

# AI 驱动 软件研发 全面进入数字化时代

中国·深圳 11.24-25

AI+  
software  
Development  
Digital  
summit



## 云原生场景下可观测性AIOPS落地实践

杨金全 基调听云

# 科技生态圈峰会 + 深度研习



——1000+ 技术团队的选择



K+全球软件研发行业创新峰会

会议时间：2024.05.24-25



K+全球软件研发行业创新峰会

会议时间：2024.09.20-21



AI+ 软件研发数字峰会

会议时间：2023.11.24-25



AI+ 软件研发数字峰会

会议时间：2024.07.19-20



AI+ 软件研发数字峰会

会议时间：2024.11.15-16



## 杨金全

基调听云研发VP

中国第一批商业化APM工具缔造者、实践者，目前专注在智能观测性平台的产品研发及商业化运营上，对APM及可观测性行业有较深入的理解及洞见。常年服务于金融、运营商及高科技等行业的头部客户，为其提供专业的技术方案和产品服务。

# 目录

## CONTENTS

1. 加速的数字化转型对IT运维带来的挑战
2. 可观测性的5大信号及其价值
3. AIOPS 现状及落地思路
4. 遇见答案 - 智能运维AIOPS 落地实践
5. 行业案例



## PART 01

# 加速的数字化转型对IT运维带来的挑战

### 挑战与必要性

宏观趋势 / 技术趋势 / 业务挑战 / 能力范围

# ► 加速数字化转型是现代企业最重要的战略

十四五



2021-2025  
以数字化转型整体驱动生产方式

十三五

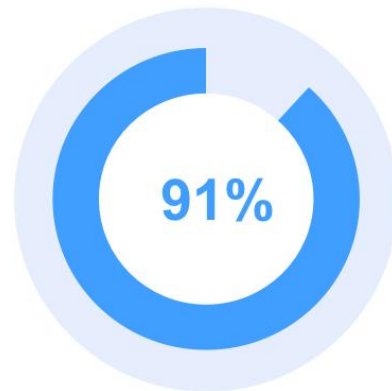


2016-2020  
推动信息技术与社会经济发展深度融合

十二五

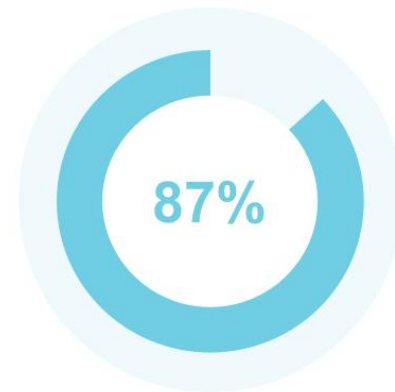


2011-2015  
推动信息化与工业化深度融合



91%的企业都参与了某种形式的数字化计划

----- By Gartner



87%的企业认为数字化将颠覆他们的行业

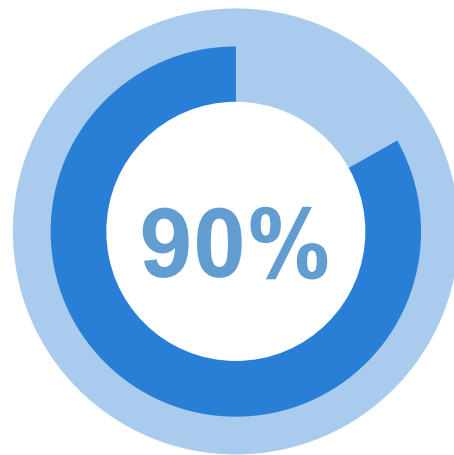
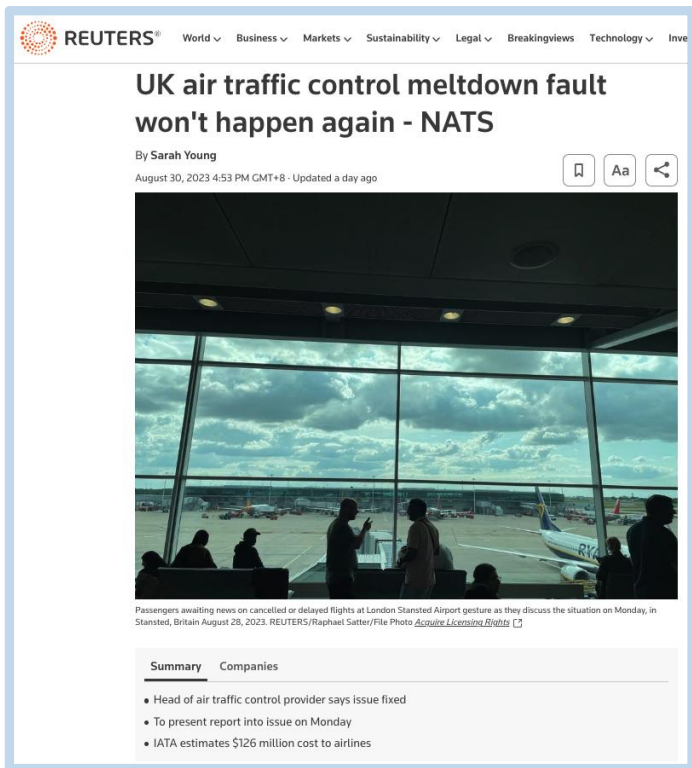
----- By 德勤

无论是改善用户体验、合作伙伴体验、员工体验、供应链效率、加快创新和产品交付，或其他方面的一些原因，企业对于数字化转型的需求从未如此强烈

AI驱动软件研发全面进入数字化时代

**AI+DD** AI+ 软件研发数字峰会  
AI+ software Development Digital summit

# ▶ 数字化业务复杂性急剧增加，IT稳定性受到严峻挑战



**Gartner:** 数字化转型以业务为中心，服务和用户体验是关键目标。而**IT**监控以系统可用为中心，仅关注系统可用性指标对于转型中的企业而言是一场灾难。到**2023**年，依赖于“正常运行时间”指标的监控实践将抑制**90%**的转型计划。



用户体验决定业务增长



分布式架构大行其道



依赖关系错综复杂



多云且动态变化



创新加速

IT团队需要变革性的技术，打破数据孤岛，理清系统运行状态，更快的故障响应、更准的根因定位、更少的用户影响，确保系统稳定性，驱动数字化转型

## AI驱动软件研发全面进入数字化时代

# ▶ 传统监控在新的场景下无法有效作用

## 某大型国有银行

- **告警多**：业务故障时会产生大量告警（日均严重告警500+），一些关键故障被告警风暴掩盖
- **故障定位难**：无法深入分析根因，影响业务恢复
- **用户体验差**：客诉增加，运维疲于救火，领导不满意

## 某省医保

- **资源多**：监控对象覆盖不全，粒度过粗
- **指标多**：监控对象类型多、指标多，当某个指标告警时运维人员很难理解其含义，如何快速处置
- **变更难**：资源依赖关系梳理不清，提心吊胆做变更



## 某运营商

- **工具多**：业务快速发展，IT规模急剧扩大，IT工具烟囱式建立
- **视角单一**：固定Dashboard，模型僵化
- **数据割裂**：数据模型不统一，无法获取“单一事实来源”“需要的数据”

## 某跨国奢侈品企业

- **监控难**：全面采用微服务、云原生技术栈，业务复杂度高，运维难度大
- **依赖复杂**：服务治理无从下手，无法驱动业务治理
- **用户流失**：用户粘性降低，流失严重

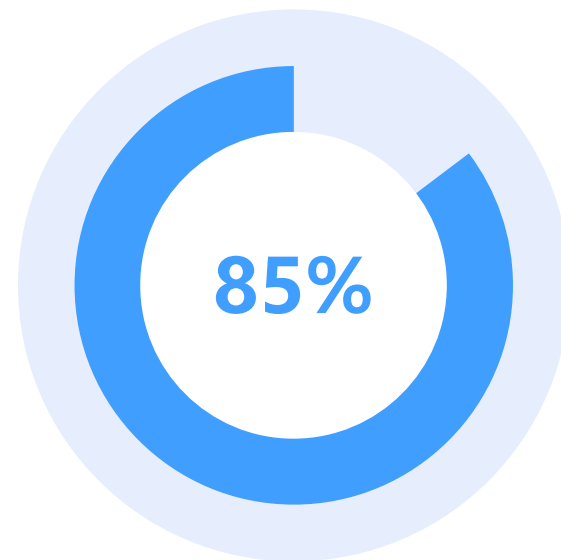
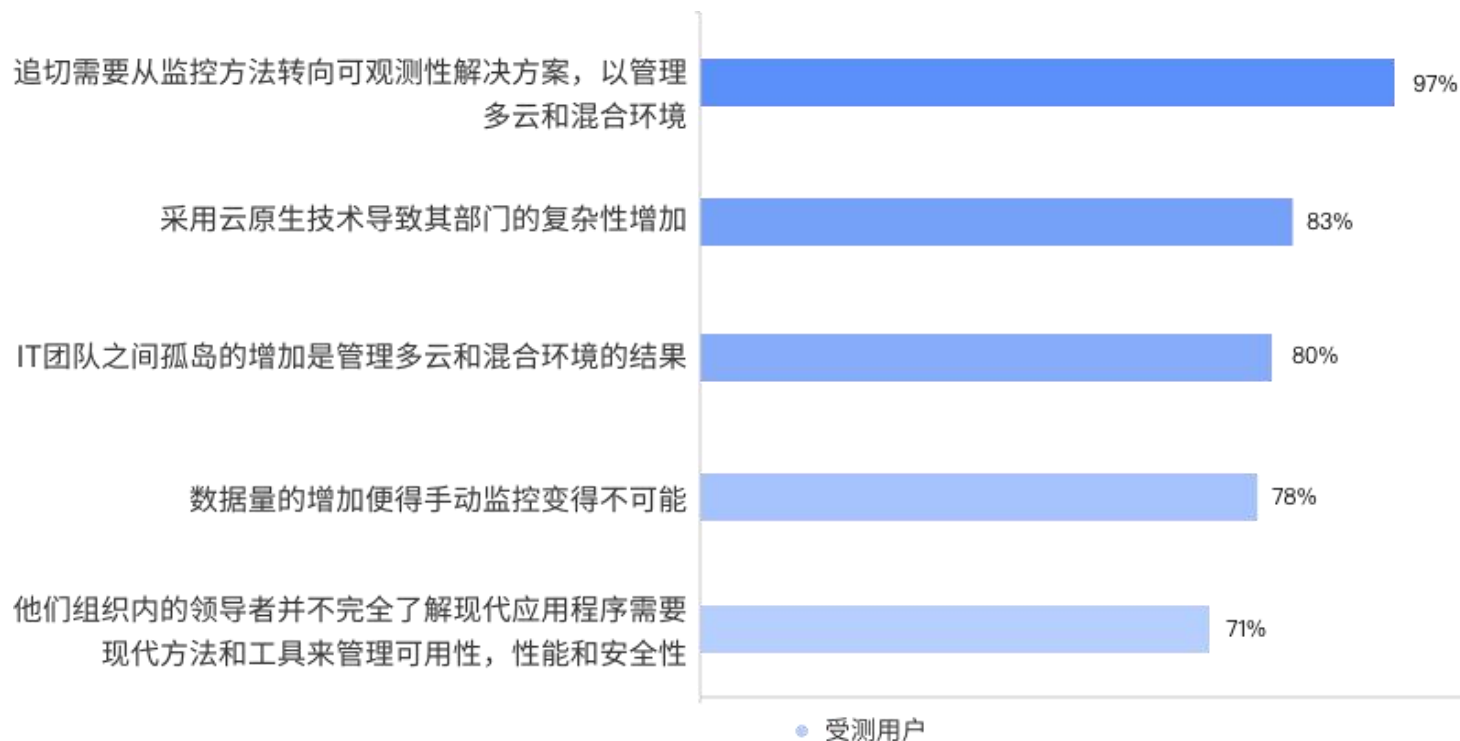
现有的工具和分析模型 **智能化程度不够**，运维数据 **未能很好转化为运维知识**，需要变革性技术方案解决运维痛点

**AI驱动软件研发全面进入数字化时代**

**AI+ 软件研发数字峰会**  
AI+ software Development Digital summit



# ► 97%的IT从业者迫切需要由监控上升到可观测性



85%的受访者表示  
可观测性现在是其企业的战略重点

该研究包括来自全球市场的 14,013 名 IT 专业人员的调查结果

AI驱动软件研发全面进入数字化时代

**AI+DD** AI+ 软件研发数字峰会  
AI+ software Development Digital summit

## PART 02

# 可观测性的5大信号及其价值

实现路径与价值

概念 / 可行性 / 实现路径 / 价值场景

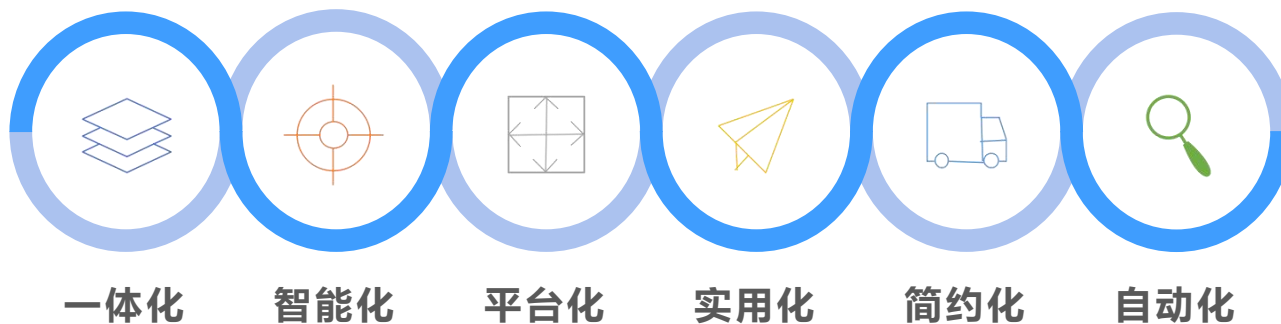
# ▶ 可观测性概念及其特点

可观测性是一种 **方法**，通过检查系统的外部输出来 **衡量系统内部状态的能力**。外部输出的数据称为信号。Metric、Trace、Log、Profile 和 Dump 是CNCF约定的主要信号，**基调听云**认为，需要增加 **用户体验** 这一重要视角，形成以 **用户为中心** 的可观测性体系。



给出答案 是衡量可观测性平台的唯一标准。

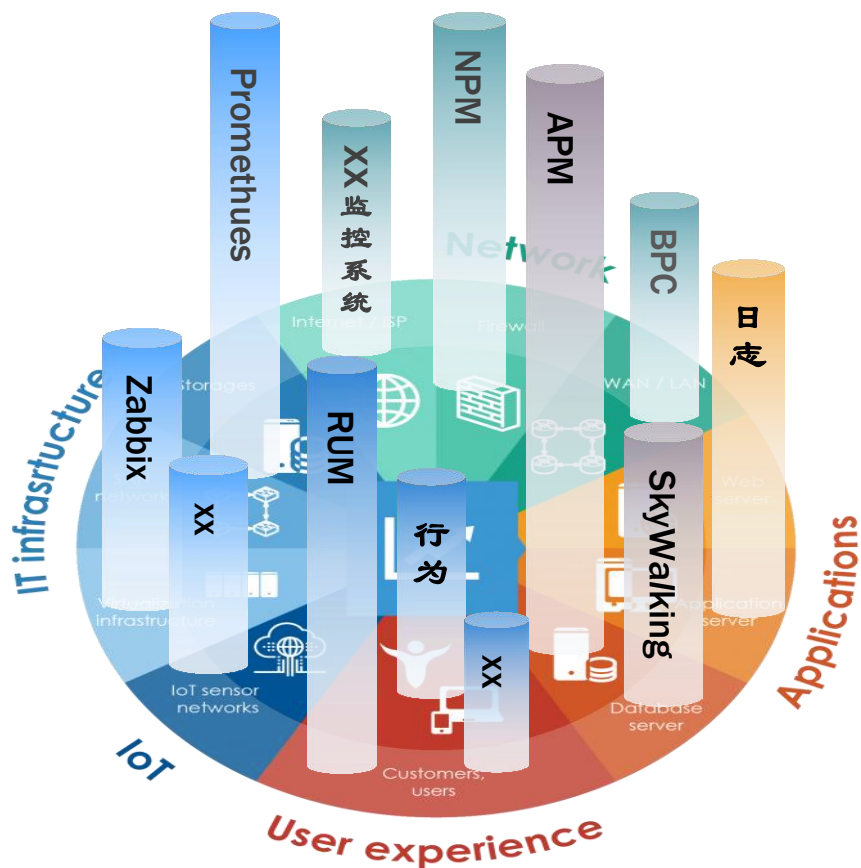
-- By 基调听云



一体化 智能 可观测性 平台

# ► 为什么需要“一体化”智能可观测性平台？

烟囱式的监控工具，形成数据孤岛



每个监控工具仅适配一个技术栈

每个监控工具数据模型不同，无法关联分析

故障处理需要在不通的监控工具间来回切换

团队间责任链不清晰，容易推诿

业务恢复正常受阻



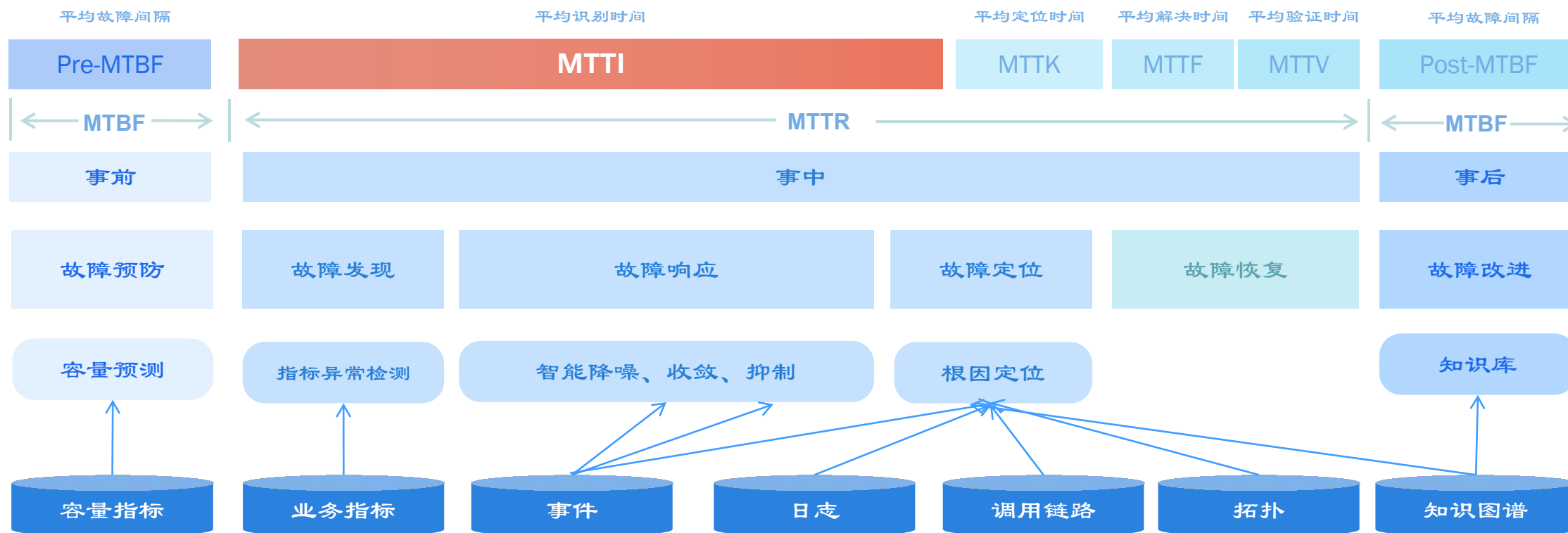
# ► 为什么需要一体化“智能”可观测性平台？

平均故障识别时间占整个故障域时间的**70%以上**

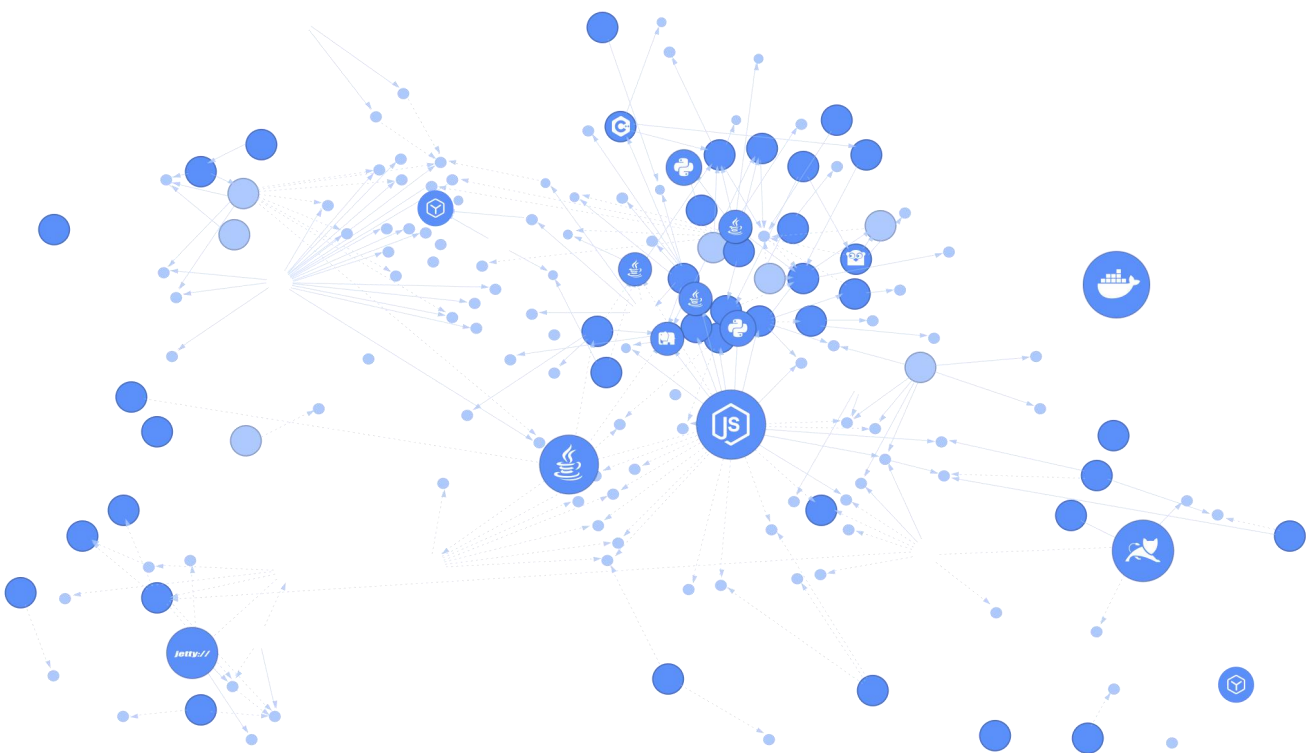
– By EMA Radar

大部分问题识别、定位依赖人肉运维

– By EMA Radar



# ► 为什么需要一体化智能“可观测性”平台？



多云、复杂、弹性的架构无法实时全景观测

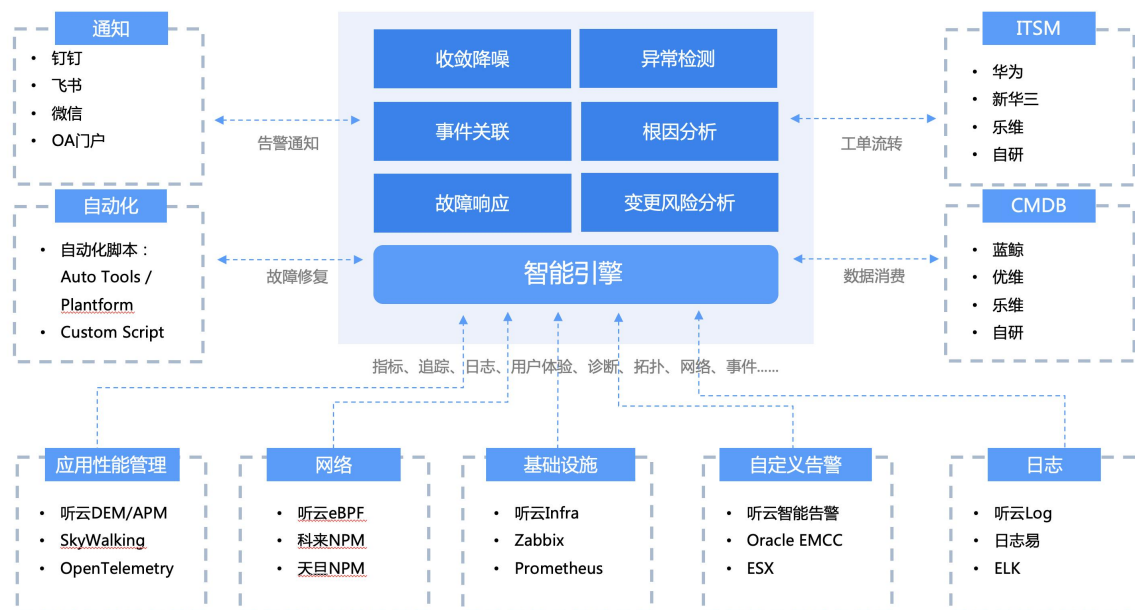
指标繁多，告警风暴，无法治理

数据散落，没有关联性，故障排查困难

缺乏应用安全监控与漏洞检测

IT与业务割裂，需要数据洞察和决策支持

# 为什么需要一体化智能可观测性“平台”



需要针对不同团队人员统一沟通语言，高效协同

需要打破孤岛并在问题影响最终用户之前主动预防

需要将可观测性、安全、数据分析集中一处

需要双向开放，保障不是另一个孤岛

需要简单、开放、自动化的集成多源数据

需要平台+应用的模式，打通可观测性上下游

需要差大规模的计算能力，主动提供答案

# ▶ 智能可观测性平台应该具备的能力



## 持续自动化

自动发现  
自动告警  
自动分析



## 智能全栈可观测

全栈拓扑可视化  
自适应技术栈变化



## AI 驱动

智能分析  
主动提供答案



## 用户体验

体验感知  
旅途回放



## 业务分析

业务转化  
业务影响



## 团队协作

统一沟通语言  
赋能组织

自动化、可扩展、AI驱动和超大规模计算



智能可观测性平台全景

一体化运维

Dashboard

指标体系

全局拓扑

数据导出

多维分析

运维门户

智能运维AIOps

告警收敛

知识图谱

故障管理

根因分析

容量管理

服务水平管理

混合云可观测性

Serverless

CMDB

基础资源  
可观测性

Namespace

Workload

Pod

云原生  
可观测性

网络流量拓扑

报文回溯

请求响应治理

网络  
可观测性

日志分析

业务指标

日志溯源

日志  
可观测性

分布式链路追踪

代码级根因分析

服务治理与诊断

应用和微服务  
可观测性

用户会话

网络拨测

崩溃卡顿

数字终端  
可观测性

运行时应用防护

运行时漏洞分析

运行时风险修复

应用安全  
可观测性

实时业务洞察

业务影响分析

业务流程分析

业务  
可观测性

性能对比

上线前压测

业务连续性保障

信创  
可观测性

数据湖仓

OneAgent

OneTrace

OneTopology

OneLog

AI中台

指标体系

业务分析引擎

超大规模计算

链路追踪 指标 日志 Dumps Profiles

十大信号、模型统一、全景可观测

拓扑 业务属性 用户旅途 元信息 网络

用户 App 小程序 网页 业务 网络 应用 请求

自动识别、自动采集、智能关联、600+技术栈、全面全量

代码 数据库 容器 进程 中间件 K8S 主机

OpenTelemetry Prometheus Zabbix Skywalking Istio

开放生态，融合共建，价值第一

NétiS 天旦 科来 日志易 爱数 阿里云 腾讯云 华为云 私有云

可观测性为AIOps提供全景高质量的数据、AIOps是可观测性故障域价值体现

# ► 智能可观测性平台价值

## ⑤ 数据驱动的决策，加速数字化转型

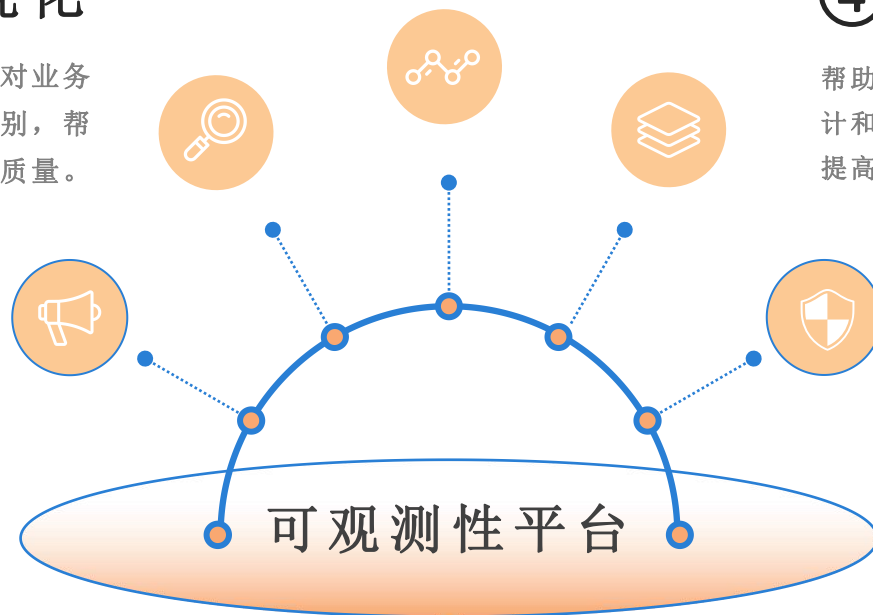
可观测性可以提供实时、准确、全面的数据，以支持企业管理人员在业务决策中作出更有效、更快速的决策。这些数据可以来源于业务流程、成本、客户满意度、业务运维等多维度数据

## ③ 业务流程可视化

业务流程执行情况各个流程的依赖和影响，对业务中存在的瓶颈点、缺陷和潜在风险进行快速识别，帮助企业改善业务流程，提供业务效率和质量。

## ① 持续自动化的实时监控和提供确定性答案

可观测行通过持续自动的监控，采集全量、全面的数据，基于AI持续自动的分析，及时发现并提供答案



## ④ 优化用户体验

帮助企业更好地了解用户的行为、需求和体验，通过对用数据的统计和分析，发现用户在业务中遇到的问题，进行业务的优化和改进，提高客户留存率和满意度，提高市场竞争力。

## ② 快速故障诊断和修复

提高业务执行的稳定性和可靠性。实时了解故障信息，快速定位、分析和解决潜在缺陷，缩短业务恢复时间，减少业务停机时间和用户受到的影响。

给出确定性答案，让运维更简单

## PART 03

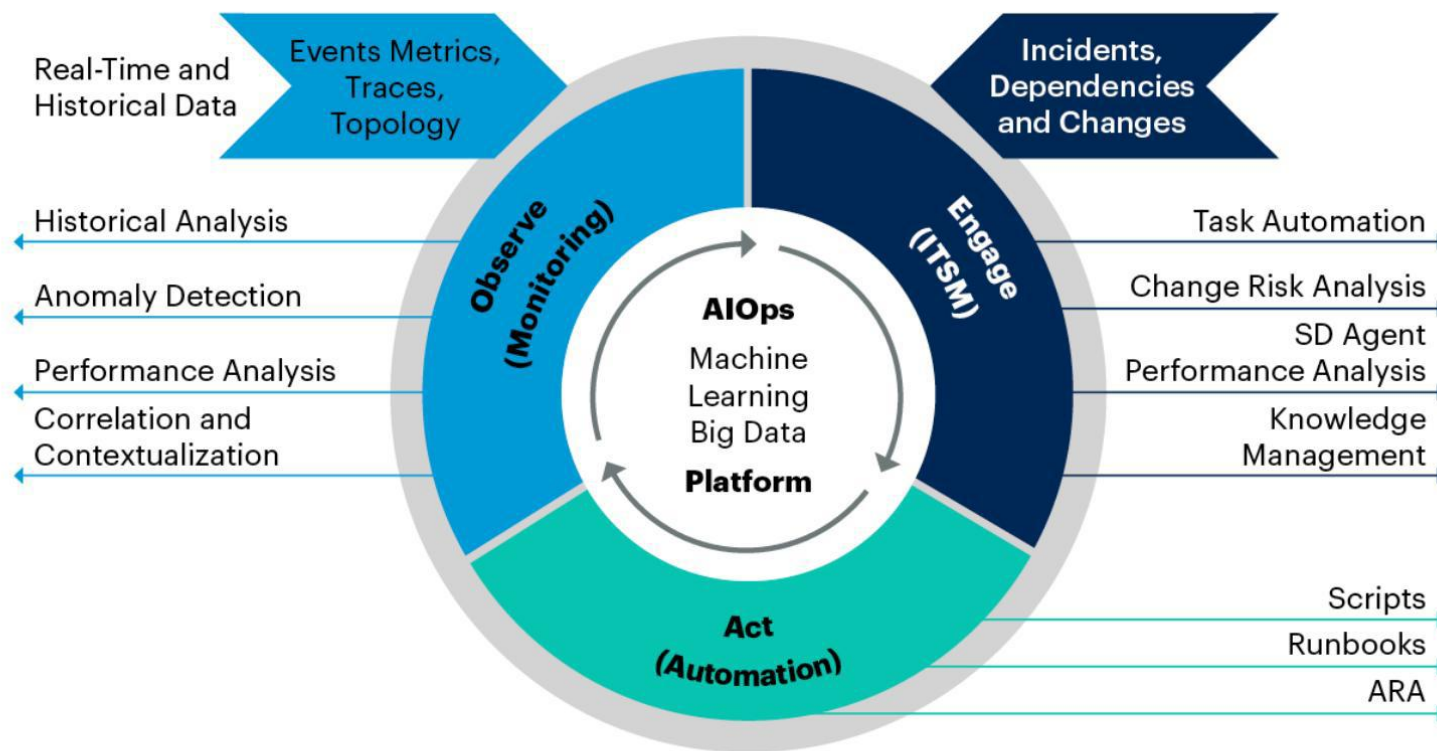
# AIOPS 现状及建设思路

智能运维AIOPS

行业现状 / 建设思路

# ▶ AIOPS的定义

## AIOps Platform Enabling Continuous Insights Across IT Operations Monitoring (ITOM)



Source: Gartner  
735577\_C

(2021)

# 国内AIOPS项目现状

超过90%的AIOPS项目落地未达预期<sup>①</sup>

1

## 缺乏落地场景

- 仅在告警收敛、关联分析上略有成效

2

## 数据质量不高

- 数据模型不统一，无关联性，存在噪声、丢失、不完整等问题

3

## 业务领域不匹

- 国内众多A

“活的”数据是资产，  
“死的”数据是负债，只会产生“噪声”

4

## 技术成熟的低

- 单指标异常检测、多指标异常检测、相关性分析、因果推导、机器学习、深度学习等技术进展缓慢

5

## 成本高

- 依赖人工为数据打标签、清洗、建模，反复增加或调整参数

6

## 周期长

- 以年为单位推进

没有打破数据边界的AIOPS工具，仅是在用AI“降噪”而已



# ► 智能运维AIOps项目建设思路



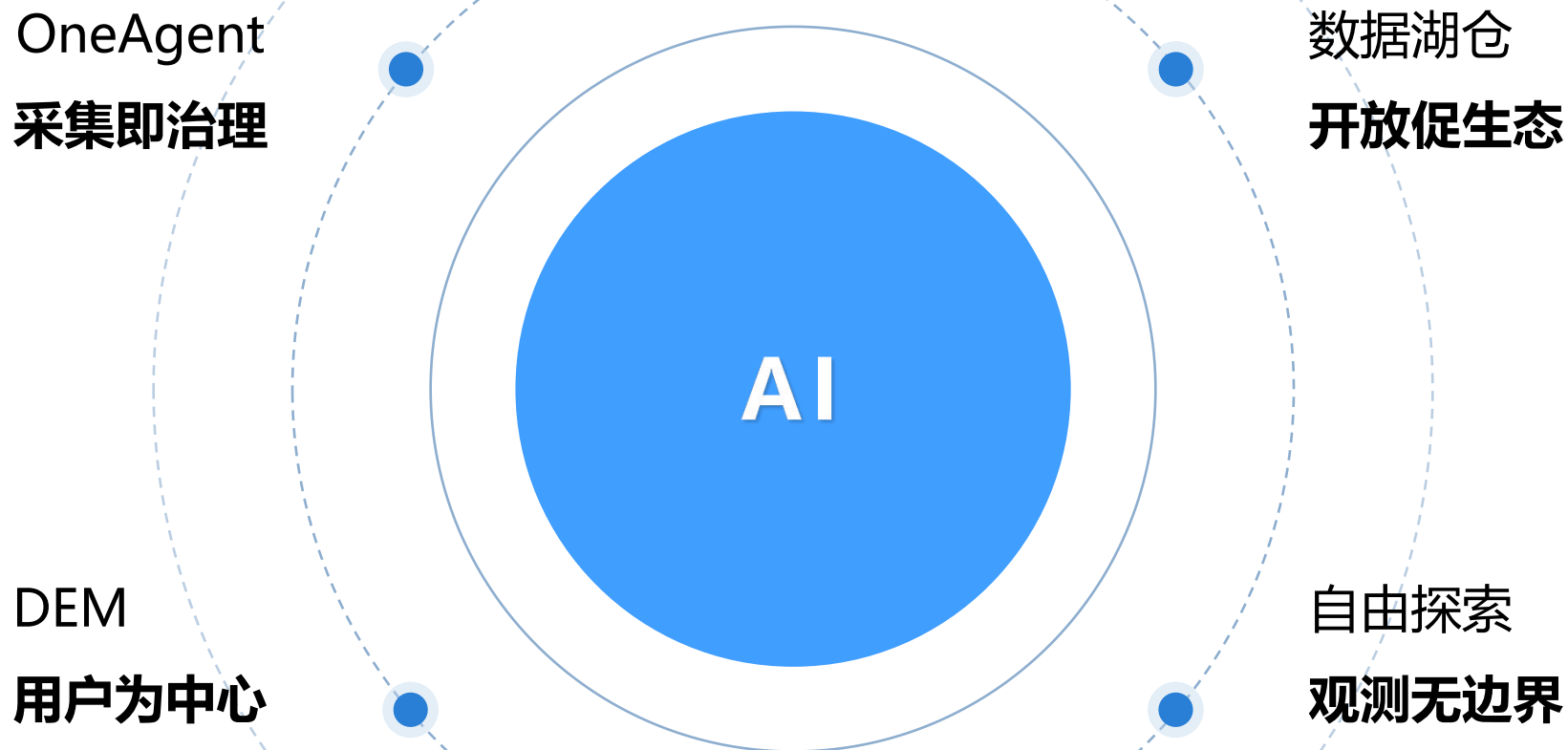
## PART 04

# 遇见答案 - 智能运维AIOPS 落地实践

能力优势与落地场景

采集即治理 / 以用户为中心 / 数据湖仓 / 自由探索

## ► 基调听云智能可观测平台5大特点



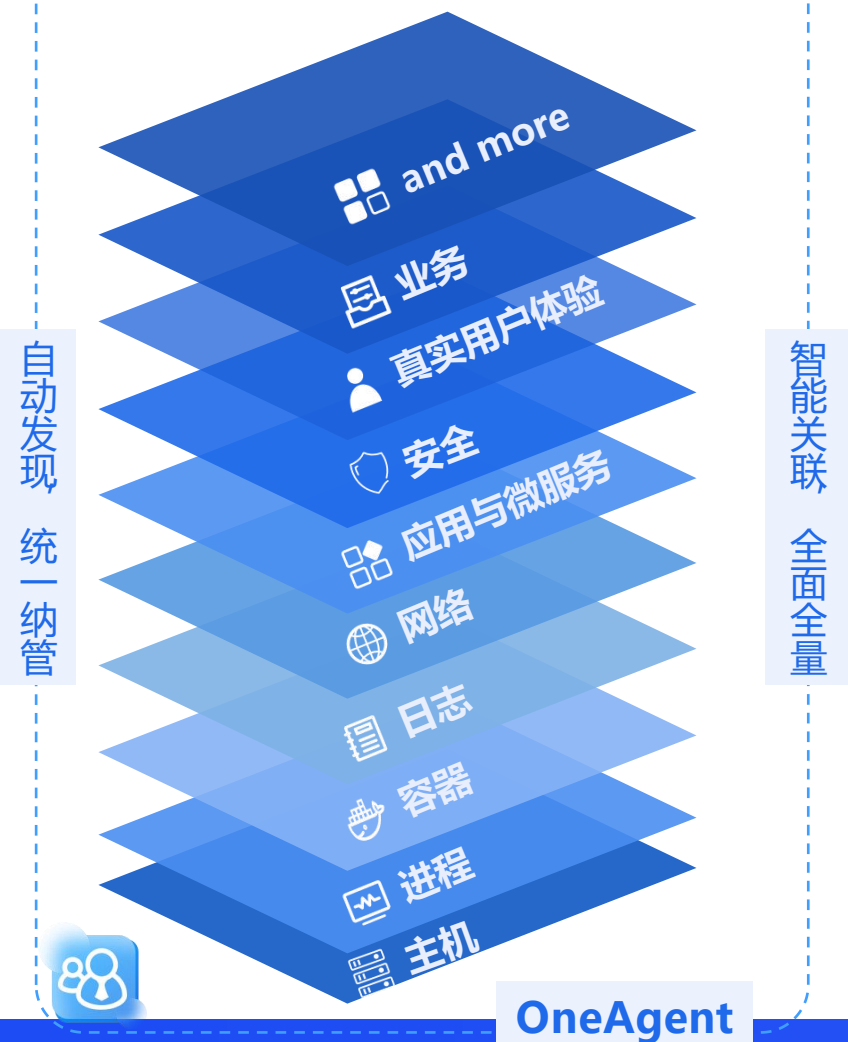
# OneAgent

---

采集即治理、采控一体、持续自动、全面全量

# ► OneAgent: 采集即治理

一次安装、静默运行



## NO.1

最大企业级部署案例 1W+

## 100+

行业头部客户适配经验

- **采集即治理**，连接数据+模型+对象+AI，实现**全景上下文**
- **自动化的端到端数据采集**，**自动识别**、**自动采集**、覆盖600+技术栈、全面全量
- **统一数据模型**，从数据采集开始连接5大支柱+5大扩展数据模型，确保所有人获得一致的“**单一事实来源**”，无需在工具间跳转和数据校准
- **面向未来的可扩展性**，基于**主机**或**Kubernetes**部署，无忧升级、灵活配置、按需编排和加载
- **统一纳管**，采集对象包含用户、业务、Hybrid App、网页、小程序、网络、应用、安全、请求、代码、进程、容器、中间件、数据库等
- **生态兼容**，全面兼容开源标准**OpenTelemetry**

安装它，忘记它 - 它会处理好一切



# ► Payload、代码深度观测，让应用安全顺理成章

## 多维提升漏洞检测准确度

核心规则全部可编辑，可自定义更匹配业务模式的检测策略，我们不仅提供安全能力，更帮助企业进行自己的安全能力沉淀。

## 跨服务全链路漏洞污点追溯

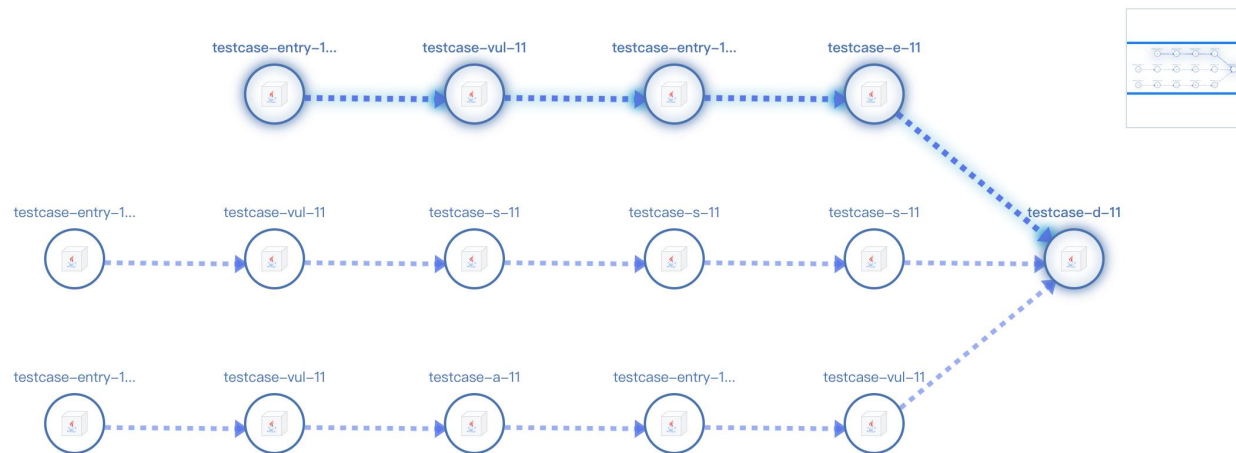
基调安云IAST特有的轻Agent端+重服务端，可在服务端动态加载检测引擎，可基于微服务中的跨服务调用等追溯重难点漏洞定位，帮助安全人员极速修复。

## 全栈安全测试

联动黑盒、白盒、SCA、API等安全检测/测试工具，助力DevSecOps概念落地不可或缺的一部分。

### 漏洞描述

命令执行漏洞是指由于Web应用程序对用户提交的数据过滤不严格，导致黑客可以通过构造特殊命令字符串的方式，将数据提交至Web应用程序中，并利用该方式执行外部程序或系统命令实施攻击，非法获取数据或者网络资源等。



上游Service Beta ^

testcase-entry-11 高危 1 中危 0 低危 0 提示 4

http://127.0.0.1:8012/spring-cloud/feign/vul/unsafe/cmd-injection/runtime-exec-Entrance-e

### 数据流

### 污点流

|        |                                                                             |    |
|--------|-----------------------------------------------------------------------------|----|
| 污点来源方法 | 数据对象传播<br>org.springframework.web.method.support.InvocableHandlerMethod:167 | /s |
| 危险方法   | 数据对象返回<br>feign.ReflectiveFeign\$FeignInvocationHandler:100                 | /s |



联动条件：操作名称:登陆

清除所有联动

总触发次数 20,740 次

总活跃用户数 0 人

0.980%

报错率

触发次数Top5操作

### 操作响应时间分布趋势

贷款申请笔数 1,432

信审审核次数 1,790

信审退回工单数 354

信审完结工单 723

信审耗时详情 ▾

| custRequestNo | 贷款申请时间              | 信审通过时间              | 工单信审耗时    |
|---------------|---------------------|---------------------|-----------|
| 0202107497893 | 2021-07-02 13:39:16 | 2021-07-02 15:04:08 | 1.41 hour |
| 0202107496405 | 2021-07-02 13:14:40 | 2021-07-02 14:41:03 | 1.44 hour |
| 0202106456125 | 2021-07-02 13:11:06 | 2021-07-02 13:46:27 | 35.35 min |
| 0202106484549 | 2021-07-02 13:09:38 | 2021-07-02 14:10:51 | 1.02 hour |
| 0202107496838 | 2021-07-02 13:09:28 | 2021-07-02 15:20:33 | 2.18 hour |

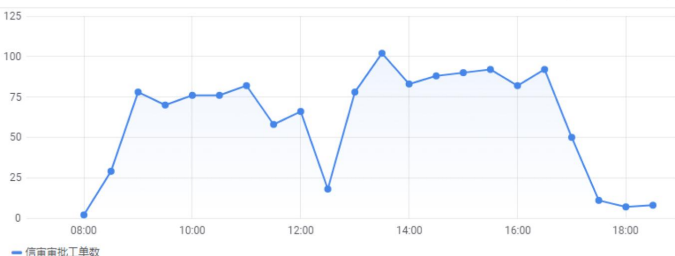
### 一 不同品牌车辆贷款金额

| Country | Number of people |
|---------|------------------|
| USA     | 383000           |
| UK      | 221236           |
| France  | 171500           |
| Germany | 120680           |
| Italy   | 119000           |
| Spain   | 100000           |
| Japan   | 90000            |
| China   | 80000            |
| India   | 73500            |
| Brazil  | 70200            |

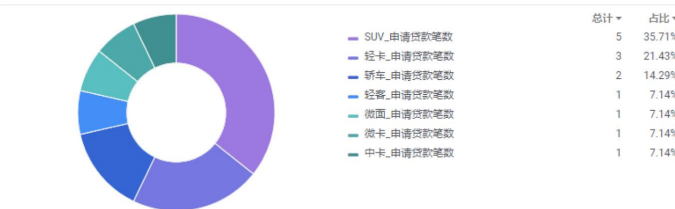
贷款业务监控看板

<
最近7天
>
+
↺
关闭

信审审核业务量趋势 ▾



#### 一 不同类型车辆贷款笔数

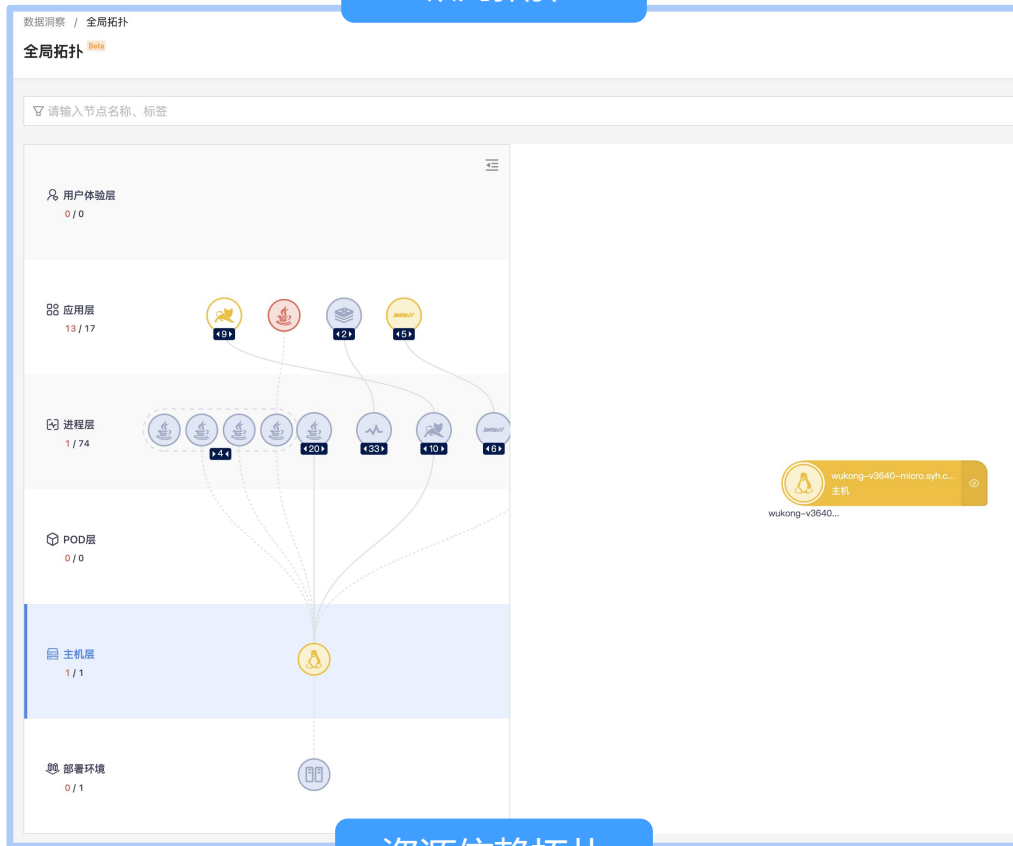


不同类型车辆贷款金额



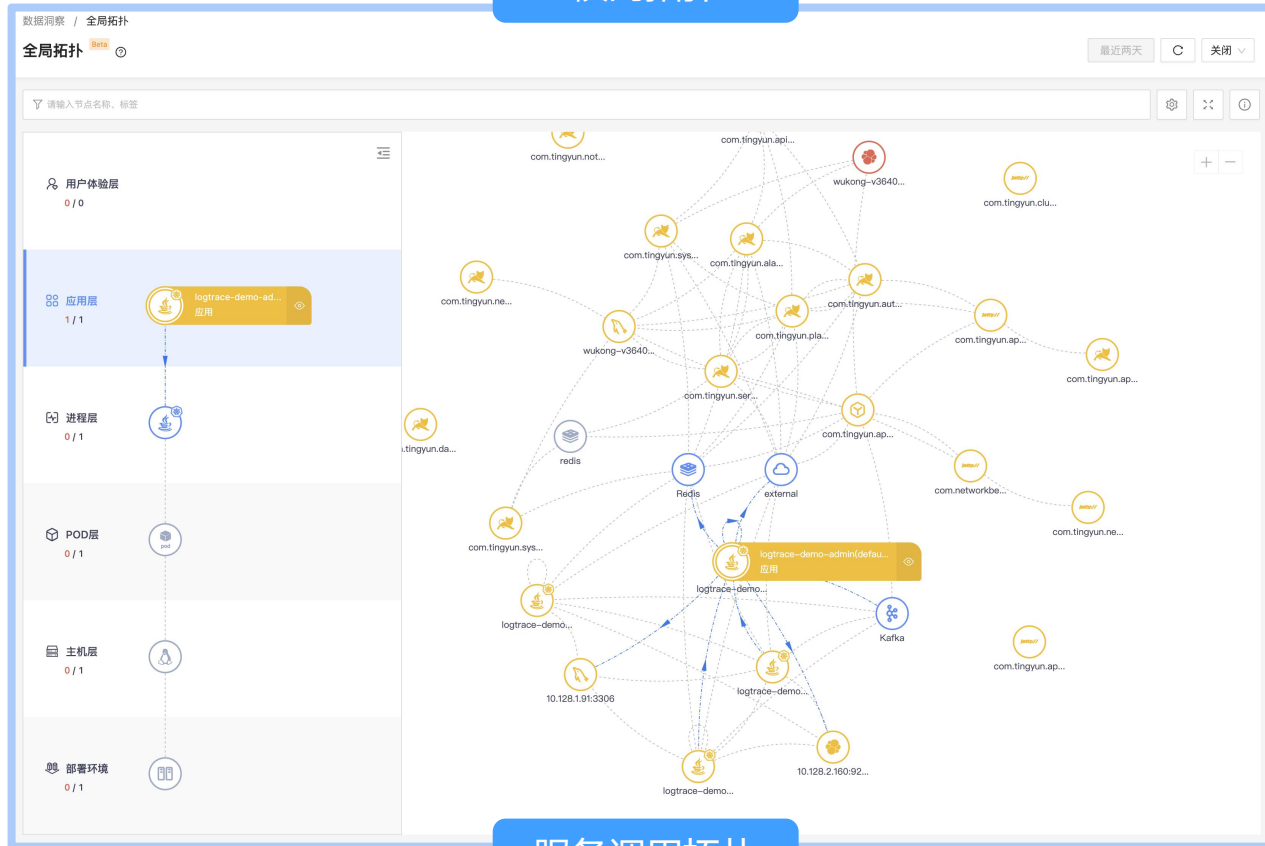
## ▶ 数据全链接，场景深融合，全景可观测

## 纵向拓扑



## 资源依赖拓扑

## 横向拓扑



## 服务调用拓扑

# 数据湖仓

---

湖仓一体、超大规模计算、AI4Data、生态开放



# 数据湖仓：全栈可观测性大数据基础设施

观云数据湖仓全景



## 存算分离

- **三层池化的存算分离架构**：算子Native、冷热数据自动分级处理。
- **交互式OLAP**：支持高性能分析，支持资源弹性伸缩

## 智能化数据生产线

- **全栈数据AI4Data**：数据治理全流程智能化。
- **一键实时数据湖集成**：一站式任务管理，AutoETL自动作业，提升集成效率。
- **智能运维**，血缘分析，数据资产管理与数据安全。

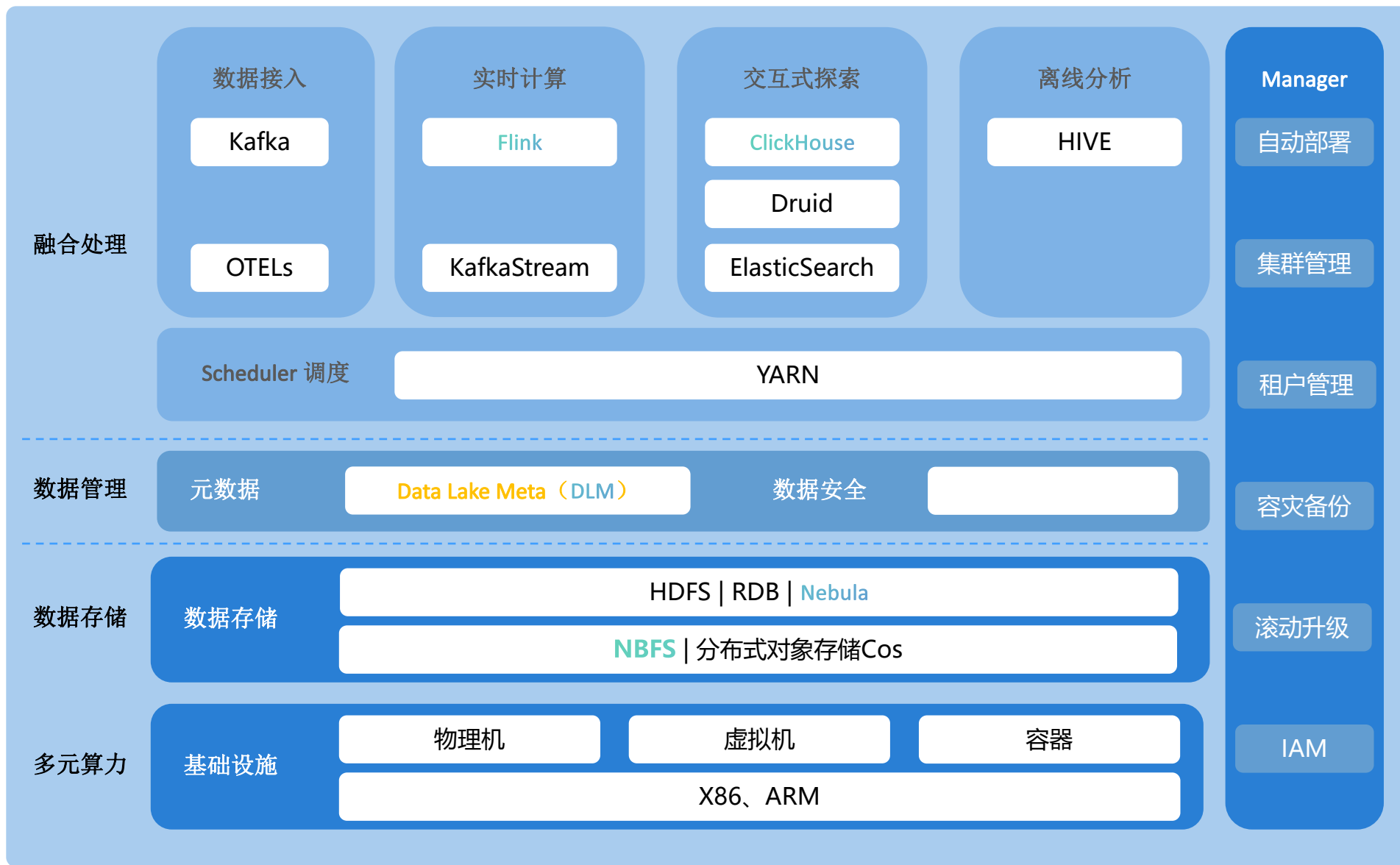
## 数智融合

- **统一模型与元数据**：打通数据和模型，支持数据+AI灵活编排。
- **融合镜像**：AI平台与大数据平台统一融合镜像，支持统一资源调度。



# 大数据引擎：一站式大数据平台

- 存算分离
- 联邦查询
- 向量化计算
- 横向扩容
- 多模态



# DEM

---

以用户为中心，驱动业务韧性

# ▶ 一个都不能少：DEM - 可观测的重要组成

- 以用户为中心的观测视角
- 端到端的可见性
- 关注并实时反馈用户体验
- 用户旅途及会话观测
- 业务洞察
- CDN、跨云和SaaS支持

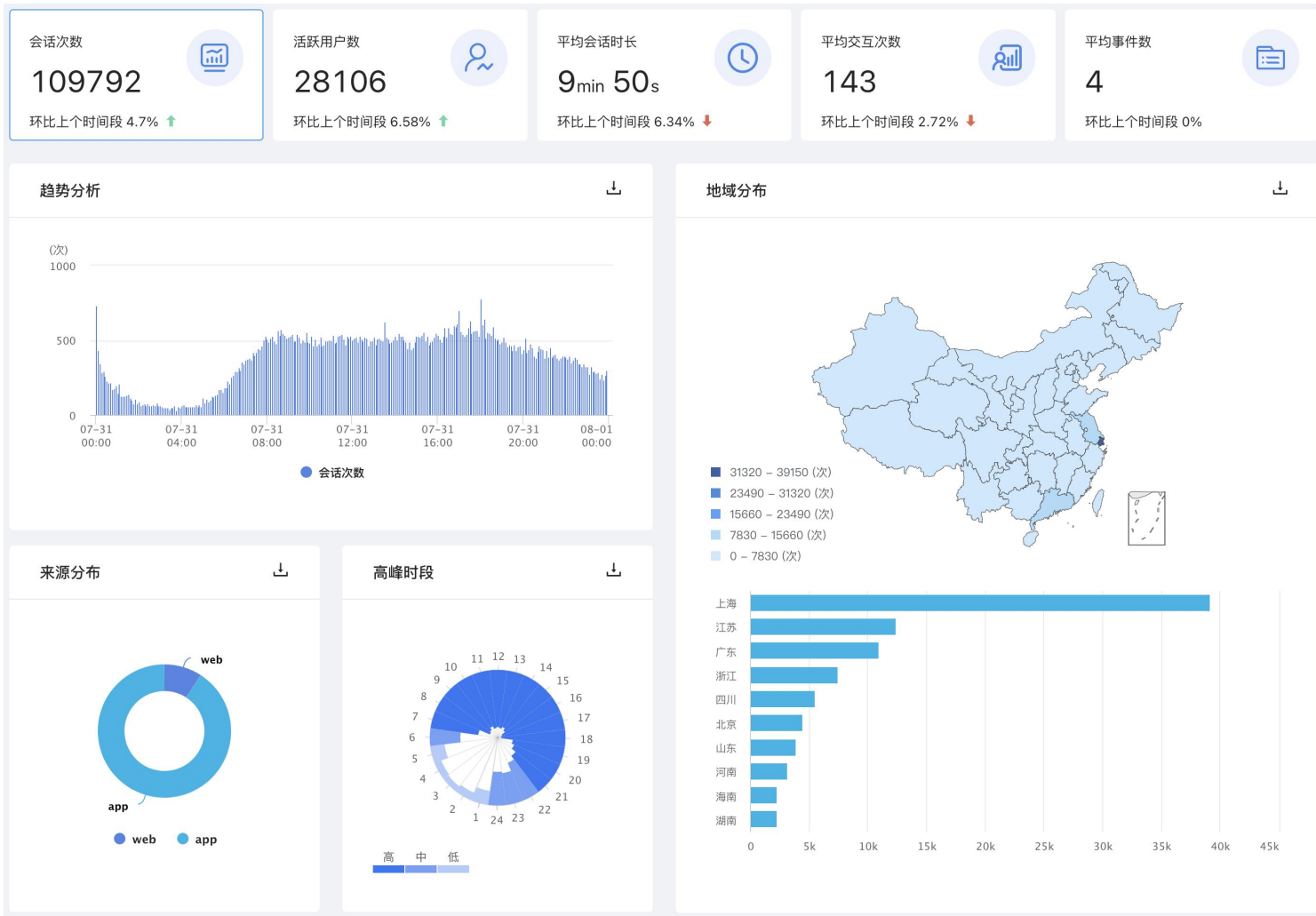


# 用户体验监测的核心能力





# 用户体验监测重点功能-用户旅途





# ▶▶ 用户体验监测重点功能-视频回溯



| 系统事件                                      |
|-------------------------------------------|
| 异常事件                                      |
| 交互类型                                      |
| 2022-07-29 19:22:41 冷启动 (app.coldstart)   |
| 2022-07-29 19:22:41 页面加载 (app.viewload)   |
| 2022-07-29 19:22:44 页面加载 (app.viewload)   |
| 2022-07-29 19:22:53 页面加载 (app.viewload)   |
| 2022-07-29 19:23:03 页面加载 (app.viewload)   |
| 2022-07-29 19:23:10 页面加载 (app.viewload)   |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |
| 2022-07-29 19:23:12 交互操作 (app.useraction) |

00:00

结束录制

# AI

---

给出确定性答案，让运维更简单

# ► 基调听云AI引擎：AIOPS 方法论



## 基于机器学习的预测式AI

- 通过**机器学习**来识别事件之间的**相关性**。
- 该方法努力确定复杂云原生环境下的各种对象中的故障是源于相同的问题根源，还是源于不相关的问题。
- 这些相关性可以为评估故障的范围提供一些有用的见解。但要明确问题根源，工程师必须通盘了解各种报表、告警、日志、链路关系，以及其他数据的相关性，以识别发生的故障。



## 基于因果关系的确定性AI

- 使用可观测性全景上下文数据和确定性AI来**精确查找故障根源**，例如响应时间恶化，吞吐率抖动或应用安全威胁。
- 确定性AIOPS不是根据间接证据关联2个事件或多个事件，而是**确定触发这些事件的确切根源**。
- 这种方法通过**准确、实时、可解释的答案**来指导工程师解决故障，而不是简单地提供最佳猜测。



## 基于大模型的生成式AI

- 这一方法利用大型神经网络和深度学习技术，以生成与问题相关的数据和见解。这可以包括生成实时的**异常检测、预测或建议**。
- 生成式AI在可观测性中可以用于**自动生成仪表盘、分析大量日志数据、发现隐藏的模式等**。这种方法可以帮助自动化决策和分析过程。

# ► 基调听云AI引擎：每一场遇见，都是“处心积虑”的安排



AI驱动软件研发全面进入数字化时代

# ► 观云AI引擎：确定性AI的业务收益

## ① 夺回时间

通过基于因果关系而非仅仅相关性的方法，我们能够自动生成疑似问题，从而帮助运维团队减少手动、重复性任务和故障排除所需的时间。

传统AIOps方法仅关注于关联数据点，这意味着工程师需要耗费时间手动查找问题的根本原因。

## ② 回归创新

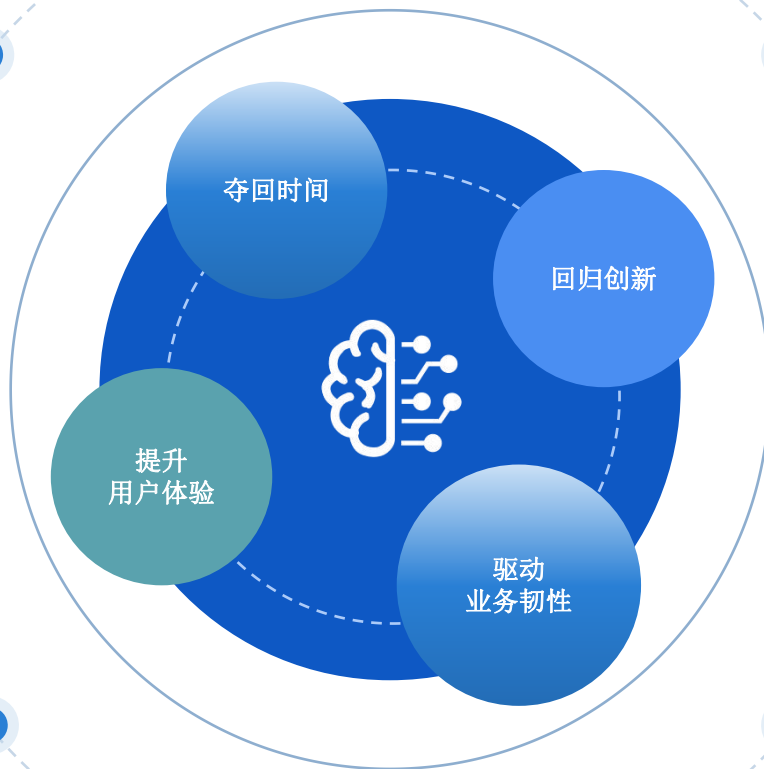
通过确定性AI，不仅有助于工程师加速工作，还有以下好处：团队可以获得更多的时间和对系统的精确掌握，从而能够通过创新的新解决方案和工具为企业创造真正的价值，而不仅仅是维护现有资产。

## ④ 驱动业务韧性

面对不断变化的环境和未知的未知问题的出现，确定性AI还能够提高业务的韧性。通过AI驱动的业务分析和可观测性，IT团队能够就多云环境的性能如何影响业务做出决策。这种决策能力有助于业务更好地适应和应对各种挑战。

## ③ 提升用户体验

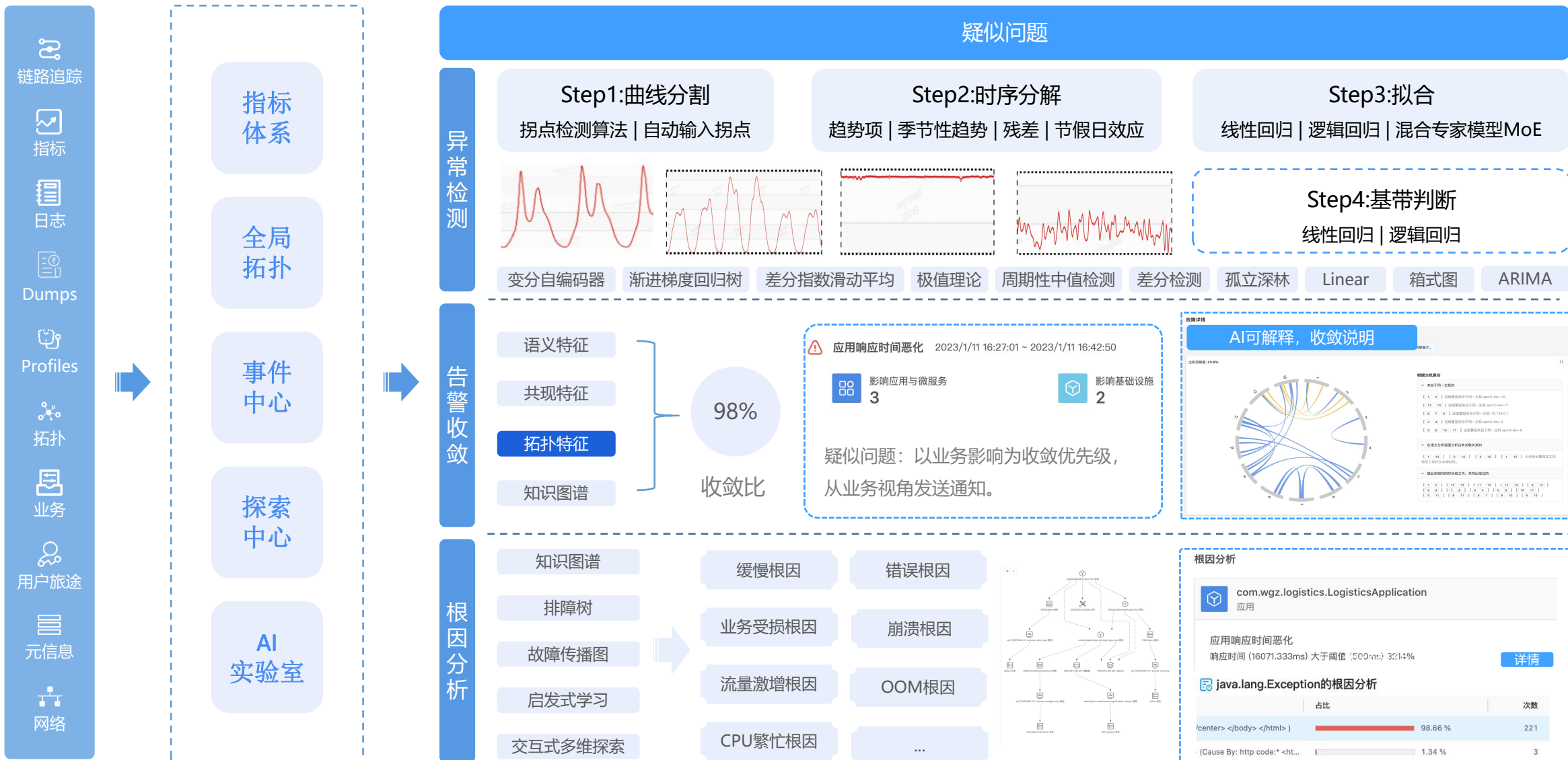
确定性AI还使团队能够实时了解用户体验，以在客户受到影响之前自动发现问题。因此，团队可以根据业务影响动态扩缩容并确定改进的优先级。这种自动化的洞察力使团队能够降本增效并提升用户体验。



确定性AI



# ▶ 基调听云AI引擎 – 基于因果关系的确定性AI能力模型



# 自由探索

---

实现高级可观测性，让观测无边界

# 指标体系化是实现高级可观测性的基础

数据洞察 / 指标体系 / 指标列表

## 指标列表

全部指标 (1585)

请输入指标名称

Q

我的关注 (1)

总响应时间

应用与微服务 (76)

业务系统 (9)

服务组 (9)

应用 (9)

请求 (10)

实例 (11)

外部服务 (6)

异常 (1)

事务错误 (1)

数据库连接池 (1)

线程池 (3)

组件 (16)

基础设施 (977)

用户体验 (226)

App (104)

MP (51)

Web (71)

自定义指标 (0)

第三方 (306)

Linux主机 (109)

Windows主机 (52)

MySQL (73)

Oracle (39)

无类型指标 (33)

新建指标

★ 总响应时间

指标分析

总响应时间

越短越好

apm.app\_action\_duration\_total\_ms

GAUGE

单位: ms

内置

求和

最近采集时间: 2023-10-10 16:27:00

指标属性

指标名称

总响应时间

指标Key

apm.app\_action\_duration\_total\_ms

指标类型

GAUGE

衡量标准

越短越好

单位

ms

指标来源

内置

聚合方式

求和

维度

触发时间、应用名称、业务系统、服务组名称

度量类型

时长

数据类型

Float

指标分级

一般指标

引用次数

0

采集频率

1分钟

标签

⌵

关联信息

关联对象

应用

关联对象

业务系统应用请求实例

关联记录

请求追踪

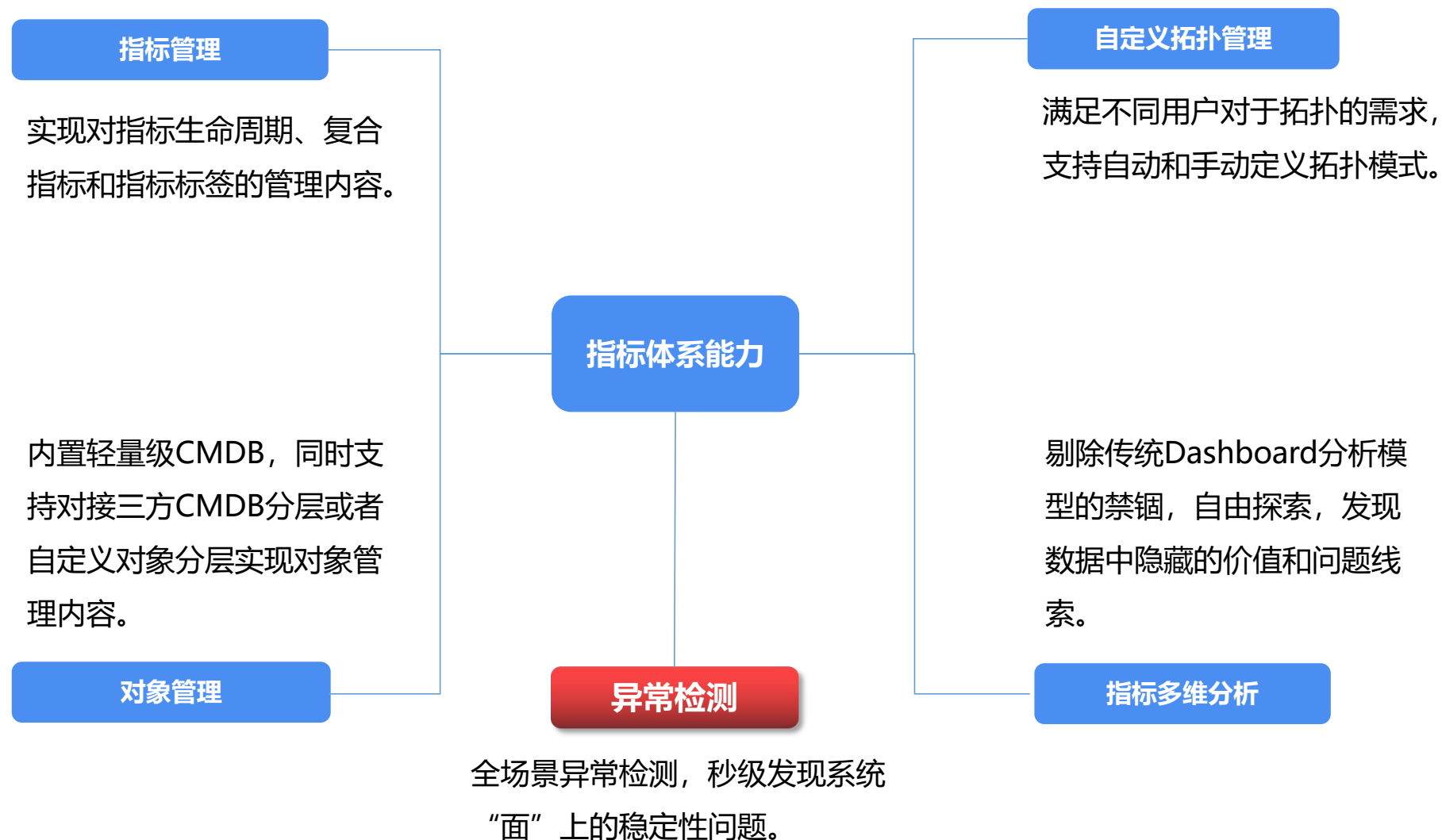
相关指标

Apdex请求次数响应率

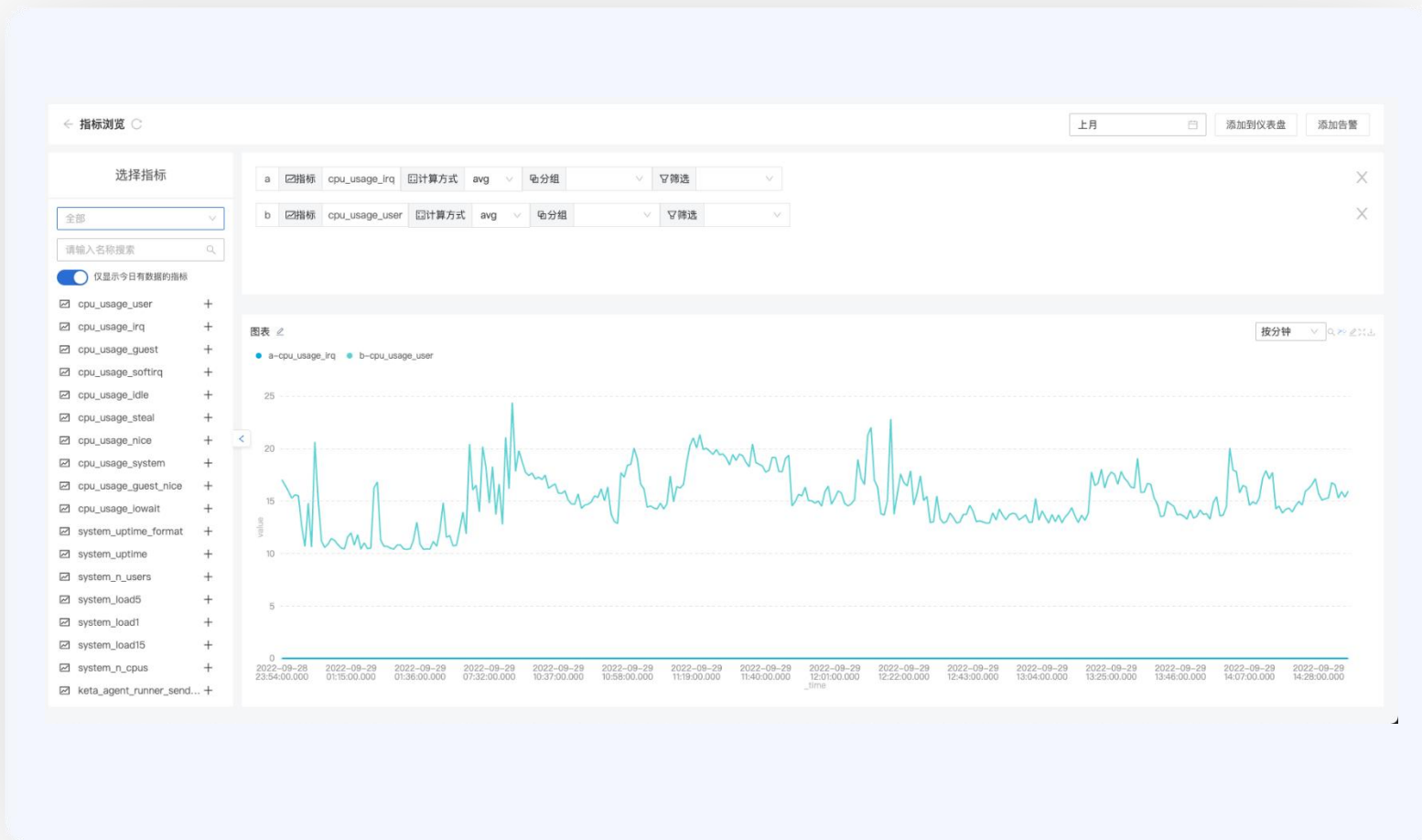
AI驱动软件研发全面进入数字化时代

**AI+ 软件研发数字峰会**  
AI+ software Development Digital summit

# ▶ 指标体系：全面了解系统稳定性，实时预警



# 自由探索：发现数据中的数据价值



- 单 UI 探索，无需跳转，保障探索思路连续性
- 完整覆盖听云Network, RUM和APM所有指标分析功能和场景
- 高自由度、多维度、多标签、高基维指标数据过滤和聚合查询
- 支持直接编写NBQL查询语句
- 通过指标所属实体标签关联追踪、日志和事件，实现详细根因定位
- 百万级指标实时相关性分析，探索表象下的根因及影响范围



# AIOPS落地实践

---

全景拓扑可视化、确定性根因

# ▶ 遇见答案 – 数据全融合，结果可视

通过具备横纵向关联能力的一体化全局拓扑，解决企业复杂多变的服务治理难题、业务流程治理难题和变更影响分析难题。关联指标、追踪、日志、网络、诊断、警报等数据，实现拓扑中台化。



全景可观测（服务治理、业务流程治理、变更影响分析）

## ► 遇见答案 - 全局根因分析

数据洞察 / 全局拓扑

## 全局拓扑 Beta

C

关闭 

▼ 请输入节点名称、标签

👤 用户体验层

0 / 0

应用层

17 / 38

进程层

1 / 80

 POD层

0 / 0

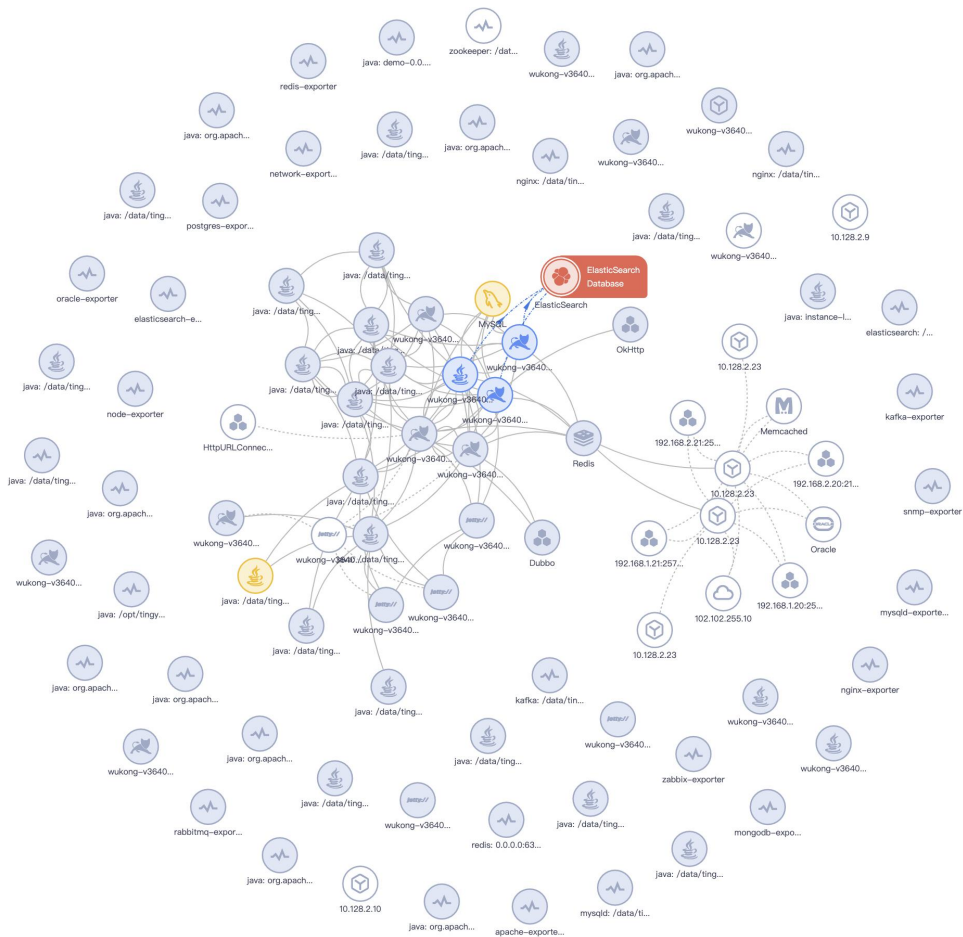
主机层

1 / 1

## 部署环境

0 / 1

+



在拓扑中台的基础上，利用AI技术，自动异常检测、全面收敛故障、推导全局根因节点。

# AI驱动软件开发全面进入数字化时代



# ► 遇见答案：全局拓扑 - 资源变更影响分析

数据洞察 / 全局拓扑

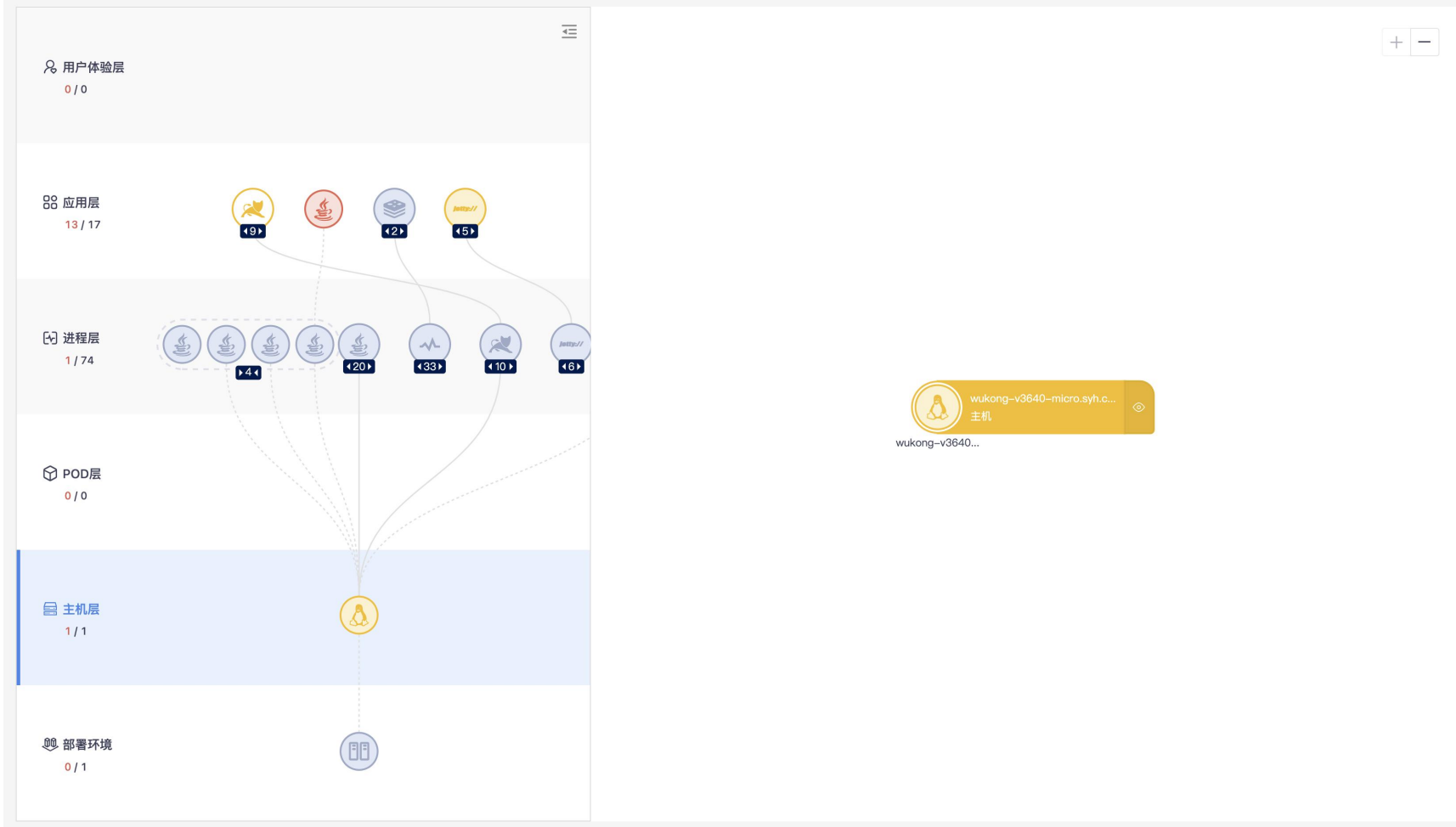
全局拓扑 Beta

最近两天

C

关闭

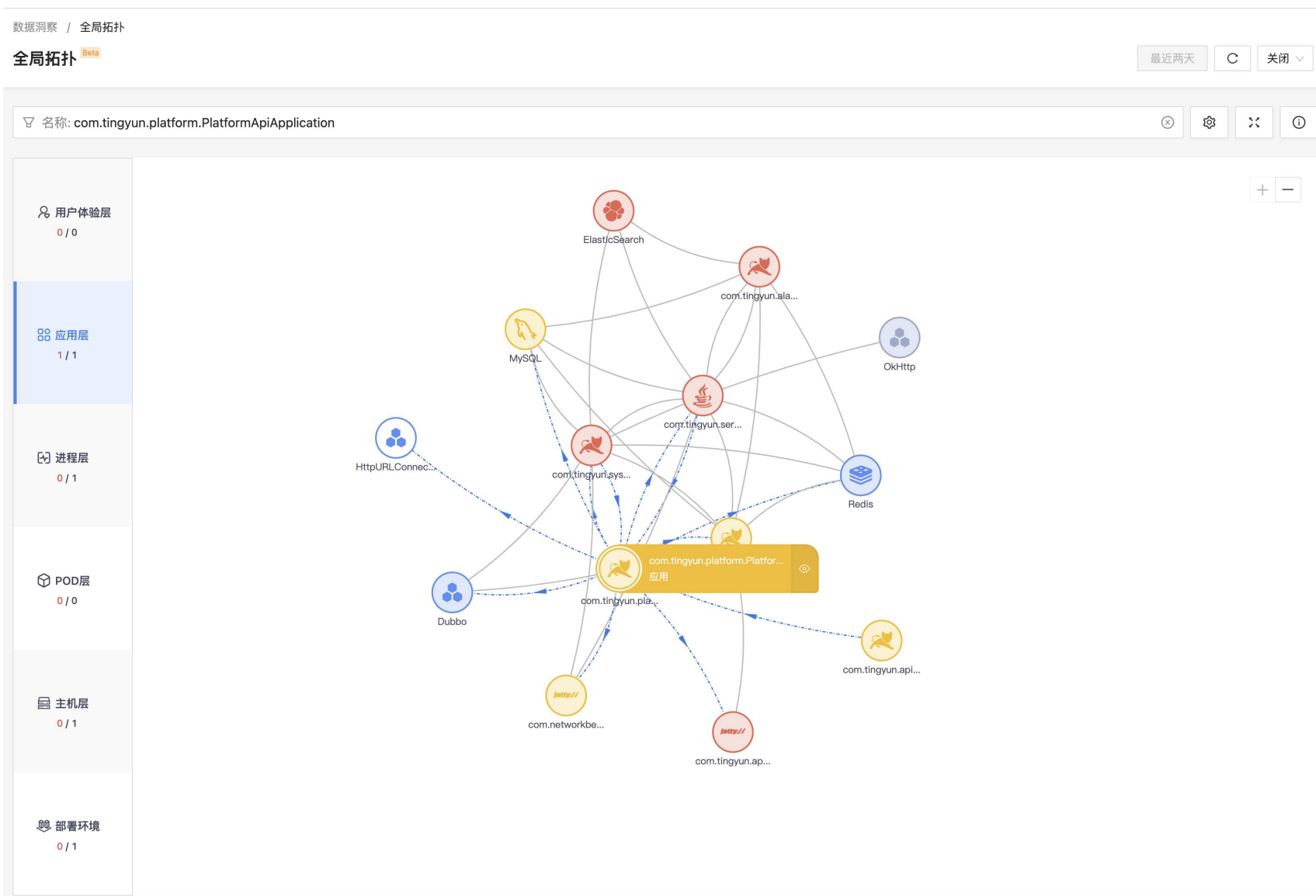
请输入节点名称、标签



AI驱动软件研发全面进入数字化时代

**AI+ 软件研发数字峰会**  
AI+ software Development Digital summit

# 遇见答案：全局拓扑 - 服务变更影响分析





# ▶ 遇见答案：多指标异常检测

配置 / 全局配置

## 异常检测

应用

实例

进程

Database

主机

### 应用异常检测 (skywalking-service01-0314)

自动检测与应用相关的性能异常，例如响应时间恶化和错误率增加。以下配置用来调整检测灵

#### 响应时间

☒ 响应时间恶化

检测模式

动态基线

#### 平均响应时间

当应用的的平均响应时间同时超出绝对值和相对阈值时，触发告警。

绝对阈值

200

ms

相对阈值

200

%

#### 告警抑制

每分钟请求数大于

10

异常状态持续超过

5

分钟

触发警告

#### 错误率

☒ 错误率增加

检测模式

动态基线

当请求的错误率同时满足以下阈值时，触发告警。

绝对阈值

5

%

相对阈值

100

%

例如：动态基线当前值为 2.4%

错误率绝对阈值为  $2.4\% + 5\% = 7.4\%$

错误率相对阈值为  $2.4\% + 2.4\% * 100\% = 104.8\%$

同时满足以上两阈值，触发告警。

#### 告警抑制

每分钟请求数大于

异常状态持续超过

配置 / 全局配置

## 异常检测

应用

实例

进程

Database

主机

### 进程异常检测

自动检测与进程相关的性能异常，例如cpu使用率过高 或内存使用率过高等。以下配

Linux

Windows

#### 打开文件数使用率

☒ 进程打开文件数使用率

检测模式

静态阈值

当打开文件数使用率在5分钟内3次超过以下阈值时，触发告警。

打开文件数使用率：

97

%

#### CPU使用率

☒ 进程 CPU 使用率过高

检测模式

自动检测

#### 内存使用率

☒ 进程内存使用率过高

检测模式

自动检测

保存

AI驱动软件研发全面进入数字化时代

**AI+ 软件研发数字峰会**  
AI\* software Development Digital summit

# ▶ 遇见答案：疑似问题-故障全生命周期管理

在拓扑中台的基础上，通过基于AI的决策树算法，将异常检测出来的指标告警收敛至一个疑似问题，并推导根因，实现可解释型AI。

疑似问题列表，作为运维故障处理的入口，用来管理系统出现的疑似问题。

疑似问题详情，通过影响分析，评估对业务的影响及范围，通过根因分析，推导根因。

通过问题路径传播图，还原问题生命周期状态变化。



# ▶ 遇见答案：疑似问题：故障全生命周期管理 – 故障影响及根因分析

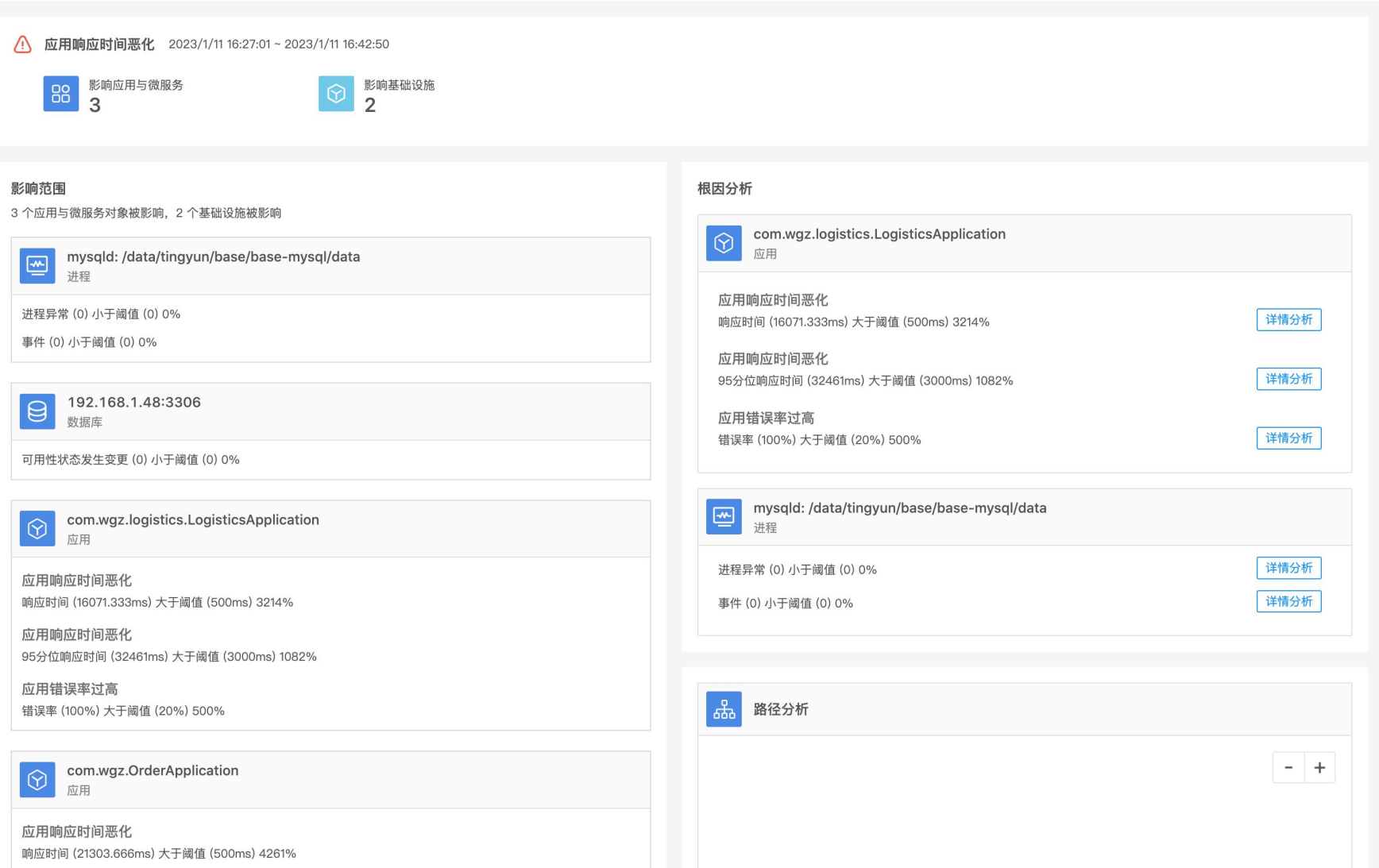
在拓扑中台的基础上，通过基于AI的决策树算法，将异常检测出来的指标告警收敛至一个疑似问题，并推导根因，实现可解释型AI。

疑似问题列表，作为运维故障处理的入口，用来管理系统出现的疑似问题。

疑似问题详情，通过影响分析，评估对业务的影响及范围，通过根因分析，推导根因。

通过问题路径传播图，还原问题生命周期状态变化。

## 疑似问题



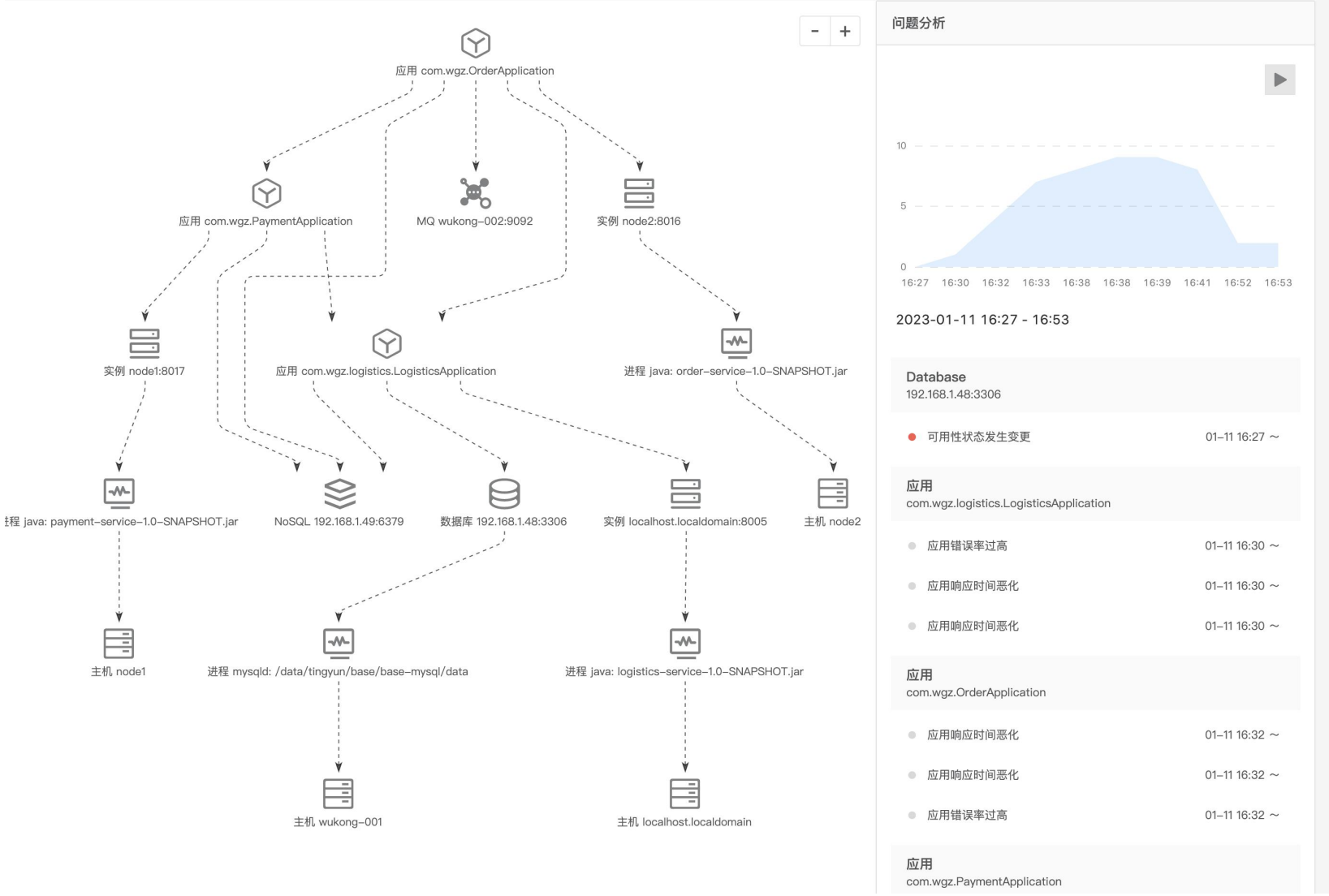
# ▶ 遇见答案：疑似问题-故障全生命周期管理-故障传播图

在拓扑中台的基础上，通过基于AI的决策树算法，将异常检测出来的指标告警收敛至一个疑似问题，并推导根因，实现可解释型AI。

疑似问题列表，作为运维故障处理的入口，用来管理系统出现的疑似问题。

疑似问题详情，通过影响分析，评估对业务的影响及范围，通过根因分析，推导根因。

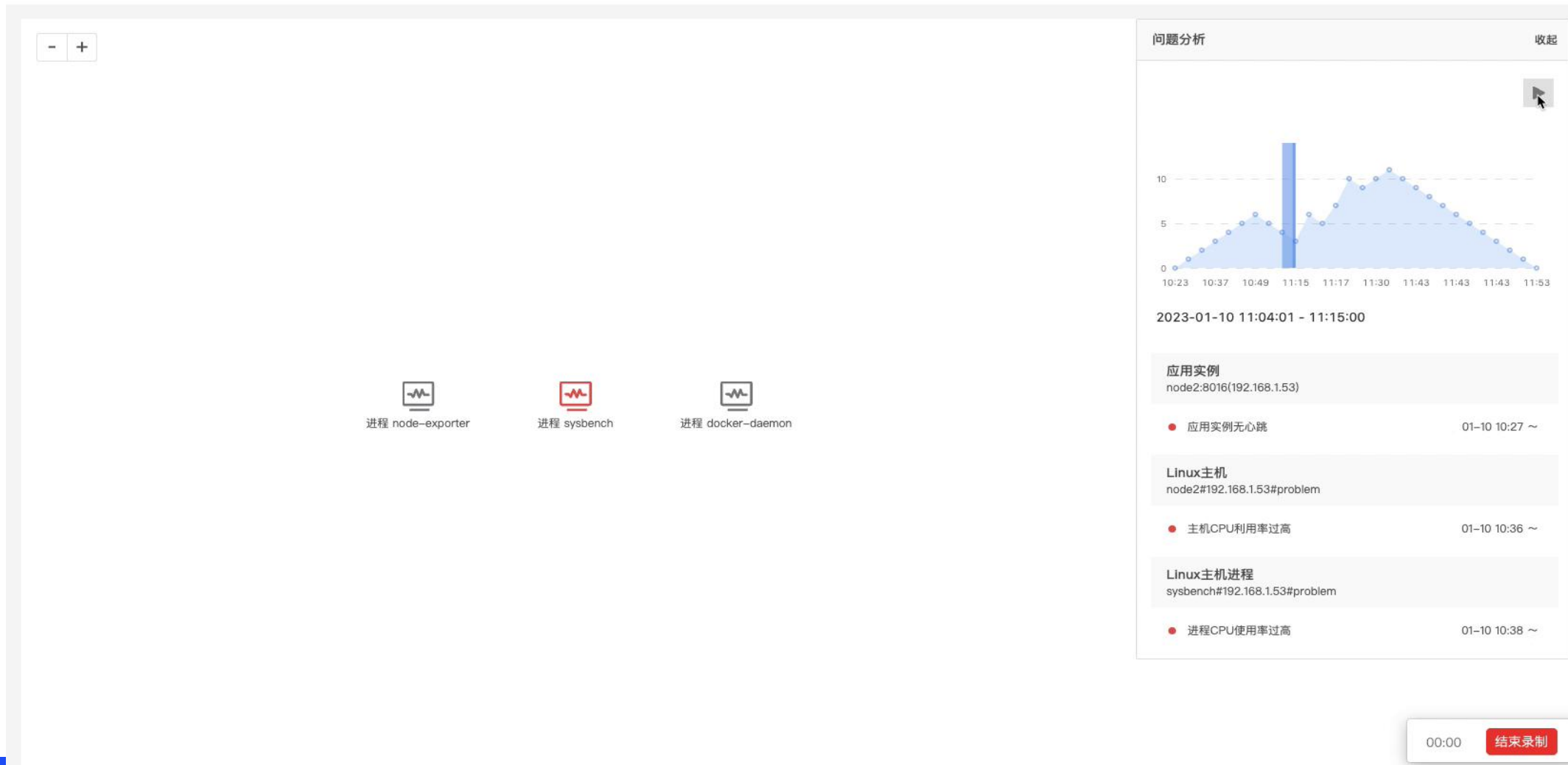
通过问题路径传播图，还原问题生命周期状态变化。



# ▶ 遇见答案：疑似问题-故障全生命周期管理-故障传播路径

数据洞察 / 疑似问题 / 问题详情 / 问题路径

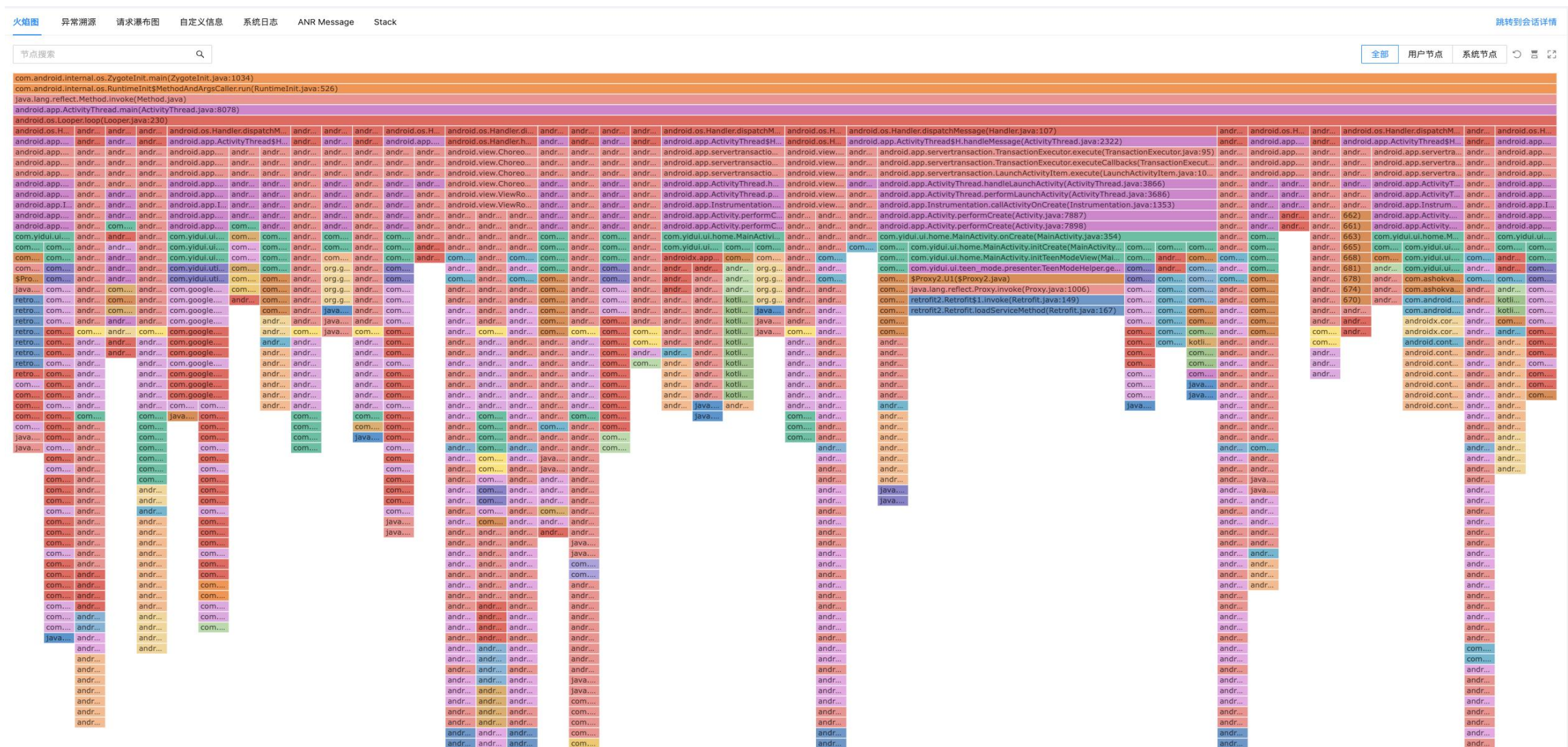
疑似问题



异常检测-告警收敛-根因分析-影响分析



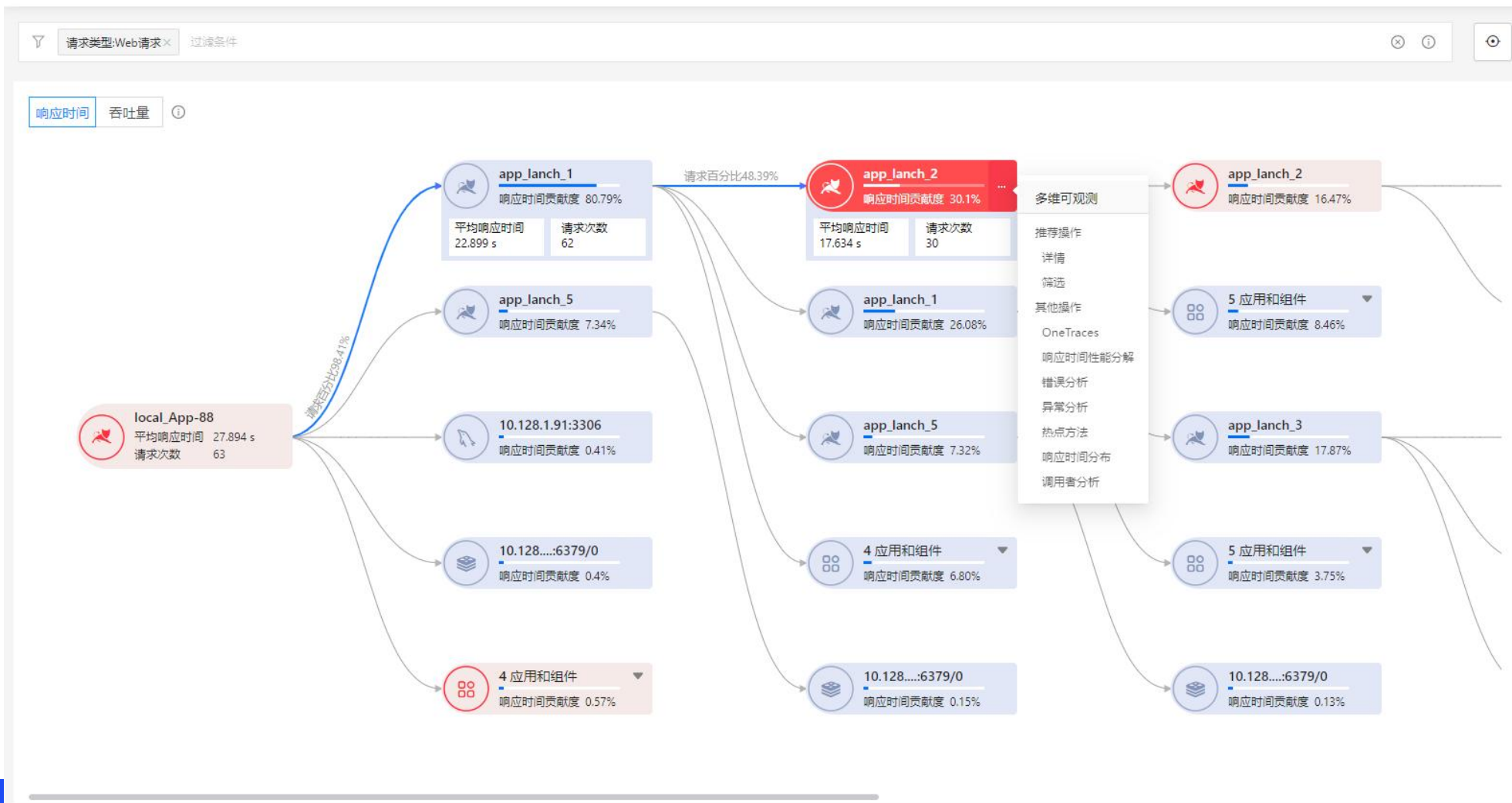
## ► 遇见答案：端侧卡顿异常堆栈分析



# ▶ 遇见答案：调用全流程可视化-根因界定

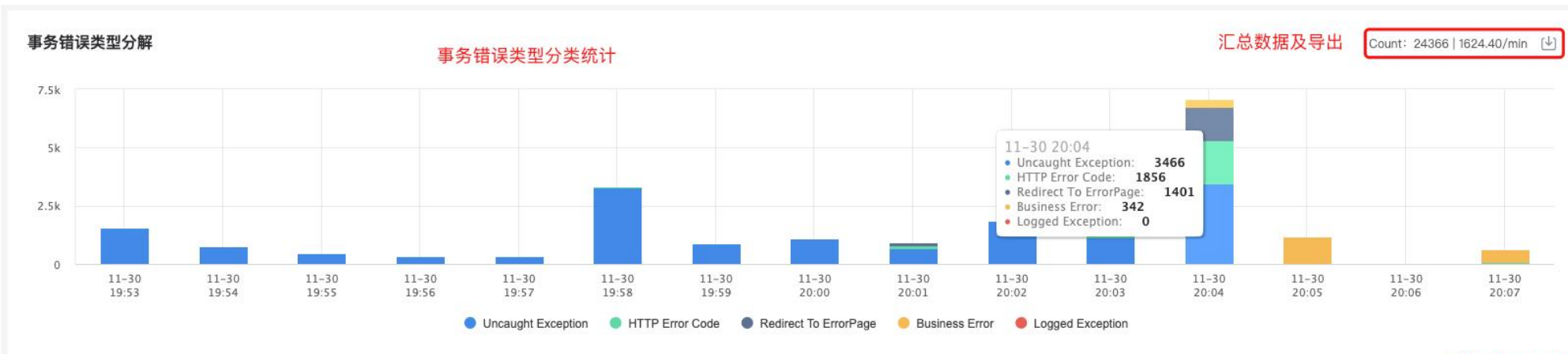
应用与微服务 / 应用 / local\_App-88 / 详情 / Service Flow

local\_App-88应用的Service flow 分析时间范围: 2023-09-28 09:51:00 至 2023-09-28 10:21:00



Service Flow：调用依赖梳理，服务治理、问题诊断和定位瓶颈





导航至配置页面

| 事务错误列表     | 影响的事务      |
|------------|------------|
| 事务1：更新A    | 事务2：更新A    |
| 事务3：更新B    | 事务4：更新B    |
| 事务5：更新C    | 事务6：更新C    |
| 事务7：更新D    | 事务8：更新D    |
| 事务9：更新E    | 事务10：更新E   |
| 事务11：更新F   | 事务12：更新F   |
| 事务13：更新G   | 事务14：更新G   |
| 事务15：更新H   | 事务16：更新H   |
| 事务17：更新I   | 事务18：更新I   |
| 事务19：更新J   | 事务20：更新J   |
| 事务21：更新K   | 事务22：更新K   |
| 事务23：更新L   | 事务24：更新L   |
| 事务25：更新M   | 事务26：更新M   |
| 事务27：更新N   | 事务28：更新N   |
| 事务29：更新O   | 事务30：更新O   |
| 事务31：更新P   | 事务32：更新P   |
| 事务33：更新Q   | 事务34：更新Q   |
| 事务35：更新R   | 事务36：更新R   |
| 事务37：更新S   | 事务38：更新S   |
| 事务39：更新T   | 事务40：更新T   |
| 事务41：更新U   | 事务42：更新U   |
| 事务43：更新V   | 事务44：更新V   |
| 事务45：更新W   | 事务46：更新W   |
| 事务47：更新X   | 事务48：更新X   |
| 事务49：更新Y   | 事务50：更新Y   |
| 事务51：更新Z   | 事务52：更新Z   |
| 事务53：更新AA  | 事务54：更新AA  |
| 事务55：更新AB  | 事务56：更新AB  |
| 事务57：更新AC  | 事务58：更新AC  |
| 事务59：更新AD  | 事务60：更新AD  |
| 事务61：更新AE  | 事务62：更新AE  |
| 事务63：更新AF  | 事务64：更新AF  |
| 事务65：更新AG  | 事务66：更新AG  |
| 事务67：更新AH  | 事务68：更新AH  |
| 事务69：更新AI  | 事务70：更新AI  |
| 事务71：更新AJ  | 事务72：更新AJ  |
| 事务73：更新AK  | 事务74：更新AK  |
| 事务75：更新AL  | 事务76：更新AL  |
| 事务77：更新AM  | 事务78：更新AM  |
| 事务79：更新AN  | 事务80：更新AN  |
| 事务81：更新AO  | 事务82：更新AO  |
| 事务83：更新AP  | 事务84：更新AP  |
| 事务85：更新AQ  | 事务86：更新AQ  |
| 事务87：更新AR  | 事务88：更新AR  |
| 事务89：更新AS  | 事务90：更新AS  |
| 事务91：更新AT  | 事务92：更新AT  |
| 事务93：更新AU  | 事务94：更新AU  |
| 事务95：更新AV  | 事务96：更新AV  |
| 事务97：更新AW  | 事务98：更新AW  |
| 事务99：更新AX  | 事务100：更新AX |
| 事务101：更新AY | 事务102：更新AY |
| 事务103：更新AZ | 事务104：更新AZ |
| 事务105：更新BA | 事务106：更新BA |
| 事务107：更新BB | 事务108：更新BB |
| 事务109：更新BC | 事务110：更新BC |
| 事务111：更新BD | 事务112：更新BD |
| 事务113：更新BE | 事务114：更新BE |
| 事务115：更新BF | 事务116：更新BF |
| 事务117：更新BG | 事务118：更新BG |
| 事务119：更新BH | 事务120：更新BH |
| 事务121：更新BI | 事务122：更新BI |
| 事务123：更新BJ | 事务124：更新BJ |
| 事务125：更新BK | 事务126：更新BK |
| 事务127：更新BL | 事务128：更新BL |
| 事务129：更新BM | 事务130：更新BM |
| 事务131：更新BN | 事务132：更新BN |
| 事务133：更新BO | 事务134：更新BO |
| 事务135：更新BP | 事务136：更新BP |
| 事务137：更新BQ | 事务138：更新BQ |
| 事务139：更新BR | 事务140：更新BR |
| 事务141：更新BS | 事务142：更新BS |
| 事务143：更新BT | 事务144：更新BT |
| 事务145：更新BU | 事务146：更新BU |
| 事务147：更新BV | 事务148：更新BV |
| 事务149：更新BW | 事务150：更新BW |
| 事务151：更新BX | 事务152：更新BX |
| 事务153：更新BY | 事务154：更新BY |
| 事务155：更新BZ | 事务156：更新BZ |
| 事务157：更新CA | 事务158：更新CA |
| 事务159：更新CB | 事务160：更新CB |
| 事务161：更新CC | 事务162：更新CC |
| 事务163：更新CD | 事务164：更新CD |
| 事务165：更新CE | 事务166：更新CE |
| 事务167：更新CF | 事务168：更新CF |
| 事务169：更新CG | 事务170：更新CG |
| 事务171：更新CH | 事务172：更新CH |
| 事务173：更新CI | 事务174：更新CI |
| 事务175：更新CJ | 事务176：更新CJ |
| 事务177：更新CK | 事务178：更新CK |
| 事务179：更新CL | 事务180：更新CL |
| 事务181：更新CM | 事务182：更新CM |
| 事务183：更新CN | 事务184：更新CN |
| 事务185：更新CO | 事务186：更新CO |
| 事务187：更新CP | 事务188：更新CP |
| 事务189：更新CQ | 事务190：更新CQ |
| 事务191：更新CR | 事务192：更新CR |
| 事务193：更新CS | 事务194：更新CS |
| 事务195：更新CT | 事务196：更新CT |
| 事务197：更新CU | 事务198：更新CU |
| 事务199：更新CV | 事务200：更新CV |
| 事务201：更新CW | 事务202：更新CW |
| 事务203：更新CX | 事务204：更新CX |
| 事务205：更新CY | 事务206：更新CY |
| 事务207：更新CZ | 事务208：更新CZ |
| 事务209：更新DA | 事务210：更新DA |
| 事务211：更新DB | 事务212：更新DB |
| 事务213：更新DC | 事务214：更新DC |
| 事务215：更新DD | 事务216：更新DD |
| 事务217：更新DE | 事务218：更新DE |
| 事务219：更新DF | 事务220：更新DF |
| 事务221：更新DG | 事务222：更新DG |
| 事务223：更新DH | 事务224：更新DH |
| 事务225：更新DI | 事务226：更新DI |
| 事务227：更新DJ | 事务228：更新DJ |
| 事务229：更新DK | 事务230：更新DK |
| 事务231：更新DL | 事务232：更新DL |
| 事务233：更新DM | 事务234：更新DM |
| 事务235：更新DN | 事务236：更新DN |
| 事务237：更新DO | 事务238：更新DO |
| 事务239：更新DP | 事务240：更新DP |
| 事务241：更新DQ | 事务242：更新DQ |
| 事务243：更新DR | 事务244：更新DR |
| 事务245：更新DS | 事务246：更新DS |
| 事务247：更新DT | 事务248：更新DT |
| 事务249：更新DU | 事务250：更新DU |
| 事务251：更新DV | 事务252：更新DV |

### 错误/异常采集配置

Filter by 错误名称

Q 显示12/12

影响的用户

## 导出

导出任务列表

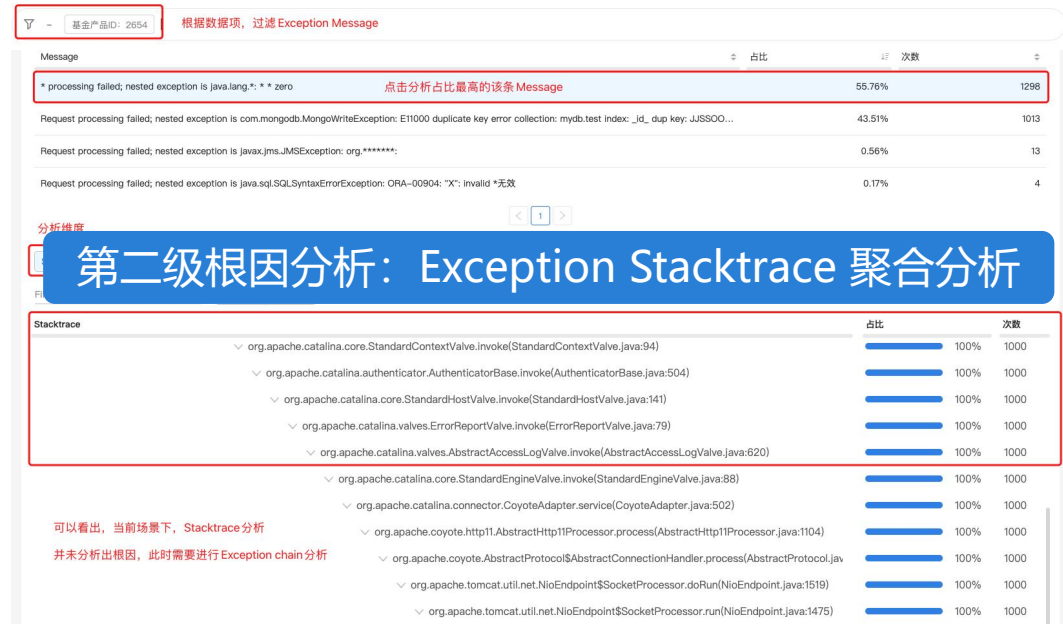
## 自定义表头

| 开始出现...        | 最后发生...        | 持... | 错误类型                  | 错误名称                                                                          | 影响的业务数据 | 影响用... | 次数   | 发生频率       | 占比     | 追... | 应用        | 操作 |
|----------------|----------------|------|-----------------------|-------------------------------------------------------------------------------|---------|--------|------|------------|--------|------|-----------|----|
| 11-30 20:01:00 | 11-30 20:07:00 | 6分钟  | Redirect To ErrorP... | 404<br>基金产品ID (5) 认购额度 (3)                                                    |         | 3      | 4126 | 275.07/min | 41.26% | 4126 | kongji... | 🔍  |
| 11-30 20:01:00 | 11-30 20:07:00 | 6分钟  | HTTP Error Code       | HTTP ERROR CODE: 404<br>基金产品ID (3) 认购额度 (2)                                   |         | 2      | 2076 | 138.4/min  | 20.76% | 2076 | kongji... | 🔍  |
| 11-30 20:01:00 | 11-30 20:07:00 | 6分钟  | Uncaught Exception    | org.springframework.web.util.NestedServletException<br>基金产品ID (4)<br>认购额度 (2) |         | 3      | 1559 | 103.93/min | 15.59% | 1559 | kongji... | 🔍  |
| 11-30 20:04:00 | 11-30 20:07:00 | 3分钟  | Business Error        | 认购超限<br>基金产品ID (2) 认购额度 (3)                                                   |         | 3      | 1422 | 94.8/min   | 14.22% | 1422 | kongji... | 🔍  |
| 11-30 20:04:00 | 11-30 20:07:00 | 3分钟  | Business Error        | 售罄<br>基金产品ID (1) 认购额度 (1)                                                     |         | 1      | 639  | 42.6/min   | 6.39%  | 639  | kongji... | 🔍  |
| 11-30 19:58:00 | 11-30 20:04:00 | 6分钟  | HTTP Error Code       | HTTP ERROR CODE: 505<br>基金产品ID (3) 认购额度 (3)                                   |         | 2      | 42   | 2.8/min    | 0.42%  | 42   | kongji... | 🔍  |

# 遇见答案：错误/异常4级根因分析



## 第一级根因分析：Exception Message 聚合分析



## 第二级根因分析：Exception Stacktrace 聚合分析

Stacktrace Root cause(cause by) 错误追踪 Referring pages Client IPs Caller Applications

## 第三级根因分析：Exception Chain (Root cause) Message 聚合分析

| Root cause(cause by)                     | 占比     | 次数   |
|------------------------------------------|--------|------|
| java.lang.ArithmeticException: / by zero | 54.24% | 3698 |
| java.lang.NullPointerException           | 45.76% | 3120 |

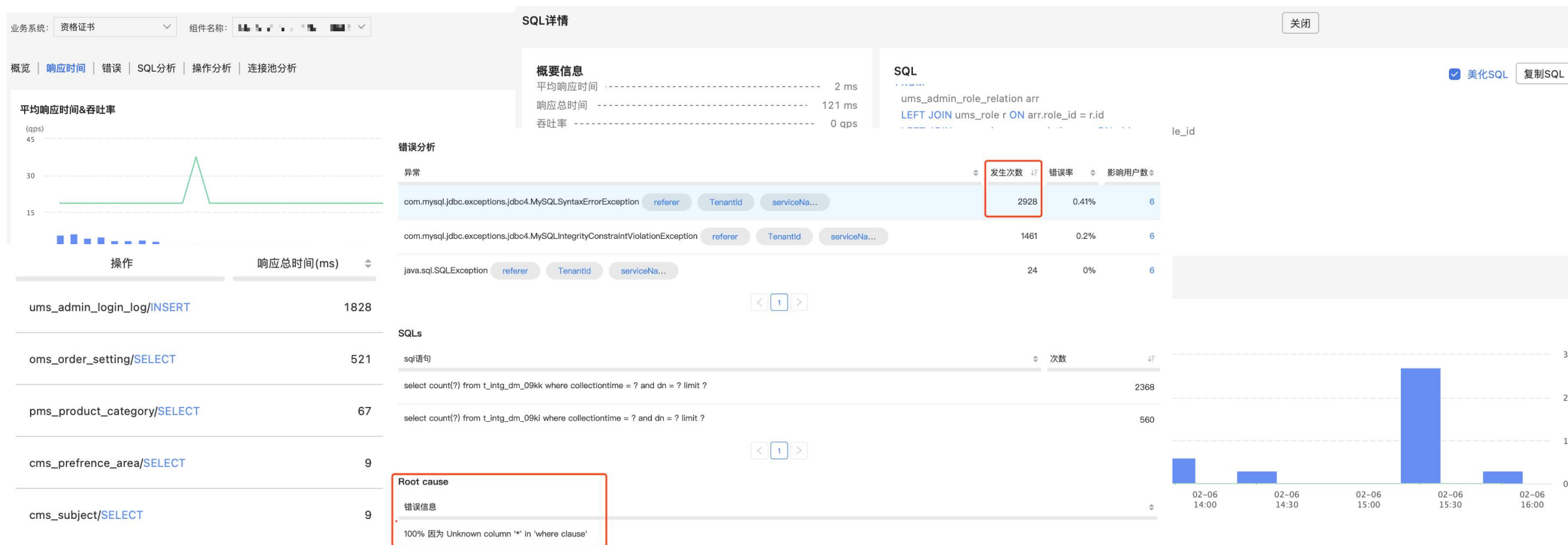
## 第四级根因分析：Exception Chain (Root cause) Stacktrace 聚合分析

|                                                                                         |       |     |
|-----------------------------------------------------------------------------------------|-------|-----|
| > com.Exceptions.SQLExceptions.MySQLExceptionTest1(SQLExceptions.java:283)              | 68.8% | 688 |
| > com.Exceptions.SQLExceptions.MySQLExceptionTest2(SQLExceptions.java:309)              | 31.2% | 312 |
| > sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)         | 1.9%  | 6   |
| > sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) | 98.1% | 306 |

## 4级根因分析、让异常/错误根因浮出水面

# ▶ 遇见答案：SQL错误根因分析

基调听云中对数据库数据的分析更细一步，以 SQL语句和NoSQL的操作作为分析单元，并可以关联调用者、分析错误和异常，使得数据更具价值。





# ▶ 遇见答案：提前预知内存溢出，先于故障前解决故障

应用与微服务 / 诊断工具 / 对象统计 / 20230308161926 / 环比分析

192.168.1.53:8083 实例的环比分析 分析时间范围: 2023-03-08 12:14: 2023-03-08 17:14: >

近3小时的数据分析发现，以下对象数有增长趋势，请结合实际情况判断是否有内存泄漏风险。如需进一步分析内存情况，可以通过 [内存Dump](#) 进一步分析内存引用情况。

| 类名                                       | 评估增量 ① | 增量比 ① | 增长趋势 ① | 统计快照数 ① | 分析结论    |
|------------------------------------------|--------|-------|--------|---------|---------|
| 1 com.saas.memory.ObjectStatistics.test3 | 58,469 | 24.16 | 0.006  | 25      | 对象数持续增长 |
| 2 com.beta.memory.ObjectStatistics.test2 | 58,469 | 24.16 | 0.006  | 25      | 对象数持续增长 |
| 3 com.test.memory.ObjectStatistics.test1 | 58,469 | 24.16 | 0.006  | 25      | 对象数持续增长 |

Top 10

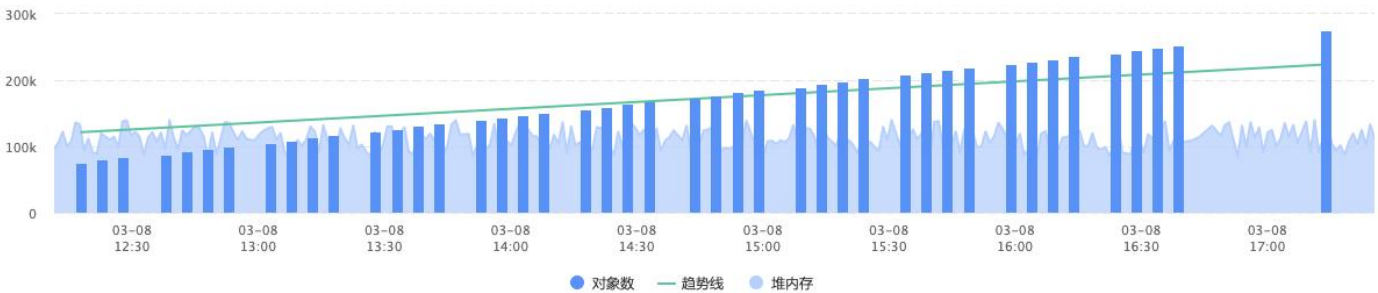
| 对象数                                               | ①       | 全部 |
|---------------------------------------------------|---------|----|
| <input checked="" type="checkbox"/> 类名            | 对象数     |    |
| <input checked="" type="checkbox"/> c.s.m.O.test3 | 275,464 |    |
| <input checked="" type="checkbox"/> c.b.m.O.test2 | 275,464 |    |
| <input checked="" type="checkbox"/> c.t.m.O.test1 | 275,464 |    |
| <input type="checkbox"/> c.m.m.O.test_zfd         | 37      |    |
| <input type="checkbox"/> c.m.m.O.test_zgq         | 4       |    |

共展示 3 个环比分析，分析出 3 个有增长趋势，其中 3 个为持续增长。

JVM

com.saas.memory.ObjectStatistics.test3 的环比趋势分析

对象数持续增长，评估增量：102546，增量比：45.80



com.beta.memory.ObjectStatistics.test2 的环比趋势分析

对象数持续增长，评估增量：102546，增量比：45.80



通过“评估增量”和“增量比”两个指标，推导增长趋势，判定对象是否持续增长。

后置处理：像该实例下发“获取内存Dump”指令，听云OneAgent打印并转储Dump文件，通过内存Dump分析增长详情、引用关系。

内存增长趋势判断、实时预警

# 遇见答案 - 分布式链路根因推荐

OneTrace  URI/sense-api/vi/share/eyJzY3JlZW5JZCI6MTc0MX0/vi/dataSource/component/getData/\*/\*

请求ID:aa3498cc6e10cd16

追踪ID:aa3498cc6e10cd16



开始时间: 2023-03-23 16:36:57...

响应时间: 169.347 ms

执行时间: 169.468 ms

用户标识: --

异常数量: --

性能分解



|          |            |       |          |
|----------|------------|-------|----------|
| External | 214.158 ms | NoSQL | 0.474 ms |
| Code     | 89.243 ms  | Pool  | 0.042 ms |
| 网络       | 21.097 ms  |       |          |
| Database | 4.212 ms   |       |          |

疑似问题

 http://10.194.10.12:80/druid/v2/sql 消耗214.158ms  14次Database调用耗时: 4.212ms

拓扑 Call Table **Call Tree** 全栈快照  异常 参数信息 Code统计 SQL统计 NoSQL统计 数据项 Servers 日志

独占时间 > 30 ms

名称

☒ 过滤



Span个数: 1/105

折叠时间 < 20

% (≈ 33 ms) 的 Span

确定 设为默认

☐ 独占时间

☐ 投影时间

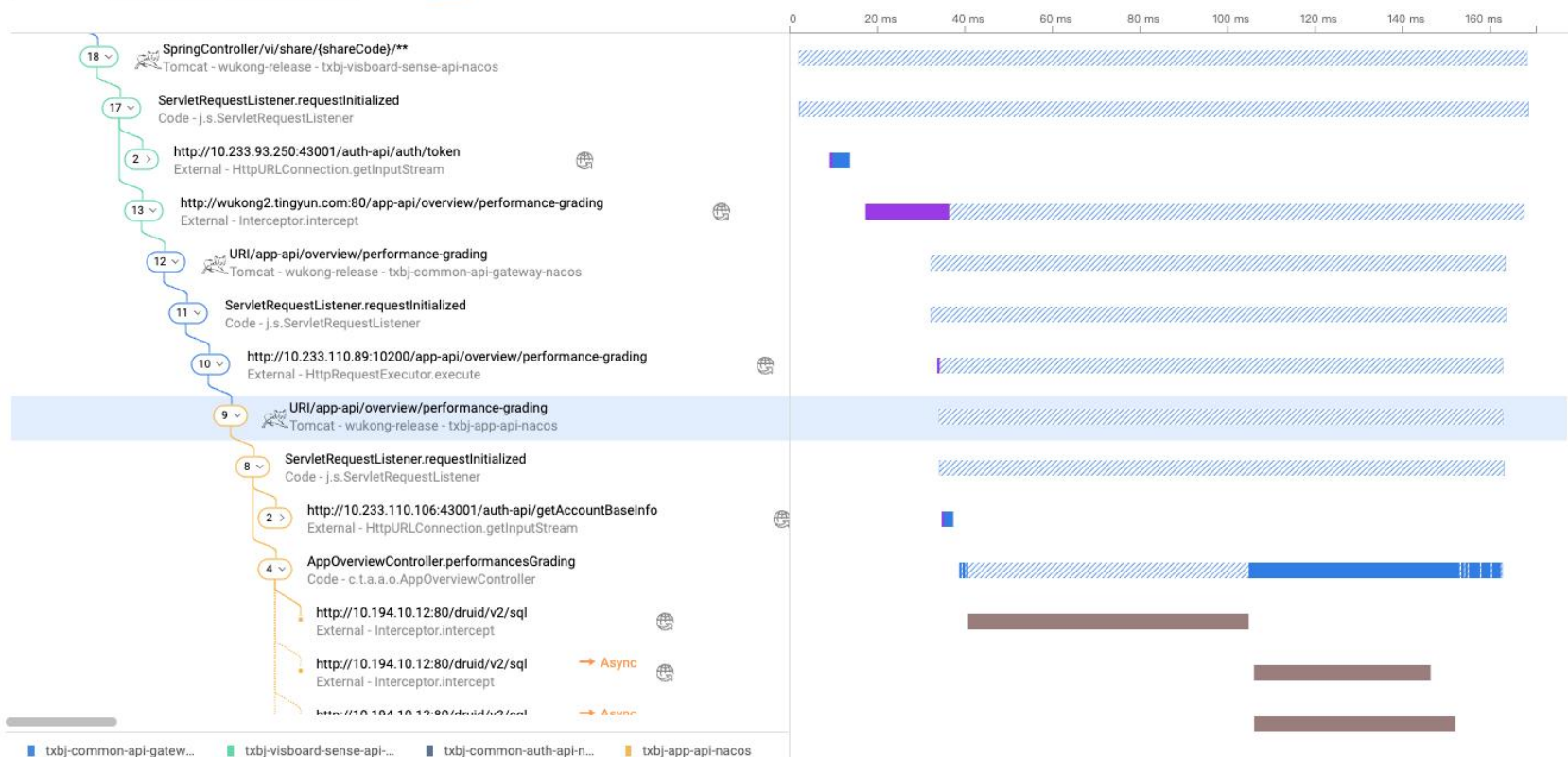
☐ 网络

☐ External

☐ Pool

☐ Database

☐ NoSQL



请求: URI/app-api/overview/performance-grading

业务系统: wukong-release

应用: txbj-app-api-nacos

实例: txbj-app-api-nacos-5bb56f7b4-72tvb\_kube-wk-plf-b2:10200

响应时间: 128.781 ms

请求信息 详情 日志 异常

基础信息

|                  |                                                                 |
|------------------|-----------------------------------------------------------------|
| URL:             | http://wukong2.tingyun.com/app-api/overview/performance-grading |
| HTTP method:     | POST                                                            |
| Response Status: | 200                                                             |
| Client IP:       | 140.143.182.29                                                  |

Request headers

|             |                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------|
| Referer:    | https://wukong2.tingyun.com/visboard/sense-vis/screen/share/eyJzY3JlZW5JZCI6MTc0MX0                             |
| User-Agent: | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 |

AI驱动软件研发全面进入数字化时代

 AI+ 软件研发数字峰会  
AI\* software Development Digital summit

# 遇见答案 - 分布式链路根因推荐

OneTrace TX URI/sense-api/vi/share/eyJzY3JlZW5JZCI6MTc0MXQ0/vi/dataSource/component/getData/\*/\*

请求ID:aa3498cc6e10cd16

追踪ID:aa3498cc6e10cd16



开始时间: 2023-03-23 16:36:57...  
响应时间: 169.347 ms  
执行时间: 169.468 ms  
用户标识: --  
异常数量: --

性能分解



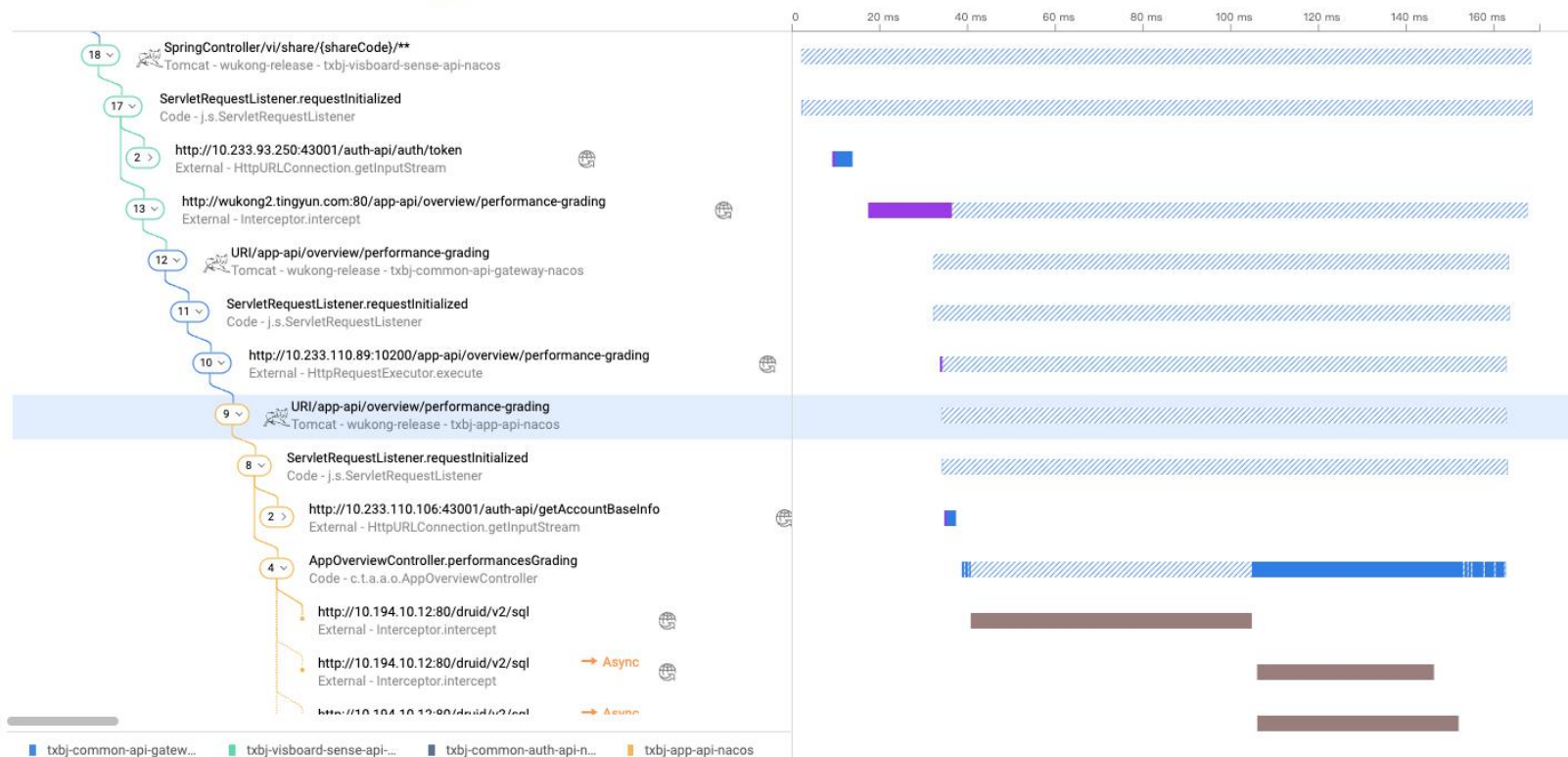
|          |            |       |          |
|----------|------------|-------|----------|
| External | 214.158 ms | NoSQL | 0.474 ms |
| Code     | 89.243 ms  | Pool  | 0.042 ms |
| 网络       | 21.097 ms  |       |          |
| Database | 4.212 ms   |       |          |

疑似问题

http://10.194.10.12:80/druid/v2/sql 消耗214.158ms 14次Database调用耗时: 4.212ms

拓扑 Call Table **Call Tree** 全栈快照 Beta 异常 参数信息 Code统计 SQL统计 NoSQL统计 数据项 Servers 日志

独占时间 > 30 ms 名称 ☐ 过滤 ☐ Span个数: 1/105 折叠时间 < 20 % (≈ 33 ms) 的Span 确定 设为默认



请求: URI/app-api/overview/performance-grading

业务系统: wukong-release

应用: txbj-app-api-nacos

实例: txbj-app-api-nacos-5bb56f7b4-72tvb\_kube-wk-plf-b2-10200

响应时间: 128.781 ms

**请求信息** 详情 日志 异常

基础信息

|                  |                                                                 |
|------------------|-----------------------------------------------------------------|
| URL:             | http://wukong2.tingyun.com/app-api/overview/performance-grading |
| HTTP method:     | POST                                                            |
| Response Status: | 200                                                             |
| Client IP:       | 140.143.182.29                                                  |

Request headers

|             |                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------|
| Referer:    | https://wukong2.tingyun.com/visboard/sense-vis/screen/share/eyJzY3JlZW5JZCI6MTc0MXQ0/vi/dataSource/component/getData/*/* |
| User-Agent: | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36          |

AI驱动软件研发全面进入数字化时代

**AI+ 软件研发数字峰会**  
AI+ software Development Digital summit



# PART 05

## 行业案例

### 案例分享

客户背景 / 建设规划 / 建设成果

# ► 遇见答案 - 业务访问量增加导致系统异常根因分析（案例）

某银行因前一天上线版本同时新增接入10个系统，次日上午进入业务高峰期后，因新增接入系统较多，致使缓存数量超过设定参数，上游kafka出现数据堆积，同时出现多个线程获取缓存失败进而重复查询数据库，致使Mysql数据库CPU上升和应用内存飙升，应用监控系统出现卡停。此时系统产生了大量的告警，并导致多个业务系统业务办理受影响。听云提供了告警收敛和故障定位能力，快速提高生产团队进行问题排查的效率。

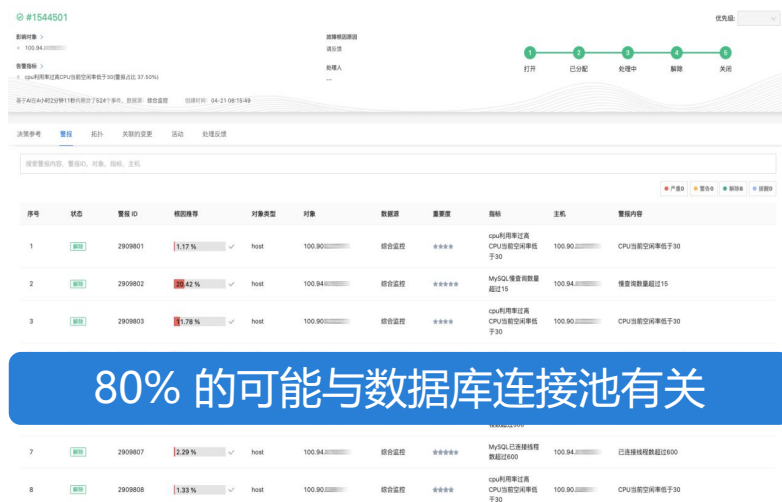
## 收敛+故障定位逻辑

1. 在时间很相近的情况下，发现了大量相类似的指标告警，如CPU利用率过高、空闲率过低、线程数超过设定阈值、数据库连接数大于阈值、慢查询等告警。
2. 根据时间相似性、指标相似性、拓扑关系等特征将这些告警聚合在一起。
3. 结合运维知识（数据库连接数超时是由于访问次数过多导致的，而访问次数过多会导致cpu利用率上升）和因果关系证据，推断出概率根因警报是“数据库连接数超时”这个告警导致的。故障原因最后排查到是缓存容量不足。

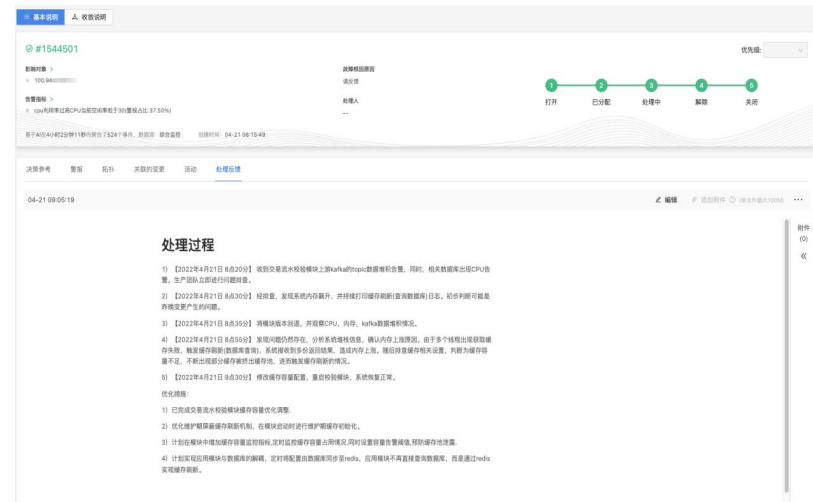
## 案例名称

某头部股份制银行

## 交付效果



## 处理过程沉淀为知识





# ▶ 遇见答案 - 交易失败故障根因分析（案例）

某银行上午9:50分，监控告警网银系统动账信息通知MQ堆积。紧接着10:58分，商务公司来电反馈、企业网银客户反馈交易提交后交易状态显示提交成功，但是未扣款，后台监控网银数据库私网流量超过400M，响应时间在170 ms 左右。由于数据库问题导致不正常交易（未扣款）从而引发系统产生了大量的告警，听云提供了告警收敛能力，让用户更聚焦于分析问题产生的原因。

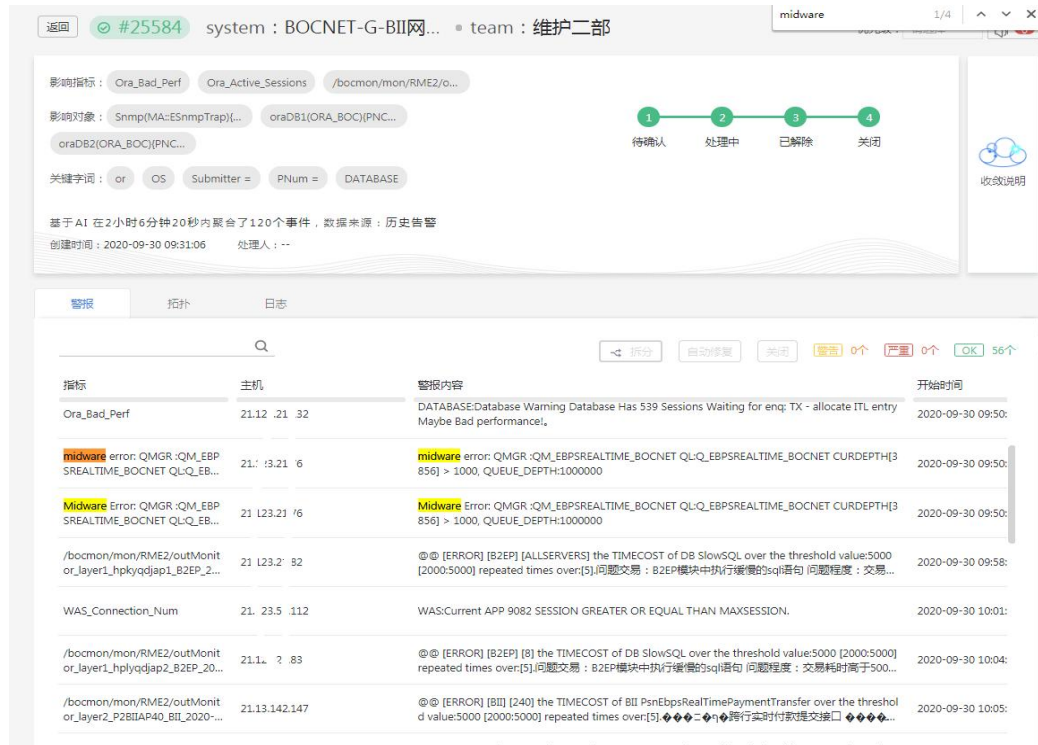
## 收敛逻辑

1. 在时间很相近的情况下，发现了大量指标告警，根据时间相似性、指标相似性、警报内容描述提取关键词计算文本相似度、使用NLP分析得到彼此之间的相关性。
2. 结合拓扑关系和故障根因发生时间的关系，推断出数据库指标Ora\_Bad\_Perf是根因的概率最大。

## 案例名称

某头部城商行

## 交付效果



# 让运维更简单



简化入口、全景关联、给出答案

# THANKS

