

IT基础监控的精细化运维管理

告别告警疲劳，实现智能高效运维

主讲人：监控易

2026年4月2日

您是否正身处“告警疲劳”？



海量告警，难以分辨

每日面对海量告警信息，有效告警占比极低，关键信息极易被淹没。



真实案例警示

某大型制造企业每日产生**12000+**条告警，导致核心故障信号被海量噪音完全淹没，造成重大损失。



信息洪流中的告警困境

CONTENTS



01 趋势篇

精细化运维的时代必然性



02 痛点篇

粗放式监控的三大核心痛点



03 机会篇

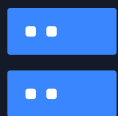
精细化运维的四大落地维度



04 案例与总结

从理论到实践的价值实现

运维发展的三个阶段



粗放监控时代

2000 - 2010

看设备在不在，事后发现



标准化监控时代

2010 - 2020

多工具拼凑，数据孤岛



精细化运维时代

2020 - 至今

数据驱动、智能分析、流程闭环

行业趋势数据：现状堪忧



9.8个

平均每个企业使用的监控工具数量

数据来源：Gartner 2025



70%-80%

告警为重复或无效告警的比例

数据来源：Gartner

数据来源：Gartner行业报告；国内调研显示，超80%的企业存在告警冗余问题

传统监控体系面临工具碎片化严重与告警噪音过载的双重挑战，亟需智能化升级。

行业趋势数据：价值凸显

告警疲劳代价

关键告警忽略概率上升 **45%**

告警量长期超阈值，导致关键信号被海量噪音淹没，风险感知严重迟钝。

精细化运维价值 (IDC数据)

MTTD 缩短

65%

MTTR 缩短

52%

通过智能化手段实现故障快速定位与自动恢复，显著提升IT服务连续性与效率。

IDC对100家企业的追踪研究数据，MTTD缩短65%，MTTR缩短52%，效果非常显著。

从被动告警到主动运维，数据驱动的精细化管理已成为降本增效的关键抓手

政策与技术的双重驱动



政策法规

政策要求

随着《关键信息基础设施安全保护条例》及等保2.0标准的落地，监管层面对企业安全运营提出了明确的强制要求，强调对资产和威胁的持续监控与合规审计。



技术演进

技术演进

技术栈正从单一监控向全链路可观测性转变，AI/ML、自动化编排工具与一体化安全平台的结合，正在成为应对复杂威胁环境的主流技术方向。

告警管理的三大顽疾



告警风暴

海量无效告警泛滥，
导致关键有效告警被淹没



告警孤岛

监控数据分散割裂，
故障故障定位只能靠“猜”



告警无闭环

处理流程缺乏规范，
陷入低水平重复劳动

监控数据的四大浪费



采集不全

只采“基础项”，漏采“关键项”，导致数据维度单一，无法支撑深度分析。



质量不高

数据“有了”，但“不能用”，存在大量噪音、延迟或错误，影响决策准确性。



数据沉睡

海量数据只在故障时“用一次”，平时缺乏挖掘，未能转化为资产价值。



数据不关联

IT数据与业务数据“两张皮”，无法通过技术指标直接反映业务影响。

运维人员的三个无奈



被动救火

全年无休的“告警消防员”



价值难显

做的都是“隐形工作”



技能瓶颈

把一年经验重复了八年

精细化运维的四大落地维度



深度采集

打好数据基础，实现全链路可观测性，覆盖基础设施到业务应用。



智能降噪

基于AI算法过滤无效告警，提升告警准确率，减少运维干扰。



流程闭环

打通告警、工单与复盘流程，形成标准化管理体系，确保件件有回应。



数据驱动

挖掘历史监控数据价值，辅助容量规划与性能调优，实现主动式运维。

深度采集：从“监控有无”到“监控多少”



采深：深挖核心指标

不仅采集基础指标，更深入CPU各核负载、数据库锁等待等深层性能数据。



采全：全栈资源覆盖

实现IT硬件、应用软件、虚拟化、云平台、机房设施及物联网设备的全域覆盖。



采准：数据质量保障

建立严格的数据校验机制，确保监控数据的准确性、一致性与高可用性。



全栈IT架构监控示意图

深度采集详解：采深、采全、采准

采深：挖掘核心指标

- **服务器**：CPU负载、上下文切换、IO延迟、磁盘SMART信息。
- **数据库**：会话数、锁等待、缓存命中、慢查询、事务日志。
- **网络**：丢包错包率、光模块收发光功率、温度电压。

采全：全栈无死角覆盖

- **IT资源**：服务器、存储、网络设备、安全设备全覆盖。
- **软件资源**：OS、数据库、中间件及业务应用。
- **云与物联**：容器/公有云/私有云、UPS/空调/传感器等IoT设备。

采准：确保准确可用

- **时间同步**：确保所有系统时间戳统一，日志精准对应。
- **定义一致**：统一指标名称、单位、采样方式，便于横向对比。
- **频率合理**：关键指标秒级采集，精准还原故障瞬间状态。

智能降噪：从“告警风暴”到“精准定位”



告警压缩

合并冗余告警，大幅减少无效信息干扰，聚焦关键问题。



动态基线

替代传统固定阈值，基于AI学习动态调整，适应业务波动。



故障分析

快速定位故障根源，缩短排障时间。



信号过滤与降噪示意

价值转化：实现从海量冗余告警到精准故障定位的质变，提升运维效率。

智能降噪详解：从告警风暴到精准定位

告警压缩

技术原理：基于CMDB和拓扑关系，识别告警因果链。

效果：将数十条冗余告警合并为一条核心告警。

价值：无需海量筛选，一眼掌握故障全貌。

动态基线

技术原理：机器学习历史数据，建立动态正常基线。

效果：自动适配峰谷，识别渐变与瞬态异常。

价值：解决固定阈值漏误报，实现事前预警。

故障分析

技术原理：打通指标日志拓扑，关联分析全量数据。

效果：秒级输出最可能故障及处理建议。

价值：解放人工排查，大幅提升定位效率。

流程闭环：从“告警通知”到“问题解决”



闭环价值：通过沉淀知识优化告警策略，减少无效告警，实现从“被动响应”到“主动预防”的转变。

数据驱动：从“数据成本”到“数据资产”



容量规划

基于历史数据建模，精准预测未来资源需求，避免过度采购。



成本优化

智能识别“僵尸服务器”和闲置资源，持续降低基础设施TCO。



趋势分析

通过时序数据挖掘，提前发现性能拐点，变被动响应为主动预防。



业务决策

量化运维对业务的支撑价值，为技术投入产出比提供数据支撑。

数据驱动详解：从数据成本到数据资产




¥

成本优化：识别浪费，降低支出

- 识别“僵尸资源”：定位长期低负载服务器与闲置虚机
- 资源整合：对闲置资源进行下架、降配或回收利用
- 量化节约：直观展示优化动作带来的IT成本降幅

落地路径（一）：切入点与量化指标

第一步：选准切入点

-  **从高频痛点切入**
聚焦数据库性能监控、网络告警等频发问题。
-  **从核心业务切入**
优先保障支付、交易等关键系统的稳定性。
-  **从团队擅长领域切入**
结合现有技术栈，选择易于上手场景建立信心。

第二步：设定量化指标

-  **效率与质量指标**
关注 MTTD/MTTR、有效告警率及系统可用性。
-  **成本控制指标**
优化硬件资源利用率，降低 IT 运维成本占比。
-  **设定 SMART 目标**
确保目标具体、可衡量、可实现、相关且有时限。

 **核心策略：**不追求“大而全”，而是通过“小切口”实现“大突破”，用数据驱动运维改进的每一步。

落地路径（二）：用数据验证效果，复制推广

第三步：用数据验证效果

- **制作前后对比报表**
对比优化前后的关键指标（如告警量、故障处理时间），用数据说话。
- **分析改进效果**
深入分析指标变化的原因，总结成功经验和不足之处。
- **形成案例报告**
将改进过程和成果整理成案例，向上汇报，争取更多资源支持。

第四步：复制推广

- **总结方法论**
将第一个场景的成功经验提炼成可复制的方法论。
- **逐步扩展范围**
应用到其他业务系统或技术领域，如从数据库推广到中间件、服务器。
- **建立持续优化机制**
定期回顾和评估运维效果，持续迭代优化方案。

案例：某三甲医院的精细化运维实践

运维痛点

- 每日告警：**8000+**条
 - 故障定位：耗时**2小时**
- 海量无效告警淹没真实故障，排查效率低下。

关键措施

1. 告警压缩与降噪
2. 动态基线异常检测
3. 故障处理流程闭环
4. 运维知识库自动沉淀

实施效果

- 日均告警：降至**300**条
- 定位时间：缩短至**15分钟**

告警量减少**96%**，响应效率提升**8倍**以上。

核心观点总结（一）：聚焦监控与告警的本质

监控更对的指标，而非更多的指标

核心思想：精细化运维的关键不在于采集海量指标，而在于聚焦能反映系统健康度和业务影响的核心指标。

行动指南：识别最关键的20%指标，用这20%覆盖80%的核心问题，实现精准监控。

告警的终点是解决，而非通知

核心思想：告警只是手段，解决问题才是目的。完整的告警体系必须包含从通知到解决的全流程。

行动指南：建立告警与工单、知识库的联动机制，确保告警及时处理、复盘和沉淀，形成闭环。

“精准监控，高效闭环，让每一次告警都成为系统优化的契机”

核心观点总结（二）：释放数据价值，即刻行动

让数据从成本变为资产

核心思想：运维数据是企业的宝贵财富，不应仅用于故障排查，更应成为容量规划、成本优化及业务决策的重要依据。

行动指南：建立数据驱动的运维文化，利用分析结果指导实践，让数据真正为业务发展赋能。

精细化运维，每一天都可以开始

核心思想：精细化运维是持续改进的过程，而非一蹴而就的项目。不必追求一步到位，从最小可行性场景切入即可。

行动指南：从当前最痛点入手，设定小目标，用数据验证效果，逐步推广，积小胜为大胜。

“数据驱动决策，行动创造价值”

监控易：精细化运维的核心支撑平台



采得深：全栈深度采集

覆盖网络、服务器、数据库等全栈资源，实现无死角数据采集



算得准：智能分析与降噪

精准定位故障，减少误报干扰



联得通：流程闭环管理

集成工单系统，告警自动触发流程，实现运维处置闭环



看得远：数据驱动决策

通过历史趋势分析与容量规划，辅助管理层进行前瞻性决策



监控易-IT基础监控涵盖范围概览

接下来：产品功能现场演示



深度监控



智能降噪



流程闭环



数据驱动

搜索 [监控易官网](#) [监控易公众号](#) [联系我们](#) | 获取演示资料 ·
专家实时答疑 · 技术深度交流

感谢观看

Q & A

欢迎提问与交流

