人工核查工作量降低60%+。

5.2 监控运营智能体

1. 解决的核心问题

告警有效率的持续提升是可观测性治理最难坚持的部分：噪音告警的识别需要分析大量历史数据，告警规则的优化建议难以系统性产出，监控覆盖盲区的发现依赖人工经验。

2. 核心能力



告警质量分析

自动统计各告警规则的触发频次、响应率、误报率、处理时长，识别「高频低效」告警（频繁触发但长期被忽略/沉默的告警），生成告警规则优化建议。



噪音告警识别

基于历史处理记录，识别与故障无关的噪音告警模式；对持续产生的噪音告警自动推荐沉默规则或阈值调整方案，供运维负责人审核确认。



覆盖盲区发现

对比CMDB资产清单与监控覆盖情况，自动识别「有资产无监控」的盲区；对新上线资产的监控配置完整性进行自动验收。



运营报告与治理复盘

自动生成日报、周报、月报和专项治理报告，展示告警有效率、噪音下降率、覆盖提升率、MTTA/MTTR变化、规则优化成效和待治理清单，支撑团队复盘和管理。



知识沉淀与规则推荐

将已确认的噪音模式、有效规则、处置经验、复盘结论和SOP沉淀为知识库内容，在后续规则配置、告警分析和运营报告中复用。

3. 治理价值

告警有效率从典型的40-50%提升至70%+的目标，不再依赖运维人员的经验判断，而是由Agent持续分析并产出可操作的优化建议，将告警治理从「被动应对」变为「主动优化」。

5.3 知识库运营智能体

1. 解决的核心问题

知识库的持续更新是知识治理最难坚持的环节：故障案例沉淀依赖工程师主动填写（实际执行率普遍偏低），知识时效性检查依赖人工定期审核，SOP可执行性评估缺乏系统化方法。

2. 核心能力



故障案例自动提取

故障处理结束后，Agent自动从工单记录、操作日志、对话记录中提取结构化草稿（根因/影响/处置步骤/预防措施），推送给处理人确认入库，将「主动填写」变为「被动确认」，大幅提升沉淀率。



知识时效性巡检

定期扫描知识库中的文档，识别「长期未更新」的知识；结合变更记录和架构文档的变化，自动标记可能已失效的知识并推送责任人复核。



SOP可执行性评估

对SOP文档进行结构化分析，评估其可执行性：步骤是否有明确的执行命令、前置条件是否清晰、异常处理路径是否完整；低分SOP自动推送改进建议。



重复知识合并

识别知识库中语义相似的重复文档，推荐合并或引用，避免知识库膨胀导致RAG检索准确率下降。

3. 治理价值

故障案例沉淀率从通常不足30%提升至70%+，知识库的覆盖率和时效性持续改善，直接提升故障诊断Agent和知识问答Agent的推理质量。

5.4 ITSM流程质量运营智能体

1. 解决的核心问题

ITSM流程的数字化建设完成后，流程质量的持续运营同样需要系统化支撑：意图识别及调度的准确率监控、SLA达标趋势的分析、高频问题的识别与推进——这些工作如果依赖人工统计，往往滞后且片面。

2. 核心能力



调度质量分析

持续监控调度中心性能与调度准确性，以及低响应度、低满意度AI员工，提供配套的AI运营看板。



SLA趋势分析与预警

持续追踪各类工单的SLA达标率趋势，识别持续恶化的场景并提前预警；对即将SLA超时的工单自动推送提醒。



高频问题识别

对工单内容进行聚类分析，识别重复出现的高频问题；对已有SOP但仍重复出现的问题，推送知识库覆盖情况供责任人评估。



变更质量复盘

定期汇总变更成功率、回滚率、影响时长等质量指标，生成变更质量分析报告，识别高风险变更类型和高频失败场景。

5.5 自动化覆盖运营智能体

1. 解决的核心问题

自动化覆盖率的提升需要持续识别：哪些业务系统还没有使用自动化，哪些IT对象还不支持自动化，哪些操作还没有自动化，但这个识别过程本身耗时且依赖经验。

自动化覆盖运营Agent通过结合CMDB业务系统和IT资源对象、ITSM变更工单、主机操作日志等多维度数据，自动统计业务/IT对象/标准操作等多维度的自动化覆盖率，自动识别高价值的自动化空白场景。



业务系统覆盖分析

业务系统覆盖分析：结合CMDB、ITSM和自动化平台数据，统计各业务系统是否接入自动化能力，识别未接入、低使用和绕行自动化的系统。



IT对象覆盖分析

结合CMDB各类IT对象数据，按操作系统、数据库、中间件、网络设备、安全设备、存储、应用、页面UI等对象类型统计自动化通道覆盖情况，识别对象和型号覆盖盲区。



标准操作覆盖分析

梳理巡检、重启、清理、查询、扩缩容、配置变更、回滚等标准操作，判断哪些已有自动化、哪些仍依赖人工处理。



运营看板与任务推动

输出业务系统、IT对象、标准操作、脚本质量等多维度覆盖看板，自动生成治理任务并推送给责任人跟踪闭环。

5.6 AI辅助治理的整体价值

将上述治理智能体汇总来看，其核心价值在于将「周期性人工治理」转变为「持续自动治理」：

治理领域	AI治理智能体	核心转变
CMDB配置治理	配置数据质量运营Agent	月度人工核查→持续自动监控，异常精准推送
可观测性治理	监控运营Agent	经验判断优化→数据驱动持续改善，告警有效率量化提升
知识治理	知识库运营Agent	主动填写沉淀→被动确认入库，沉淀率从<30%升至70%+
ITSM流程治理	流程质量运营Agent	滞后统计分析→实时趋势感知，问题提前预警
自动化能力治理	自动化覆盖运营Agent	依赖经验识别→日志驱动发现，高价值场景自动推荐

这些治理智能体本身也是Agentic Ops智能体生态的一部分，只不过它们的「用户」是运维治理负责人和平台团队，而非一线运维工程师。飞轮的双向转动，正是体现在这里：AI落地场景和AI治理工具共享同一套基建和平台，相互促进，协同演进。

PART-6

客户案例实践



6.1 案例：某大型组织——从0到30+运维数字员工

CMDB是Agent的「认知地图」，服务依赖关系、资产归属、环境配置都在这里。CMDB不准确，意味着Agent对整个IT环境的认知是失真的。

1. 背景

该组织运维场景复杂，覆盖测试环境管控、生产环境可靠性保障等运维全链路场景。在启动Agentic Ops建设之前，已完成一体化运维平台基础建设，具备相对完整的治理底座：CMDB准确率和监控覆盖率维持在较高水平，核心运维流程已数字化。

2. 建设思路

核心思路：场景从效率出发+场景构建要平台化+一体化运维能力要丰富（MCP+数据+知识）。关键策略分三条主线并行推进：



丰富一体化运维能力

通过复用API网关将平台API快速转化为MCP接口，沉淀结构化运维数据和历史事件知识库，确保Agent「不仅会说话，更会干活」。



平台化构建

建立统一智能体开发底座，集成RAG知识库、MCP接口管理、Skill管理等能力，新场景快速复用已有组件，避免重复建设。



提效场景驱动

每个Agent参照运维服务目录清单，明确职责边界，以可量化的工时效率提升为核心目标，而非追求宏大的顶层设计。

3. 典型场景成效

场景	核心成效
业务巡检Agent	巡检覆盖率60%→100%；日报生成时间2小时→5分钟内；告警漏分析率接近零
岗位运营Agent（群聊Bot）	标准请求响应时间4小时→15分钟；80%+低风险请求无需人工介入
SQL风险排查Agent	SQL审批处理时间数小时→10分钟内；运维人员从流程完全解放；敏感信息脱敏归零
线上代码诊断Agent	P2/P3故障根因定位15分钟→2分钟以内；新手工程师定位效率显著提升
告警根因分析Agent	快速识别根因，故障定位和处置时间大幅压缩；多平台人工逐一排查成为历史
CMDB查询Agent	数据统计需求15分钟→2分钟内；自然语言驱动，CMDB消费易用性大幅提升

4. 当前规模与关键启示

目前已生成30+每天工作量超过8小时的运维数字员工，调度500+智能体，各类典型场景持续迭代优化中。

◆ 场景落地反向推动治理

Agent对数据质量和工具接口的要求，倒逼一体化运维能力持续完善，形成正向飞轮。

◆ 治理底座决定AI天花板

当CMDB准确率从60%提升到85%，故障诊断Agent的误判率从30%+下降至个位数，治理质量与AI效果线性正相关。

◆ 平台化是规模化的前提

统一的智能体开发底座使新场景快速复用已有组件，30+数字员工的规模依赖平台化而非逐一开发。

结语

没有银弹，但有飞轮。

AI大模型本身的进步会持续压低算法层的壁垒——通用推理能力会趋向商品化。但运维数据资产和MCP工具生态是难以快速复制的积累，将成为Agentic Ops时代的核心竞争壁垒。能够最先建立起运维数据、MCP工具生态、Agent能力库这三类资产的组织，将在Agentic Ops时代获得持续领先优势。

Agentic Ops的演进，不依赖某个单一技术的突破，而依赖治理与AI能力的持续相互强化。治理夯实AI落地的数据基础，AI反过来加速治理的持续运营——每一次循环都让飞轮转得更快，让AI覆盖更多场景，让治理质量再上一个台阶。



嘉为蓝鲸

研运至简 · 创新无限

www.canway.net



北京 | 上海 | 广州 | 深圳 | 杭州 | 成都 | 香港 | 福州

广州嘉为科技有限公司（简称“嘉为科技”）成立于2001年，依托自主研发的“嘉为蓝鲸”一体化平台，构建覆盖IT研发、运维、运营全领域的产品与解决方案，全面支撑政企客户数字化转型！

嘉为蓝鲸，是中国一体化智能研发与运维解决方案领先品牌，深度融合AI原生能力与蓝鲸PaaS架构，结合嘉为科技20余年研运经验，打造出智能化程度持续提升的一体化数智运维解决方案AIOps、一体化智能运维订阅服务WeOps、一站式研发效能解决方案DevOps三大产品系列，并朝着AI驱动的运维自治方向持续迈进。

嘉为科技是腾讯、红杉及钟鼎资本战略投资企业，在北京、上海、广州、深圳、成都、杭州、武汉、福州、香港等地设有核心基地。公司及产品获工信部、信通院、ITSS、Gartner等国内外权威机构认可与推荐。嘉为科技的解决方案已广泛应用于政务民生、金融、能源、运营商、交通、制造、科技、消费等行业超千家中外行业领军企业。



公众号



视频号



北京 Beijing

地址：朝阳区东三环中路24号楼双井乐成中心B座6层602室
邮编：100022 电话：010-50950167



上海 Shanghai

地址：徐汇区云锦路600号航汇大厦8楼803室
邮编：200232 电话：021-61269880



广州 Guangzhou

地址：天河区天河东路67号丰兴广场A座11楼
邮编：510620 电话：020-38847288



深圳 Shenzhen

地址：南山区粤海街道深圳湾创新科技中心T1栋4902室
邮编：518040 电话：0755-83668518



杭州 Hangzhou

地址：拱墅区申花路99号运河财富中心8幢405室
邮编：310020 电话：021-61269880



成都 Chengdu

地址：高新区天府大道中段500号东方希望天祥C座42楼4216号
邮编：610095 电话：0755-83668518



武汉 Wuhan

地址：洪山区徐东大街79号中兴时代·数贸港第A栋5层509号房
邮编：430000 电话：020-38847288



福州 Fuzhou

地址：马尾区中铁福船大厦23楼2301-3室
邮编：350000 电话：0755-83668518



香港 HongKong

Add: 46th Floor, Lee Garden One, 33 Hysan Avenue, Causeway Bay, Hong Kong (香港铜锣湾希慎道33号利园一期46楼)
Tel: +852 47430985