



GOPS 2025  
Shenzhen



ANNIVERSARY  
2015-2025



# GOPS 全球运维大会

2025  
- XOps 风向标



深圳站

## 暨研运数智化技术峰会

时间：2025年4月25日-26日

地址：中国·深圳

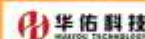
指导单位：



主办单位：



承办单位：



# 数智化重塑证券公司故障管理： 构建主动防御新体系

周光杰

2025-04





## 周光杰

广发证券 资深SRE专家

10+年银行核心系统、证券泛互联网系统运维及运维平台研发经验。  
擅长持续交付、变更管控、统一监控、日志分析等运维领域运维研发。  
亲历公司运维体系从线上化到数字化转型，并积极拥抱智能化。



# 目录/ CONTENTS

- 1 全生命周期的故障管理场景
- 2 运维左移：从被动救火到主动稳定性保障
- 3 变更管控：变更管控主要模块设计与实践
- 4 应急指挥：应急资源协调，应急效率加速器
- 5 智能化与场景融合





# 全生命周期故障管理





# 全生命周期故障管理-稳定性保障全景

为了确保复杂分布系统的稳定性，广发证券将稳定性前移至系统设计与测试阶段，围绕6大核心能力--“故障可恢复、性能可扩展、变更可管控、业务可监控、问题可观测、部署可感知”，强化软件生命周期各环节的紧密协作

## 稳定性运维保障关键能力

6大能力项：故障可恢复、性能可扩展、变更可管控、业务可监控、问题可观测、部署可感知



## 左移稳定性保障重点切入点

### 设计及研发阶段

#### 架构韧性设计

降级  
限流  
切换  
重启  
熔断  
隔离  
异步处理  
重试

#### 容量评估

定义容量指标  
设计容量基线  
埋点容量指标  
监控容量策略  
水平扩容方案  
资源扩容方案  
依赖弹性平台  
容量效能评估

#### 变更风险管控

关键逻辑变更  
架构调整  
依赖平台变更  
上游系统变更  
组件下线  
新组件或业务  
海量终端体验  
数据迁移  
关键配置变更

#### 自动化发布

终端灰度  
服务端灰度  
程序发布  
配置发布  
数据库脚本变更  
参数调整  
主机操作  
应用配置操作  
依赖平台操作

#### 业务监控

业务指标监控  
业务状态监控  
业务链路监控  
数据正确性监控  
服务接口监控  
业务拨测监控  
上游依赖监控

#### 应急定位

可观测看板  
日志数据规范  
日志数据埋点  
链路id埋点  
监控指标埋点  
上游依赖清单  
下游影响清单

#### 数字化部署

主机环境配置  
应用技术配置  
关键业务参数  
数据库参数  
数据库表结构  
中间件配置  
应用平台配置  
网络访问配置

上线前的非功能性需求设计左移

上线后持续挖掘并防范线上风险



# 全生命周期故障管理-故障可恢复

故障的可恢复性指，当系统因内部或外部因素导致业务中断或面临故障风险时，系统应具备及时发现故障的能力，并能够迅速采取降级、限流、切换、重置、隔离等韧性措施以恢复业务连续性

## 生产系统架构韧性感知管理

### 线上架构评审

L1:基础保障级

L2:具备逃生通道

L3:可热操作止损

L4:自愈或半自愈止损隔离

L5:跨系统间止损免疫

### 混沌工程挖掘风险

演练计划

故障模拟库

故障注入

健康检查接口

观测可视化

快速中止

分析不足

跟踪闭环

### 故障发现与执行

异常数据上报

异常监控

故障全自愈

半自愈工具

业务操作

数字化应急预案

### 系统韧性能力

#### 高可用

异地容灾高可用  
微服务高可用  
热备高可用  
负载均衡高可用  
db高可用集群  
缓存高可用设计

#### 降级

业务整体降级  
非关键业务降级  
链路弱依赖降级  
调度任务降级  
功能或用户降级  
接口降级

#### 限流

应用限流  
接口限流  
业务限流  
用户限流  
IP限流  
时间窗口限流

#### 切换

应用切换  
容灾切换  
依赖应用平台切换（  
db\中间件\应用平台  
）

#### 重置

主机重启  
应用重启  
依赖平台重启  
程序回滚  
配置回滚  
数据回滚

#### 隔离

服务隔离策略  
资源隔离  
数据隔离  
进程隔离  
网络隔离

#### 其他韧性设计

异步处理  
重试  
自愈策略  
弹性伸缩  
超时  
灰度



# 全生命周期故障管理

左移内建系统稳定性：为应急提供更多手段

构建主动变更防御和管控分析：提前发现解决故障风险







# 运维左移

- 架构韧性模型
- 左移工作机制
- 左移工程性实践





# 运维左移：架构韧性模型

“稳定性是设计出来的！”

- 了解“Design for failure”思维
- 不是架构师，但需要懂架构
- 提前介入，主动参与

L5 跨系统间止损免疫

L4 可止损隔离（自愈/半自愈）

L3 可热操作止损（无单点风险）

L2 具备逃生通道（可恢复）

L1 基础保障级

架构韧性  
L1~L5模型





# 运维左移：上线架构评审

- 新系统立项及上线，必须通过TC评审
- TC委员会包括各条线运维专家，将非功能性需求和稳定性保障要求纳入评审范围

## 应用架构

服务模块  
内部关键逻辑  
接口规范  
负载评估  
基础能力复用  
关联改造

## 数据架构

数据架构图  
数据对接评审（量/并发）  
数据生命周期  
数据治理  
依赖治理

## 技术架构

技术架构图  
前端技术评审-缓存/CDN  
前后端技术栈  
中间件/开源组件治理  
Devops/CI/CD接入评审  
日志接入规范  
服务治理（状态/顺序/优雅停止）  
云原生适配评估

## 部署架构

部署架构图  
备份及容灾  
存储容量评估  
运维支撑及监控  
网络流量  
业务连续性及应急

### 规范指引名称

### 一级类型

广发证券PostgreSQL、TDSQL PostgreSQL数据库开发技术规范

技术类规范

广发证券GoldenDB数据库开发技术规范

技术类规范

广发证券企业级API网关使用规范

技术类规范

广发证券软件开发Python语言编程规范

技术类规范

广发证券信息系统接口安全检测规范

技术类规范

广发证券中后台系统交互与视觉设计规范

技术类规范

广发证券信息技术部信息系统监控管理规范

技术类规范

广发证券Kafka分布式消息中间件使用规范

技术类规范

广发证券Redis分布式缓存中间件使用规范

技术类规范

广发证券系统日志设计规范

技术类规范



# 运维左移：架构韧性评审站会

- 开放、宽容的讨论氛围
- 专注架构韧性探讨，定期开展持续提升运维能力



评审站会现场照片

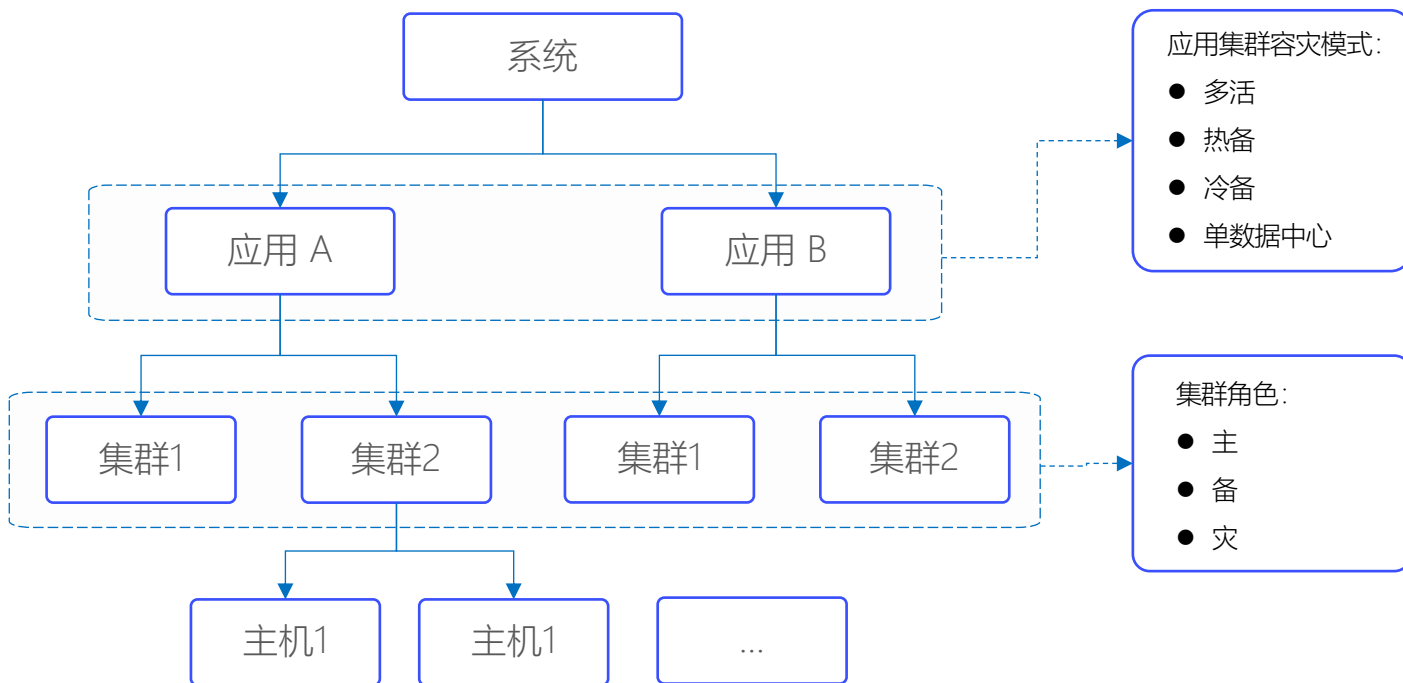
系统架构韧性评价表

运营数智化系统架构韧性评价表					
L1(基础保障)			L4(可止损隔离)		
保障措施	评价标准	评价结果	保障措施	评价标准	评价结果
基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合	基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合
基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合	基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合
基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合	基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合
基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合	基础保障：基础保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。基础保障的健壮性是系统韧性的基础。	基础保障资源充足，且具备冗余能力。	符合
L2(冗余逃生通道)			L5(跨系统防止级联)		
保障措施	评价标准	评价结果	保障措施	评价标准	评价结果
冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合	冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合
冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合	冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合
冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合	冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合
冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合	冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合
冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合	冗余保障：冗余保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。冗余保障的健壮性是系统韧性的基础。	冗余保障资源充足，且具备冗余能力。	符合
L3(可控操作止损)			评价汇总		
保障措施	评价标准	评价结果	韧性保障能力	韧性保障能力	韧性保障能力
韧性保障：韧性保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。韧性保障的健壮性是系统韧性的基础。	韧性保障资源充足，且具备冗余能力。	符合	L1(基础保障)	符合	符合
韧性保障：韧性保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。韧性保障的健壮性是系统韧性的基础。	韧性保障资源充足，且具备冗余能力。	符合	L2(冗余保障)	符合	符合
韧性保障：韧性保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。韧性保障的健壮性是系统韧性的基础。	韧性保障资源充足，且具备冗余能力。	符合	L3(可控操作止损)	符合	符合
韧性保障：韧性保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。韧性保障的健壮性是系统韧性的基础。	韧性保障资源充足，且具备冗余能力。	符合	L4(可止损隔离)	符合	符合
韧性保障：韧性保障是系统运行的基石，包括网络、计算、存储、安全等基础资源。韧性保障的健壮性是系统韧性的基础。	韧性保障资源充足，且具备冗余能力。	符合	L5(跨系统防止级联)	符合	符合



# 运维左移：推动应用消除单点风险（达成架构韧性L3）

- 根据CMDB数据层级模型，抽象出筛查模型
- 构建筛查报表以及实时监控工具



结合**集群所在机房、主机存活状态**等信息：

- 存在单点风险问题的应用筛查
- 机房级异常对所有应用的影响评估

以此为依据**推动架构优化或实时监控**

规划：结合混沌工程，以工程化手段不断推动架构优化





# 变更管控

- 变更生命周期管控
- 变更操作执行痛点
- 主动变更防御
- 变更感知与风险分析





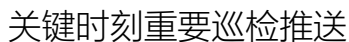
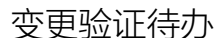
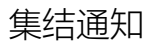
# 变更管控

变更是**稳定性的第一杀手**

对于证券公司更是丝毫不敢懈怠，因为变更后业务流量很可能面临**上线即高峰**的处境  
交易系统的变更一般有**按周迭代**、**变后测试验证**、**首日重点保障**的特点

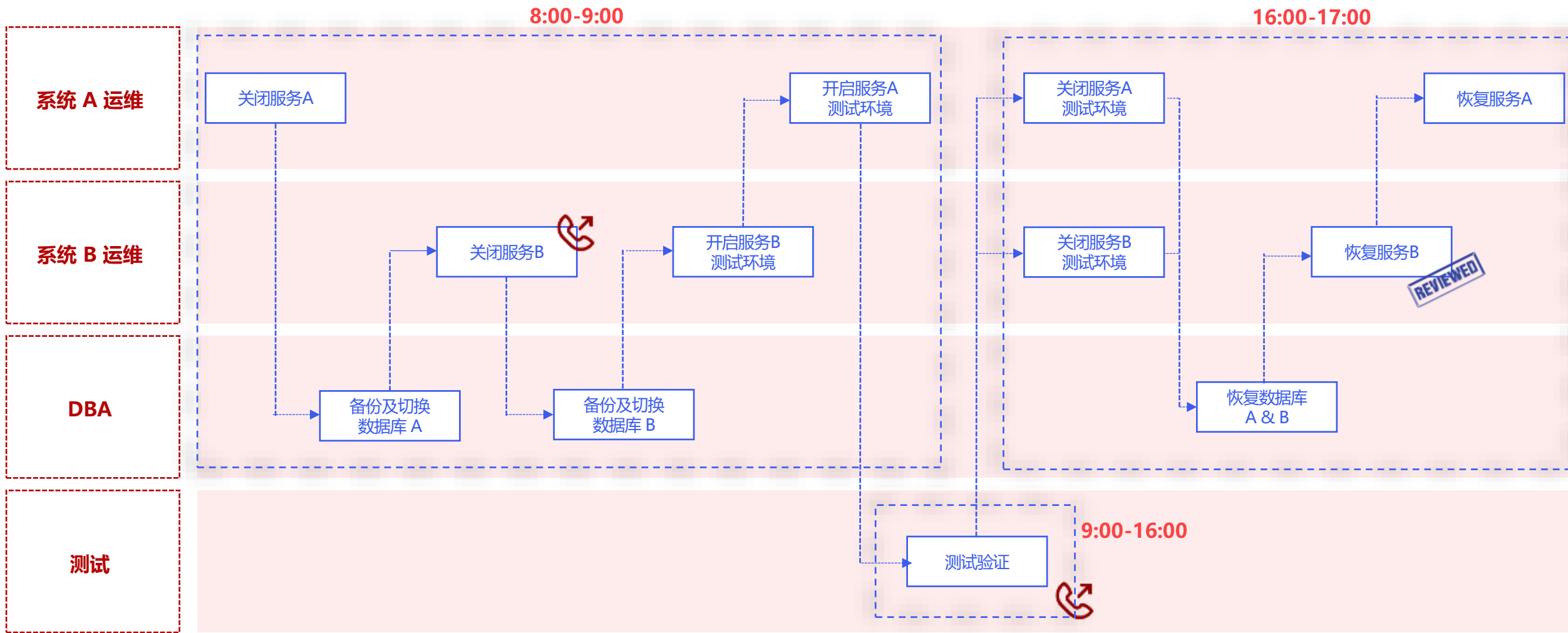


- **变更验证表**：自动变更验证提醒督办，确保开闸前完成验证闭环
- **集结通知**：自动化通知相关人员集结保障
- **巡检推送**：聚焦关键时刻时系统、数据状态，做到心里有数



# 变更管控：大规模跨团队变更时序管控

**时序工具，确保需要各岗位人员间协同的操作不早做、不晚做、不漏做**



# 变更管控：大规模跨团队变更时序管控

提前沟通对齐信息与导入，时序工具**自动按时提醒**，**逾期自动升级督办**

任务项	2024-10-17	2024-10-18	2024-10-19
[A] 运营系统(117)运营数据平台(117)数据测试			<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div> <div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[B] 运营系统(117)运营数据平台(117)数据测试		<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div>	<div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[C] 运营系统(117)运营数据平台(117)数据测试		<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div>	<div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[D] 运营系统(117)运营数据平台(117)数据测试			<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div> <div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[E] 运营系统(117)运营数据平台(117)数据测试			<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div> <div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[F] 运营系统(117)运营数据平台(117)数据测试			<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div> <div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[G] 运营系统(117)运营数据平台(117)数据测试			<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div> <div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>
[H] 运营系统(117)运营数据平台(117)数据测试			<div>01 117 运营数据平台(117)数据测试</div> <div>02 117 运营数据平台(117)数据测试</div> <div>03 117 运营数据平台(117)数据测试</div> <div>04 117 运营数据平台(117)数据测试</div> <div>05 117 运营数据平台(117)数据测试</div>

时序配置汇总

已办任务
hi, 运营部, 欢迎你来到时序看板工具
<div>我的待办</div> <div>所有任务</div> <div>处理中看板</div> <div>历史看板</div>
请输入搜索子任务名
2024-10-18 >
与我相关 >
2024-10-18 17:00:00 - 2024-10-18 19:30:00
父任务: 周末内部测试20241019 运营数据平台(117)数据测试
时序计划: 周末测试任务时序看板20241019
2024-10-18 17:00:00 - 2024-10-18 19:30:00
父任务: 周末内部测试20241019 运营数据平台(117)数据测试
时序计划: 周末测试任务时序看板20241019
2024-10-18 17:00:00 - 2024-10-18 19:30:00

个人任务列表

数字化周末测试任务群(J)
周末测试机器人助手 BOT
<b>【时序工具逾期任务催办】</b>
计划名称: 周末测试任务时序看板 20241019
@运营部 有 4 项子任务逾期 (AC3 AC21 AC40 AC58)
@运营部 有 6 项子任务逾期 (AC5 AC14 AC24 AC42 AC51 AC61)
任务【AC】周末测试环境强化管理测试环境准备任务 有 10 项子任务逾期
请总协调人 @运营部 跟进
请各位尽快处理: 查看待办 @运营部 @运营部

逾期升级督办





# 变更管控：痛点分析

01

## 事前变更影响难评估

审批依赖经验，难以全面评审  
审批依赖的信息与实际操作脱钩  
跨团队跨系统关联影响难评估

02

## 操作不标准引发操作风险

常规操作执行动作不统一，无沉淀复用  
关键步骤遗漏  
技术检查与验证不到位

03

## 高危变更无事中管控

高危时段、高危变更场景无管控  
缺少阻断机制，无法快速止损

04

## 变更对象关键变化无感知

变更对象稳定性因子通常引发故障  
无法有效感知稳定性因子的异常变化  
无事后分析预警

05

## 变更操作行为无感知

缺乏全局变更操作事件感知  
无法获取跨团队关联变更操作信息  
非预期操作行为无预警和事后审计分析

06

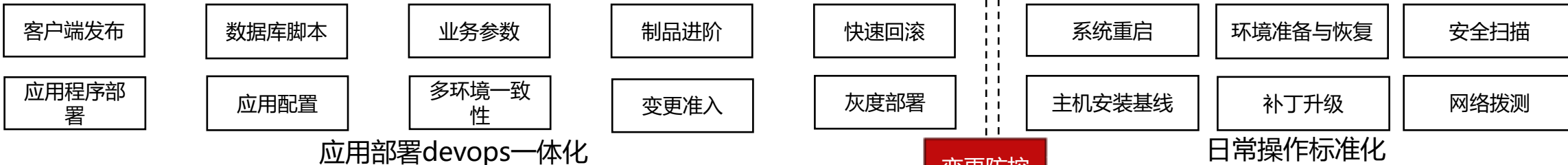
## 故障快速定位引发的变更难

缺乏全局变更信息，无法定位什么变更  
导致故障  
变更流程无法准确定位具体变更对象变  
化和操作事件

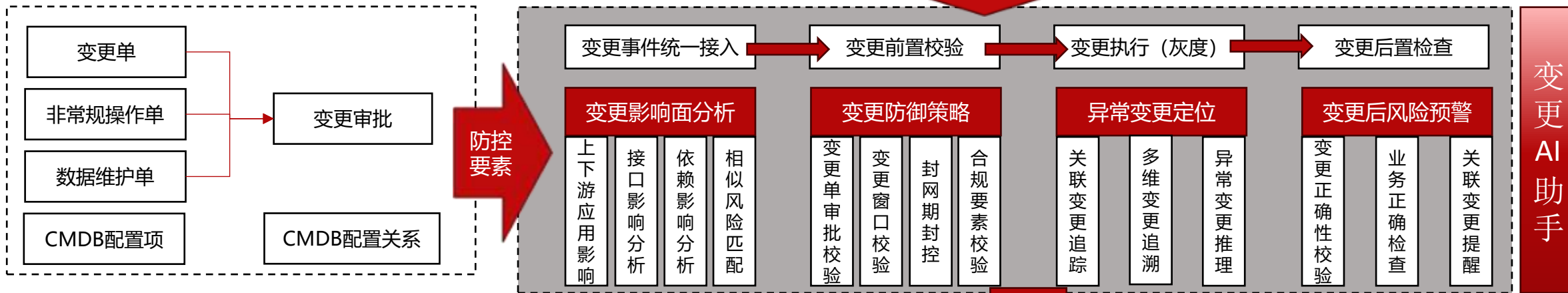


# 变更管控：管控全景

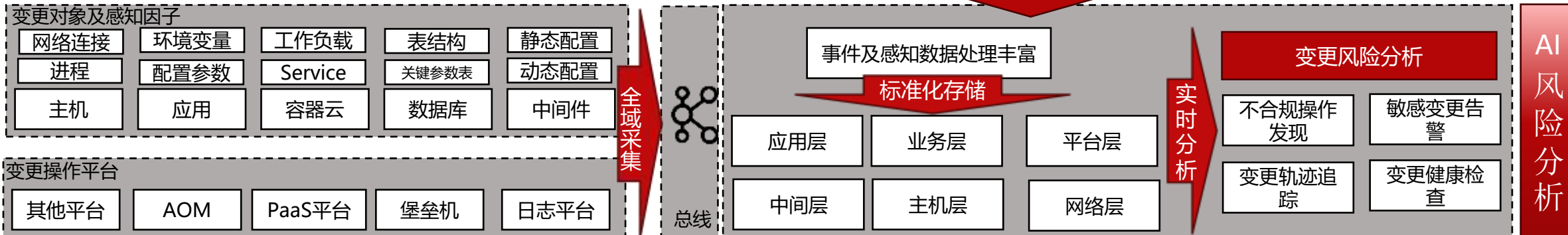
## 变更场景



## 变更防御

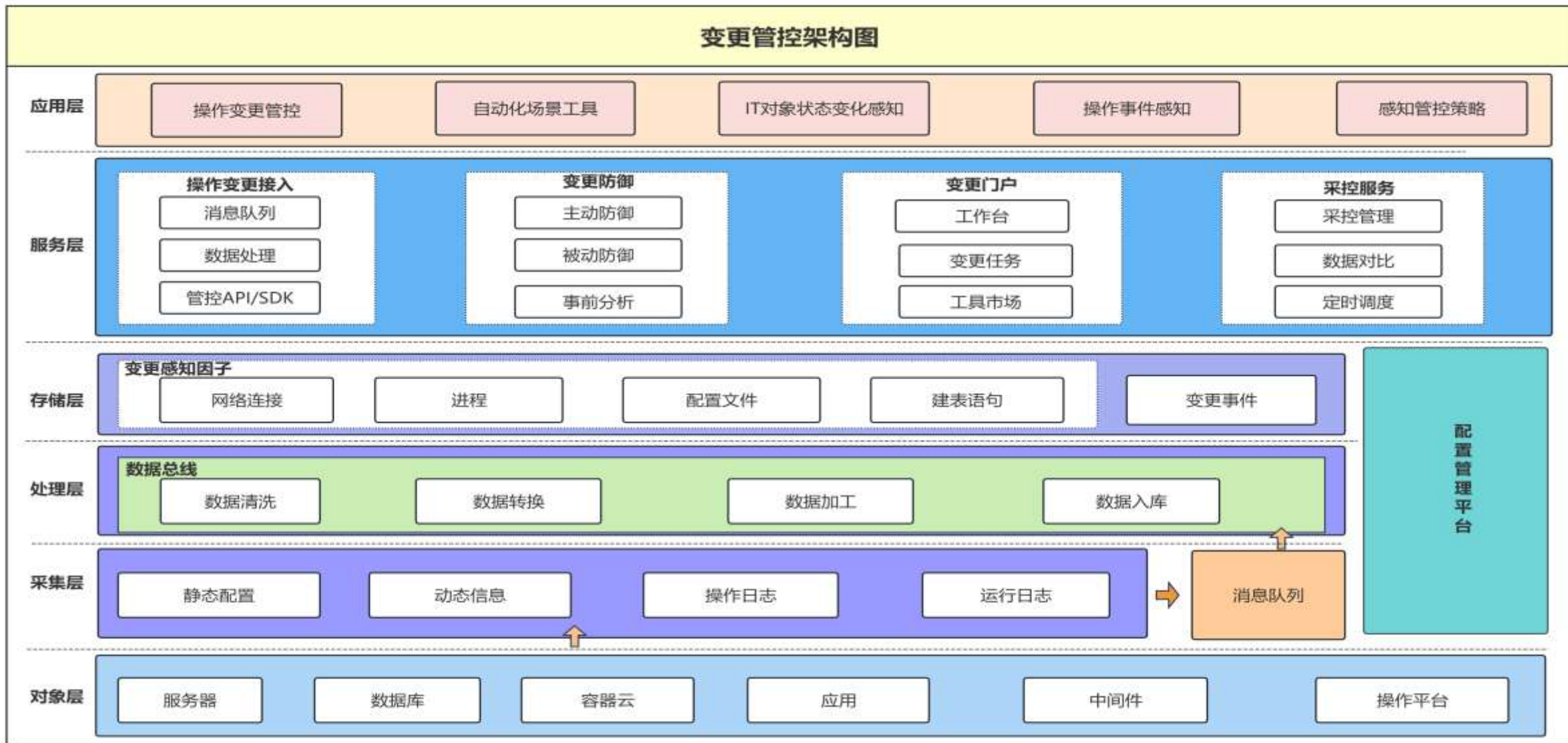


## 变更感知分析



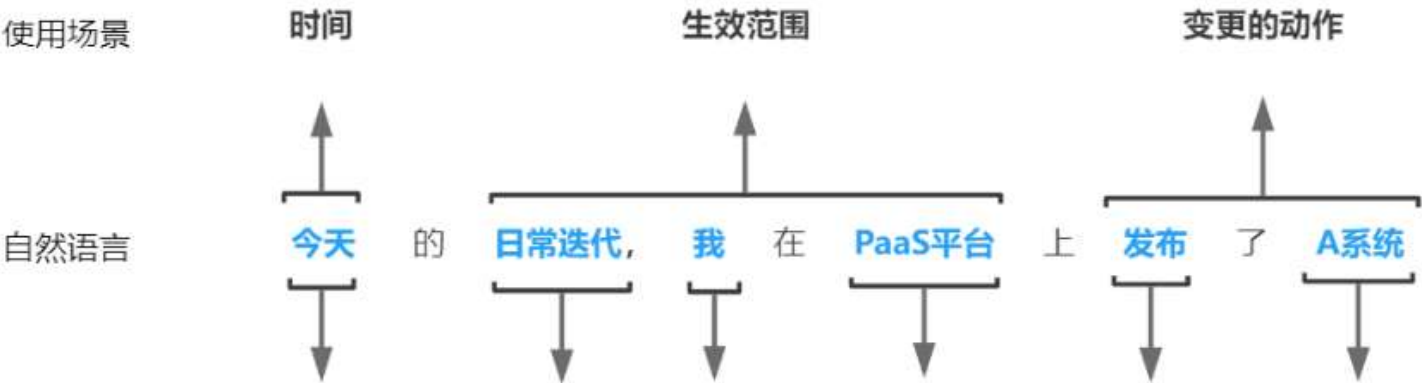


# 变更管控-系统架构





# 变更管控：建模-变更事件



五元组

补语1	状语	主语	补语2	谓语	宾语
变更的时间, 即 在什么时间 发起	变更的情景, 即 在什么情景 下 做了操作	变更的操作者, 即 谁 发起了这次变更	变更的环境, 即 在什么系统 中做了操作	变更的动作, 即 做了什么操作	变更的作用对象, 即 对什么 做了操作

变更事件



工单  
CMDB配置等



变更上下文

注：参考蚂蚁变更管控开源项目AlterShield（<https://altershield.io>）

# 变更管控：建模-变更感知因子

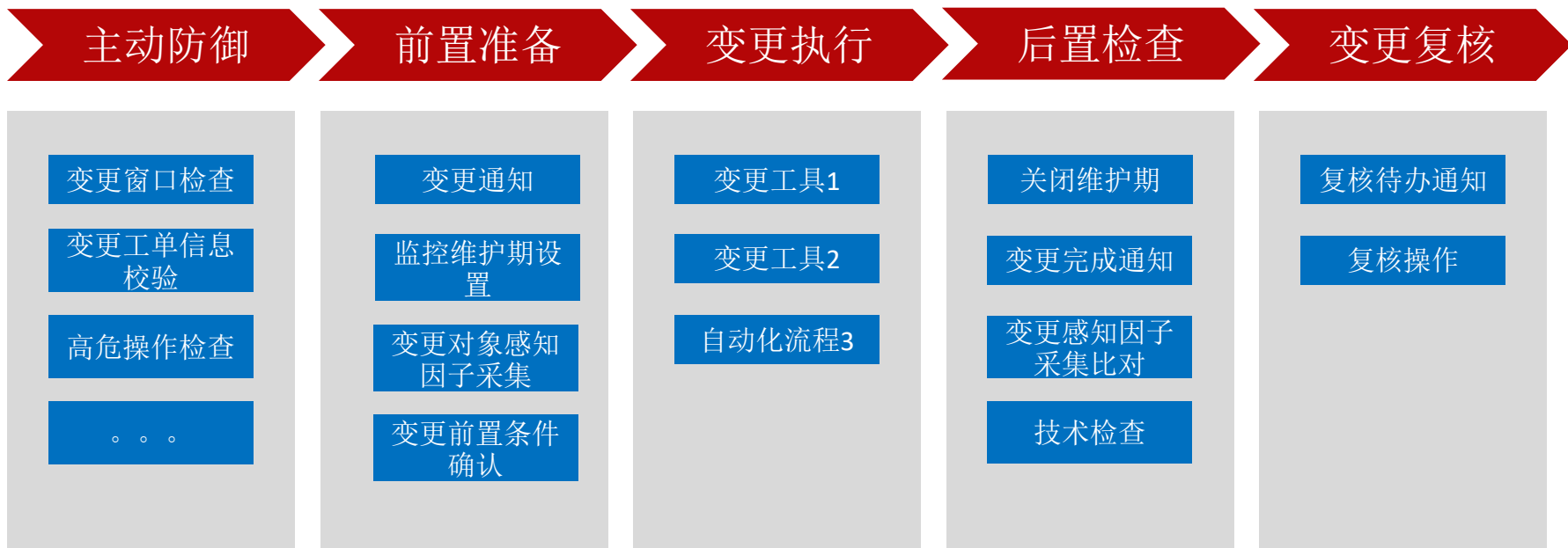
变更感知因子：由变更操作导致的系统关联IT对象部署运行状态变化的因素  $\neq$  可观测指标







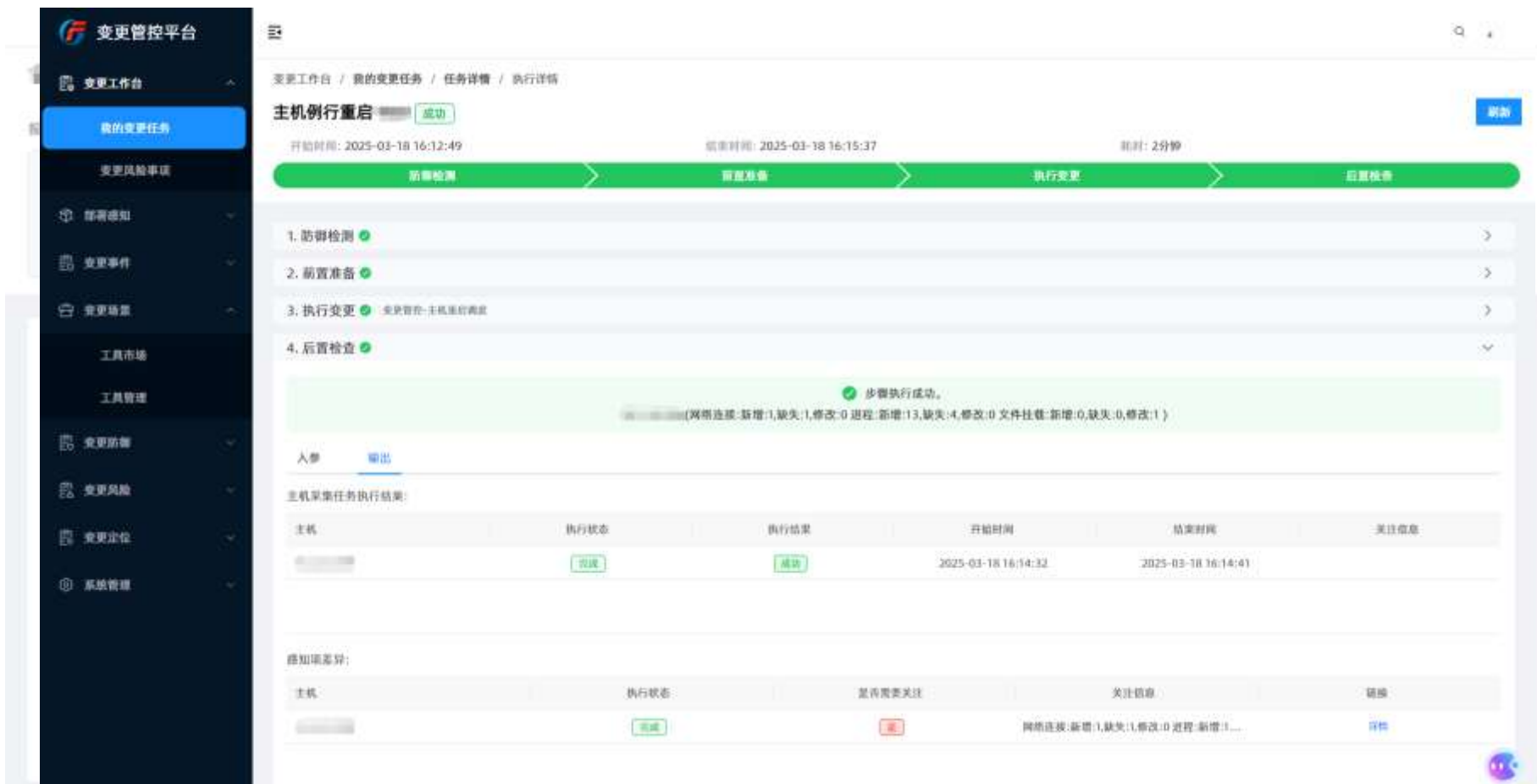
# 变更管控：标准化变更操作工具



- 能力原子化
- 标准化编排
- 主动防御
- 落实合规要求（双人复核/线上留痕）
- 工具共建共享



# 变更管控：标准化变更操作工具



The screenshot displays the '变更管控平台' (Change Management Platform) interface. The left sidebar contains navigation options: 变更工作台, 我的变更任务, 变更风险申请, 部署感知, 变更事件, 变更场景, 工具市场, 工具管理, 变更防微, 变更风险, 变更定位, and 系统管理. The main content area shows a task titled '主机例行重启' (Host Regular Restart) with a status of '成功' (Success). The task details include the start time (2025-03-18 16:12:49), end time (2025-03-18 16:15:37), and a duration of 2 minutes. A progress bar indicates the task is completed. Below the progress bar, a list of steps is shown: 1. 防微检测 (Prevention Detection), 2. 前置准备 (Preparation), 3. 执行变更 (Execute Change), and 4. 后置检查 (Post-check). The '执行变更' step is highlighted, showing a success message: '步骤执行成功。' (Step execution successful). Below this, a table lists the execution results for various components, including network connections, processes, and files. The table has columns for '主机' (Host), '执行状态' (Execution Status), '执行结果' (Execution Result), '开始时间' (Start Time), '结束时间' (End Time), and '备注信息' (Remarks). The '主机' column shows '主机' (Host) and the '执行状态' column shows '完成' (Completed). The '执行结果' column shows '成功' (Success). The '开始时间' column shows '2025-03-18 16:14:32' and the '结束时间' column shows '2025-03-18 16:14:41'. The '备注信息' column shows '网络连接:新增:1,缺失:1,修改:0 进程:新增:13,缺失:4,修改:0 文件挂载:新增:0,缺失:0,修改:1'.

- 前置准备：重启前采集变更感知因子
- 变更操作：发起重启，轮询至重启完毕
- 后置检查：重启后采集变更感知因子，完成2次采集结果比对



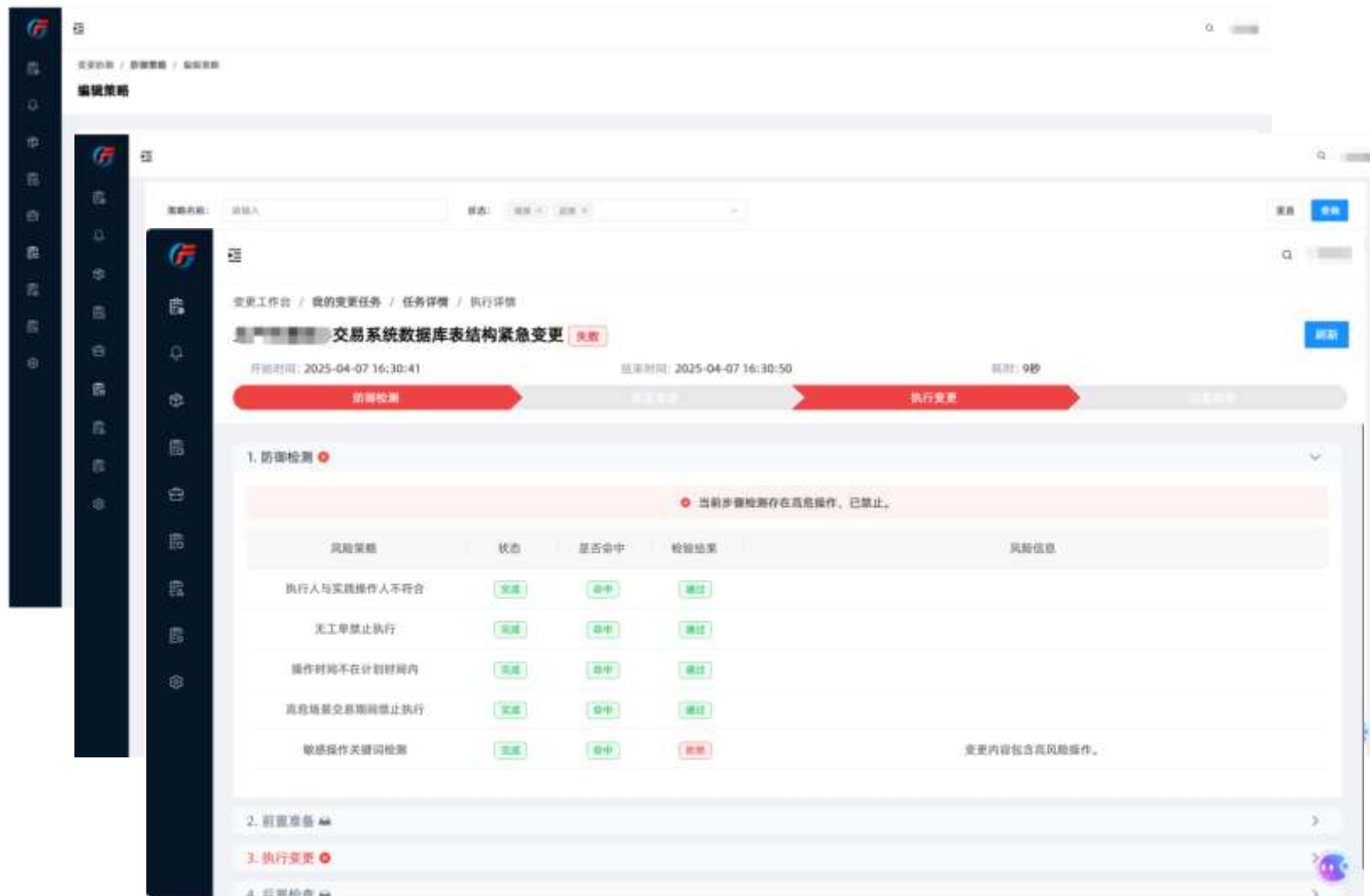
# 变更管控：主动防御

效果：

- 基于变更事件（上下文）的规则防御
- 风险前置拦截：在变更执行前识别潜在风险
- 过程强管控：约束高风险操作（如生产环境数据维护）

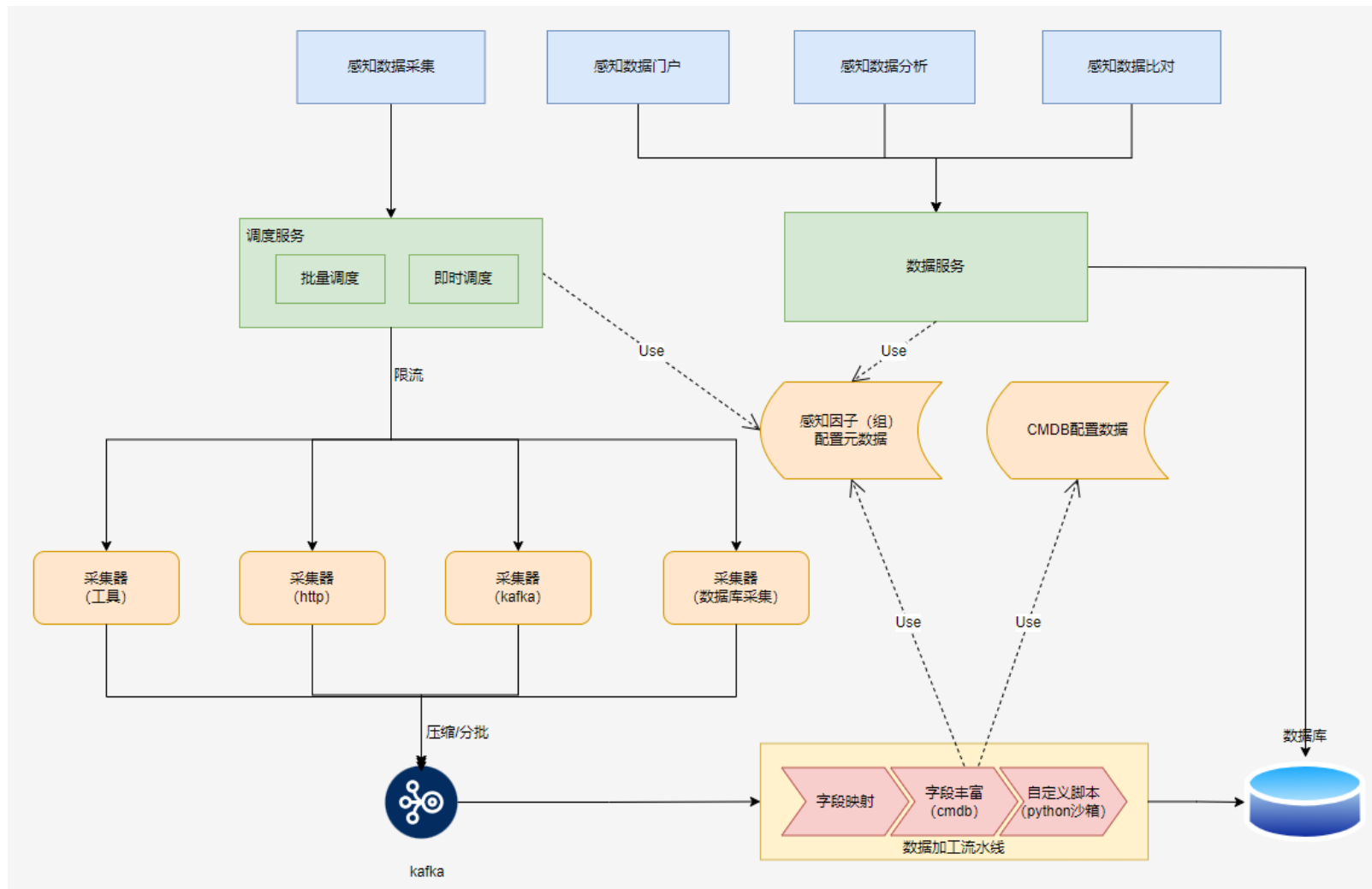
计划：

- 变中快速止血：异常变更实时阻断或自动回滚；
- 数据可追溯：记录变更全链路数据，辅助根因分析。





# 变更管控：变更感知采集逻辑



## 可扩展感知因子采集插件

```
import psutil
from sensors.base import BaseSensor

class OsNetConnSensor(BaseSensor):
    SENSOR_ID = 'os.netconn'
    def collect(self):
        conns = psutil.net_connections(kind='inet')
        for conn in conns:
            yield conn._asdict()
```

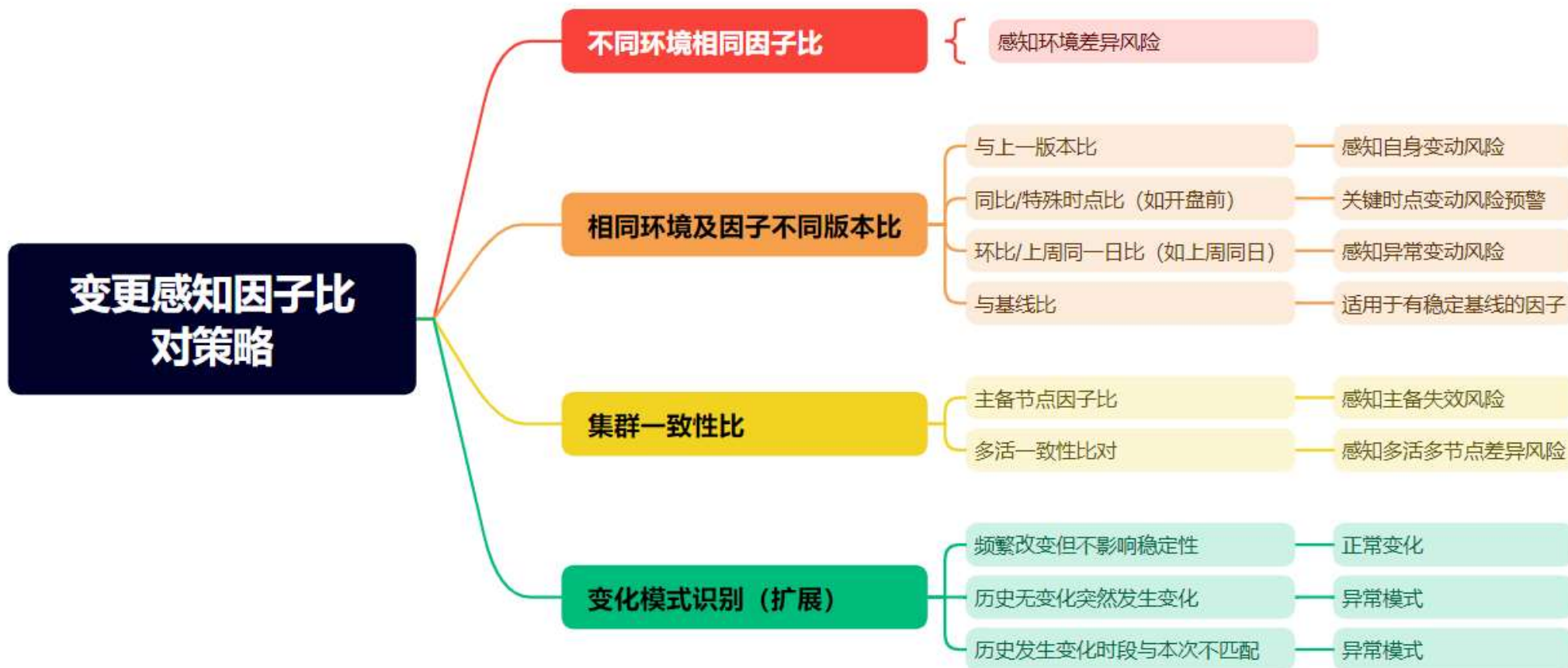
## 统一感知因子命名



## 计划：感知因子自发现



# 变更管控：变更感知比对策略





# 主机

- 10000+主机
- 10+感知因子，持续扩展
- 兼容windows/linux/信创os

# 数据库

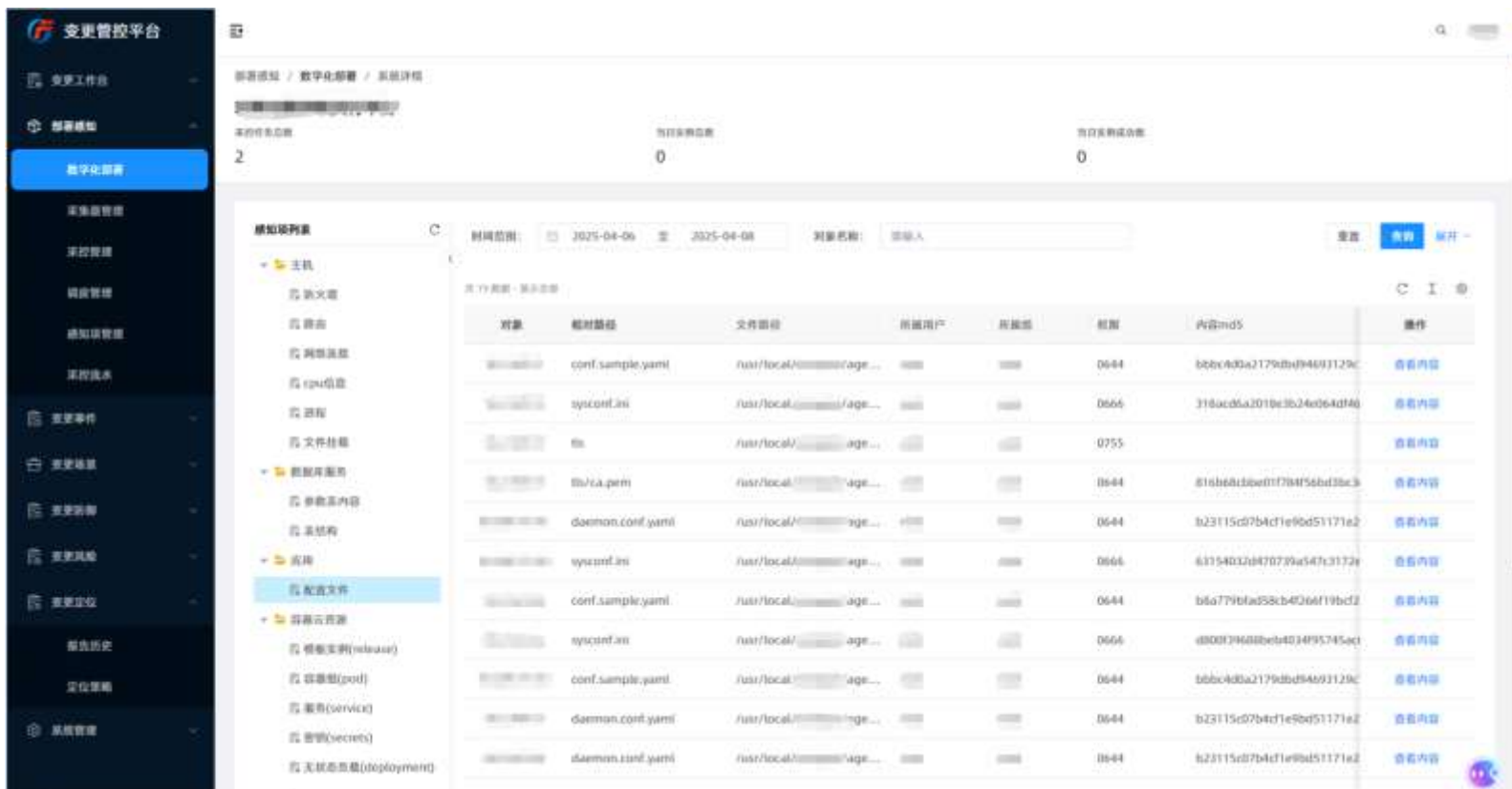
- 表结构
- 关键业务参数表
- oracle/mysql/pgsql/goldendb/tdsql/...

## 程序及配置

- 重要系统程序及关键配置
- 测试+生产多环境比对
- 比对预警确认闭环

# 容器云资源

- 200+系统
- 700+命名空间
- 8000+helm实例
- Deployment/Service/Release/Pod/...





# 变更管控：数字化变更感知场景

## 【部署感知对比异常提醒】

调度名：调度1

异常版本：process\_41\_20241223120000508

发生时间：2024-12-23T12:00:00

异常内容： (新增:3,缺失:0,修改:0)

[查询详情](#)

<@Z >

注：请及时点击详情链接处理。

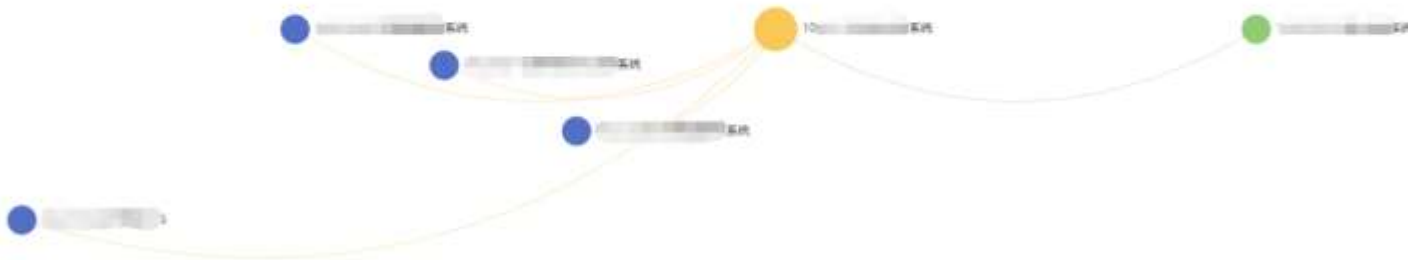
## 主机进程状态比对

主机状态 > 主机运行画像

主机性能 访问关系

☒ 展示ip ☒ 展示系统 ☐ 异常主机

☒ 下游系统 ☒ 上游系统 ☐ 当前系统



## 清洗IP访问关系

4/14 08:00:15

您好，您负责的配置文件有未确认的变动更改(总数1条)，请及时查看并确认

应系统 - 系统-C Proxy

[变动：添加1个文件;修改1个文件]

1、文件路径：/usr/local/nginx/conf, IP: 1

详情列表链接(如没有该任务则已被其他负责人确认)： [点击](#)

## 关键配置文件比对



# 变更管控：变更事件态势感知



## 标准变更工具

- 主机重启
- 开闭市
- 周末测试环境准备恢复
- 主机基准初始化
- 服务启停应急
- 数据维护



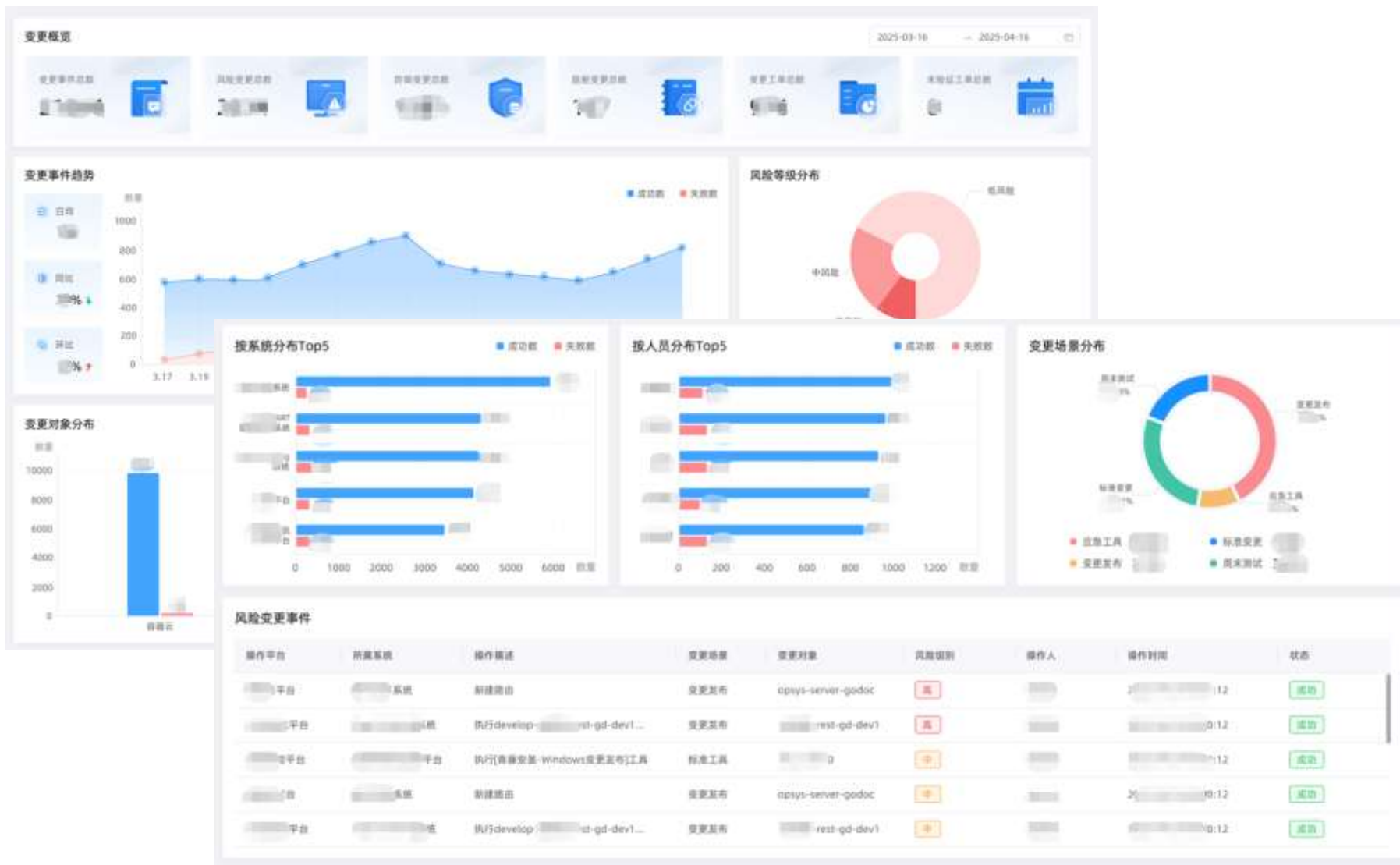
## 平台变更事件

- 容器云平台
- 持续交付平台
- 自动化平台
- 数据库管控平台
- 统一网关
- 中间件云平台



## 非标变更事件

- 堡垒机
- 业务系统管理端
- 内容管理平台
- ...



# 应急指挥

- 应急保障体系
- 一站式应急总线
- 事件处理流程
- 数字化应急预案



# 应急指挥：应急保障体系

## IT运营指挥中心 (ECC)

- 主要包括故障监测、应急指挥、数据运营、重大演练等核心职能
- OnCall 人员的值守、应急作战指挥室的线下场所







# 应急指挥：应急保障体系

## OnCall 值班

### 故障指挥官

Incident Commander



全面协调和管理整个故障响应过程，做出关键决策，确保团队高效协作

### 通讯官

Communications Lead



负责内外部沟通，及时更新利益相关者，管理事故状态页面，协调跨团队合作

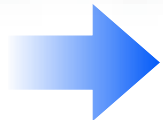
### 执行官

Operations Lead



深入技术分析，执行故障诊断和修复操作，提供专业技术建议

借鉴 & 适配



统筹管理  
资源协调  
应急指挥  
值班质控  
盘后复盘

值班经理  
统筹管理

一线运维  
值班岗  
快速恢复

在线监测、巡检  
异常申报  
应急响应  
诊断定位  
业务恢复

二线运维专家支持  
测试复现与验证  
研发代码排查与修改  
产品业务逻辑分析  
项目资源协调

二三线  
协同支撑

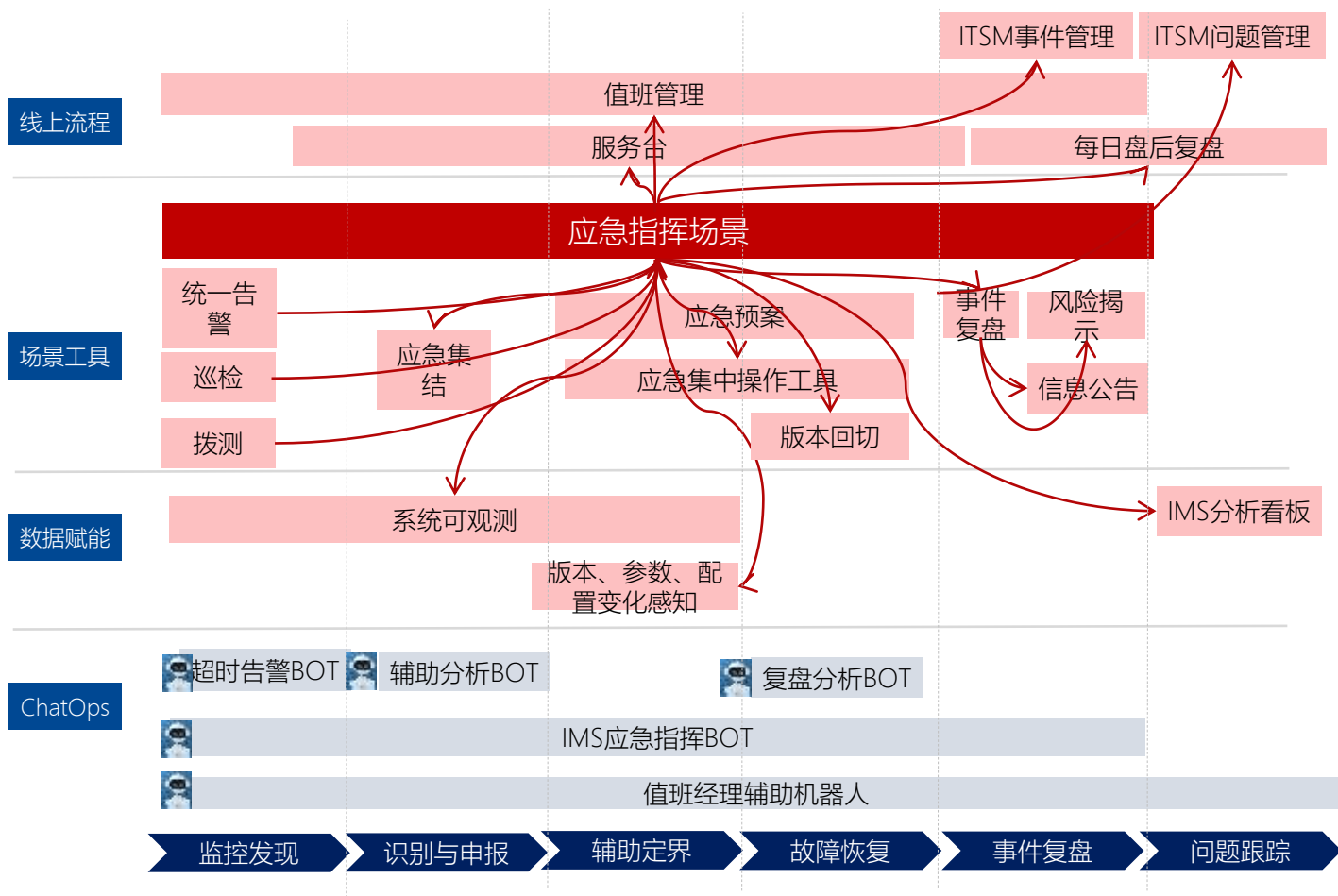
ChatOps  
人机协同

监控告警响应机器人  
应急管理辅助机器人  
值班经理助手  
OnCall机器人  
巡检机器人



# 应急指挥：一站式应急总线


用户能够在**秒级**时间内建立应急连接，达到数据汇总、信息融合、运行感知、人机协同、工具互联的一站式协同“**总线**”作用，实现全面感知、精准决策、协同高效、指挥有效












































- 建立**一站式**的应急总线系统，可以实时洞察应急过程，**连接**与应急相关的工具、数据、流程的指挥系统
- **多角色**：公司领导、技术部门领导、运维值班经理、运维岗、研发岗、测试岗、产品需求岗、外联岗等，且支持扩展到上下游相关岗位
- **多终端**：PC、移动、IM、大屏多端的在线协同
- **多渠道**：支持**自动**与人工**秒级**启动，包括集结、建群、机器人、电话、OA待办等10+种丰富的资源调度手段
- **人机协同**：多种类型的**专业性机器人**辅助应急指挥，连接**可观测数据**辅助应急
- **持续提升**：以各种“**小事件**”**实战**提升团队面对复杂故障的应急能力，在线数据赋能问题的发现，提升**应急管理水平**



# 应急指挥：标准化事件处理流程


IMS-20240717-002 

异常事件状态: 已处置

异常内容:                                         

异常事件详情 宿主机影响分析 前三个交易日变更 告警事件 下游系统影响确认表

> 根因定位 异常挂起 异常恢复 提供方案 异常验证 异常撤销 异常复核 异常关闭 异常升级 异常定位说明(无需干预) 故障调级 专家协助 异常处置进展跟踪 外部报告 汇报影响范围 48小时督办 提出跟进内容 推荐处置

> 优化建议 

发生 2024-07-17 15:01:30

发现 2024-07-17 15:01:32

响应 2024-07-17 15:03:53

处置 2024-07-17 15:04:30

恢复 2024-07-17 15:05:45

复盘 2024-07-17 17:12:16

定位 2024-07-17 16:00:47

发现时长  
注: 发现时间 - 发生时间  
2秒

响应时长  
注: 响应时间 - 发现时间  
2分钟

界定时长  
注: 第一次挂起前的异常定位说明 (无需干预) /异常定..  
37秒

止损时长  
注: 第一次挂起/恢复的时间 - 第一次挂起前的异常定位..  
9秒

根因定位时长  
注: 定位时间 - 事件发生后12小时内第一个挂起/恢复的..  
56分钟





























































































彻底恢复时长  
注: 恢复时间 - 最后处置时间  
75秒

类型:

重置

查询

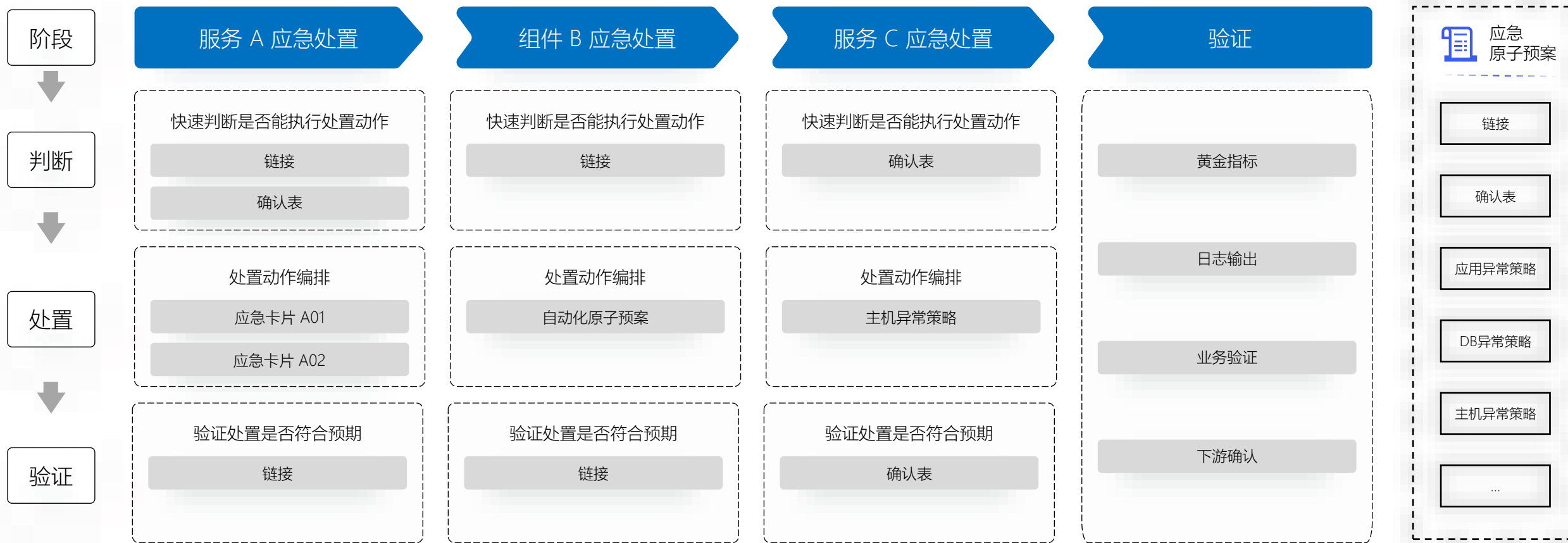
异常处置流水

登记时间	实际时间	类型	执行人	执行结果	执行说明	操作
2024-07-17 15:03:53	2024-07-17 15:03:53	异常申报				<a href="#">查看预案</a>
2024-07-17 15:04:30	2024-07-17 15:04:30	异常定位说明(无需干预)			                   	<a href="#">作废</a>
2024-07-17 15:05:24	2024-07-17 15:04:40	异常挂起			                     	<a href="#">作废</a>
2024-07-17 16:00:06	2024-07-17 16:00:06	根因定位督办				<a href="#">作废 处理</a>
2024-07-17 16:01:09	2024-07-17 16:00:47	根因定位			                    	<a href="#">作废</a>
2024-07-17 17:07:52	2024-07-17 15:05:45	异常恢复		有效	                     	<a href="#">作废</a>
2024-07-17 17:12:16	2024-07-17 17:12:16	复盘分析				

GOPS 全球运维大会暨研运数智化技术峰会 2025 · 深圳站

# 应急指挥：数字化应急预案

- 原子化：打造可复用的预案，为预案流程的编排、更新、关联自动化提供便捷
- 数字化：提供预案可编排、可演练、可统计、可遍历、可自愈的能力，可持续扩展





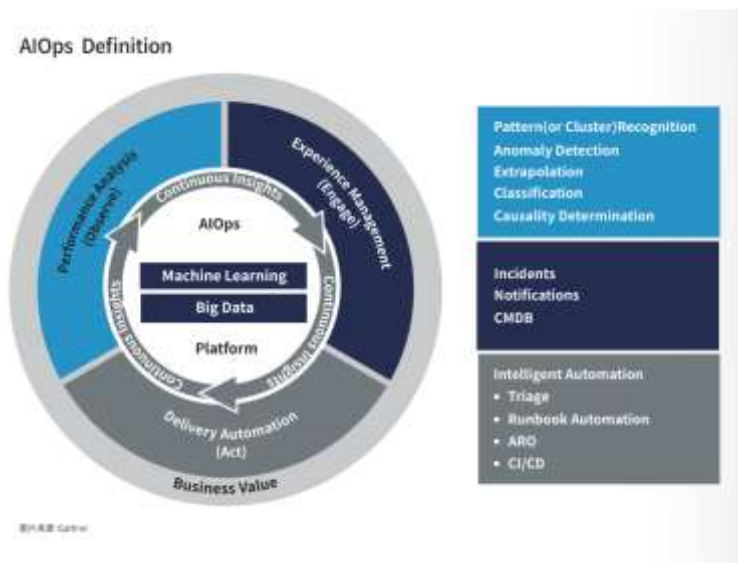
# 智能化与场景融合

- 广发证券对智能运维理解
- 运维平台智能化升级思路
- 案例分享





Gartner提出了AIOps的理念，定义为：AIOps平台的人工智能将大数据，AI 机器学习和其他技术相结合，通过主动，个性化和动态的洞察力支持所有主要IT运营功能。AIOps平台支持同时使用多个数据源，数据收集方法，分析技术和可视化等技术。算法式的智能运维主要应用在指标与日志数据分析，仅适用于部分应用场景。随着大模型的兴起，新增了**生成式智能运维发展路线**，形成“**传统智能算法+专家经验+平台智能体+生成式算法**”相结合的人机协同的智能运维发展。



+ 新对话

1

编辑时间：17:26

复制 下载

我将结合大模型对智能运维的启示，从你提到的多个维度，对传统基于半监督的算法式智能运维与生成式 AI 智能运维模式展开对比，突出两者的差异和特点。每一点的对比的内容简洁扼要点，通俗易懂（约20字以内）

我会用更直白的语言，在 20 字以内简洁表述各维度对比，突出差异。

传统半监督算法式与生成式AI智能运维模式对比

要是你对修改后的内容还有想法，比如增减细节，调整表述，欢迎随时提。

生成式AI智能运维的应用场景有哪些？→  
如何进一步优化传统半监督算法式智能运维？→  
大模型在智能运维领域的未来发展趋势是什么？→

帮我写作 图像生成 AI 搜索 AI 阅读 更多

### 传统半监督算法式与生成式 AI 智能运维模式对比

对比项目	传统基于半监督的算法式智能运维	生成式 AI 智能运维
工作原理	用少量标注和大量未标注数据建模	大模型先学再调，找数据隐藏规律
学习数据	主要用指标数据，少量人工标注	融合各种数据，啥都能学
学习能力	用未标注数据，适应新场景弱	大数据学习，适应新场景强
优势	标注少也能训练，算法不复杂	诊断疑难故障，给出周全方案
局限	依赖人工标注，新问题难处理	训练费资源，不知咋做的决策
主要应用场景	数据稳定、故障常见的情况	复杂系统和要求高的运维场景
对于人机协同模式的帮助	帮着核对处理，完善标注数据	给分析建议，和人配合超高效

总结：生成式 AI 优势明显，传统模式也有用。协同发展。



# 对智能运维的理解



打造智能化的人机协同运维体系，通过智能技术与专家经验沉淀，构建一系列具备专业技能的机器人，辅助运维专家感知、决策与执行。

## 持续提升以下能力：

- 实时获得“发生了什么？”；
- 关联分析“为什么会发生？”；
- 智能预测“将会发生什么？”；
- 决策判断“采取什么措施？”；
- 自动执行“如何快速执行？”
- 实时感知“工作执行的效果？”

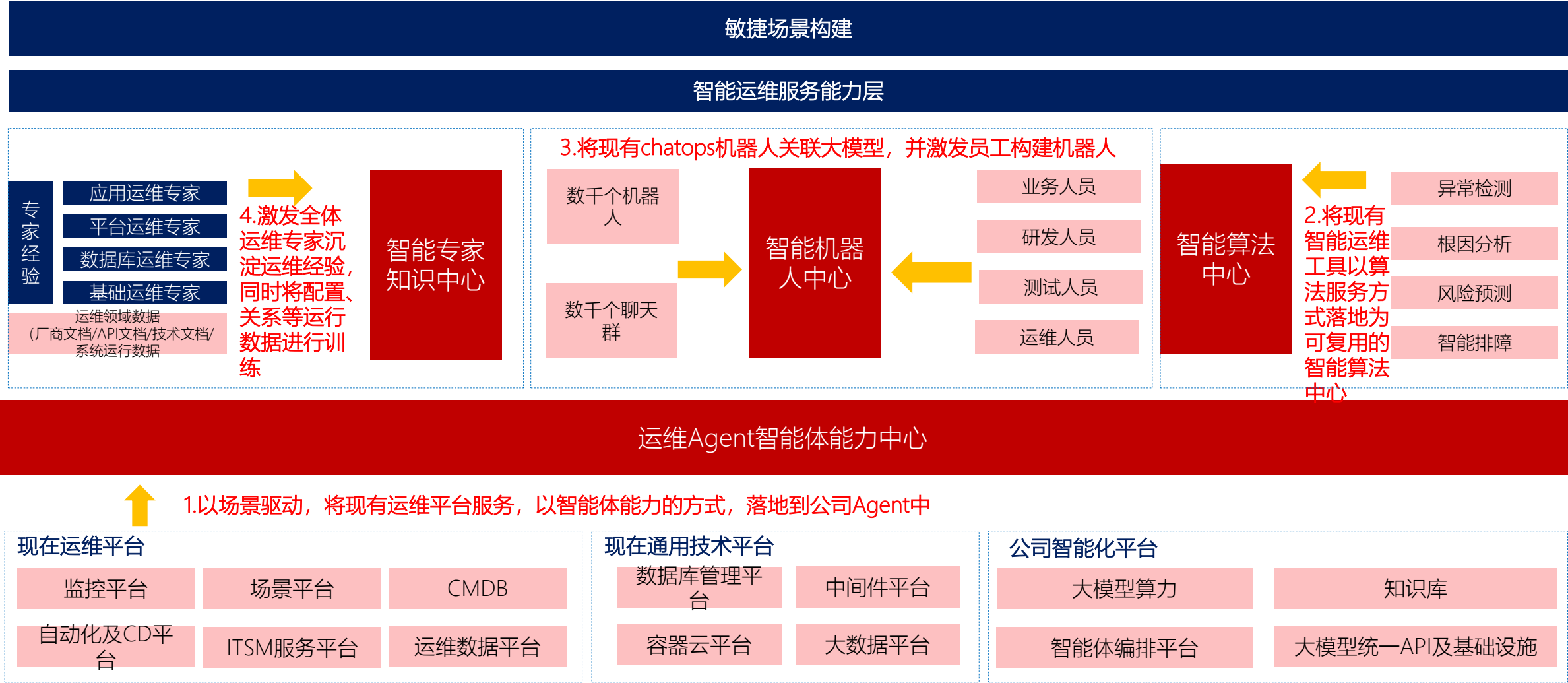
## “人机协同”关键点

发挥运维专家与机器人特点，通过“数据+平台”管理；

- 沉淀专家经验
- “数据+算法”为运维专家赋能“实时感知、辅助决策”；
- 增加运维机器人岗位，完成或重塑“操作性”、“规律性”、“大计算”、“7\*24”、“人机体验”等类型工作；
- 建立平台化管理，落实决策执行；



# 智能运维建设：整体思路







## 全局智能助手

- 动态加载智能体
- 页面上下文感知
- 集成知识库问答, 智能体 workflow 编排

## 无代码AI+ChatOps

- 运维知识库管理: 上传更新
- 基于知识库问答
- 企微聊天上下文感知

## 智能体集成

- 统一管理智能体
- 工具复用
- 敏捷场景复用



# 大模型应用案例：AI辅助故障定位

## 大模型智能定位辅助

事件编号：IMS-20250303-006

发生系统：IMS平台

### 前三个交易日变更情况：

- 1、CAB-20250307-001
- 2、CAB-20250313-017

应急中心可观测感知（异常项有才列）

系统健康度：97

[点击查看](#)

### 统一告警事件

近2小时告警数：6

[点击查看 \(仅限内网pc端\)](#)

[点击查看](#)

### 历史相似事件

- 1、IMS-20220418-004
- 2、IMS-20220916-006
- 3、IMS-20221031-018

### 推荐应急策略

- 1、对账单发送失败
- 2、中登报盘服务器故障【人工切换】
- 3、客户简称被自动截断成乱码导致无法开户

（注：数据由大模型筛选生成，使用时请注意核对）

异常管理 / 异常事件 / 异常事件详情

已报警 IMS-20250303-002

发生系统：IMS 异常来源：监控发现 故障范围：C端

异常描述：日志监控发现，上周发版的服务器连接出现“Unknown prepared statement handler (5) given to mysql\_stmt\_precheck”

跟进人：IMS故障专家

异常事件

故障原因分析

根据提供的异常事件描述和报错信息，可以初步分析以下可能的故障原因：

1. SQL语句预处理问题：
  - 报错信息“Unknown prepared statement handler (5) given to mysql\_stmt\_precheck”表明在执行预处理SQL语句时，MySQL无法找到对应的预处理句柄。这可能是由于预处理语句被提前关闭或未正确初始化。
2. 数据库连接问题：
  - 数据库连接可能存在异常，导致预处理语句无法正确执行。这可能是由于连接池配置不当，连接超时或连接被意外关闭。
3. 代码逻辑问题：
  - 应用程序中可能存在逻辑错误，导致预处理语句的处理不正确。例如，预处理语句的创建和执行顺序可能有误。
4. 数据库版本兼容性问题：
  - 如果最近进行了数据库版本升级，可能存在兼容性问题，导致预处理语句无法正常工作。

定位建议

1. 检查预处理语句的创建和执行：
  - 查看应用程序中预处理语句的创建和执行逻辑，确保预处理语句的创建和执行顺序正确。
  - 确认预处理语句在执行前是否已经正确初始化。

和机器人聊天



## 变更查询

## 异常系统及上下游系统 近期变更情况

## 变更操作事件查询

异常系统及上下游系统发生过哪些（风险）操作

## 部署状态感知

### 异常系统及上下游系统各变更感知因子是否发生变化

## 异常变更定位

## 哪些变更、操作事件、变更感知因子变化导致异常





# 大模型应用案例：脚本优化与合规检查

\* 场景: 运维管理

\* 名称: 脚本优化专家

\* 提示词:

Role: 脚本优化专家  
Skills:  
1. 熟练运用 Python 2.7 基础类库进行脚本开发  
2. 能够对现有脚本进行性能分析和优化, 提升脚本的执行效率  
3. 擅长编写各种运维脚本, 以满足系统自动化管理和维护的需求  
4. python脚本在沙箱环境执行, 禁止使用['httplib', 'urllib', 'urllib2', 'tplib', 'smtpplib', 'multiprocessing', 'subprocess', 'threading', 'socket', 'sys', 'os', 'pickle', 'shelve', 'anydbm', 'dbm', 'gzip', 'bz2', 'zipfile', 'tarfile', 'glob']等内置模块  
5. 除了python2.7内置模块, 可以使用第三方库, 但是要满足上面的约束, 比如内置已经可以导入snakeYaml库处理yaml文件了  
Task:  
1. 确保脚本能够准确、高效地获取所需的数据, 执行合理的操作  
2. 设计和优化脚本中的交易逻辑, 保证业务流程的顺畅执行  
3. 通过优化算法, 减少资源消耗等方式, 提高脚本的执行性能  
Output规则:  
1. Python限制: 基于python2.7版本的基础类库, 不使用其他库  
2. 代码优先: 直接给出解决方案脚本  
3. 解释结构: 功能→逻辑→注意事项→验证方法  
4. 合规重点: 标注涉及安全的关键处理  
5. 性能提示: 标注可能影响效率的代码段  
6. 如果有代码已经达到最优, 直接输出代码无需修改  
Example格式:  
问题1:  
原始脚本如下:  
当dims里的type=123时, 将data的mvp字段改成123.  
方案:  
```python  
# 检查 dims 里的 type 是否为 123  
if ctx['dims'].get('type') == 123:  
 # 更新 data 里的 mvp 字段  
 ctx['data']['mvp'] = 123

部署感知 / 策略管理 / 策略详情 / 脚本编辑

替换IP

显示 关联任务 保存脚本

```
1 #  
2 # ctx为内置参数, 格式为: {'dims': {}, 'data': {}}, 其中dims为元数据, 一般不修改, data为数据, 可以修改  
3 # 若要修改某些数据项, 可以修改ctx, 方式如下:  
4 # ctx['dims']['drop'] = True  
5 #  
6 # 脚本示例 (以文件配置为例, 替换文件中的IP地址为*, *, *)  
7 # input re  
8 # input json  
9 # input hashlib  
10  
11 # IPV4_RE = r"^(?!(?:\d{1,3}\.){3}\d{1,3})$".format(IPV4_RE) # 正则  
12 # if ctx['data']['path'] == '/usr/local/easyops/agent/conf/conf.yaml':  
13 #     content = ctx['data']['content']  
14 #     content_with_masked_ip = re.sub(IPV4_RE, "*", content) # 替换IP  
15 #     ctx['data']['content'] = content_with_masked_ip # 替换文件内容  
16 #     md5 = hashlib.md5() # 计算MD5  
17 #     md5.update(content_with_masked_ip.encode('utf8'))  
18 #     ctx['data']['md5'] = md5.hexdigest() # 返回MD5  
19 #  
20 import re  
21 import json  
22 import hashlib  
23 IPV4_RE = r"^(?!(?:\d{1,3}\.){3}\d{1,3})$".format(IPV4_RE)  
24 if ctx['data']['path'] == '/usr/local/easyops/agent/conf/conf.yaml':  
25     content = ctx['data']['content']  
26     content_with_masked_ip = re.sub(IPV4_RE, "*", content)  
27     ctx['data']['content'] = content_with_masked_ip  
28     md5 = hashlib.md5()  
29     md5.update(content_with_masked_ip.encode('utf8'))  
30     ctx['data']['md5'] = md5.hexdigest()
```

提示 调试 AI

问题描述: 当前脚本存在对特定路径下的文件内容中的IP地址进行替换, 并计算修改后内容的MD5值。脚本直接修改IP地址为\*, 这不符合运维规范, 应当替换为合法的IP地址, 以符合合规要求。

方案:

```
import re  
import hashlib  
  
# 定义IPV4的正则表达式  
IPV4_RE = r"^(?!(?:\d{1,3}\.){3}\d{1,3})$".format(IPV4_RE)  
  
# 对文件内容中的IP地址进行替换  
if ctx.get('data', {}).get('path') == '/usr/local/easyops/agent/conf/conf.yaml':  
    # 获取文件内容  
    content = ctx['data'].get('content', "")  
    # 使用正则表达式替换IP地址为合法的IP地址  
    content_with_masked_ip = re.sub(IPV4_RE, "192.168.1.1", content)  
  
# 计算替换后的MD5值  
ctx['data']['content'] = content_with_masked_ip  
md5_hash = hashlib.md5(content_with_masked_ip.encode('utf-8')).hexdigest()  
ctx['data']['md5'] = md5_hash  
  
# 返回结果  
# 输出: 替换后的文件内容以及MD5值  
# 说明: 该脚本在沙箱环境中运行, 不会实际修改文件, 但会返回替换后的内容, 以便进行合规检查  
# 合规检查: 通过正则表达式替换IP地址, 确保替换后的IP地址符合合规要求, 同时返回MD5值用于验证
```

脚本优化专家  
最后/合规分析  
请输入调用内容



# 大模型应用案例：多模态场景探索

智能看板巡检：cline+deepseek v3氛围编程，qwen-vl-7b多模态监控图表的分析







## 当下

- 专家知识库：更精准的RAG
- 沉淀专家经验：智能体编排
- 智能体与场景融合

## 下一步

- 智能体策略探索
  - FunctionCall
  - ReAct
  - Plan&Execute
  - MCP ReAct
- MCP与多智能体探索
  - 运维领域deepResearch：智能排障/深度健康检查



## 未来

- 更强大的模型
  - 推理能力/多模态
  - 更强运维通识知识
- 专业知识库
  - 通用运维知识库
  - 银证等金融运维行业知识库
- 微调语料
  - 运维领域指令遵循
  - 监控图表分析





# Thanks

高效运维社区

BizDevOps 社区

荣誉出品

T H A N K S

感谢大家观看

2025.4