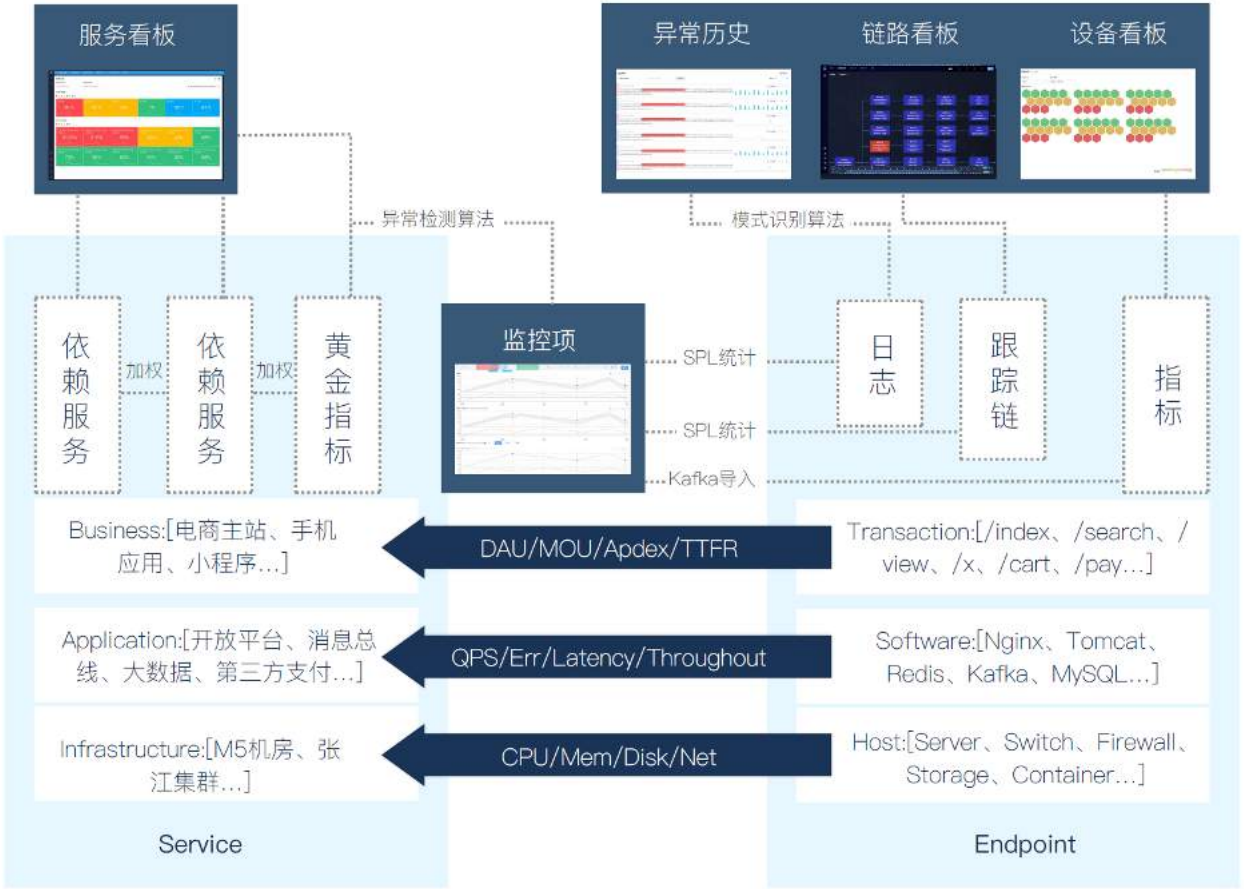
AIOPS：智能运维做智能决策

智能运维

智能运维AIOps，是指将人工智能算法应用于分析运维大数据。有了AIOps，当IT出现故障隐患， 运维人员不需要再等待系统发出故障告警，通过内置的机器学习算法以及大数据技术，系统就能自动发现各类异常，进而实现从异常入手判断故障发生的可能性、严重性和影响，依赖智能分析结果，判断最佳的应对方案。



智能运维功能及价值

日志易 rizhiyi.com

机器学习

智能运维应用回归、分类、聚类等几十种算法，开箱即用，适用场景丰富

智能告警

通过告警归并、LogReduce数据概要归并、KPI相关度计算等，实现海量告警的智能应对

智能异常检测

依据平台的智能算法，智能运维可自动判断各类指标异常与否，无需用户手动设定监控阈值

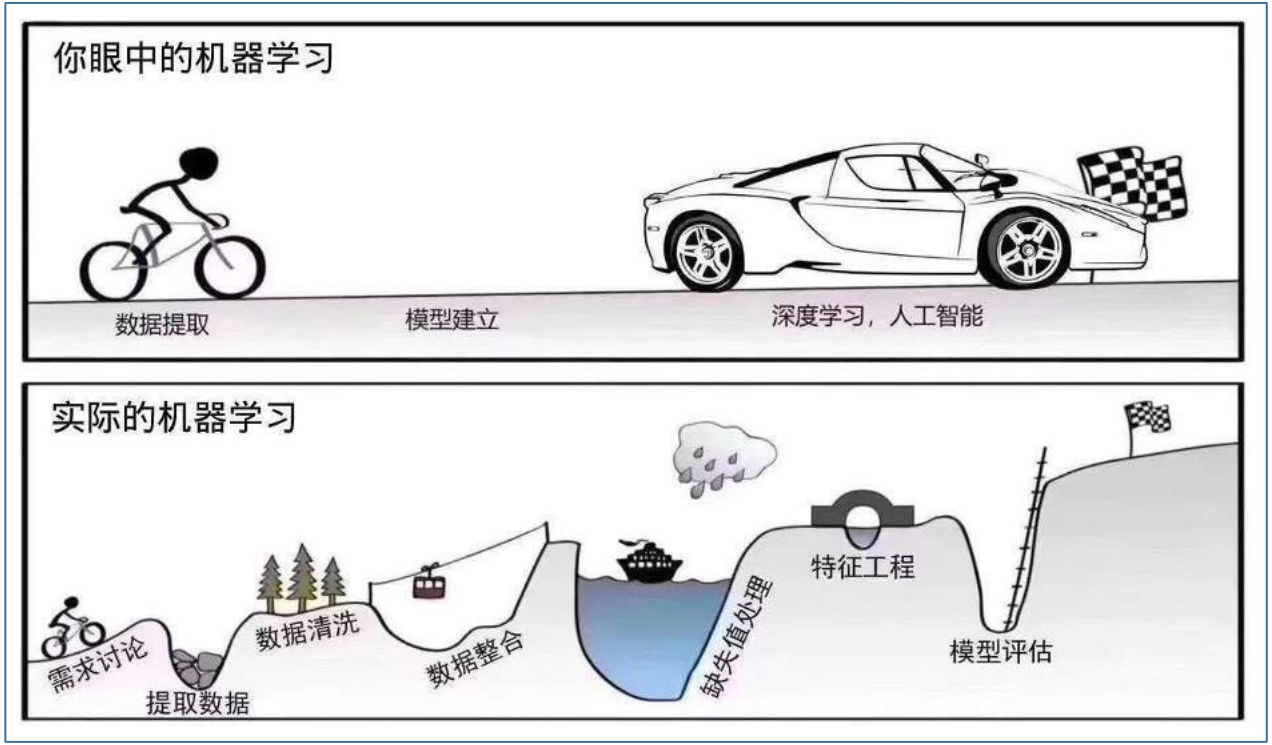
智能决策分析

对多维数据集指定目标字段的临界点后，自动定位得到影响最大的组合，实现快速修复

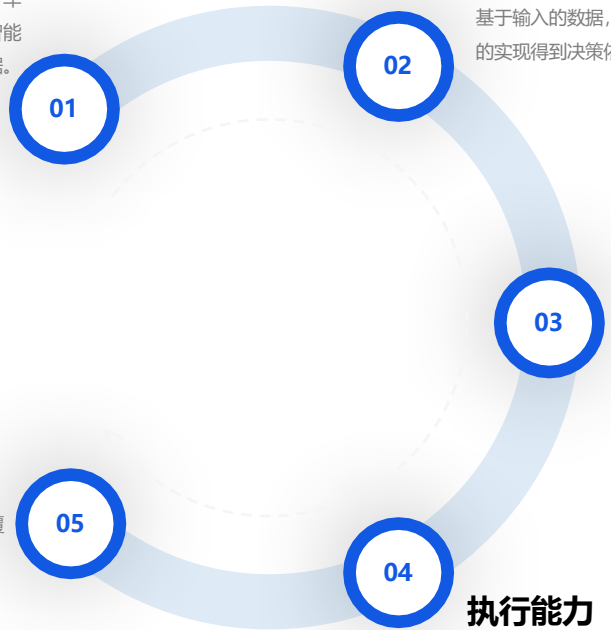
智能运维-建设认知

在AIOps体系逐步建设和完善的过程中，我们在不同的极端会碰到不同的问题，比如取数据问题，检测训练问题，模型迭代问题，告警风暴问题等等

- 指标抽取
- 数据训练
- 模型迭代
- 准确性
- 告警风暴



智能运维-能力建设



感知能力

智能驾驶过程中，感知层借助与各类传感器感知，来收集行车周边环境信息。智能化运维能力感知层借助于数据输入为智能运维场景了解系统实际运行状况提供数据。

分析能力

基于输入的数据，进行数据分析，并由此为智能运维场景功能的实现得到决策依据的过程。

决策能力

基于分析过程推理得到的依据或选项，选择并确定智能运维场景中的任务安排和决策方案。

执行能力

基于决策过程确定的策略，根据场景不同做出进一步运维操作的过程。

知识更新能力

基于过往操作、决策/经验或新业务/场景，进行知识迁移覆盖，更新知识以提升现有能力的过程。

智能运维-建设等级划分

维度/分级	L1-初始智能化运维 系统工具辅助数据采集，人工分析决策	L2-辅助智能化运维 部分场景基于静态策略自动化分析，人工决策	L3-进阶智能化运维 特定场景实现动态策略自动分析，预先设计场景系统辅助人工决策	L4-全面智能化运维 系统实现动态策略完整闭环，预先设计场景系统辅助人工决策	L5-高度智能化运维 全部场景完成全部闭环，系统自动完成运维决策操作
执行	系统为主+人工为辅	系统	系统	系统	系统
感知	人工为主+系统为辅	系统为主+人工为辅	系统	系统	系统
分析	人工	人工为主，系统为辅	系统为主+人工为辅	系统	系统
决策	人工	人工	人工为主，系统为辅	系统为主+人工为辅	系统
知识更新	人工	人工	人工	人工为主，系统为辅	系统

智能运维-建设目标

□ 事前保障：

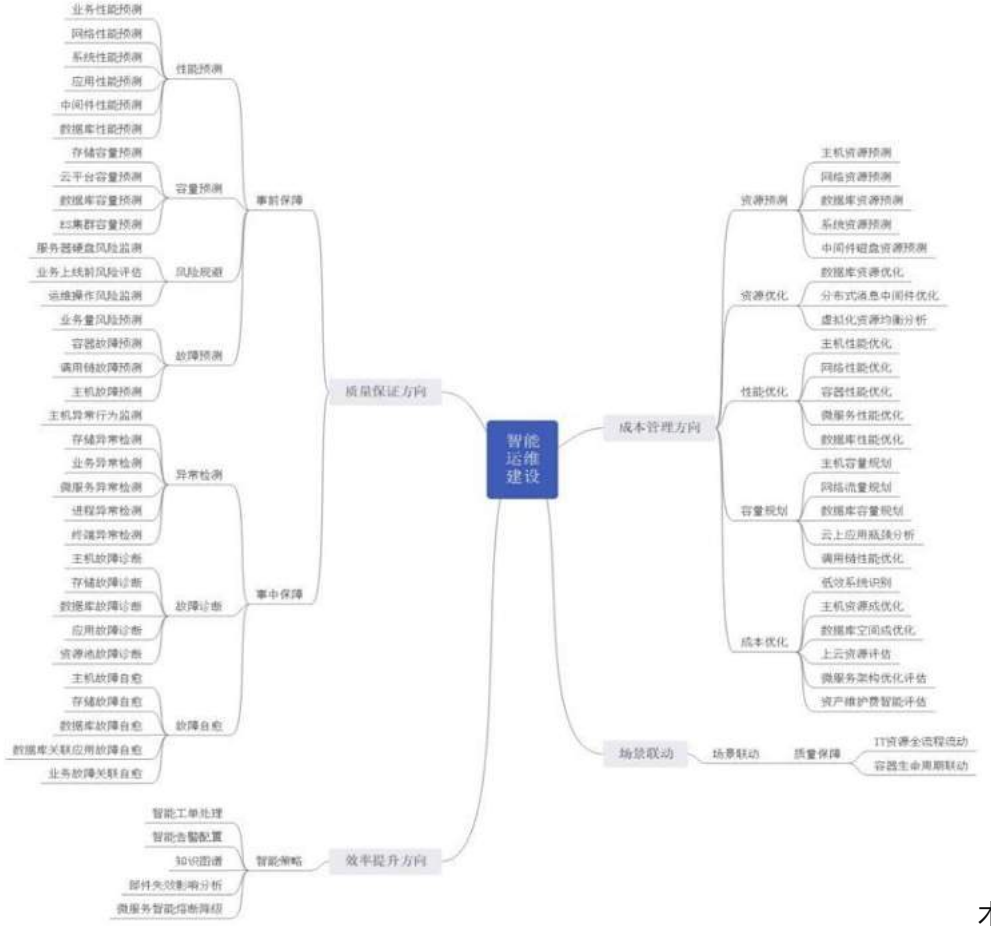
性能预测、容量预测、风险规避、故障预测

□ 事中保障：

异常检测、故障诊断、故障自愈

□ 事后优化：

资源优化、容量规划、成本优化

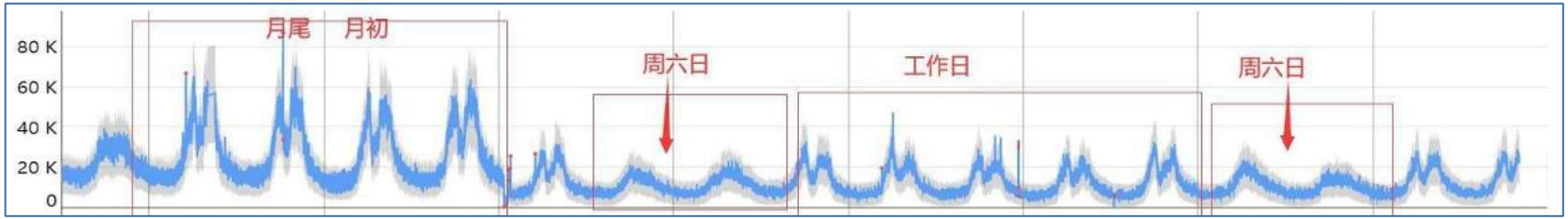


AIOps优势-感知诊断能力

日志易 rizhiyi.com

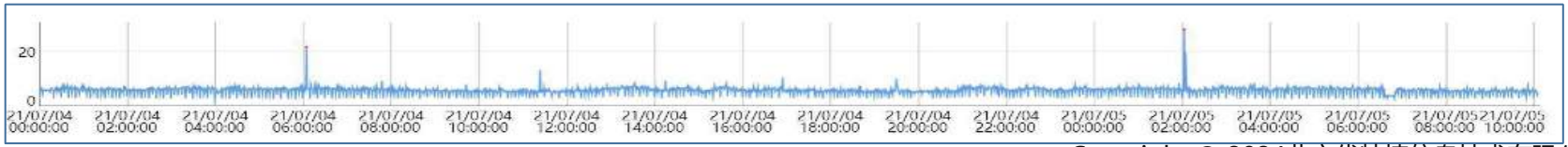
1 **解决周期性指标监控问题**

相较于传统监控，使用AI进行指标监控能够更完美的解决周期型指标的监控问题，能够适应不同的季节性。



2 **解决动态阈值配置问题**

同类对象的常规值存在差异，如果使用传统的阈值监控，配置阈值需要较多的历史经验及配置成本。AI解决了这个难题。



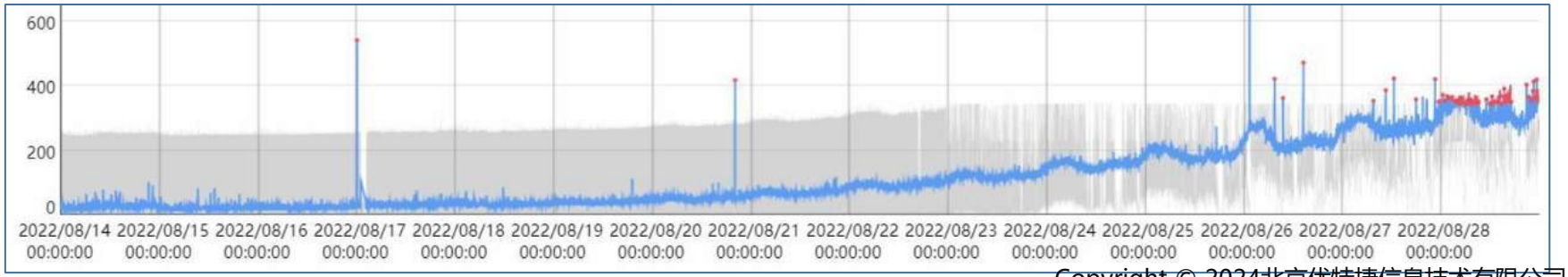
AIOps优势-感知诊断能力

4 **劣变过程中发现问题**

在我们使用传统监控时，容易存在一些难以覆盖的盲区，导致我们难以故障发生前感知风险。

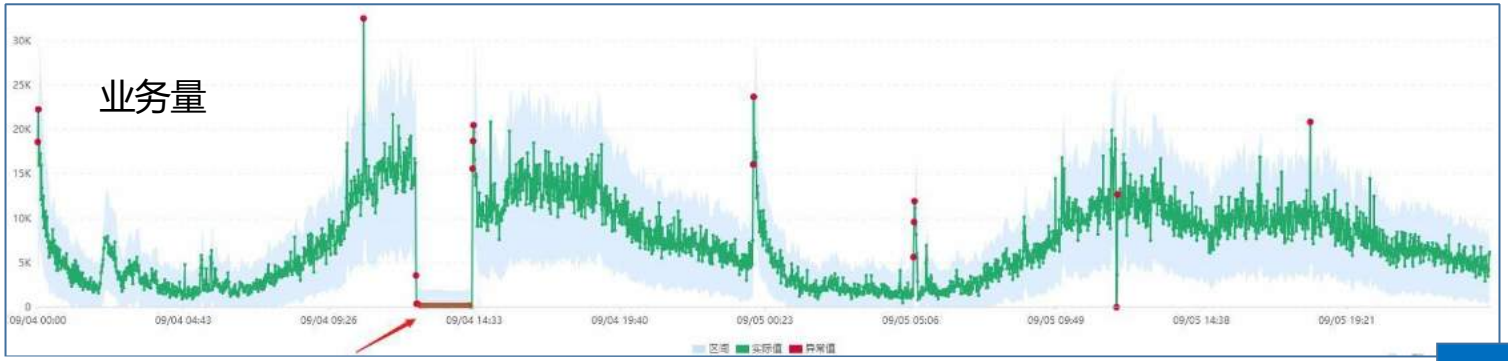
盲区1：偏离历史模式并持续，但未超过阈值。

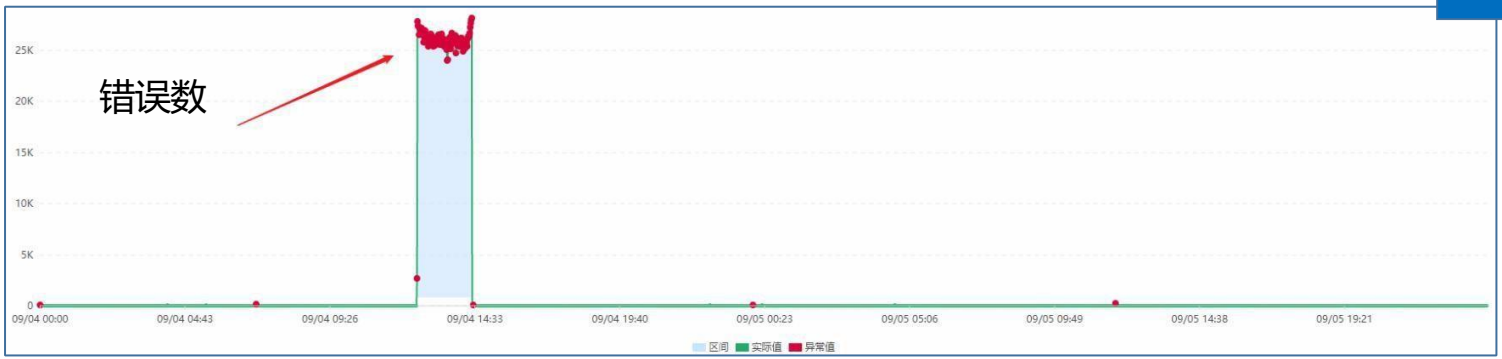
盲区2：突增未超过阈值
盲区3：缓慢增长未超过阈值



AIOps优势-感知诊断能力

3 **健康度分析/相关性分析** 传统监控的指标都是独立的，只能比较片面的体现问题。使用AIOps，能够将统一对象的不同指标进行关联，达到共同 计算健康度的效果。





原理-根因分析

我们以重点业务指标**监控告警为切入点**，对该业务进行横向根因分析，在整个业务串联的线条中，找到出现问题最深的子服务，以异常子服务作为焦点，找到该服务所属的应用，主机，网络，调用中间件等，并联合相关对象，进行立体的纵向分析，从而得到问题根因。

点

我们以关键业务的关键指标作为监控目标，实现关键业务最小粒度的点对点监控。

线

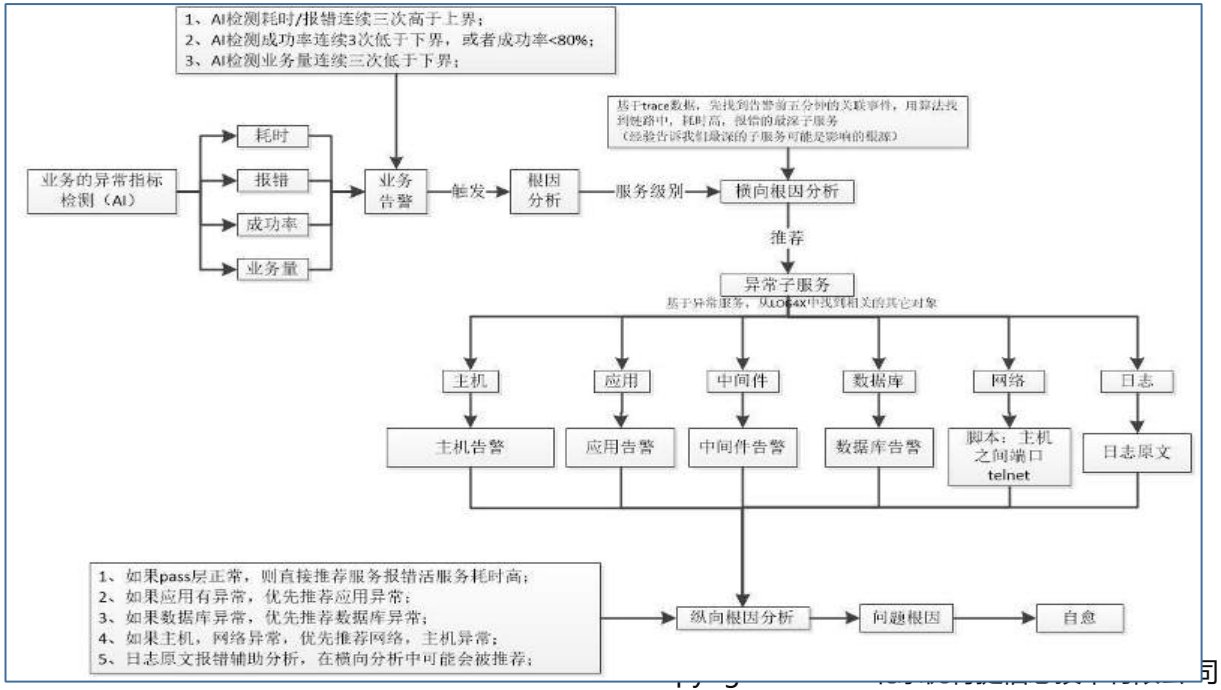
以异常服务为触发点，构建对应服务的所有调用关系图，并通过MicroDigger算法，找到调用链路中最深的异常子节点。

面

以异常子服务作为焦点，从日志中找到与该异常子服务相关的所有资源对象，如主机，网络，调用的数据源，调用的中间件等。

体

找到异常服务的所有相关联对象后，我们会从告警平台获取所有对象状态，并结合业务日志原文，通过时间，优先级，深度判断，最终帮用户找到问题根源。



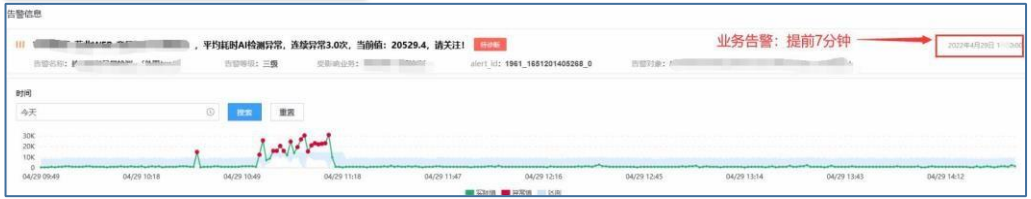
案例-根因分析

日志易 rizhiyi.com

2022-04-29 11:03:00

2022-04-29 10:56:00

2022-04-29 11:00:00



案例-故障预测

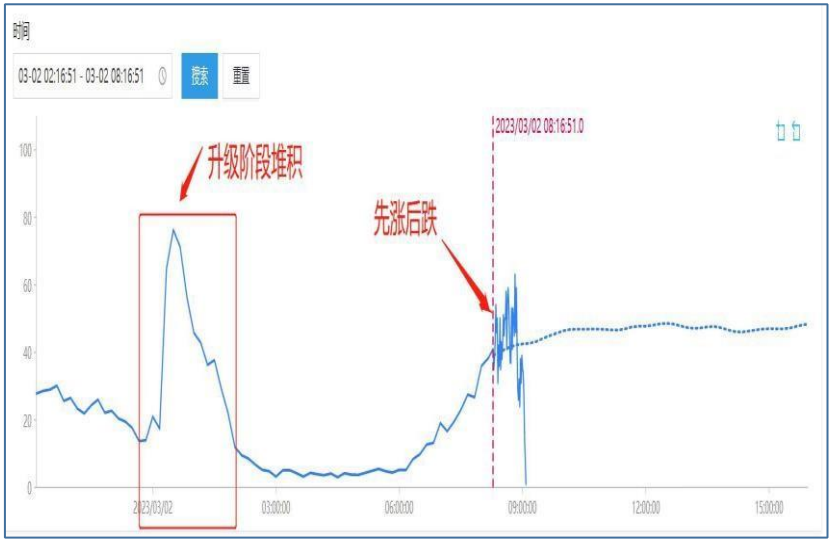
我们能够通过趋势预测算法，预测在未来一定周期内的指标趋势变化，当预测的趋势变化超出置信区间后，产生预测告警，提示未来某个周期可能产生异常。

2023-03-02 00:03:00 → **2023-03-02 08:16:00** → **2023-03-02 09:00:00**

【**告警**】业务升级，导致业务积压，产生检测告警。

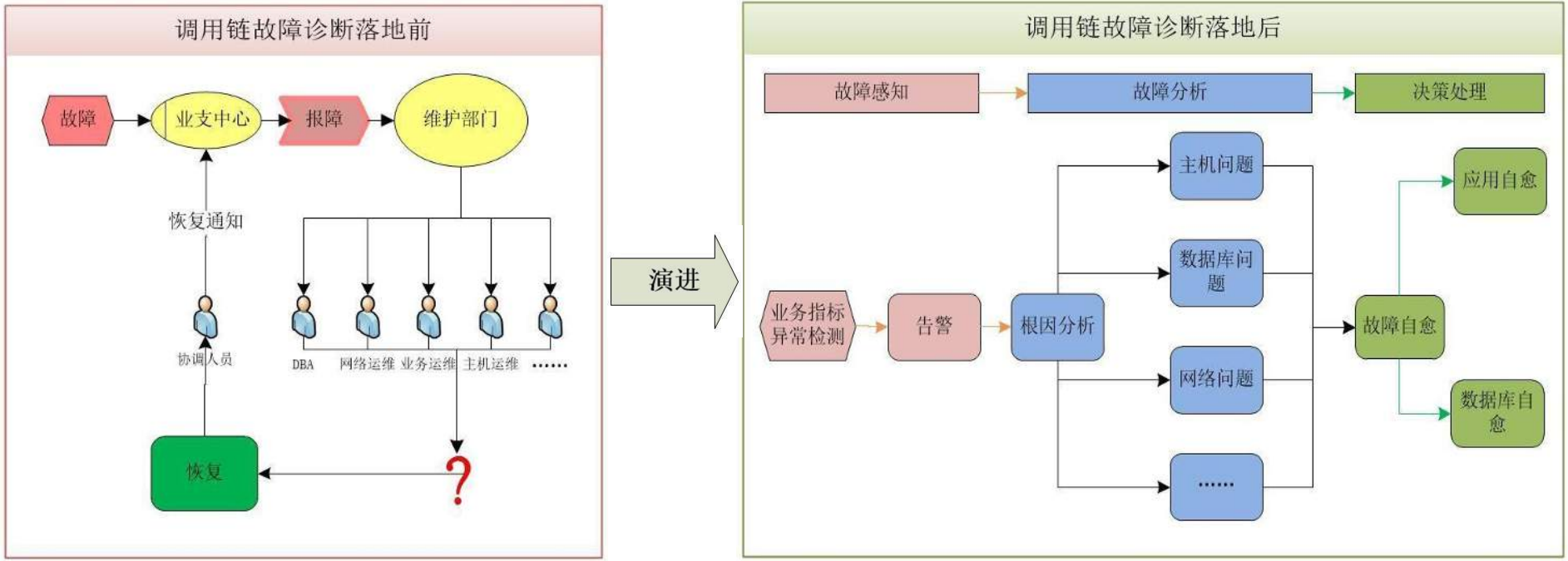
【**预警**】业务积压后业务批量提交，导致业务量超出预测区间，产生大量预测告警。

【**故障**】业务积压导致server端负载过高，进程挂死，产生业务故障。



智能运维-建设收益

调用链故障诊断场景落地之后，用户的最大收益是处理故障流程上的改变。原来是依赖人工定位，且整个处理周期耗时长。使用日志易调用链故障诊断之后，从问题的感知，到问题的分析，再到问题的处理以及后续知识库的积累，基本实现全自动化。



智能运维-建设收益

从我们公司多个智能运维项目中调查分析，发现AIOps平台建设完成后，对于我们的运维团队能够从监控的完整度，故障的发现及时率，故障处理时长等几个方面分别得到提升。

+60%

指标监控率

AIOps的引入，使得原本不好监控的指标变成更加简单。如服务级别的耗时，成功率和调用量，使用传统监控难以完全覆盖。而日志易的大数据+AI平台，恰恰能够进行补充。

-15%

故障率

由于AI对于趋势是敏感的，所以一般在趋势变化，但是还没有造成故障的时候，通过AI告警，我们能够及时的发现一些潜在异常，并做出及时处理，从而达到降低故障率的目标。

-10min

故障处理时长

在故障发生后，我们能够通过根因分析工具和诊断工具，缩小故障定位范围，缩短问题定位时长，并且提升问题定位的准确性。通过自愈功能能够更快的做出处理响应。

+7min

故障发现速度

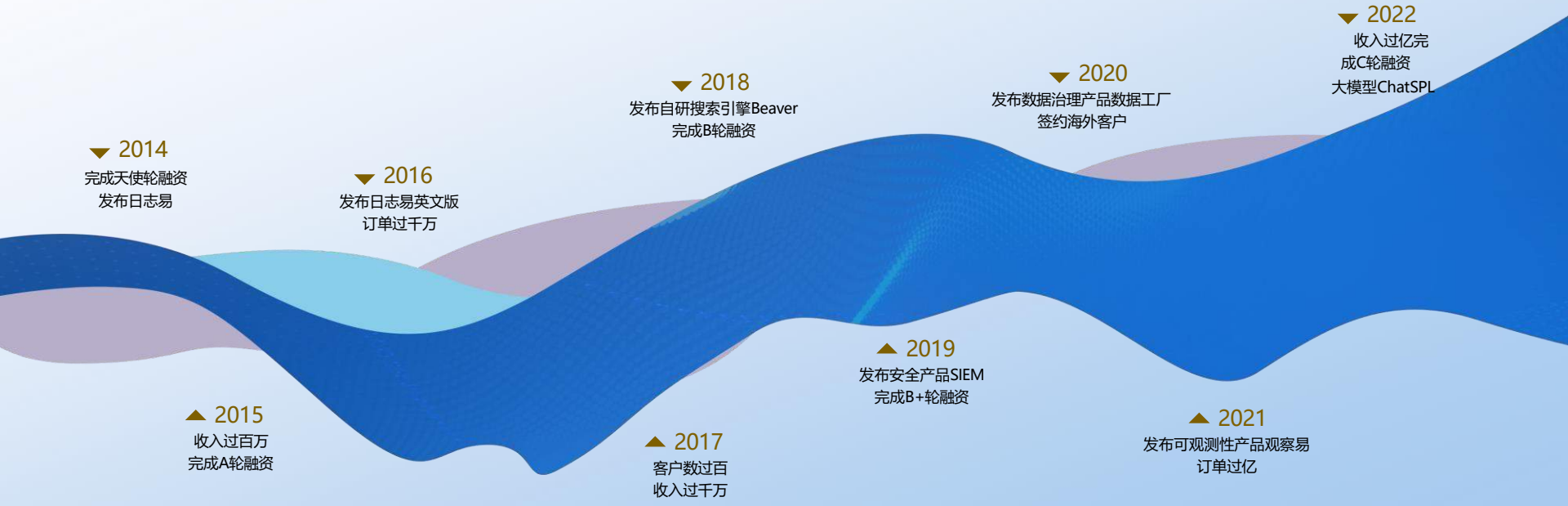
对指标的异常检测和预测，往往是对于趋势敏感的。这就使得AI在发现问题的时候，相较于传统的阈值会有先天优势。正是这种优势使得我们能够更早的发现问题。

公司介绍

北京优特捷信息技术有限公司（简称“日志易”）是国家级专精特新“小巨人”企业，领先的信创日志管理与分析平台开发商，致力于帮助各行业用户挖掘和利用机器数据价值，实现运维分析、智能运维、可观测性、安全分析、数据治理等场景，提升数字化运营能力，加速实现数字化转型，轻松应对IT及业务挑战。

公司介绍

北京优特捷信息技术有限公司是专注于机器大数据平台、服务和解决方案的开发商，致力于帮助 各行各业用户挖掘和利用机器数据价值，提升数字化运营能力，轻松应对IT及业务挑战。公司推 出智能日志中心、SIEM安全大数据分析平台、日志易LAS日志审计一体机、观察易、智能运维 AIOps、数据工厂、日志易大屏等系列产品，一站式解决机器数据采集、清洗、存储、搜索、分 析、可视化等需求，帮助企业轻松实现查询统计、业务关联分析、监控告警、安全信息与事件管 理(SIEM)、等保日志审计、用户与实体行为分析(UEBA)、智能运维、IT可观测性等应用场景。



公司资质

软件著作权：28项
专利证书：56项

服务客户 700+

日志易
rizhiyi.com

——谢谢——

吴浩
Tel 18610836173
Wechat 18610836173
Email wu.hao@yottabyte.cn
北京优特捷信息技术有限公司