AI运维

AIOps

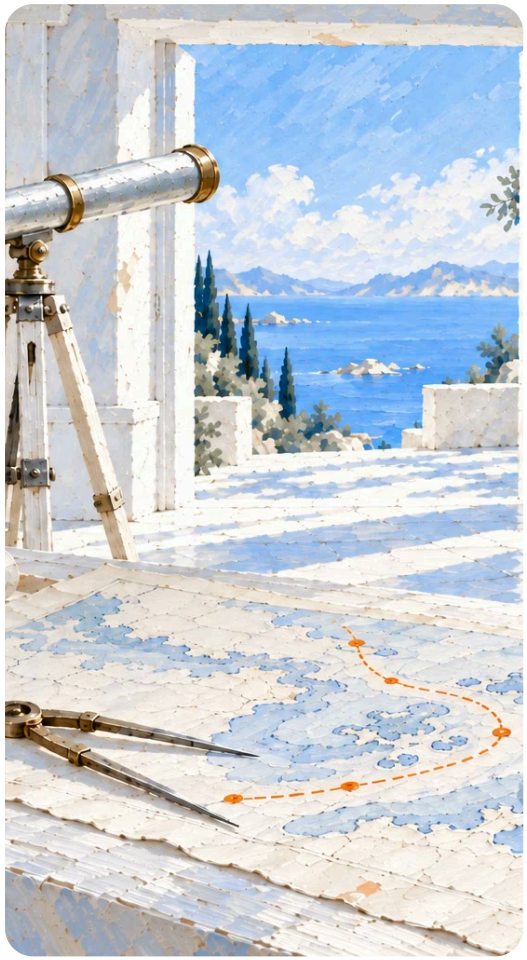
基于AI的故障预测与响应解决方案

以充分依据提前预警故障征兆，
并只在**贵公司批准的范围内**执行处置。



本手册不是功能清单，
而是从系统运维团队在故障面前
真正面临的七大难题出发。

每个难题配一页解决方案，
可按顺序依次阅读。



引言

引言	运维团队在故障面前的七大难题	p.03
解决方案	AIOps 是什么，在哪些环节化解难题	p.04

七大难题与解决

难题 01	总是比用户更晚发现故障	p.05
难题 02	告警太多，真正的原因被淹没	p.07
难题 03	查找原因比恢复还要耗时	p.09
难题 04	处置经验只掌握在少数人手中	p.11
难题 05	担心 AI 直接操作生产服务器	p.12
难题 06	不知道凭什么相信 AI 的判断	p.14
难题 07	担心要替换现有的监控工具	p.16

应用与导入

应用示例	引入 AIOps 后，故障响应如何改变	p.17
导入步骤	从审批模式起步、逐步扩展的导入步骤	p.19
咨询	演示视频 · 咨询导入	p.20

常听到的难题

面对故障，运维团队最先提出的七大难题

监控工具早已配备齐全，
为什么故障仍然要靠人熬夜解决?

这里汇集了我们在“设备多、人手少”的
运维团队中反复听到的声音。



点击您最关心的难题，即可直接跳转到
AIOps 的对应解决方案。

难题 01 “每次出故障，都是用户打电话来我们才知道。” 提前预知 →

难题 02 “几百条告警一起响，根本不知道该先看哪条。” 告警整理 →

难题 03 “查原因花的时间，比恢复还要长。” 原因分析 →

难题 04 “这种故障，到头来还是只有他一个人懂。” 处置经验 →

难题 05 “让 AI 直接动生产服务器？那我更不放心了。” 安全处置 →

难题 06 “AI 要是判断错了呢？没有依据的判断，我们没法信。” 判断依据 →

难题 07 “现在用的监控工具，都得换掉吗？” 现有工具 →

一套连贯的流程

AIOps 用一套连贯的流程化解这些难题。

基于AI的故障预测与响应解决方案

在现有监控之上叠加 AI 的判断与处置能力：故障发生前提前预警，发生后从原因分析一直衔接到处置与恢复验证。



点击“难题”下方的编号即可跳转到对应难题。

难题 01 · 事后响应



每次出故障，都是用户打电话来我们才知道。

这是我们从基础设施运维负责人那里最常听到的一句话。

现场常见的情况

告警总在越线之后才响

磁盘、连接数、内存往往要几天才逐渐涨满，固定阈值却要等越线之后才会告警。

早有征兆，却无人察觉

数百台设备的趋势，不可能每天靠人盯着看，往往等故障发生后才回头翻看监控图表。

发现得越晚，中断越久

从出现异常征兆到开始处置之间的空档，会直接变成服务中断时间。

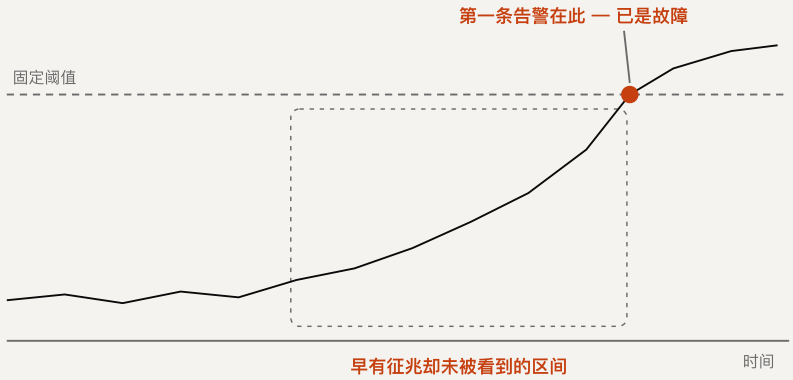
背后的担忧 “下一次故障，还是要等出了事才知道”

查看 AIOps 的解决方案 →

解决 01 · 在触及阈值之前

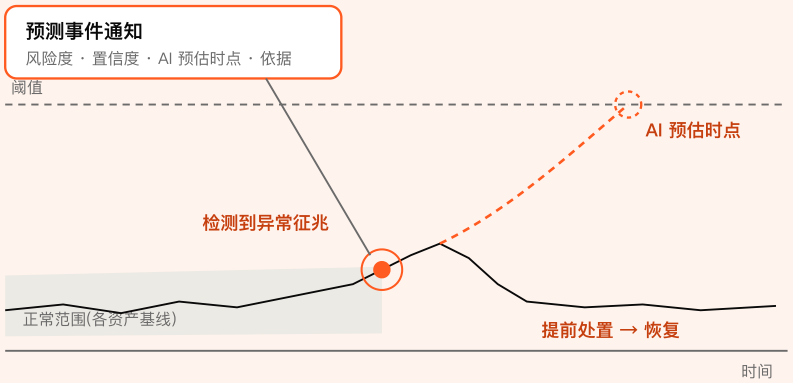
不是越线之后才告警，而是在逼近阈值的那一刻就发出预警。

现状



告警要等越过阈值才响，此前的征兆就这样被忽略。

导入 AIOps 后



一旦偏离正常范围即可察觉，在故障发生前争取处置时间。

每项资产都有自己的正常范围

以每台设备的日常运行状态为基线，按偏离程度进行评分。

综合趋势 · 日志 · 历史记录

将上升趋势与相关日志、相似的历史故障叠加比对，由 AI 判断是否会演变为故障。

风险度 · 置信度 · 预计时点

每条预测都会同时给出风险度、置信度，以及 AI 推算的预计发生时点。

确认后提前处置

运维人员确认预测无误后，即可在故障发生前执行预先验证过的处置。

您将获得

- ✓ 在故障发生之前就开始应对
- ✓ 无需每天盯着监控图表
- ✓ 以计划内的处置取代紧急抢修

难题 02 · 告警风暴

几百条告警一起响，根本不知道该先看哪条。

这是监控值守与值班人员的共同心声。



现场常见的情况

一个原因，引发几十条告警

一个 DB 变慢，上层的 WAS、Web、批处理就会同时涌出大量告警。

重要告警淹没在噪声中

对反复出现的告警习以为常后，真正该关注的告警也会被忽略。

同一个故障，多人各自追查

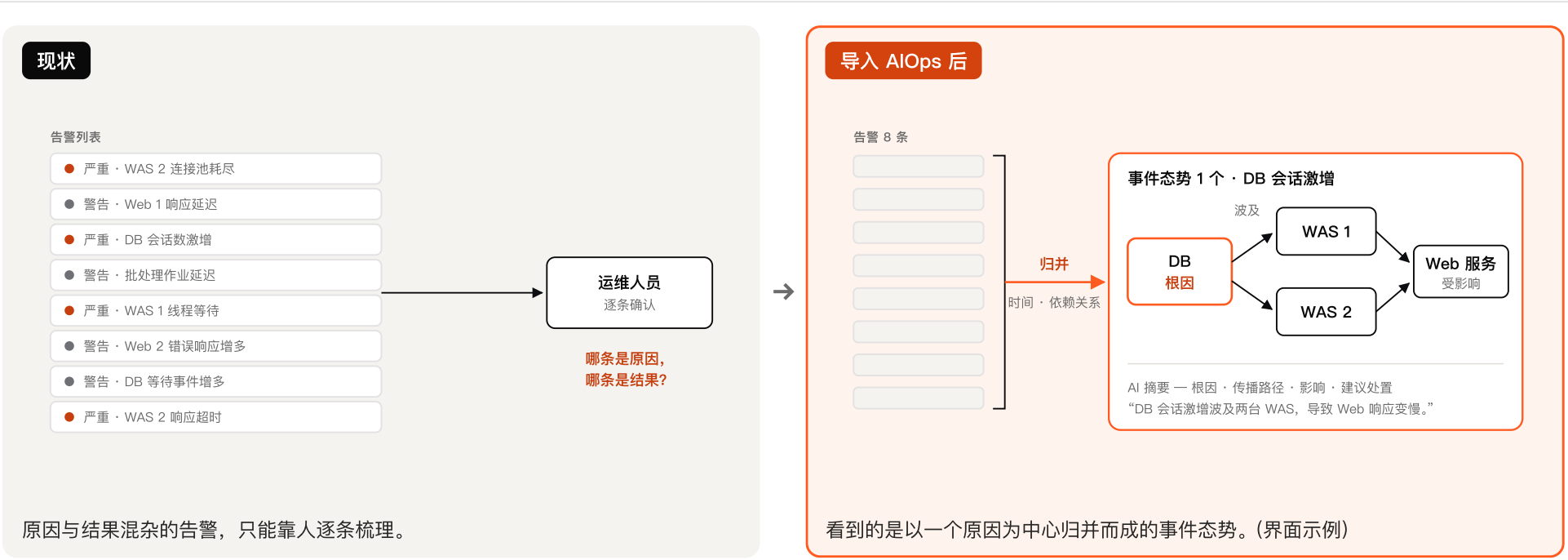
每个人盯着不同的告警，处置不是重复就是有疏漏。

背后的担忧 **“被告警搞得疲惫不堪，反而漏掉真正的信号”**

查看 AIOps 的解决方案 →

解决 02 · 看事件态势，而非逐条告警

以原因为中心，将分散的告警归并为一个“事件态势”呈现。



按时间与依赖关系归并

将同一时段内、彼此存在依赖关系的资产所产生的信号，归并为一个事件态势。

归并依据由规则决定

哪些信号需要归并，由既定规则而非 AI 推测决定；同样的情况，结果始终一致。

仅共用设备重叠时不归并

若只是存储、网络等公共设备重叠，则不予归并，减少无关故障混在一起。

一段话说清事件态势

归并的信号达到两个及以上时，由 AI 将原因、传播路径、影响范围与建议处置汇总成一段简明说明。

您将获得

- ✓ 不看告警列表，只看几个事件态势
- ✓ 从一开始就分清原因与结果
- ✓ 同一事件态势，多个团队同屏查看

难题 03 · 原因分析

查原因花的时间，比恢复还要长。

每次开故障复盘会，都会反复听到这句话。



现场常见的情况

在多个工具之间来回比对

指标在这里，日志在那里，
变更记录又在另一处。负责人只能
在多个界面间切换，逐一对齐时间。

不清楚影响波及到哪里

即使找到了故障点，受影响的服务
究竟有哪些，还要摊开架构图逐一排查。

忽略了事发前的变更

故障往往源于事发前的发布或配置变更，
但这些记录却在别的系统里。

背后的担忧 “分析拖得越久，服务就停得越久”

查看 AIOps 的解决方案 →

解决 03 · 原因 · 影响 · 处置，一屏呈现

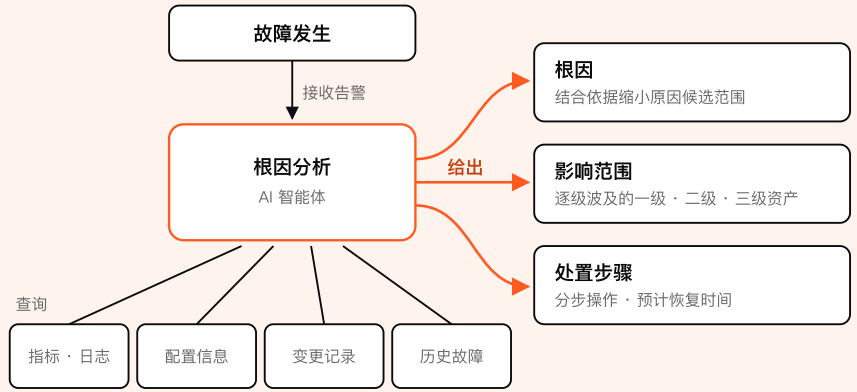
故障一旦发生，原因 · 影响范围 · 处置步骤 会同时呈现在同一个界面上。

现状



找原因全靠人工查询和个人记忆。

导入 AIOps 后



智能体汇集分散的依据，一次性给出原因、影响与处置方案。

一路缩小到根因

结合指标与日志缩小原因候选范围，并给出分步处置步骤与预计恢复时间。

影响范围一图可见

沿着配置信息中的依赖关系，直观呈现逐级波及的一级、二级、三级资产。

同步核查事发前的变更

比对故障发生前的变更与发布记录，优先确认是否由最近的变更引起。

参考相似的历史故障

按相似度检索历史故障，复用已经验证过的处置方法。

您将获得

- ✓ 无论谁值班，分析依据都一样
- ✓ 可第一时间通知受影响的服务方
- ✓ 把找原因的时间用在恢复上

难题 04 · 处置经验

这种故障，到头来还是只有他一个人懂。



有记录，却找不到

故障报告和运维手册攒了不少，
可情况紧急时，偏偏找不到需要的那一行。

人一走，方法也跟着走

资深人员一旦调岗，
他掌握的处置方法也随之消失。

背后的担忧

“每换一次负责人，处置质量就波动一次”

解决 04 · 让经验成为企业知识

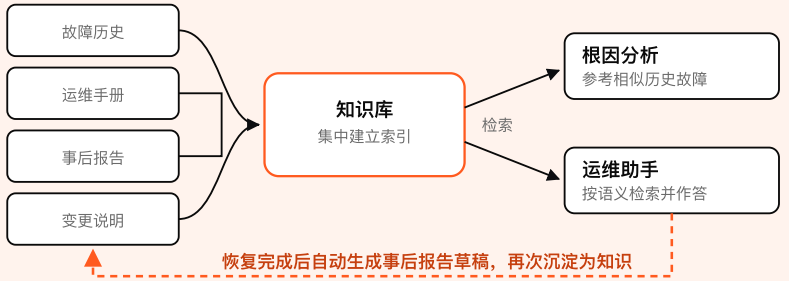
处置越多，积累越多，人人都能随时调用。

现状



经验被困在个人和分散的文档里。

导入 AIOps 后



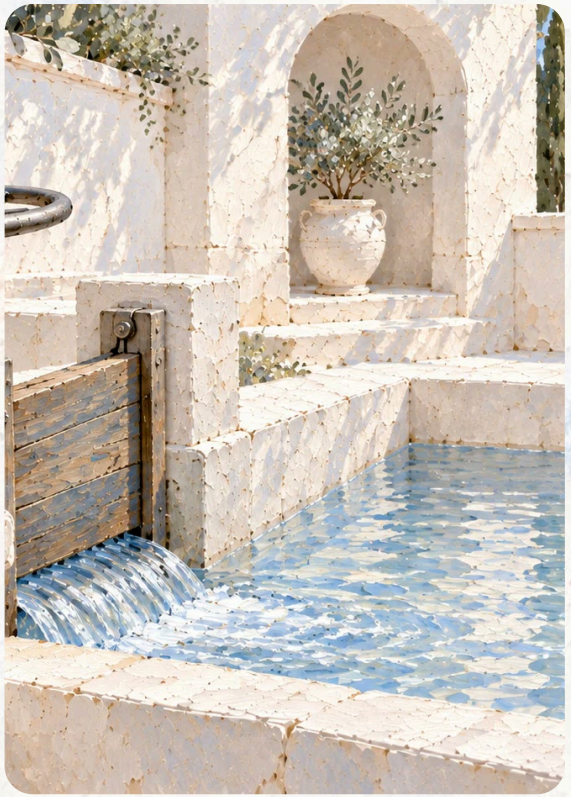
每处理完一次故障，企业的知识就多一分。

您将获得

- ✓ 即使不是资深人员，也能按同样标准处置
- ✓ 即使人员变动，处置方法依然留存

返回目录

难题 05 · 自动处置



让 AI 直接动生产服务器？那我更不放心了。

这是评估自动化方案的运维负责人在审批签字前常问的问题。

现场常见的情况

凌晨手工操作容易出错

疲惫的值班人员手工敲命令时，
恢复操作本身也可能引发新的故障。

可真要交出去，又心里没底

依据不明的自动执行，
会对生产服务器做些什么，谁也无法预料。

执行完了，事情并没有结束

即使脚本显示执行成功，
服务是否真正恢复，仍需人工再次确认。

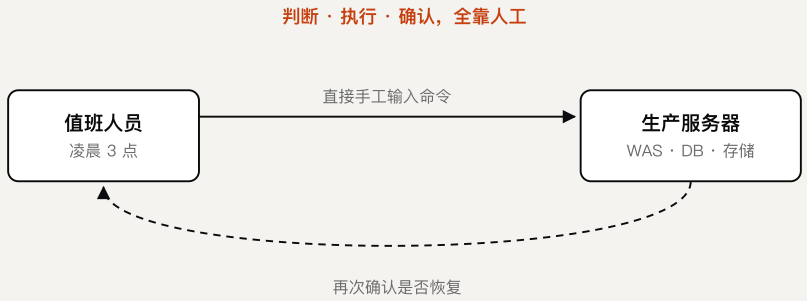
背后的担忧 **“自动化把事故闹大时，责任要由自己来扛”**

查看 AIOps 的解决方案 →

解决 05 · 可控的自动化

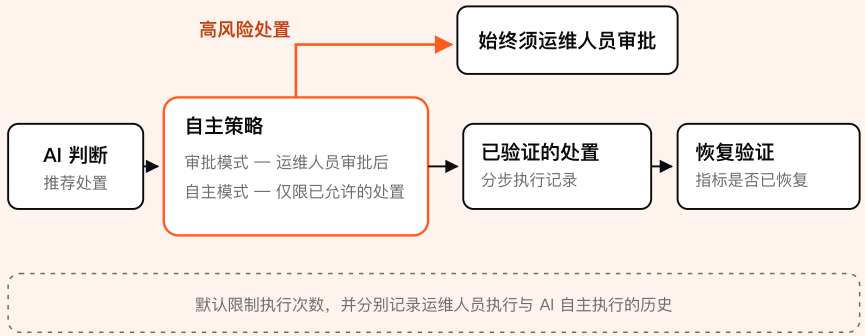
AI 只在人设定的范围内执行，并一直确认到服务真正恢复。

现状



这种模式很容易出现失误和确认遗漏。

导入 AIOps 后



哪些处置交给自动化由组织决定，结果以指标来验证。

从审批模式起步

初期所有处置均由运维人员审批，再从已建立信任的类型开始逐步扩大自主范围。

高风险处置始终需审批

为每项处置设定风险等级及是否允许自动执行；即使在自主模式下，高风险操作也须人工审批。

只执行已验证的流程

AI 不会自行编写新命令，而是从预先验证过的处置剧本中选择执行。

一直验证到效果

判断标准不是执行是否结束，而是处置后目标指标是否真正恢复。

您将获得

- ✓ 夜间、节假日也按同样流程处置
- ✓ 减少手工输入造成的失误
- ✓ 执行记录完整留存，责任归属清晰

难题 06 · AI 判断的可信度



AI 要是判断错了呢?
没有依据的判断，我们没法信。

这是正在评估引入 AI 的运维团队最为警惕的一点。

现场常见的情况

不知道为什么这样判断

只给结果的 AI，运维人员无从验证它对不对。

错误判断反复出现

即使反馈了误报，
如果不能体现在下一次判断中，
最后也只是多了一条告警而已。

看不到 AI 做了什么

AI 处理了什么、处理了多少、
花了多少成本，都难以查证。

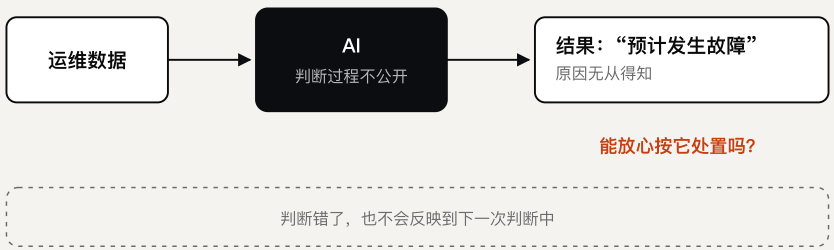
背后的担忧 “把运维交给一个说不清理由的判断”

查看 AIOps 的解决方案 →

解决 06 · 可解释的判断

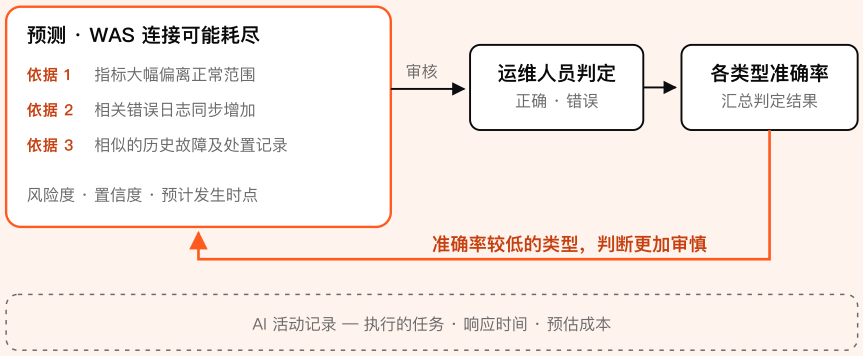
每个判断都附带依据，运维人员的判定会改变下一次判断。

现状



只有结果，既没有依据，也不会从中学习。

导入 AIOps 后



运维人员可以验证，其判定也会反映到下一次判断中。(界面示例)

每个判断都附带依据

预测会同时给出指标偏离正常水平的程度、相关日志以及相似的历史故障。

判定沉淀为准确率

运维人员的正确/错误判定按类型汇总为准确率；准确率较低的类型，后续判断会更加审慎。

规则与 AI 各司其职

结果必须始终一致的信号归并交给规则，解释与预测交给 AI。

AI 的工作同样留有记录

记录 AI 的任务、响应时间与预估成本。运维助手只分析和推荐，不直接执行。

您将获得

- ✓ 运维人员可亲自验证的判断
- ✓ 融入运维人员判定的预测
- ✓ AI 用量与预估成本清晰可见

难题 07 · 现有工具

现在用的监控工具，都得换掉吗？



已经投入了大量工具

监控、日志、自动化工具，
每一项都投入了时间和成本。

数据分散在各个工具中

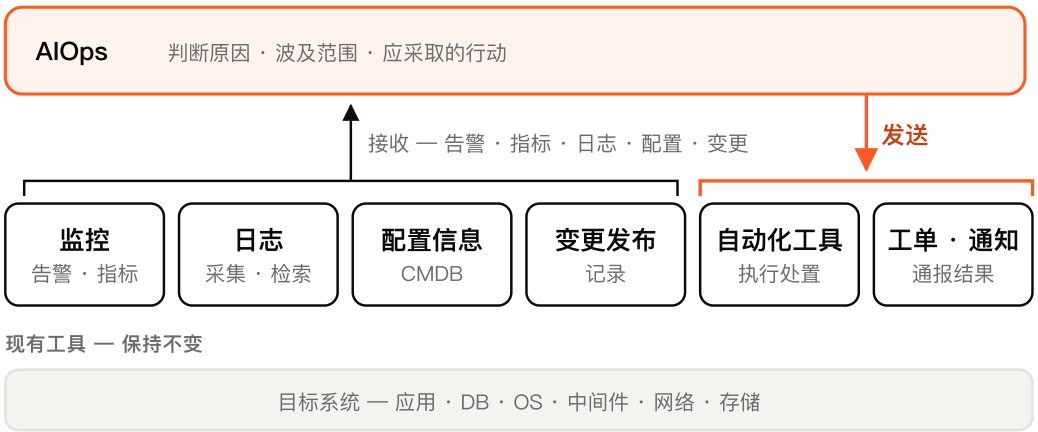
指标、日志、配置信息、变更记录各自独立，
难以统一研判。

背后的担忧

“又多了一个需要维护的工具”

解决 07 · 不替换，只叠加

现有工具保持不变，在其之上叠加判断。



监控告诉您“什么越过了阈值”，AIOps 则判断“为什么、波及多广、该做什么”。

以标准方式对接

以 Webhook、API、syslog 等标准方式为基础设计对接。

分散数据汇于一处

将指标、日志、配置信息、变更记录按统一标准整理。

对接范围共同商定

在梳理现状阶段，共同确定对接对象与对接方式。

您将获得

- ✓ 继续使用已投资的工具
- ✓ 分散的数据汇聚为统一的判断

返回目录

业务应用示例

引入 AIOps 后，故障响应将这样改变。

DB 运维 · 容量管理

在空间耗尽之前提前获知

您将获得 — 在工作时间内，以计划内的处置解决容量问题。

现在	AIOps 负责的工作	负责人要做的事
表空间使用率一点点上涨，直到越过阈值才告警，此时才开始紧急扩容。	对照正常范围，提前预警将导致空间饱和的趋势，并附上相关日志和历史记录作为依据。	确认依据并批准后，扩容操作与恢复验证将按既定流程执行。

支撑该场景的 AIOps：解决 01 提前预知；解决 06 判断依据；解决 05 受控处置

连接对象：DB 指标 · 日志；故障历史；处置剧本

服务运维 · 连锁故障

收到的不是几十条告警，而是一个事件态势

您将获得 — 从一开始就分清因果，据此确定处置顺序。

现在	AIOps 负责的工作	负责人要做的事
DB 会话激增后，WAS、Web、批处理同时告警，负责人各自追着不同的告警。	把同一时段、相互依赖的信号归并为一个事件态势，并标出根因 DB 与受影响的 WAS。	各负责团队以同一个事件态势为准，集中处置根因。

支撑该场景的 AIOps：解决 02 按事件态势监控；解决 03 影响范围；解决 07 对接现有工具

连接对象：监控告警；配置信息 · 依赖关系；日志

以上为业务应用示例。实际范围与效果将结合贵公司的系统与运维方式共同设计。

业务应用示例(续)

以同样的方式，用于其他业务。

基础设施运维 · 存储故障

不必再摊开架构图排查波及范围

您将获得 — **故障通告与恢复同步**启动。

现在

存储路径一旦发生故障，就要翻遍架构图和文档，逐一找出受影响的服务器和服务。

→

AIOps 负责的工作

在给出根因的同时，逐级标出受影响的资产，并提供事发前变更、相似历史故障与处置步骤。

→

负责人要做的事

通知受影响的服务方，并批准执行系统给出的恢复操作。

支撑该场景的 AIOps：解决 03 原因分析 | 解决 04 知识复用 | 解决 05 受控处置

连接对象：配置信息(CMDB) | 变更 · 发布记录 | 存储指标 · 日志

运维管理 · 事后报告

故障结束后，不必从零开始写报告

您将获得 — **每处理完一次故障**，运维团队的知识与依据就多一分。

现在

恢复之后，要整理经过、原因与处置写成报告，还要另外跟进防止复发的措施。

→

AIOps 负责的工作

恢复完成后生成事后报告草稿并沉淀为知识，同时将准确率、恢复时间留存为指标。

→

负责人要做的事

审阅草稿并定稿，再参考指标确定要扩大自动化的故障类型。

支撑该场景的 AIOps：解决 04 知识沉淀 | 解决 06 判定反馈 | 解决 05 自主范围

连接对象：故障历史 | 事后报告 | 成效指标

以上为业务应用示例。实际范围与效果将结合贵公司的系统与运维方式共同设计。

导入步骤

不会一开始就全部交给 AI。
先以审批模式起步，验证之后再逐步扩展。

1

共同梳理现状

梳理正在使用的运维工具和资产构成，
确定对接点与适用范围。

您将获得

要对接的系统与优先处理的故障类型

2

从审批模式起步

先在核心资产上应用预测与原因分析，
所有处置均经运维人员审批后执行。
随着审批判定不断积累，
各类型的准确率逐渐清晰可见。

您将获得

用贵公司自己的指标，
验证 AI 判断在贵公司环境中是否准确

3

从低风险处置开始自主

从准确率已趋于稳定的类型开始，
允许低风险处置自动执行。
高风险处置仍须审批。

您将获得

夜间、节假日处置负担开始减轻的第一步

4

扩大对象与范围

以恢复验证结果和积累的知识为依据，
逐步扩大目标资产与自动化范围。

您将获得

参照贵公司的预测准确率与恢复时间，
稳步扩展的运维方式

首次咨询只需准备以下部分资料

正在使用的运维工具
监控、日志、自动化、工单工具清单

近期反复出现的故障
过去几个月里反复发生的两三类故障

资产 · 配置资料
服务器、设备清单及依赖关系
(CMDB 或 Excel)

标准处置流程
现有的运维手册，以及检查、处置脚本

以 SaaS 轻松起步
确定目标资产规模和对接范围后，
从核心资产开始小范围起步。

专属环境协商
根据安全要求，协商传给 AI 的数据范围
以及客户专属云配置。

默认审批模式
所有处置均从运维人员审批开始，
自主范围可随时调整。

咨询指南

请先告诉我们
贵公司的难题。

只需告诉我们一个近期反复出现的故障，我们将通过演示，
展示类似故障在 AIOps 中如何被提前预警、审批和处置。
资料只需准备第19页清单中的部分内容即可。
如想先行了解，欢迎观看演示视频。

咨询导入 →

▶ 观看演示视频



咨询时，请告诉我们您最迫切的一个难题

- 提前预知
- 告警整理
- 原因分析
- 处置经验
- 安全处置
- 判断依据
- 现有工具

邮箱
sales@vicsnc.com

网站
vicsnc.com