AIOps 在线评测基准系统

聂晓辉 必示科技公司

科技生态圈峰会 + 深度研习

——1000 + 技术团队的共同选择

KEYLINK ing

K+峰会

上海站
K+全球软件研发行业创新峰会
时间：2024.06.21-22

敦煌站
K+思考周®研习社
时间：2024.10.17-19

香港站
K+思考周®研习社
时间：2024.11.10-12

K+峰会详情

AiDD峰会

上海站
AI+研发数字峰会
时间：2024.05.17-18

北京站
AI+研发数字峰会
时间：2024.08.16-17

深圳站
AI+研发数字峰会
时间：2024.11.08-09

AiDD峰会详情

演讲嘉宾

聂晓辉

必示科技产品总监

必示科技产品部总监、算法研究员，清华大学计算机系博士，研究领域为智能运维 (AIOps)，在 JSAC、TON、KDD、ESEC/FSE 等 CCF A/B 类国际会议或期刊上发表20余篇文章，研制的智能运维系统在银行、证券、运营商、互联网等40 多家企业实施落地，曾获得中国电子学会科学进步一等奖。

让数字世界更好地运转

INTELLIGENT OPERATIONS FOR THE DIGITAL WORLD

公司介绍
PROFILE

北京必示科技有限公司成立于2016年，源自清华大学NetMan智能运维实验室，致力于用AI技术赋能IT运维领域，打造世界领先的智能运维（AIOps）引擎——必示智能运维平台，让企业可以从复杂的IT软硬件和海量监控数据中自动、准确、快速地进行风险预警、异常发现、故障定位等，提高企业IT系统稳定性、可用性和运营管理效率，助力企业防控IT系统运行风险。

必示科技——智能运维领航企业

顶尖团队

- 依托清华大学NetMan实验室
- 产品团队拥有二十余名智能运维领域博士、硕士
- 核心管理团队平均行业经验超过15年

技术优势

- 二十余项AIOps行业领先核心算法
- 国际顶级会议、学术期刊发表论文三百余篇
- 高校合作、工程孵化、产品线三层产学研创新体系

经验优势

- 深耕落地百余家金融、运营商为代表的头部企业
- 主导及深度参与智能运维领域国家标准和行业标准
- 形成业界首个智能运维落地效果运营方法论

产品优势

- 业内率先定义“风险预警+异常发现+故障定位”的最佳工业实践
- 丰富完善的必示智能运维产品矩阵
- 以“为客户交付清晰价值”为目标的产品落地准则

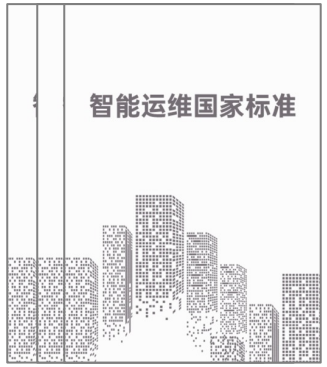
行业内科研实力最强、市场关注度最高的企业

20+核心技术发明专利

50+项软件著作权

参与编写国内仅有的两本企业级AIOps实践白皮书

国际顶会&学术期刊发表论文三百余篇



主导参与智能运维国标制定

信创适配

完成对操作系统、处理器、数据库、中间件、云平台等领域的30余家企业的产品兼容认证

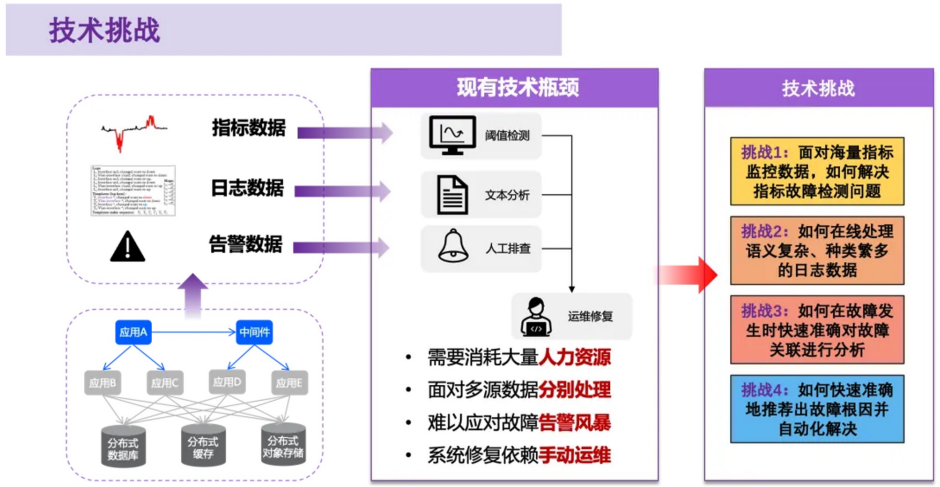
奖项荣誉

- 2023中国电子学会科技进步一等奖
- 连续三年入选IDC 中国FinTech 50榜单
- 2023成为中国移动自智网络子链成员单位
- 2023成为首批 “建行云”生态合作伙伴
- 2022数字中国年度高科技高成长企业系列榜单
- 2022未来银行科技服务商Top100榜单
- 2022第四届金融数据智能优秀解决方案评选——专家推荐top10优秀解决方案
- 2022中国云生态创新企业榜
- 2022 IDC 中国FinTech 50榜单
- 2022年度金融科技影响力品牌
- 2022年度数字化先锋产品奖
- 2022年数字中国年度高科技高成长企业系列榜单
- 2021金融行业年度卓越创新案例-智能运维（AIOps）类
- 2021年IDC 中国Fintech 50榜单
- 2020年度最具商业价值解决方案 TOP 30
- 2020中国人工智能商业落地价值潜力100强
- 2020运维创新优秀解决方案
- 2019机器之心最具创新AI产品解决方案TOP30
- 2019人工智能企业TOP100
- 2019年9月中国高质量发展创新示范单位
- 2018盛景全球创新大奖TOP20

· · · · · ·

产品顶尖AI技术，荣获中国电子学会科技进步一

- 必示科技参与的“**大模型在线服务智能智能运维核心技术及产业化**”项目荣获2023**中国电子学会科技进步一等奖**。
- 在评审会上，**费爱国院士、张宏科院士**一致认为：“该项目技术复杂，研究难度大，创新性强，项目整体成果达到**国际先进水平**，其中基于生成模型的指标异常检测、基于语言模型的日志异常检测、基于因果推理的故障定位处置等技术均达到了**国际领先水平**。项目社会效益、经济效益显著，应用前景广阔。”
- 截至目前，该项目已产生**直接经济收益数亿元**；本项目突破智能运维**技术瓶颈**，提升了在线服务的运维水平，为信息服务和数字中国提供重要支撑，具有显著的社会效益。
- 中国电子学会科技进步奖，在业内具有很高的认可度和影响力，**等同于（甚至高于）省部级奖励**。
- 该奖项具有很高的科技含量，同时期获奖有**ChatGLM大模型（清华&智谱华章，2023）**、**GaussDB数据库（清华&华为云，2022）**。



市场高度认可，大量头部客户

银行

中国人民银行清算总中心 · 中国建设银行 China Construction Bank · ICBC 中国工商银行 · 中国银行 BANK OF CHINA · 交通银行 BANK OF COMMUNICATIONS · 中国农业发展银行 · 招商银行 CHINA MERCHANTS BANK · 中国民生银行 CHINA MINSHENG BANK

广发银行 CHINA GUANGFA BANK · 华夏银行 HUAXIA BANK · 中国光大银行 CHINA EVERBRIGHT BANK · 浦发银行 SPD BANK · 浙商银行 · 恒丰银行 HENGFENG BANK · 汇丰 · 北京银行 BANK OF BEIJING · 上海银行 Bank of Shanghai

南京银行 BANK OF NANJING · 中原银行 ZHONGYUAN BANK · 天津银行 BANK OF TIANJIN · 阜新银行 BANK OF FUXIN · 九江银行 BANK OF JIUJIANG · 温州银行 BANK OF WENZHOU · 泰隆银行 TAI LONG · 台州银行 TZB · 金华银行 JHBank

湖州银行 BANK OF HUZHOU · 绍兴银行 BANK OF SHAOXING · 内蒙古银行 Bank of Inner Mongolia · 浙江民泰商业银行 ZHEJIANG MINTAI COMMERCIAL BANK · 浙江农信 · 吉林省农村信用社 JILIN PROVINCE RURAL CREDIT BANK · 陕西信合 · 威海市商业银行 WEIHAI CITY COMMERCIAL BANK · 中银富登村镇银行 BOC Fullerton Community Bank

证券/保险

深圳证券交易所 SHENZHEN STOCK EXCHANGE · 国泰君安证券 GUOTAI JUNAN SECURITIES · 广发证券 GF SECURITIES · 光大证券 EVERBRIGHT SECURITIES · 兴业证券 INDUSTRIAL SECURITIES · 中银国际证券 BOC INTERNATIONAL (CHINA) · 国信证券 GUOSEN SECURITIES · CMS 招商证券 · 泰康 Taikang 保险 资管 医养

其他

China unicom 中国联通 · 中国移动 China Mobile · 中国电信 CHINA TELECOM | 翼支付 · 国家电网公司 STATE GRID CORPORATION OF CHINA · 中国南方电网 CHINA SOUTHERN POWER GRID · 中国烟草 CHINA TOBACCO · 国家税务总局天津市税务局 · 国家计算机网络与信息安全管理中心 · GREE 格力 · 滴滴

与60+家头部金融企业达成合作

合作客户包括国有大行、股份制银行、国内TOP城商行和证券机构。

积淀近百个智能运维项目建设经验

必示科技拥有近百个深入参与的智能运维建设成功案例，构建了独有的AIOps建设方法论。

目录
CONTENTS

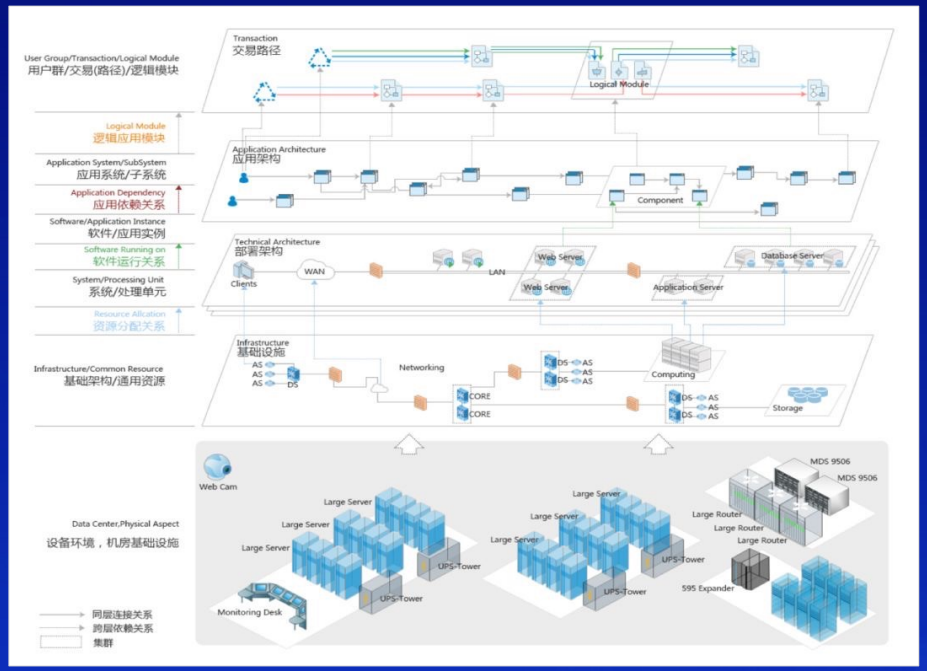
PART 01
AIOps在线评测基准背景

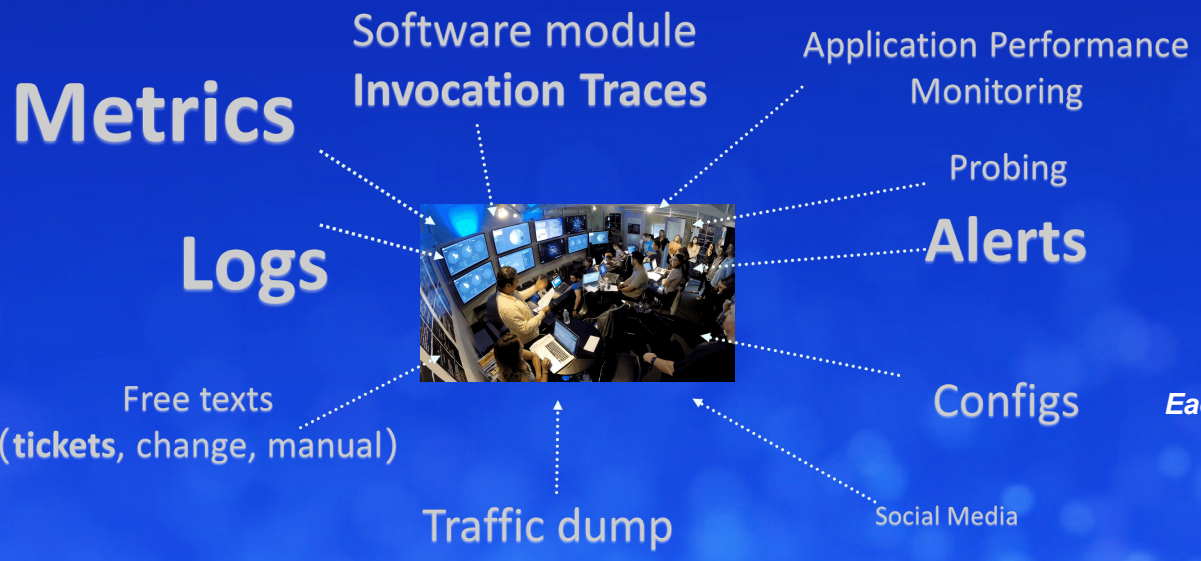
智能运维发展现状

运维在各行各业的重要性越来高

银行、证券、保险、电信、能源、工业制造、政府部门、互联网...

- 数字化程度越来越高
- 监控数据量越来越大
- 系统规模越来越大
- 新技术、新组件不断引入
- 组件监控粒度越来越细



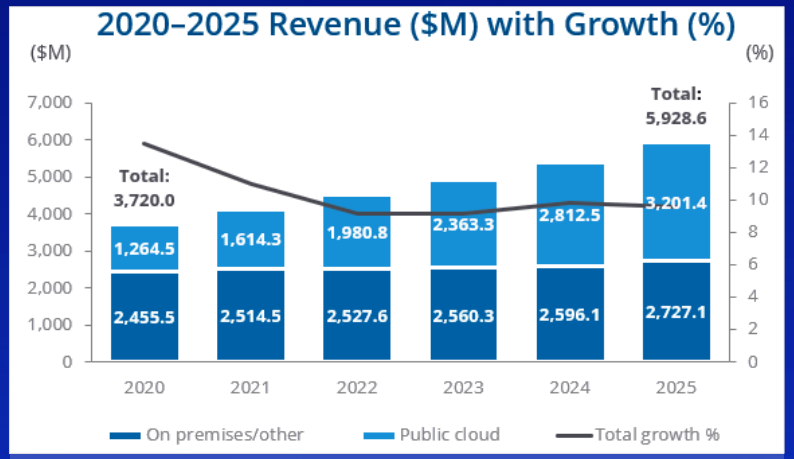


运维工程师被**海量高速运维监控数据**淹没

Each offers some clues, but due to complexity and volume,
each is hard to manually analyze, let alone collectively analyze all data sources.

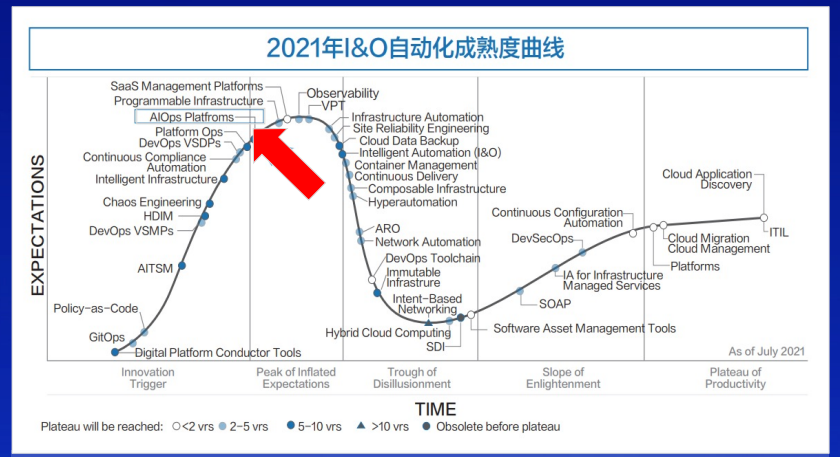
智能运维发展现状

行业趋势



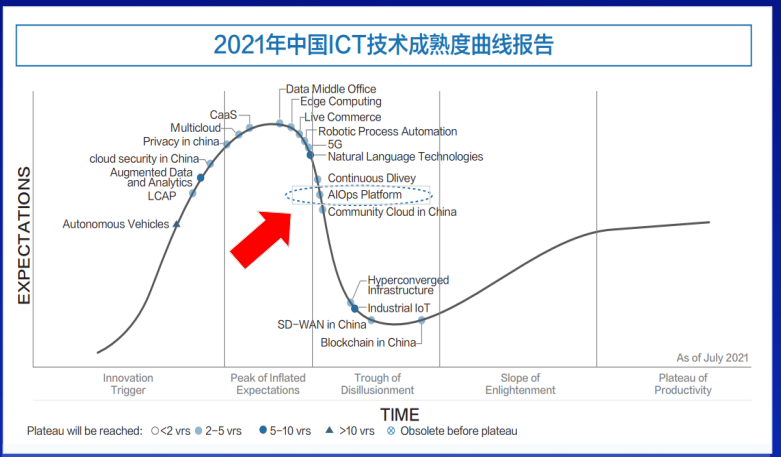
IDC国际IT运维分析预测：

2021至2025年间，IT运维分析相关软件领域的市场复合年增长率为9.8%，市场总收入预计达到59.3亿美元。



Gartner技术成熟度曲线（全球）：

- 智能运维处于通胀预期阶段的顶峰之前
- 在2到5年内达到最终成熟的实质生产阶段，5到10年内达到生产力高原的阶段



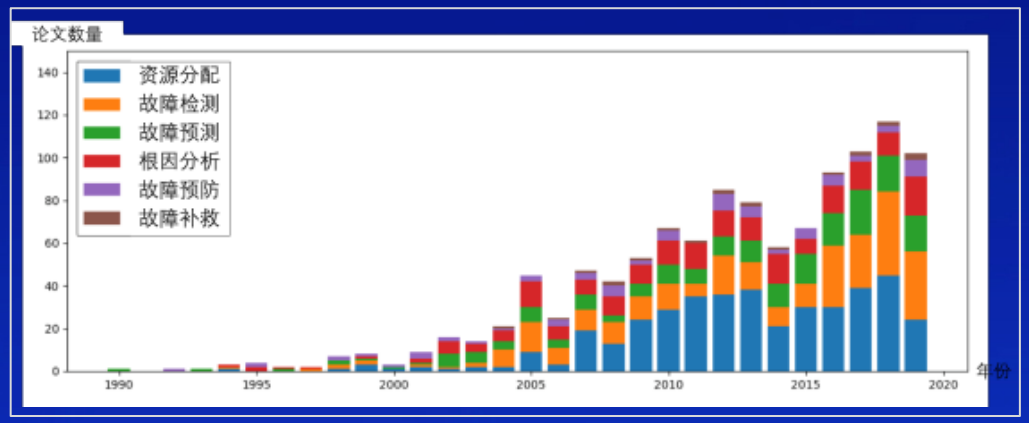
Gartner技术成熟度曲线（国内）：

- 国内智能运维技术成熟度相较于全球处于靠前位置
- 智能运维已经跨过了通胀预期阶段的顶峰并处于下滑阶段
- 将会更早地进入实质生产阶段

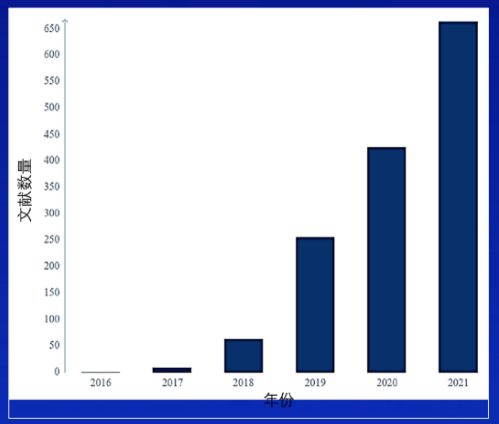
Each offers some clues, but due to complexity and volume,
each is hard to manually analyze, let alone collectively analyze all data sources.

智能运维学术研究现状

近年来论文数量



Notaro 2020

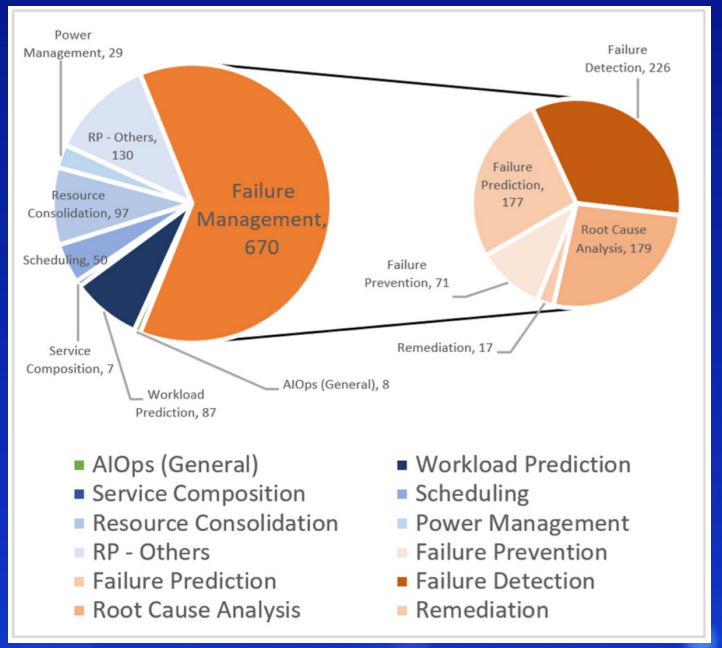


Reiter 2021

研究分类

Notaro 2020

主流研究方向



Notaro 2020

- 绝大部分论文集中在故障检测，根因分析和故障预测中
- 实际工业落地的工作占比少

智能运维的落地挑战

人工智能算法

开源工具

最佳实践

运维知识

人工智能
工程化问题

问题定义不清晰

缺乏评测标准

缺乏标准数据

运维场景
实际落地问题

运维数据质量不足

业务需求模糊

运维人员缺乏人工智能相关知识

与现有运维系统难以集成

智能运维

智能运维发展现状

标准化（Standardization）：形成普适于不同运维背景下智能运维落地实施的必要条件，提高行业整体实践能力。解决当前落地实践问题的一种可行方法

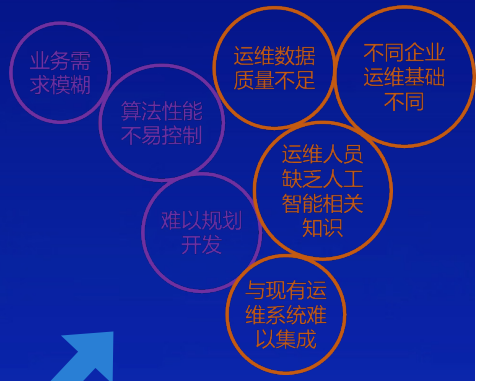


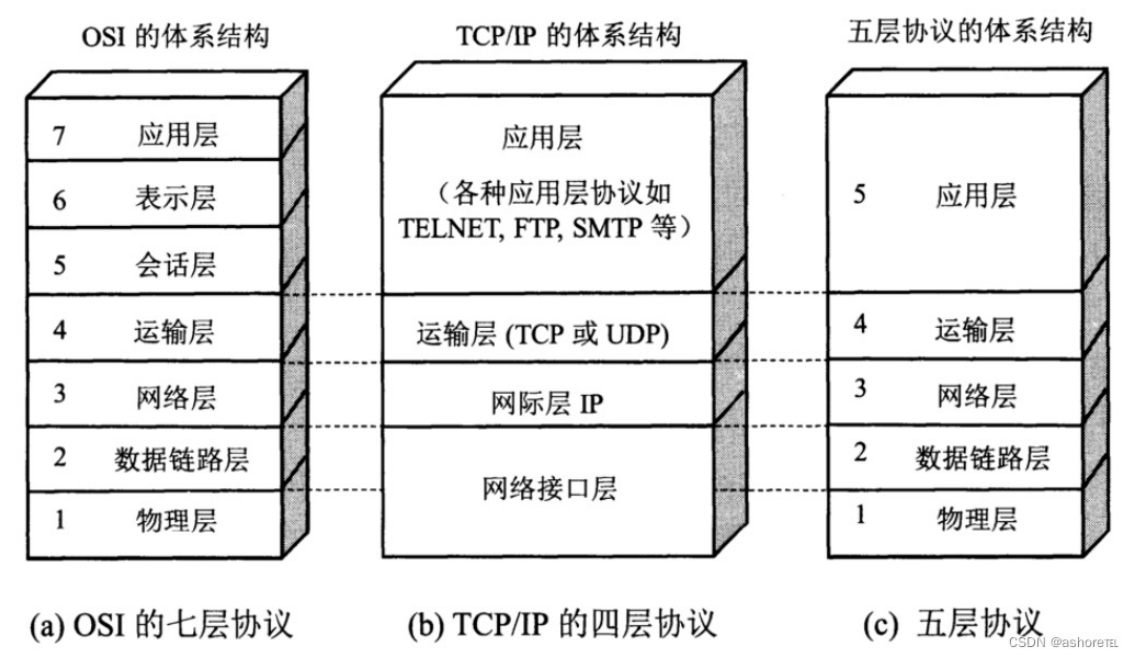
图 3–3 ITSS 5.0 体系框架图

新一版信息技术标准体系ITSS5.0中已将智能运维标准纳入规划中

序号	标准号	标准名称	类别	颁布/修订时间
1	GB/T 43208.1-2023	信息技术服务 智能运维 第1部分：通用要求	国家标准	2023.09
2	T/CCSA 382.1-2022	云计算智能化运维(AIOps)能力成熟度模型 第1部分：通用能力要求	团体标准	2022.06
3	T/CCSA 382.2-2022	云计算智能化运维(AIOps)能力成熟度模型 第2部分：系统和工具技术要求	团体标准	2023.10

良好行业的样例

计算机网络
（标准化协议）



计算机视觉
（标准化评测集）

Russakovsky, Olga, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang et al. "Imagenet large scale visual recognition challenge." International Journal of Computer Vision 115, no. 3 (2015): 211-252. [web]

运维领域同样需要标准数据集、评测标准、系统标准化协议
希望通过构建在线评测基准，推动运维行业的智能化、标准化应用落地

一种运维应用的评测样例

以 2022 CCF国际AIOps挑战赛”微服务架构电商系统下故障识别和分类“为例

混沌工程系统

流量模拟注入故障

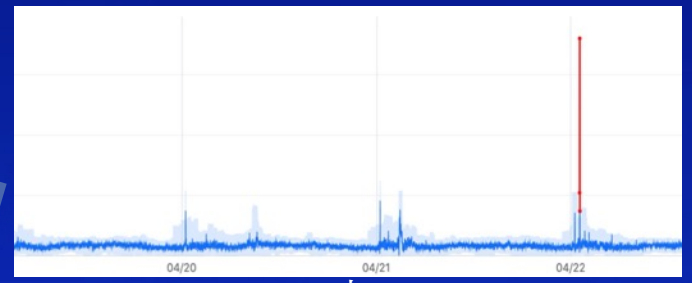
概览 数据 排行榜 规则

决赛 复赛 初赛 资源分配

该排行榜数据截止2022/06/03，最终结果排名可能会有所不同。

排名	团队名称	成员	分数	提交次数
1	Hi战队	zhangjk,LiuTa0,窗外的星星,GongYuhang,cdfw,jojo,18850564416,xuguangyao,便衣工程师,code17	2411.75	436
2	浦智运维团队	wt19536,hgjt8989,not丶today,minduo111,yoeatfish602	1984.75	436
3	翼起飞	liukuan73,成胜,xingh,xiangda,wuqian	1954.75	513
4	中南-天云	csu_dhy,ty-liuxl,junjianli,123_chenzihao,yangping,hg00,amire,tcloud-jiangy,jiaweihuang	1894.5	392
5	JustDo	hejiancsu,same_go,伊斯,xyx754,staygold,头上有天,alpha_bear	1887.75	390
6 ▲	AeroSpaceX	shayzego,chendh01,xiezhipeng1,ayin1551,hubin666,Lawliet-,看那是什么	1792.25	434
7 ▲	pa_tech_22	liwentao,xuanshou001,wubowen,aforwardzyu,zonglibo	1727.25	572
8 ▼	zsc8683	Zsc	1726.25	413
9	ABC_AIOPS	abc_zhang,donaldxuxm,木木,zhen,tree,syltaka,fuxiaopeng,gcjbit	1713.25	494

指标

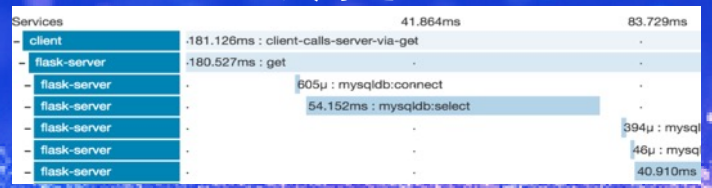


日志

L1. 1537885119 IFNET/2/linkDown_active(l):CID=0x807a0405, alarmID=0x0852003; The interface status changes.
L2. 1537885119 LACP/4/LACP_STATE_DOWN(l): CID=0x804804, PortName=40GE1/0/3; The LACP state is down. Reason = The interface went down physically.
L3. 1537885130 DEVM/3/LocalFaultAlarm_clear(l): CID=0x852003, clearType= service_resume, The local fault alarm has resumed.
L4. 1537885135 IFNET/2/linkDown_clear(l): CID=0x807a0405, alarmID=0x0852003; The interface status changes. Physical link is up, mainName=Eth-Trunk104.

L5. 1539139152 IFNET/2/linkDown_active(l):CID=0x807a0406, alarmID=0x0852007; The interface status changes.
L6. 1539138152 LACP/4/LACP_STATE_DOWN(l): CID=0x804807, PortName=40GE1/0/3; The LACP state is down. Reason = No LCAPDUs were received.
L7. 1539138164 DEVM/3/LocalFaultAlarm_clear(l): CID=0x852004, clearType= service_resume, The local fault alarm has resumed.
L8. 1539138164 IFNET/2/linkDown_clear(l): CID=0x807a0406, alarmID=0x0852007; The interface status changes. Physical link is up, mainName=Eth-Trunk104.

调用链



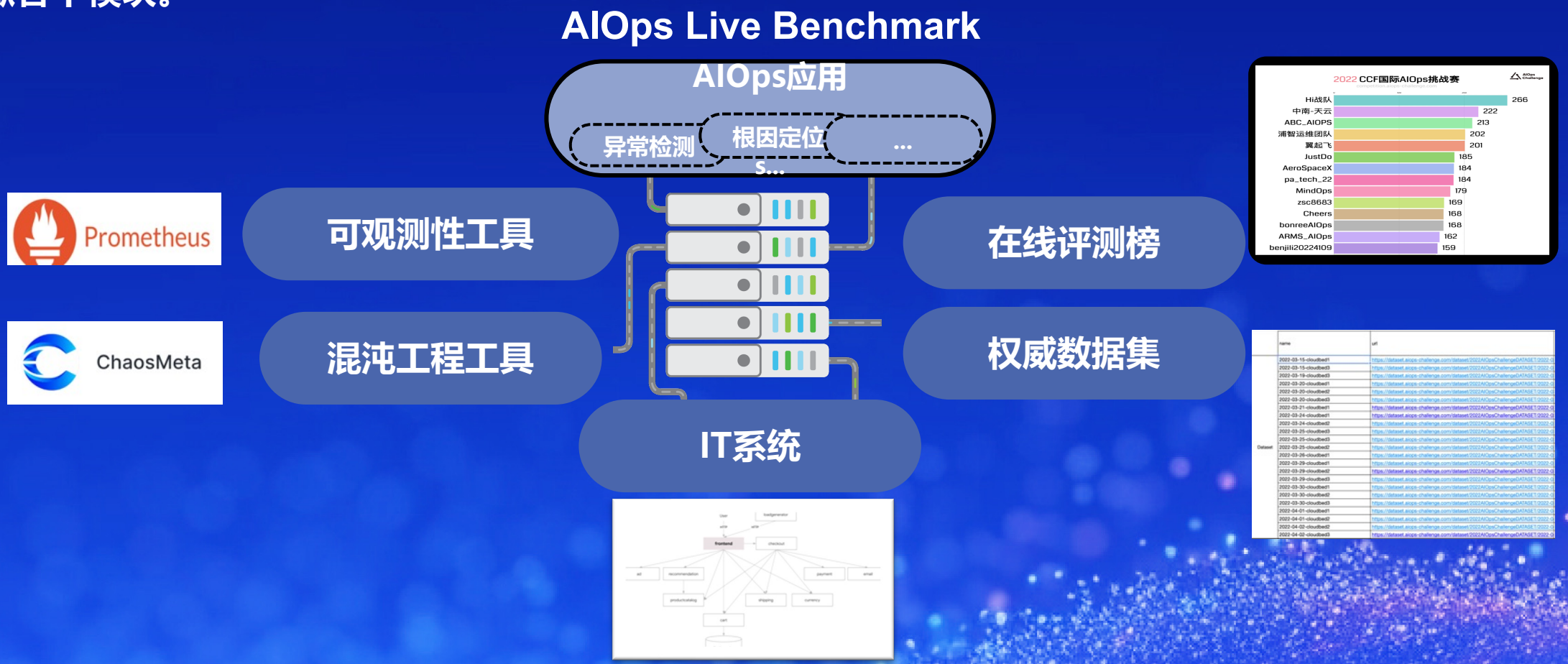
CCF AIOps挑战赛社区

CCF国际AIOps挑战赛7年历程（2018-2024）

https://aiops-challenge.com/

AIOps在线评测基准定义

在线评测基础（AIOps Live Benchmark）：在真实的IT系统上，通过混沌工程工具模拟真实的运维场景，通过可观性测工具获实时数据，在线评测AIOps应用，提供对应的评测基准和排行榜。社区成员可以参与贡献各个模块。

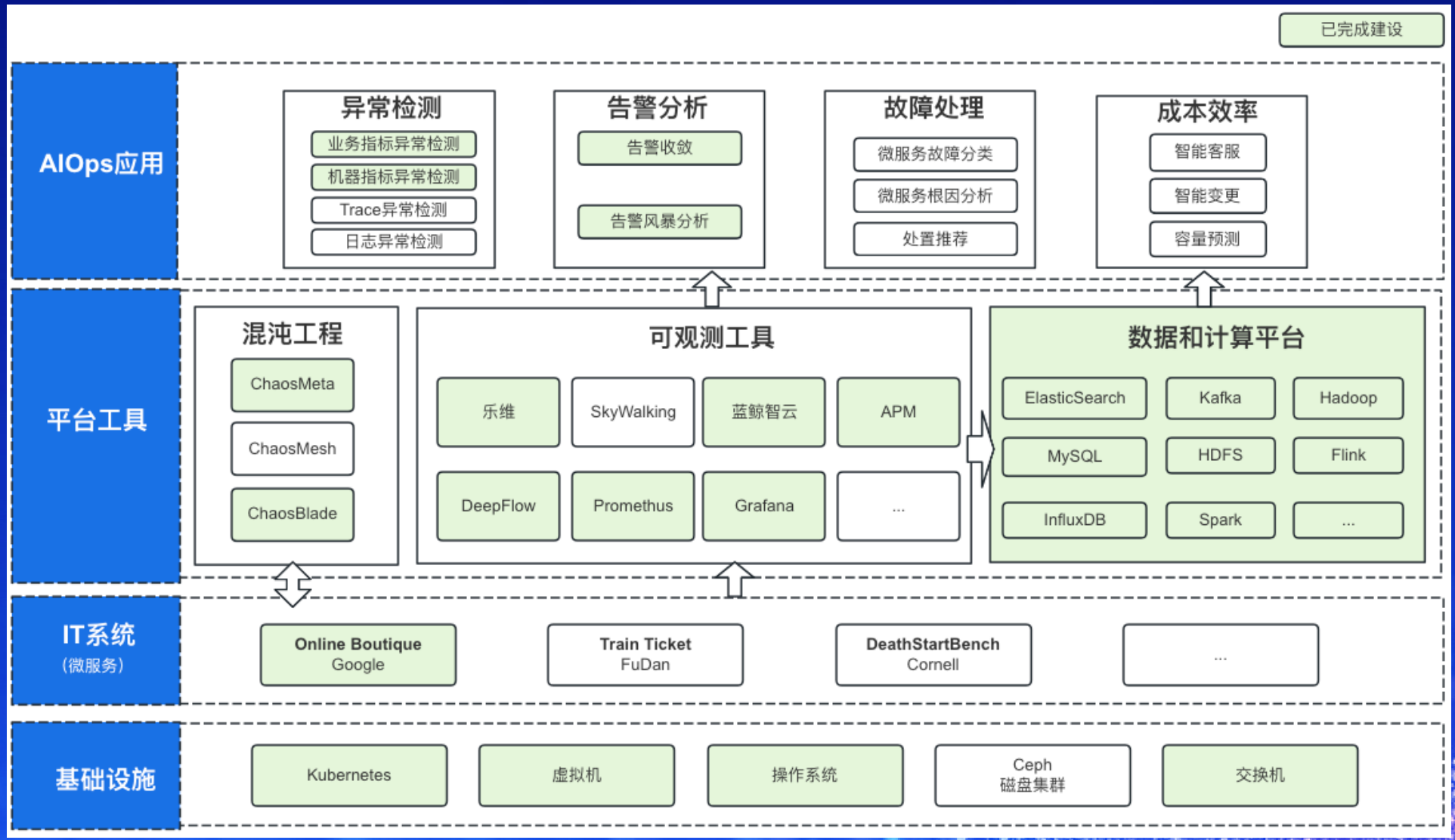


PART 02

AIOps在线评测基准系统建设现状

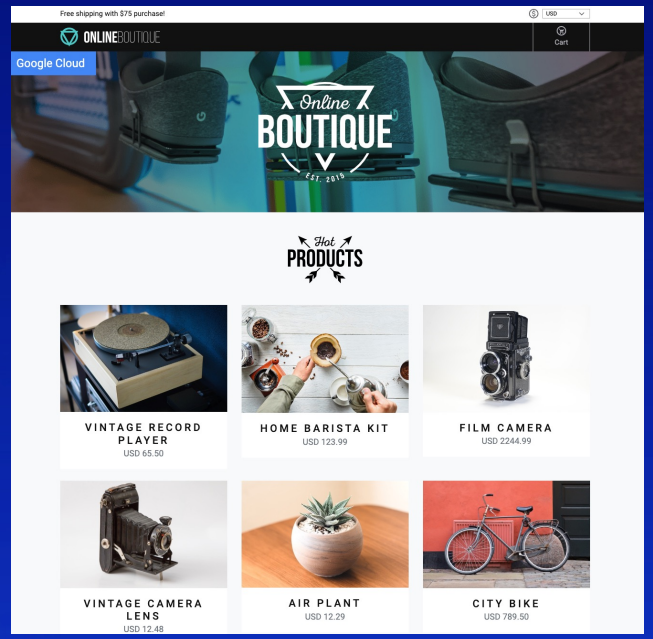
在线评测基准工作进展

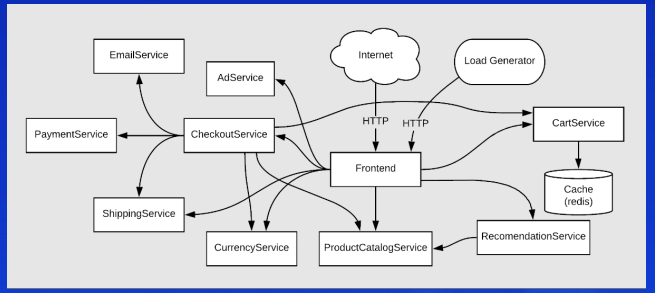
一家小型企业的IT运维工具平台，麻雀虽小五脏俱全



AIOps Live Benchmark 建设架构

微服务系统——Online Boutique

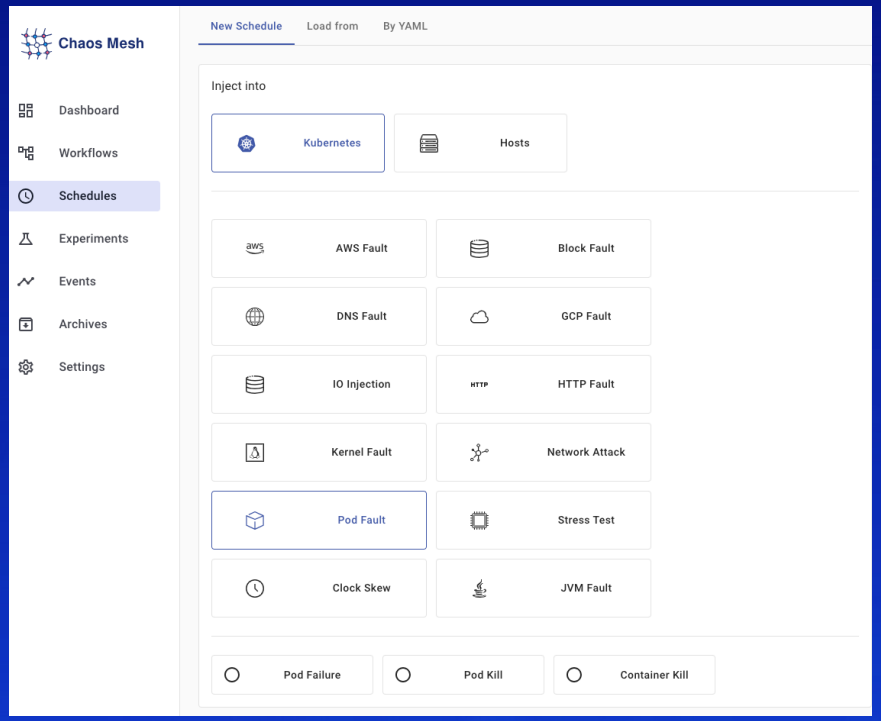


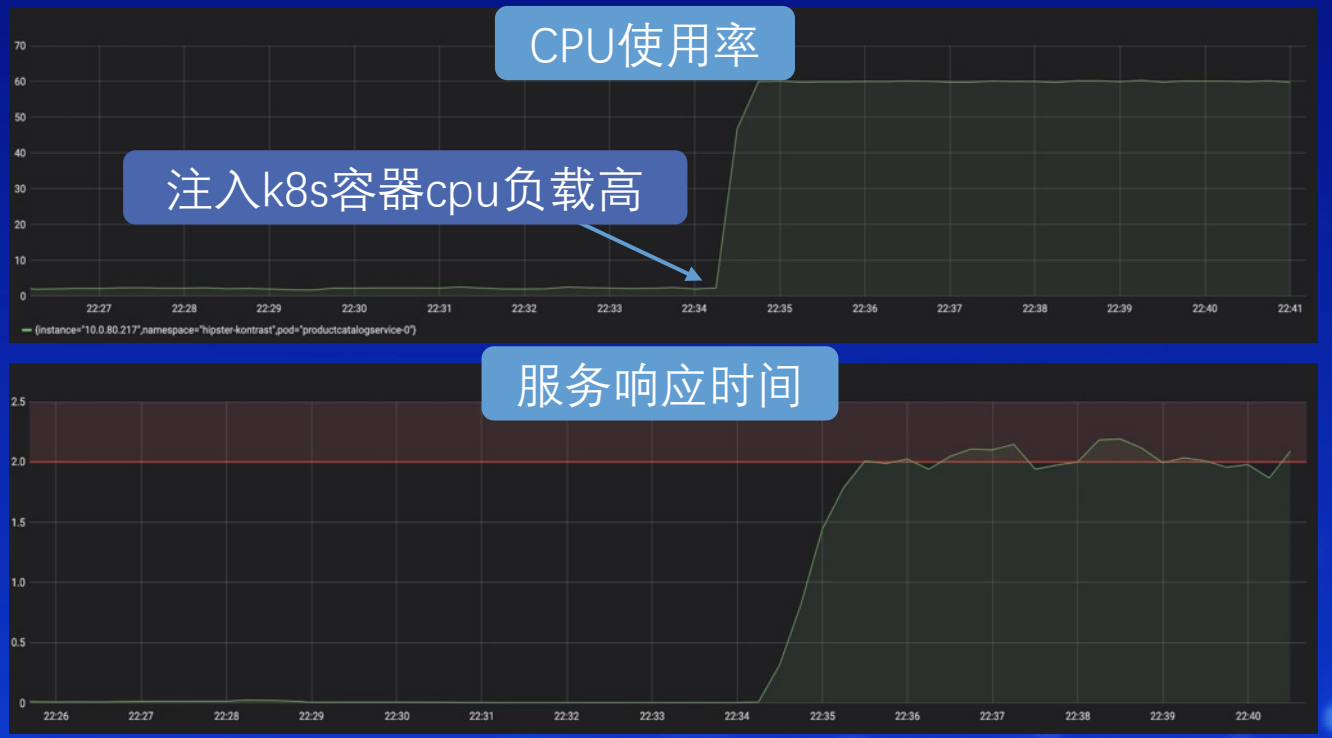


Service	Language	Description
frontend	Go	Exposes an HTTP server to serve the website. Does not require signup/login and generates session IDs for all users automatically.
cartservice	C#	Stores the items in the user's shopping cart in Redis and retrieves it.
productcatalogservice	Go	Provides the list of products from a JSON file and ability to search products and get individual products.
currencyservice	Node.js	Converts one money amount to another currency. Uses real values fetched from European Central Bank. It's the highest QPS service.
paymentservice	Node.js	Charges the given credit card info (mock) with the given amount and returns a transaction ID.
shippingservice	Go	Gives shipping cost estimates based on the shopping cart. Ships items to the given address (mock)
emailservice	Python	Sends users an order confirmation email (mock).
checkoutservice	Go	Retrieves user cart, prepares order and orchestrates the payment, shipping and the email notification.
recommendationservice	Python	Recommends other products based on what's given in the cart.
adservice	Java	Provides text ads based on given context words.
loadgenerator	Python/Locust	Continuously sends requests imitating realistic user shopping flows to the frontend.

- 覆盖多种开发语言的微服务系统，覆盖更多的系统运维场景
- 系统开源，可以根据运维场景对系统做改造
  - OpenTelemetry数据采集
  - 支持信创数据库TiDB
  - 模拟变更场景

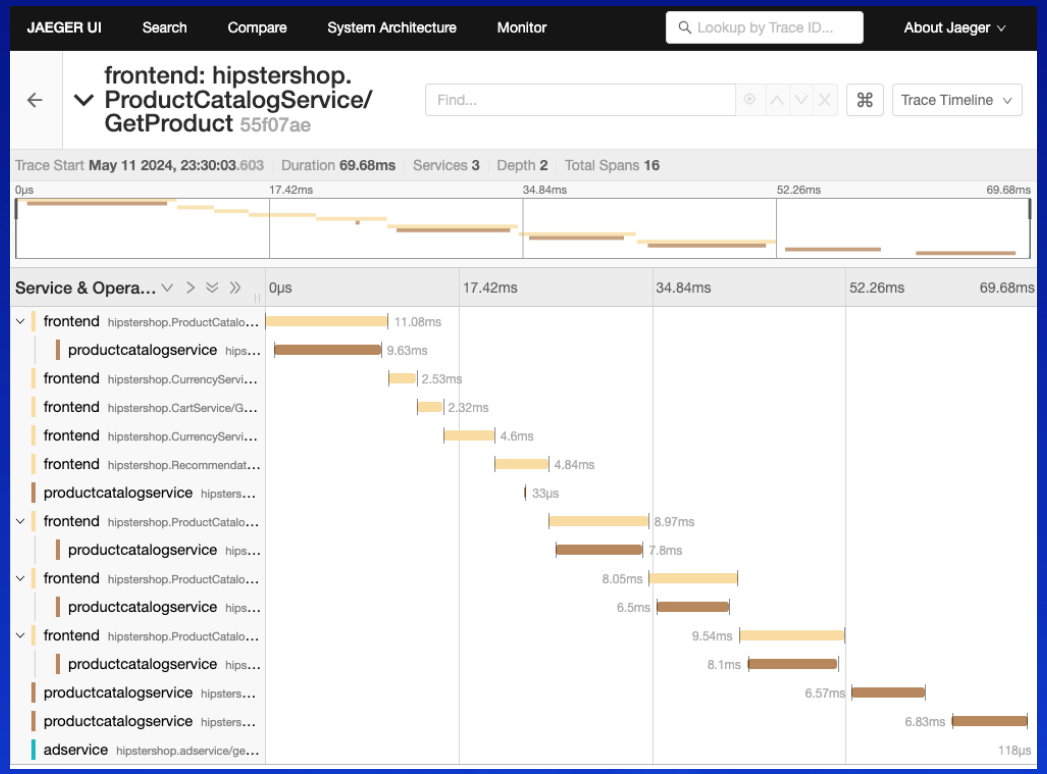
混沌工程工具





- 系统已支持注入K8S、主机上CPU、内存、网络、磁盘、应用等多种类型故障，模拟多种真实故障场景
- 支持异常检测、故障定位等多种场景评测

开源可观测性工具

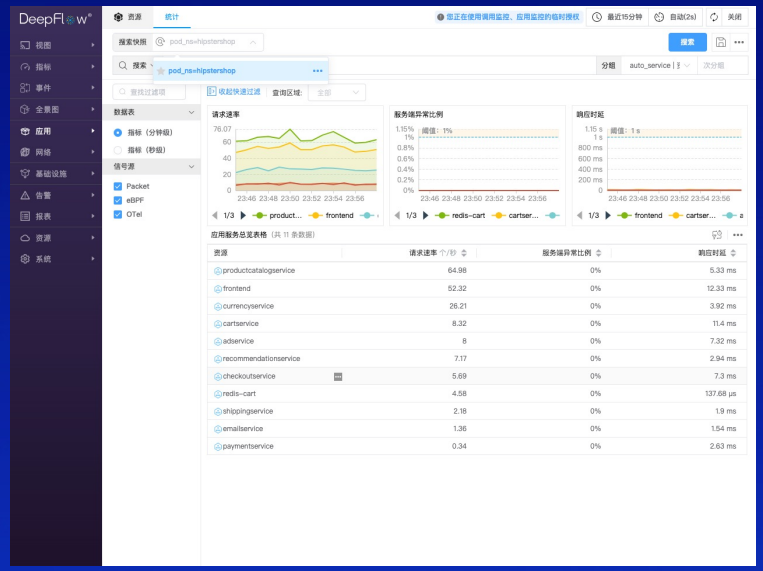


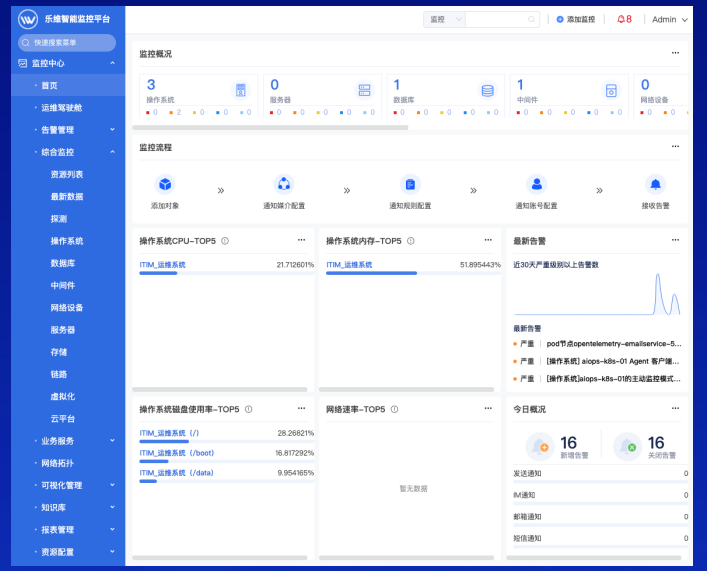
- Jeager: 开源的分布式跟踪系统，用于采集电商系统的trace数据
- Promethues：开源的监控数据采集和告警工具，用于采集电商系统的指标数据

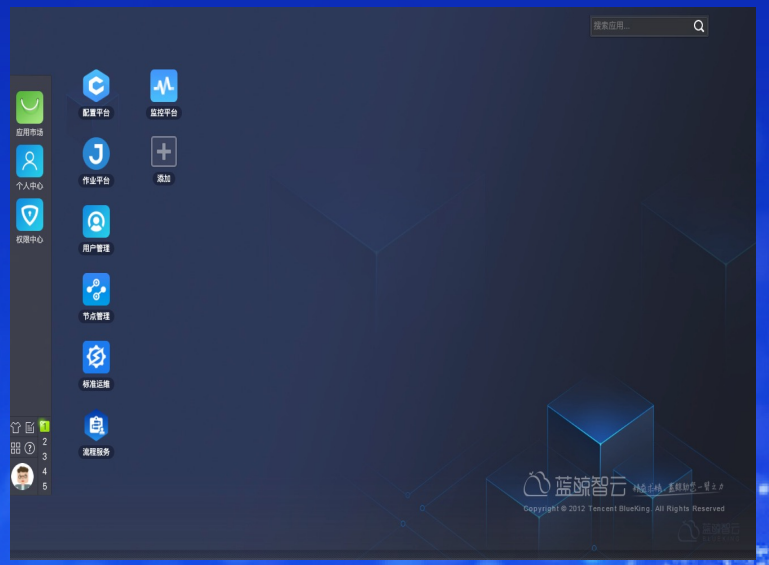
专业可观测工具

全方位的可观测解决方案

- **Deepflow**: 基于eBPF技术，实现网络、系统、应用全栈指标自动采集和全链路自动追踪
- **乐维监控**：专注于数字化运维领域的智能监控平台，提供统一告警、故障诊断、可视化、业务服务、决策辅助等全流程运维管理服务
- **基调听云**：应用性能管理(APM)的解决方案
- **蓝鲸**：腾讯游戏运营部“腾讯智营”下的子品牌，基于 PaaS 的企业研发运营一体化技术解决方案



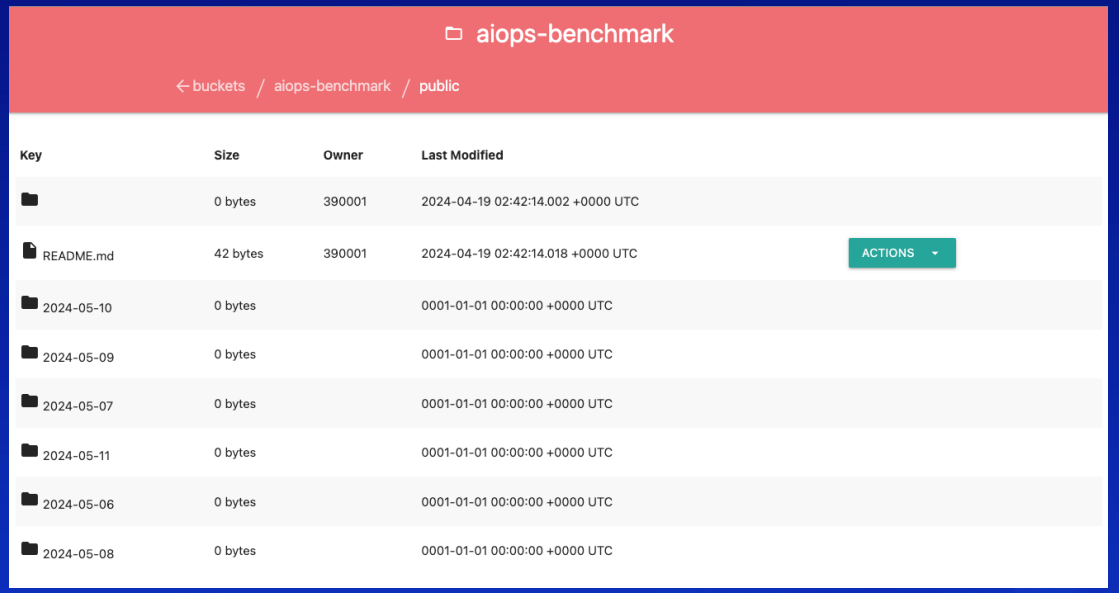




开源数据集

对象	指标编码	指标名称	指标TAG	指标粒度	指标来源	promql语句
app/service/pod	error	异常		60	deepfllow采集	sum(flow_metrics__vtap_app_port__error__1m)by(pod_ns) sum(flow_metrics__vtap_app_port__error__1m)by(pod_ns,ser sum(flow_metrics__vtap_app_port__error__1m)by(pod_ns,ser
	client_error	客户端异常		60	deepfllow采集	sum(flow_metrics__vtap_app_port__client_error__1m)by(pod_ sum(flow_metrics__vtap_app_port__client_error__1m)by(pod_ sum(flow_metrics__vtap_app_port__client_error__1m)by(pod_
	server_error	服务端异常		60	deepfllow采集	sum(flow_metrics__vtap_app_port__server_error__1m)by(pod sum(flow_metrics__vtap_app_port__server_error__1m)by(pod sum(flow_metrics__vtap_app_port__server_error__1m)by(pod
	timeout	超时		60	deepfllow采集	sum(flow_metrics__vtap_app_port__timeout__1m)by(pod_ns) sum(flow_metrics__vtap_app_port__timeout__1m)by(pod_ns, sum(flow_metrics__vtap_app_port__timeout__1m)by(pod_ns,
	error_ratio	异常比例		60	deepfllow采集	avg(flow_metrics__vtap_app_port__error_ratio__1m)by(pod_n avg(flow_metrics__vtap_app_port__error_ratio__1m)by(pod_n avg(flow_metrics__vtap_app_port__error_ratio__1m)by(pod_n
	client_error_ratio	客户端异常比例		60	deepfllow采集	avg(flow_metrics__vtap_app_port__client_error_ratio__1m)by(avg(flow_metrics__vtap_app_port__client_error_ratio__1m)by(avg(flow_metrics__vtap_app_port__client_error_ratio__1m)by(
	server_error_ratio	服务端异常比例		60	deepfllow采集	avg(flow_metrics__vtap_app_port__server_error_ratio__1m)by avg(flow_metrics__vtap_app_port__server_error_ratio__1m)by avg(flow_metrics__vtap_app_port__server_error_ratio__1m)by
POD	pod_cpu_usage	CPU使用率		60	社区Prometheus采集	sum(irate(container_cpu_usage_seconds_total{container = "s
	pod_processes	进程数		60	社区Prometheus采集	sum(container_processes{container = "server"}) by (namespa
	pod_memory_working_set_bytes	内存使用大小		60	社区Prometheus采集	sum(rate(container_memory_working_set_bytes{container = "
	pod_fs_writes_bytes	写入字节的累积计数		60	社区Prometheus采集	sum(irate(container_fs_writes_bytes_total{container = "server"
	pod_fs_reads_bytes	累计读取字节数		60	社区Prometheus采集	sum(irate(container_fs_reads_bytes_total{container = "server"
	pod_network_receive_bytes	接收字节的累积计数		60	社区Prometheus采集	sum(irate(container_network_receive_bytes_total{namespace=
	pod_network_transmit_bytes	传输字节的累积计数		60	社区Prometheus采集	sum(irate(container_network_transmit_bytes_total{namespace

指标体系

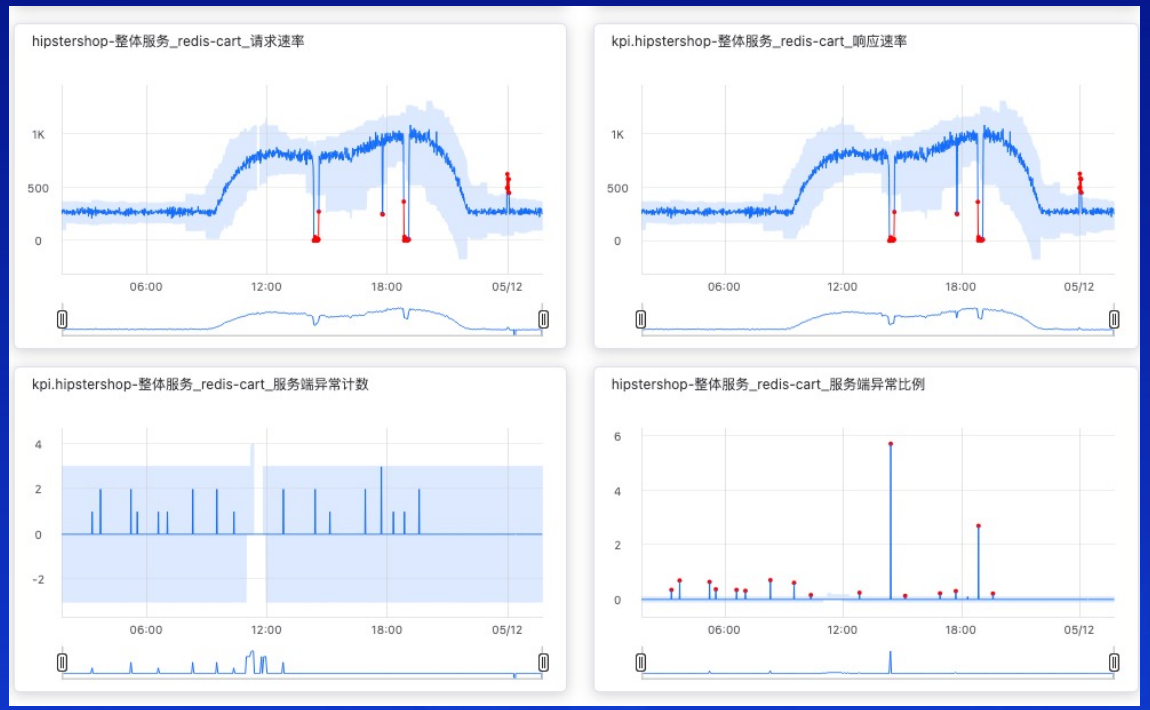


数据下载网站

- 完成初版微服务系统的约**50**种指标、**10**种对象指标体系构建
- 完成数据清洗、存储流程，每天定时发布
- 目前支持指标和trace，后续增加日志等数据，供系统评测

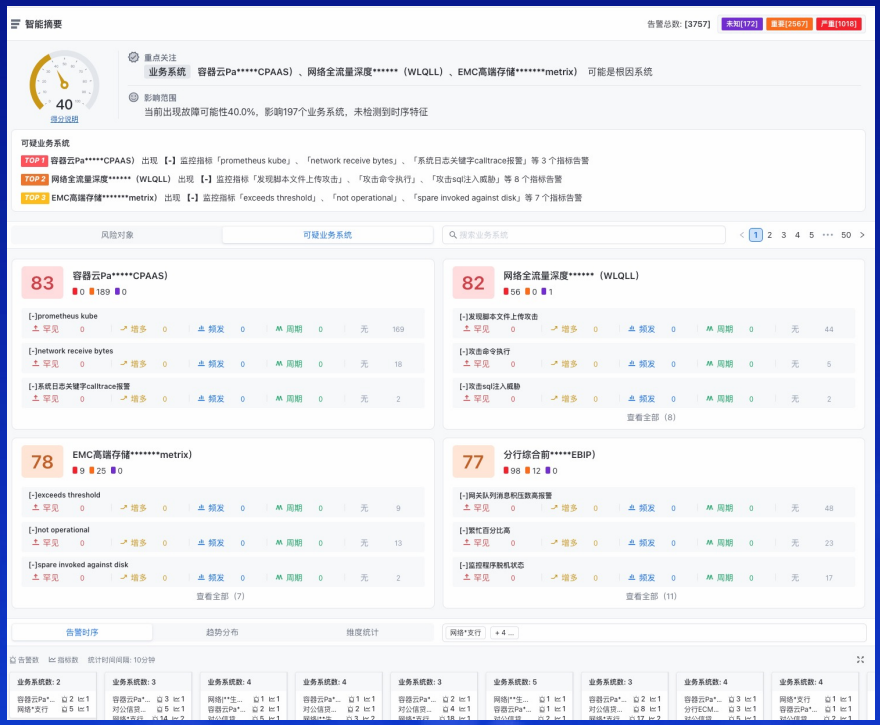
AIOps应用

智能业务指标异常检测



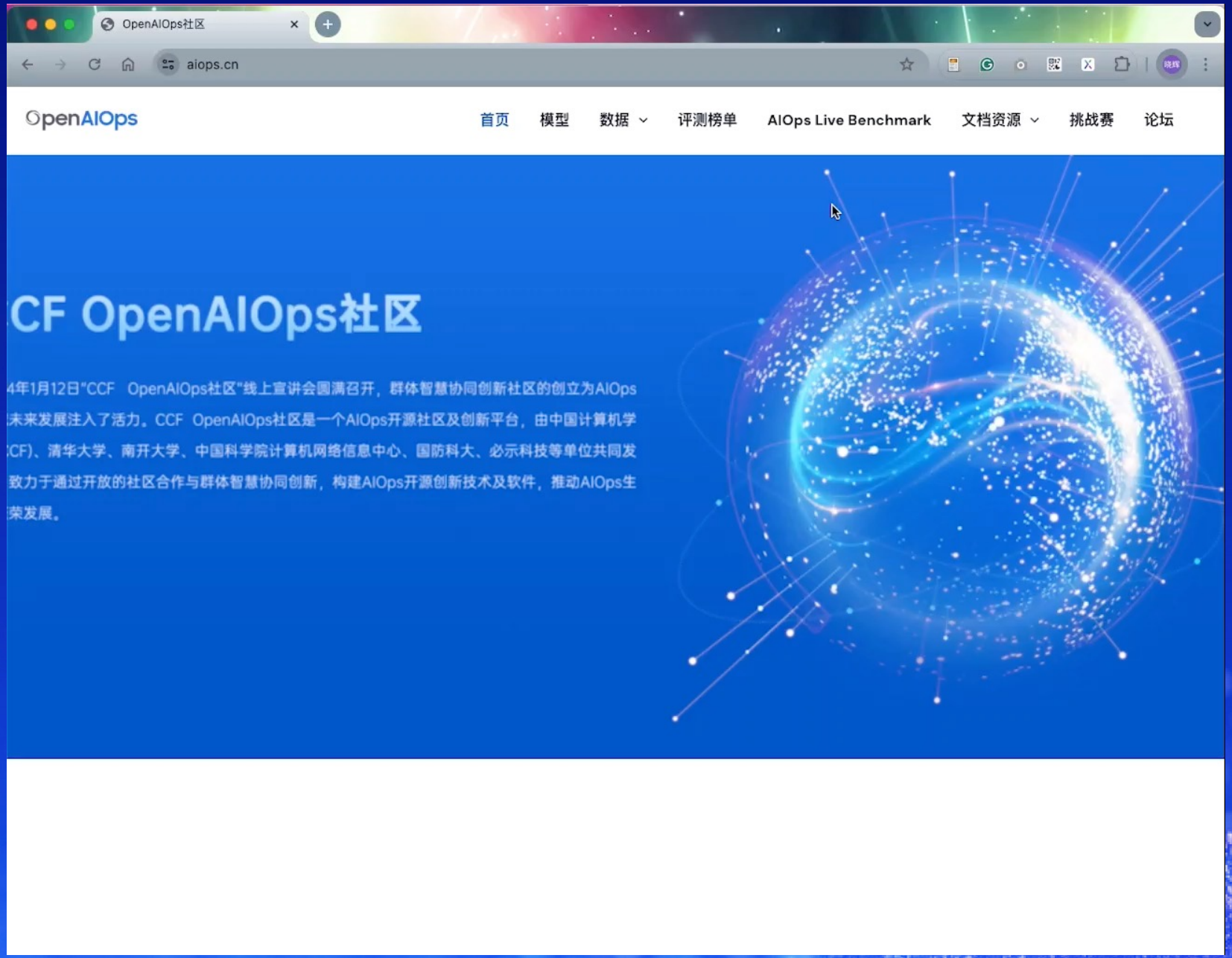
- 动态基线，无需配置阈值，算法学习
- 自动发现可监控指标，扩大监控范围

智能告警管理



- 告警风暴自动分析
- 故障定位、定界
- 告警治理

DEMO演示 https://www.aiops.cn/aiops-live-benchmark/



整体建设情况

- **建设进程**

3月

- 3月5日获得机器资源
- 3月21日完成网站框架建设

4月

- 完成Deepflow、乐维、听云、蓝鲸、必示等工具部署和调试
- 完成2个AIOps应用建设
- 初步开始评测基准建设

5月

- 完成数据清洗和发布
- 制定第一版线评测基准系统

- **当前建设人员**
  - 在线评测基准专家组**59人**，分别来自高校、研究所、科技公司、银行、证券等企业
  - 工程师**约40人**，分别来自中科院、乐维、听云、蓝鲸、DeepFlow、必示等单位

- **系统价值**

01

真实的IT运维场景

在真实的IT系统上，利用流量模拟和混沌工程工具，模拟多种运维场景，测试AIOps解决方案有效性和鲁棒性。

02

前沿的可观测性技术

集成了听云、乐维、蓝鲸、DeepFlow、SkyWalking等前沿的可观测技术工具，实现丰富的指标、日志、Trace数据收集。

03

标准化评估指标

为AIOps应用提供一套标准化的评估指标和排行榜。促进技术的发展和创新，同时也为用户选择合适的工具提供了参考。

04

权威AIOps数据集

为运维应用开发人员和科研人员提供真实的运维数据和场景，用于学术研究、产品测试和评测打榜。

PART 03

AIOps在线评测基准系统关键技术

以真实运维场景构建评测基准

数据库	为 MySQL 的内存不足异常做准备 数据库辅助故障转移时间 数据库延迟 数据库缓存检查 DynamoDB 超时测试
k8s容器	验证容器弹性机制：OOMKiller 测试存储容量限制 节流 CPU 高 CPU 可用性验证让Kubernetes 节点网络丢包 可用性验证黑洞一个区域 可用性验证DNS 中断 服务验证关闭服务 服务验证将丢包注入服务 服务验证向服务注入延迟 服务验证将丢包注入节点 服务验证向节点注入延迟 服务验证关闭节点
运维监控场景	测试 TLS/SSL 证书过期 发现异常的 CPU 消耗 监控和警报验证 onduty考验 检查后端Trace 检查由于网络问题导致的监控数据丢失 基础测试监控和警报
DNS 依赖 网络	DNS 中断系统状态验证 不可用的依赖 不可靠的网络
消息队列	检查 Kafka Broker 负载对处理延迟的影响 检查 Kafka 脑裂冲突 测试消息系统的最小节点假设 测试消息流以处理丢失的leader node 为生产者的延迟做准备
基础设施	使用状态检查验证自动缩放 验证运行状况检查 - 延迟 验证运行状况检查 - 数据包丢失 区域异常 准备主机故障 处理混合环境中的网络问题 查找单点故障

故障注入能力

故障名称	故障对象	注入方式	销毁方式	注入描述	故障表象（可直接造成的指标异常或日志片段异常）
CPU负载	容器、虚拟机	API接口、CLI	API接口、CLI	CPU占用率，CPU核心占用率	额外进程消耗CPU，CPU占用率升高
CPU爬升占用	容器、虚拟机	API接口、CLI	API接口、CLI	CPU占用率缓慢爬升，CPU核心占用率	额外进程消耗CPU，CPU占用率按爬升时间升高
内存负载	容器、虚拟机	API接口、CLI	API接口、CLI	内存（cache、mem）的控制，容易造成服务宕机（OOM）	额外进程消耗内存
网卡延迟	容器、虚拟机	API接口、CLI	API接口、CLI	对故障对象的某一网卡进行延迟控制，可隔离部分组件的网络通信	流经该网卡的请求延迟提高
网卡丢包	容器、虚拟机	API接口、CLI	API接口、CLI	对故障对象的某一网卡进行丢包控制，可隔离部分组件的网络通信	流经该网卡的请求发生丢包
网络隔离	虚拟机	API接口、CLI	API接口、CLI	定向隔断对象网络	注入对象网络指定域网络不可达
端口占用	容器、虚拟机	API接口、CLI	API接口、CLI	本地端口占用，可强制占用（关停原有服务）	本地端口占用，无法新建服务通信
网络包重复	容器、虚拟机	API接口、CLI	API接口、CLI	指定网卡、本地端口、远程端口、目标 IP 包重复	
DNS解析异常	虚拟机	API接口、CLI	API接口、CLI	篡改域名地址映射	域名解析异常，类DNS服务器异常
文件权限变更	虚拟机、容器	API接口、CLI	API接口、CLI	指定文件权限变化	部分进程指定文件读写访问异常
文件增删	虚拟机、容器	API接口、CLI	API接口、CLI	指定文件新增、删除操作	
服务中断	虚拟机	API接口、CLI	API接口、CLI	对某个服务进行宕机模拟	服务下线、虚拟机宕机
磁盘读写IO控制	服务、容器、虚拟机	API接口、CLI	API接口、CLI	对磁盘的IO控制	读写失败、读写延迟
磁盘空间控制	服务、容器、虚拟机	API接口、CLI	API接口、CLI	磁盘使用率的控制	磁盘占用空间，短时间有IO攀升
进程杀死	容器、虚拟机	API接口、CLI	API接口、CLI	杀死进程	故障进程被kill
进程暂停	容器、虚拟机	API接口、CLI	API接口、CLI	进程假死	故障进程暂停执行
JVM OOM	JVM	API接口、CLI	API接口、CLI	JVM heap堆内存异常	JVM日志报出OOM片段（支持metaspace、heap、offheap），内存使用率上升
JVM CPU满载	JVM	API接口、CLI	API接口、CLI	JVM CPU满负载	Java进程 CPU攀升
CodeCache满载	JVM	API接口、CLI	API接口、CLI	JVM JIT编译后“热代码”存放区占满	JVM关闭JIT编译且不可再开启，系统最大负载下降
声明异常抛出	JVM	API接口、CLI	API接口、CLI	在特定类上的方法上概率抛出异常	应用日志出现异常片段
自定义异常抛出	JVM	API接口、CLI	API接口、CLI	在特定类的方法上概率跑出某种异常	应用日志出现异常片段
JVM资源更改（配置变更故障）	容器、虚拟机	YAML	YAML	控制JVM资源	
K8s资源更改（配置变更故障）	虚拟机	YAML	YAML	k8s分配资源不足故障	K8s新创建Pod处于Pending状态
容器资源更改	容器	CLI	CLI	Docker分配资源不足故障	服务资源不足
Linux 内核故障（延迟）	虚拟机	API接口、CLI	API接口、CLI	对linux内核函数添加延迟	调用内核函数的相关进程发生延迟
Linux 内核故障（返回码）	虚拟机	API接口、CLI	API接口、CLI	对linux内核函数返回码修改	调用内核函数的相关进程返回码被修改
API接口故障（延迟）	服务	YAML	YAML	通过对服务中的某一单一接口进行延迟故障注入	服务某一个API接口发生延迟
API接口故障（返回码）	服务	YAML	YAML	修改服务中的某一单一接口的返回码	服务某一个API接口返回错误的返回码
MySQL数据库异常：调用延迟	JDBC层	API接口、CLI	API接口、CLI	MySQL特定SQL延迟	
代码逻辑故障（变更故障）	服务	非侵入式、侵入式	API接口、版本回滚	对内部代码进行修改，模拟变更发生的代码逻辑故障	

流量模拟

CloudAnt
流量模拟效果

CloudAnt流量模拟切入点:

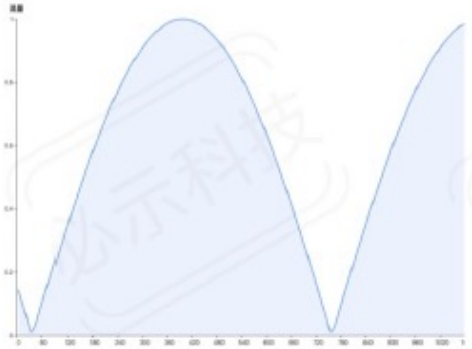
1. 负载强度模拟（LIMBO）:

- 描述方法:用一系列的特征来描述预想的负载强度，如周期性，长时趋势，噪声等。
- 获取方法:人为构建+自动化抽取:通过监控数据(日志，指标)构建流量形状，并以人工辅助进行微调。
- 负载强度实现:根据负载强度模型还原学习到的流量曲线，使用还原的流量曲线模拟负载强度。

周期曲线

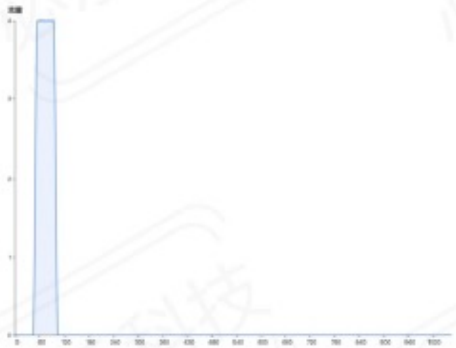
- 正弦曲线（适合具有一定周期的场景）

$$f_{sin}(x) = \lceil |Asin(x+\beta)+h| \rceil, x > 0$$



- 阶跃（适用于类似跑批的场景）

$$f_{SP}(x) = \begin{cases} \delta & \delta \in \mathbb{N}^+, \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$$



高峰曲线

- M字模型（适用于模拟双尖高峰的场景，如早晚高峰）

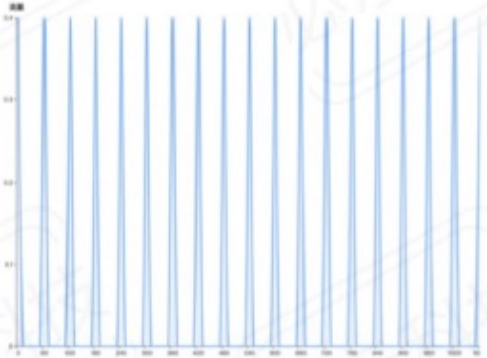
$$g(x) = \lceil -A(x-a+\theta)(x-b+\theta)(x-c+\theta)(x$$

$$f_{SM}(x) = \begin{cases} g(x) & \text{if } g(x)>0 \\ 0 & \text{otherwise} \end{cases}$$

- a, b, c, d为零点个数，theta为横向平移参数，h为纵向平移参数，A为倍率

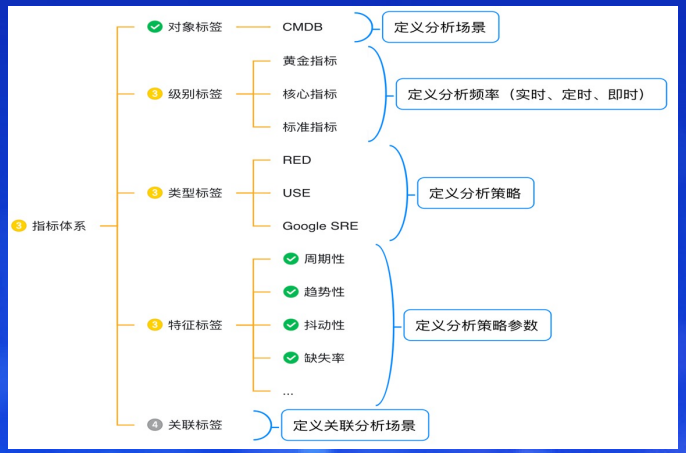
- 高斯模型（适用于模拟单尖高峰的场景，如秒杀活动）

$$f_{GM}(x) = \lceil ae^{-(x-b)^2/2c^2} \rceil$$



定义运维指标体系

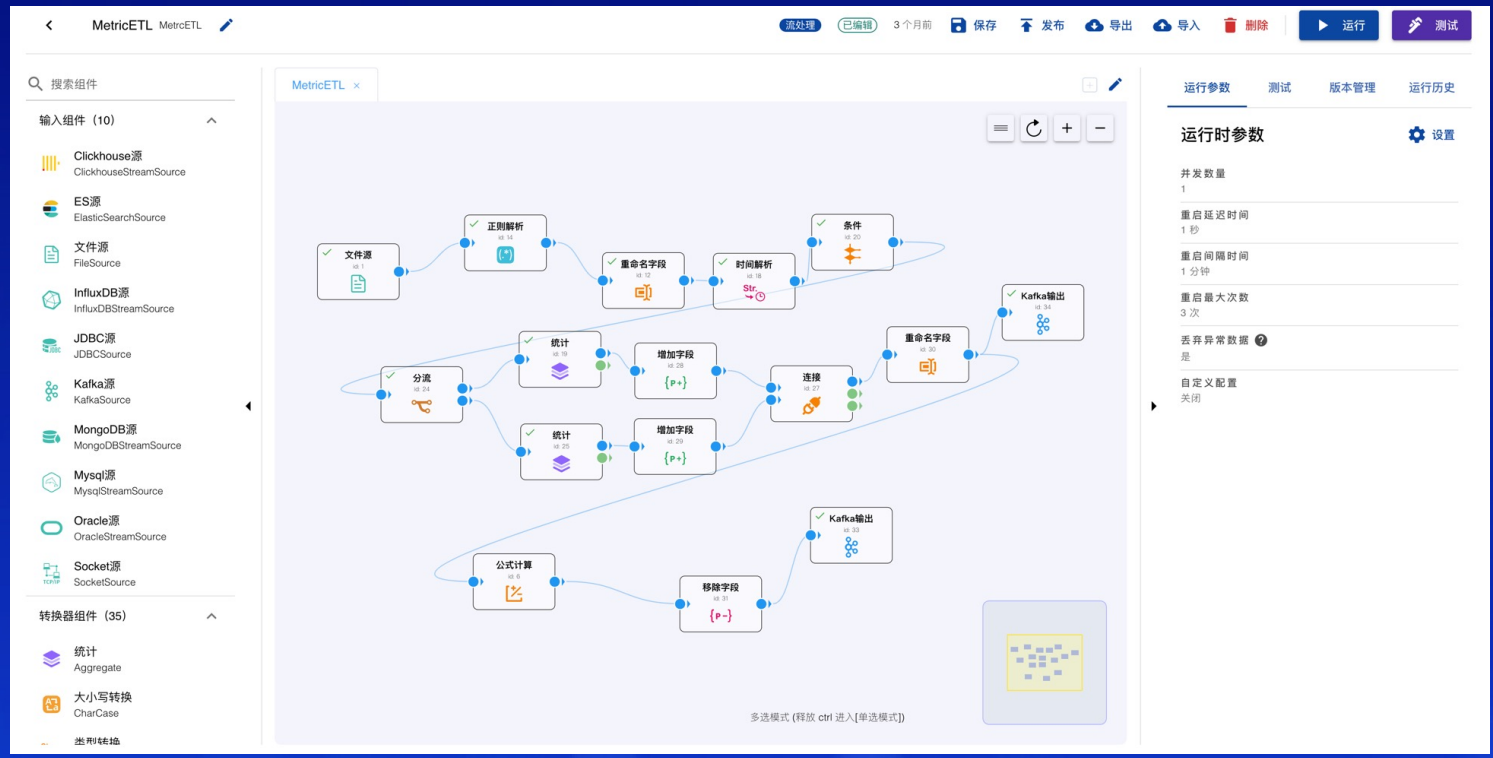
业务性能及体验	功能使用 交易数据 业务流程 客户体验 运营管理 ……	交易订单量，交易时延 交易委托量 性能时延 交易成功率 功能调用数 任务调用数
应用系统	客户端 应用服务 应用配置 应用制品 应用参数 ……	终端版本 用户IP 系统进程状态 JVM内存利用率 接口调用数 CDN质量
平台软件	应用平台 容器 数据库 中间件 操作系统 ……	CPU、内存、存储 响应时间 负载 SQL语句执行实践 缓冲区命中率 连接池数量
基础设施	环控 网络 存储 服务器 IOT 虚拟化	网络丢包率 网络链路延时 专线带宽 出口流量 存储空间 服务器设备状态
IT服务管理	变更 发布 实践 问题 服务台 ……	一线支持解决率 事件平均解决时间 座席接线量 配置数据 不准确配置数 变更失败数



数据建模 — 可视化编排

支持以可视化、可拖拽、可配置等简单、高效的方式对原始告警数据进行标准化处理，快速完成流水线式的告警数据处理和接入工作，为构建告警管理和告警智能分析场景提供可用的数据基础。

◆支持对于接入的告警数据进行数据的汇集、转换，实现数据格式标准化。



- 以图形化拖拽方式创建和配置流水线，保证任务编辑的易用性；
- 内置多种数据处理组件，开箱即用；
- 支持多种数据源和数据输出端，满足不同数据对接需求。
- 基于flink流数据处理框架，提供高并发的大数据处理能力；
- 支持任务监控，直观呈现任务运行状态。

指标基础管理-支持多源输入和输出和计算

支持多源数据接入

输入组件（10）

- Clickhouse源 ClickhouseStreamSource
- ES源 ElasticSearchSource
- 文件源 FileSource
- InfluxDB源 InfluxDBStreamSource
- JDBC源 JDBCSource
- Kafka源 KafkaSource
- MongoDB源 MongoDBStreamSource
- Mysql源 MysqlStreamSource
- Oracle源 OracleStreamSource
- Socket源 SocketSource

支持数十种数据处理算子

转换器组件（35）

- 统计 Aggregate
- 大小写转换 CharCase
- 类型转换 Cast
- 拼接字符串 Concat
- 反序列化 Deserialize
- 时间格式化 DateTimeFormat
- 时间解析 DateTimeParse
- 数据去重 DuplicateFilter
- 消息摘要 Digest
- 查询 Enrich
- 公式计算 Eval
- 字典展开 Enum
- 分流 Fork
- 过滤 Filter
- 数组展开 Flatten
- GeoIP转换 GeoIP
- 正则解析 Grok
- Javascript Javascript
- 连接 Join
- 合并多行 Multiline
- 移除字段 Prune
- 增加字段 Put
- 中文转拼音 Pinyin
- 替换字符串 Replace
- 重命名字段 Rename
- 分割字符串 Split
- 实时查询 Search
- 条件 Switch
- 序列化 Serialize
- 序列运算 SequenceCalculation
- 字符剔除 Strip
- 当前时间过滤 TimeRangeFilter
- 字符长度截断 Truncate
- 合流 Union

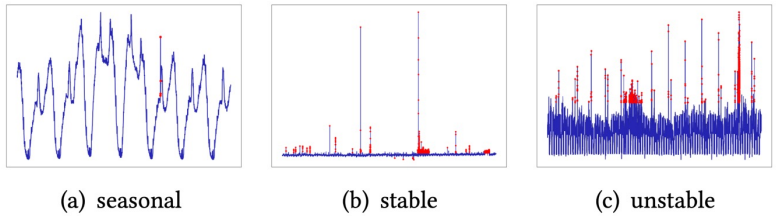
支持多源数据输出

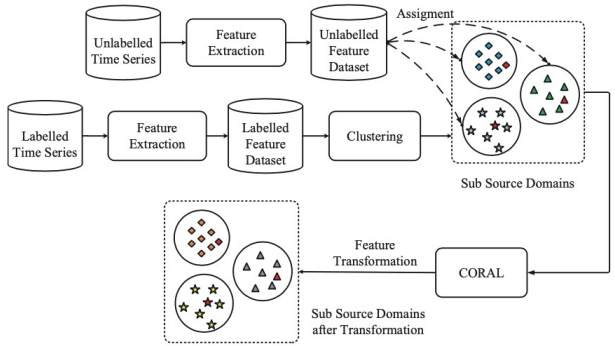
输出组件（10）

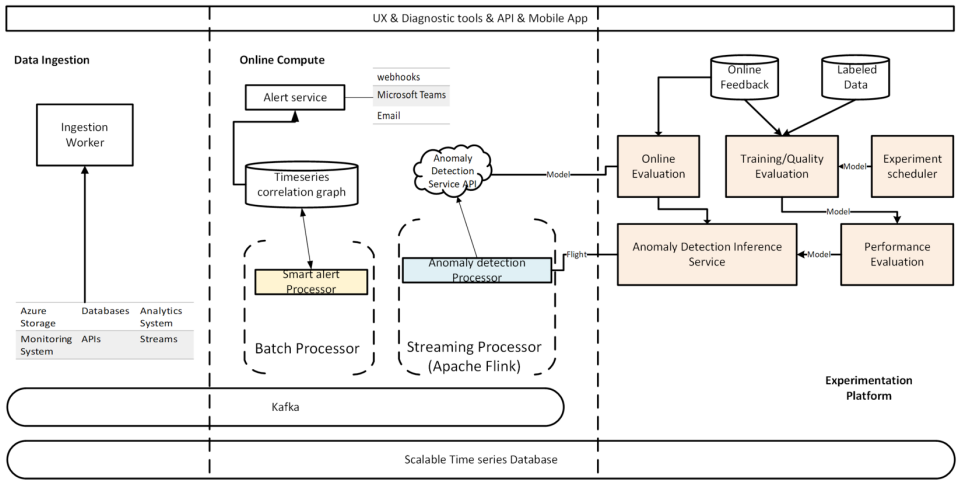
- Clickhouse输出 ClickhouseSink
- 丢弃输出 DumpSink
- ES输出 ElasticSearchSink
- 文件输出 FileSink
- Http输出 HttpSink
- InfluxDB输出 InfluxDBSink
- JDBC输出 JDBCSink
- Kafka输出 KafkaSink
- MongoDB输出 MongoDBSink
- Socket输出 SocketSink

AIOps应用：单指标异常检测

- Efficient KPI Anomaly Detection Through Transfer Learning for Large-Scale Web Services, JSAC 2022
- Robust KPI Anomaly Detection for Large-Scale Software Services with Partial Labels, ISSRE 2021
- Time-Series Anomaly Detection Service at Microsoft, KDD 2019
- Cross-dataset Time Series Anomaly Detection for Cloud Systems, ATC 2019







业务指标异常检测

- 专注于关键业务指标 – 衡量业务系统（**含交易码/功能号**）的健康状态：响应时间、成功率、响应率、交易量等, 检测**有助于及时发现异常提前揭示风险。**
- 业务指标异常检测 – **快速**准确地发现故障（**支持10秒级**），为后续的故障诊断和修复赢得宝贵的时间。

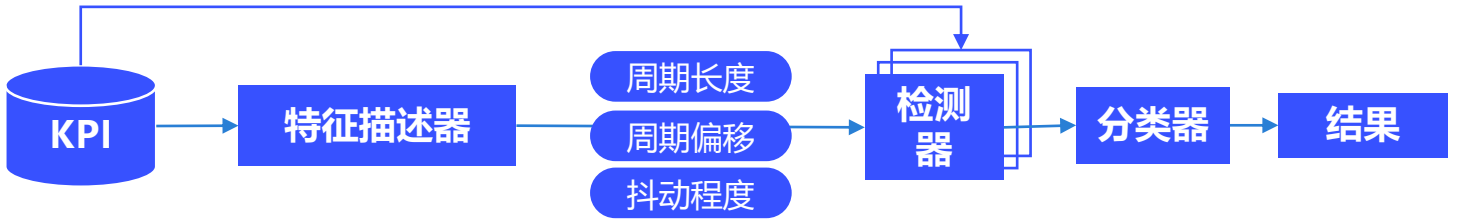
覆盖系统

- 核心系统、集中交易系统等
- 手机银行、各类网交系统等

数据对接

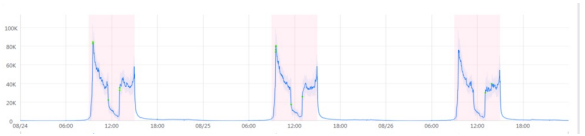
- 业务监控工具
- 日志管理工具

无监督 实时处理 海量多类型指标（几十万级）

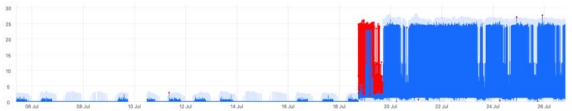


传统静态阈值监控	AIOps方式 智能检测
无法适应业务指标波动	自动适配各种KPI
阈值大小设置不准确	检测不同类型异常
阈值配置工作量大	无需人工调参
无法适应特殊日期波动	无需人工标注

✓ 针对券商交易时段特性进行适配，只训练和检测交易时段内的数据

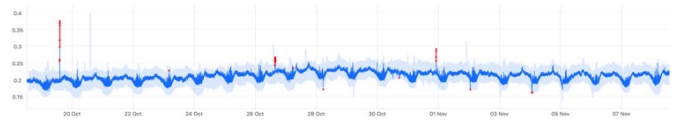


✓ 变更导致指标剧变（如版本上线）

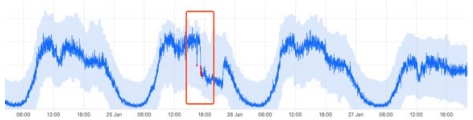


✓ 自动识别无规律性指标，并给出极限阈值

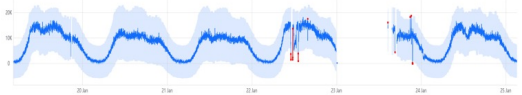
✓ 自适应整体趋势性变化



✓ 基带内的突变异常



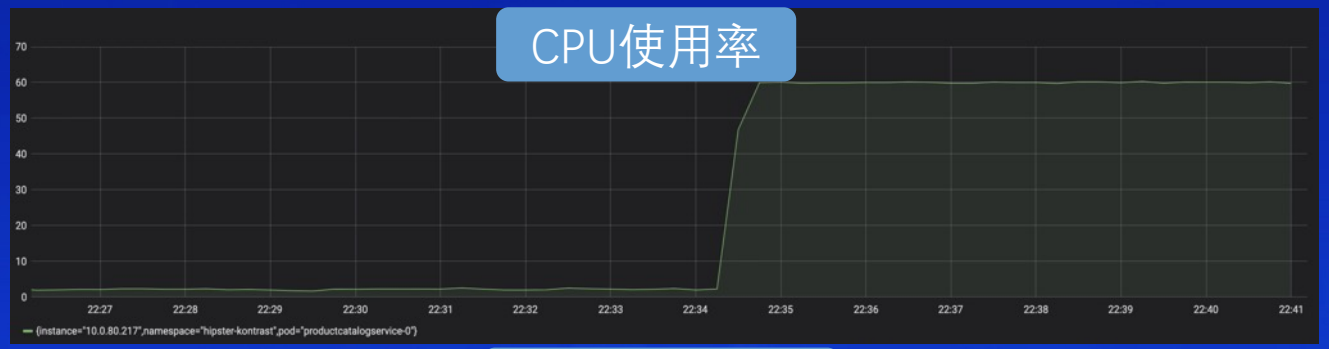
✓ 不受数据缺失、中断影响

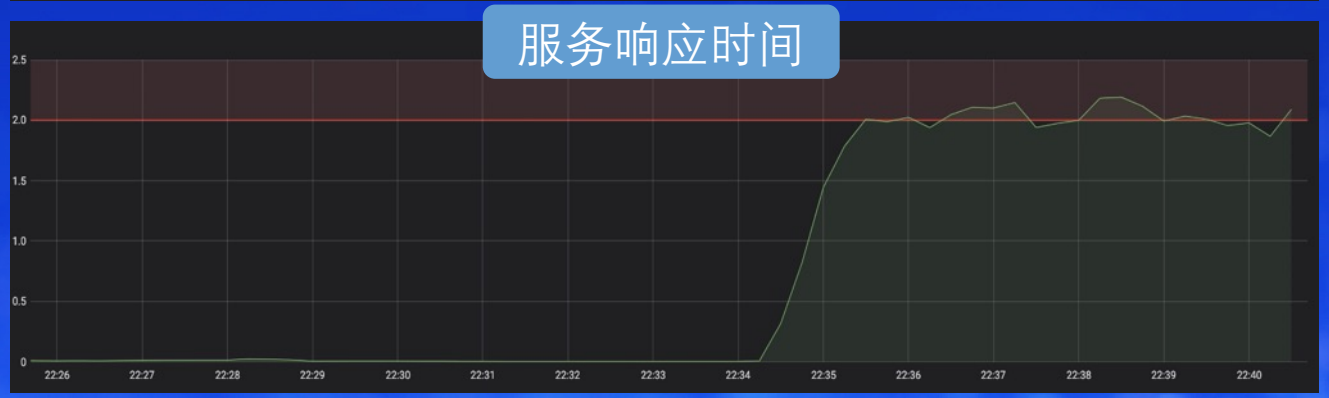


业务指标异常检测评测

故障背景：在22:34:00时刻，在productcatalogservice-0容器注入故障（非法程序），导致容器CPU使用率异常增加，影响productcategory服务响应时间从5ms涨到1s以上，影响用户体验

事件时间线

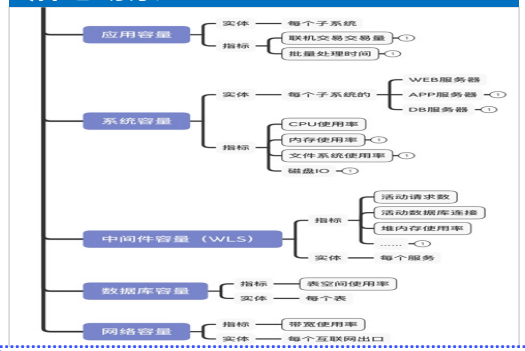




指标趋势预测

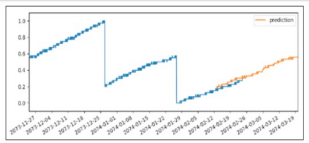
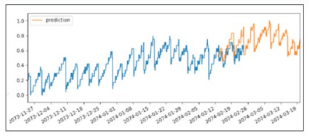
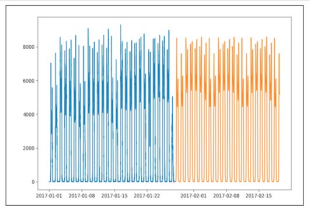
- 基于时序预训练模型，结合容量指标趋势预测任务进行微调训练，面向容量类指标超限预警的问题，预测其未来一段时间的变化走势，及时发现容量超限风险。
- 可用于应用交易量、资源池容量、数据库表空间、网络带宽等方面的趋势变化预警，提醒管理员及时采取措施，避免影响生产。

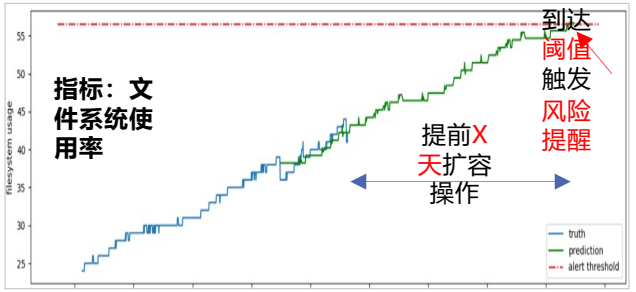
落地场景



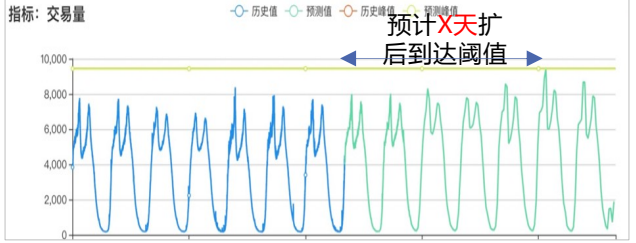
传统容量预警	AIOps方式容量预警
数据建模简单	考虑时间相关性
预测准确性低	捕捉复杂关系
无法适应变化环境	可迁移性强
缺乏个性化定制能力	个性化定制能力

落地效果

数据模式	图例	磁盘使用率	数据表空间	业务交易量	CPU使用率
稳定增长，偶尔清理		适用	适用		适用
波动增长，频繁清理		适用	适用		适用
稳定增长+小尖峰		适用	适用		适用
强周期性				适用	适用

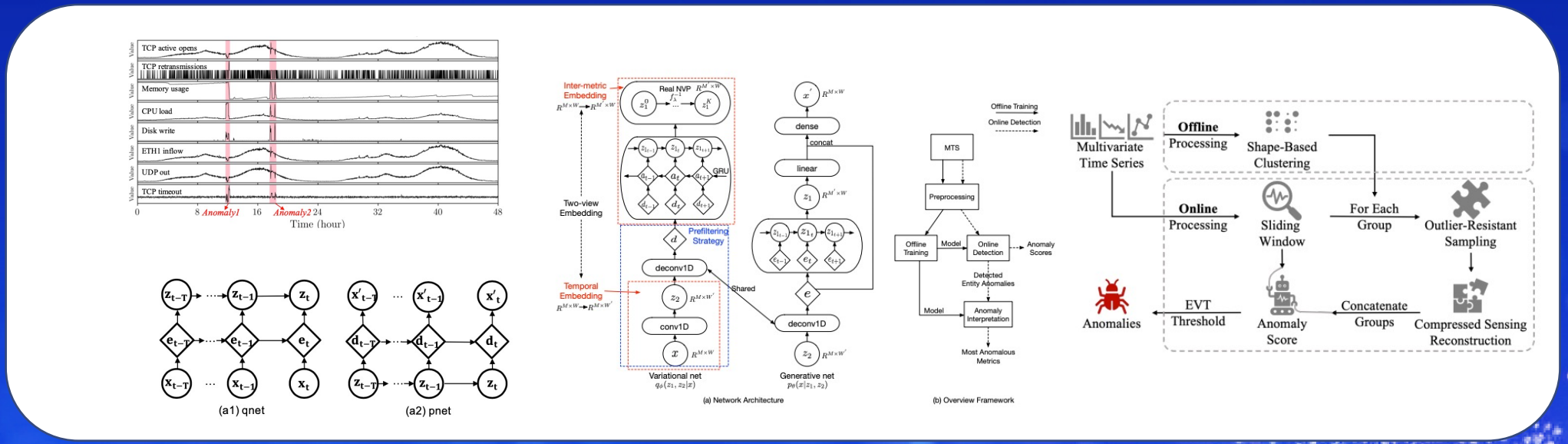


预测时间范围	值	预测峰值
2022-[redacted]:44:19 - 2022-[redacted]:44:19	120000.00 (TPM值)	9436.00



AIOps应用：多指标异常检测

- Jump-Starting Multivariate Time Series Anomaly Detection for Online Service Systems, ATC 2021
- Multivariate Time Series Anomaly Detection and Interpretation using Hierarchical Inter-Metric and Temporal Embedding, KDD 2021
- Detecting Outlier Machine Instances through Gaussian Mixture Variational Autoencoder with One Dimensional CNN, TC 2021
- Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network, KDD 2019



基于指标模式的故障检测

基础资源风险感知场景面向IT基础设施的日常巡检过程，融合运维专家的指标检查经验，针对基础资源对象运行过程中的指标异常模式进行特征分析，发现能够直观代表异常事件的某些指标波动模式，例如突增、突降、突刺、缓慢上升、缓慢下降等，实现对于基础监控数据的长周期、精细化风险识别，高效、准确的捕获海量IT基础组件运行过程中的反规律异常。

指标异常模式示例

指标类型	异常模式
文件系统使用率	缓慢上升
CPU使用率	突增、突增后保持、缓慢上升
内存使用率	突增、突增后保持、缓慢上升

传统异常检测	AIOps 预训练模型
依赖规则和阈值设置	自动化异常检测
人工排查繁琐	多维度特征分析
缺乏自适应性	自适应学习
缺乏迁移性	可迁移性

落地场景与效果

指标类型	操作系统			中间件			数据库		存储			
异常波形	CPU利用率	内存使用率	文件系统空间使用率	heap使用率	HOGGING独占线程数量	线程池排队请求数量	AAS_TOTAL	表空间使用率	Response time	IOPS	Throughput	IO size
突增	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
突降		✓					✓				✓	✓
突增然后保持	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
突降然后保持		✓					✓	✓			✓	✓
缓慢上升	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
缓慢下降						✓	✓	✓			✓	✓
向上突刺	✓				✓	✓	✓		✓	✓	✓	✓
向下突刺							✓				✓	✓
凸型	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓
凹型							✓				✓	✓
多个向上突刺	✓		✓	✓		✓	✓		✓	✓	✓	✓
多个向下突刺							✓				✓	✓
剧烈波动						✓	✓				✓	✓

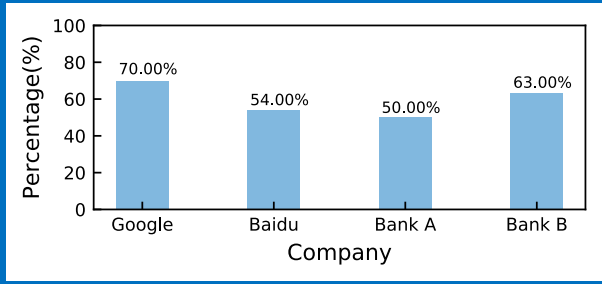
变更风险感知

系统变更在软件开发和系统维护过程中是十分频繁和不可避免的，而频繁的变更通常会给运维工作带来不可预知的风险，影响业务系统稳定运行。而目前对于变更实施后的检查多以人工验证方式完成，存在耗时耗力、脚本配置困难、容易出现漏查错查等问题。

• 变更后问题频发

变更在软件开发和系统维护过程中是频繁且不可避免的，版本投产极易引入故障

- 开发新的功能
- 修复软件bug
- 更改系统配置
- 环境适配
- 提升系统性能



• 海量数据人工验证效率低

由于各种影响因素的存在，人工验证变更结果效率低，容易导致一系列问题

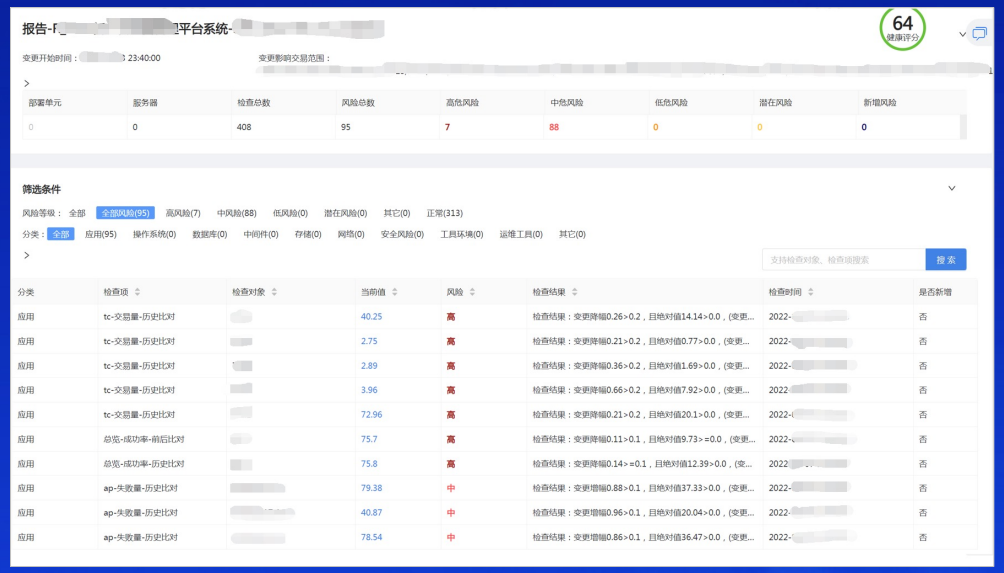
- 线上环境的复杂性
- 系统指标的种类和数量众多
- 日志数据可读性不高
- 验证标准不统一
- 依赖管理员专业素质

指标数量 × 检查点 × 单位时间 = 巨大耗时

变更风险感知案例

案例描述：某应用系统夜间变更，风险感知平台在变更后10分钟启动变更风险检查，针对该系统和相关交易码的业务指标在变更前后的变化进行分析，发现变更后该系统业务指标与多个易码业务指标均存在明显异常，生成多项高危风险，提醒客户关注变更异常问题。管理员和项目组确认问题后，及时进行了版本回退。后续排查发现，该次变更中某服务参数配置遗漏导致渠道系统无法验证通过，影响了业务正常办理。

风险检查报告



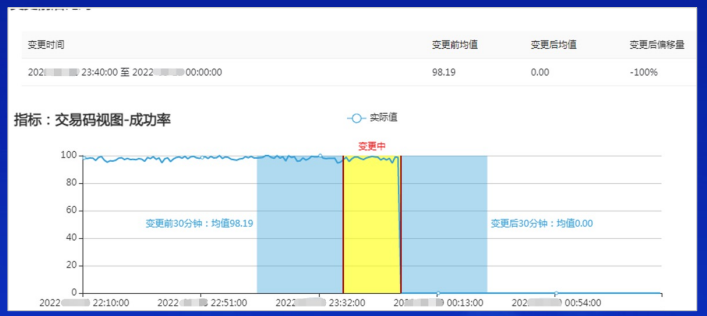
触发检查后，**共计发现系统级风险4项、交易码风险7项、主机风险72项**

系统级

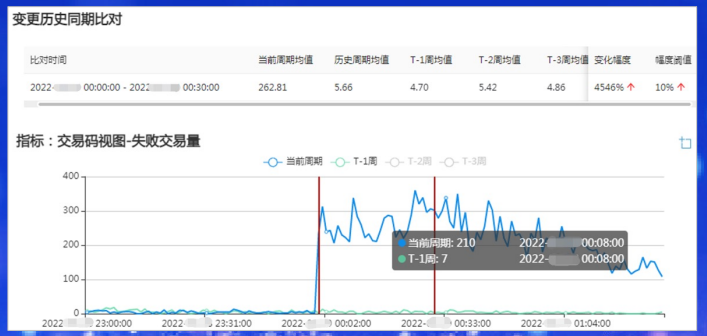
- 系统成功率相比变更前明显下降

- 失败量相比前几周明显增多

交易码级



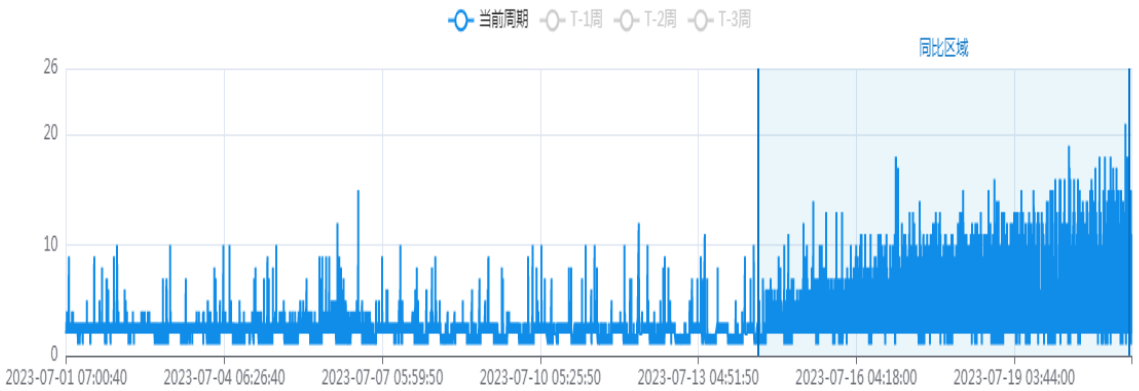
- 成功率降为0



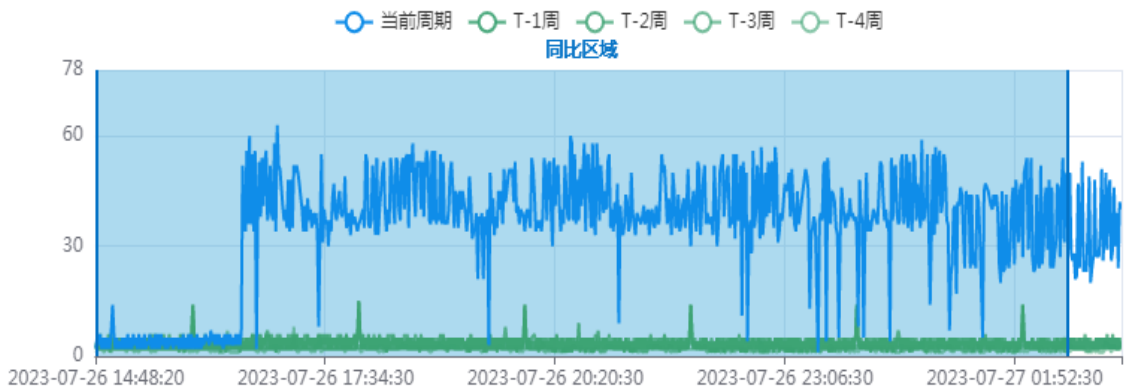
- 失败量相比前几周大幅增多

指标模式故障检测案例

经过在某城商行超过一个月的生产环境在线测试，接入60+套系统的业务指标、数千台主机的性能指标，平均每天告警约10条（相同、重复的告警进行压缩）。



系统变更后，CPU缓慢上升波形



CPU指标：非尖刺上升波形

日志分析与异常检测

- Log-based Anomaly Detection with Deep Learning:How Far Are We? ICSE 2022
- MoniLog: An Automated Log-Based AnomalyDetection System for Cloud ComputingInfrastructures, ICDE 2021
- Log-based Anomaly Detection Without Log Parsing, ASE 2021
- A Survey on Automated Log Analysis for Reliability Engineering, CSUR 2021
- LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs, IJCAI 2018
- DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning, CSS 2017

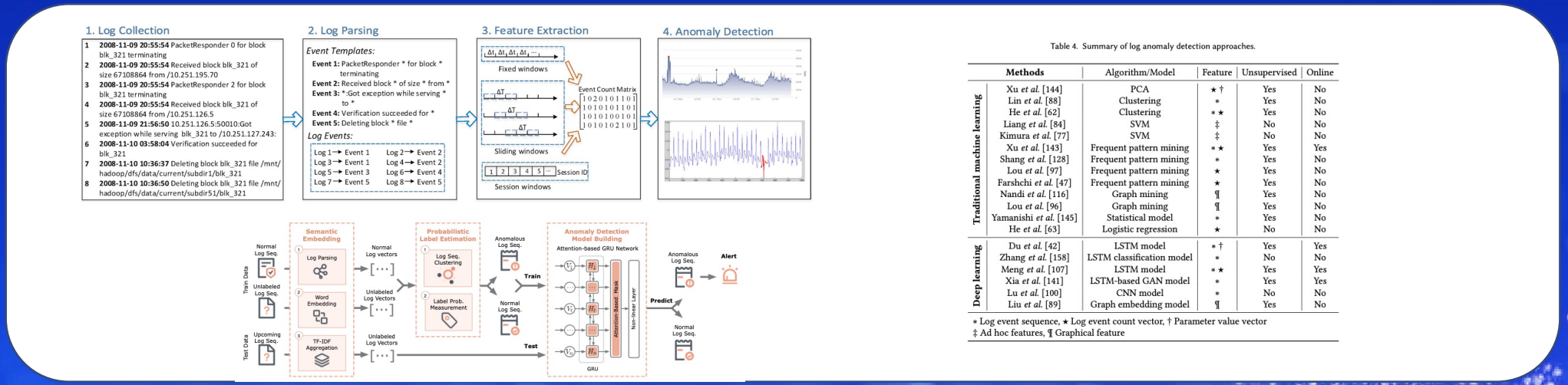


Table 4. Summary of log anomaly detection approaches.

	Methods	Algorithm/Model	Feature	Unsupervised	Online
Traditional machine learning	Xu *et al.* [144]	PCA	⋆ †	Yes	No
	Lin *et al.* [88]	Clustering	∗	Yes	No
	He *et al.* [62]	Clustering	∗ ⋆	Yes	No
	Liang *et al.* [84]	SVM	‡	No	No
	Kimura *et al.* [77]	SVM	‡	No	No
	Xu *et al.* [143]	Frequent pattern mining	∗ ⋆	Yes	Yes
	Shang *et al.* [128]	Frequent pattern mining	∗	Yes	No
	Lou *et al.* [97]	Frequent pattern mining	⋆	Yes	No
	Farshchi *et al.* [47]	Frequent pattern mining	⋆	Yes	No
	Nandi *et al.* [116]	Graph mining	¶	Yes	No
	Lou *et al.* [96]	Graph mining	¶	Yes	No
	Yamanishi *et al.* [145]	Statistical model	∗	Yes	No
	He *et al.* [63]	Logistic regression	⋆	No	No
Deep learning	Du *et al.* [42]	LSTM model	∗ †	Yes	Yes
	Zhang *et al.* [158]	LSTM classification model	∗	No	No
	Meng *et al.* [107]	LSTM model	∗ ⋆	Yes	Yes
	Xia *et al.* [141]	LSTM-based GAN model	∗	Yes	Yes
	Lu *et al.* [100]	CNN model	∗	No	No
	Liu *et al.* [89]	Graph embedding model	¶	Yes	No

∗ Log event sequence, ⋆ Log event count vector, † Parameter value vector
‡ Ad hoc features, ¶ Graphical feature

日志异常检测背景

传统日志检测方案

关键词/正则计数

固定阈值检测

- 完全依赖日志专家事先配置，工作量大
- 配置不全面（难以事先要枚举全）
- 更新开销大（无法应对日志变化）
- 检测方法简单，适应力弱

管理员想要的日志检测

- 利用数据分析、机器学习技术，**自动发现多种日志的潜在问题**，解决传统手段不足
- **新鲜事物，循序渐进：**开始把最有信心、管理员能理解的告警发出，减少误报率，提高大家信心
- **提供便捷反馈功能，持续优化：**让管理员可以通过简单操作，就将潜在问题逐步纳入正式告警
- **场景非常关键，领域知识的结合：**哪些日志用得更频繁、价值高、对发现问题和定位问题帮助大

- UNIX日志
- Linux日志
- Windows日志
- …

- Oracle日志
- DB2日志
- Informix日志
- SQLServer日志
- MySQL日志
- …

- MQ日志
- Tuxedo日志
- Weblogic日志
- Tomcat日志
- Apache日志
- …

- 电力日志
- …

- 交换机日志
- 路由器日志
- 防火墙日志
- F5日志
- 存储日志
- 存储交换机日志
- …

- 应用日志

```
  INFO [WebContainer : 15] - queryForList:IDA_TEMPLATE.LISTDATA_MOST_CLICK↓
  INFO [WebContainer : 8] - queryForList:IDA_NOTICE.LISTDATA_BY_USER↓
com.teradata.ida.auth.dto.SysUserVO@2c3d3e1d↓
[8/10/18 8:29:31:581 CST] 00000032 SystemOut     O  INFO [WebContainer : 1] - queryForList:IDA_TEMPLATE_AUTH.findTemplateByRoleId↓
 DEBUG [WebContainer : 7] - 2018-08-10 08:29:32 DEBUG |CsParamSetAction|showAtomsBygid|Start||start=0|limit=25|page=1|fromIndex=0|toIndex=25|kindid=1|↓
  INFO [WebContainer : 7] - queryForList:SEG_BIZ_ATOM_DEF.findAtomByRoleAndShowArea↓
```

```
EXPLANATION:↓
Channel program 'CS_EDI_S' ended abnormally.↓
ACTION:↓
Look at previous error messages for channel program 'CS_EDI_S' in the error↓
files to determine the cause of the failure.↓
-----  amqrmrsa.c : 487 --------------------------------------------------------↓
08/07/2018 10:14:54 AM - Process(29670.329016) User(mqm) Program(amqrmppa)↓
AMQ9513: Maximum number of channels reached.↓
```

日志异常检测流程

原始日志

模板生成

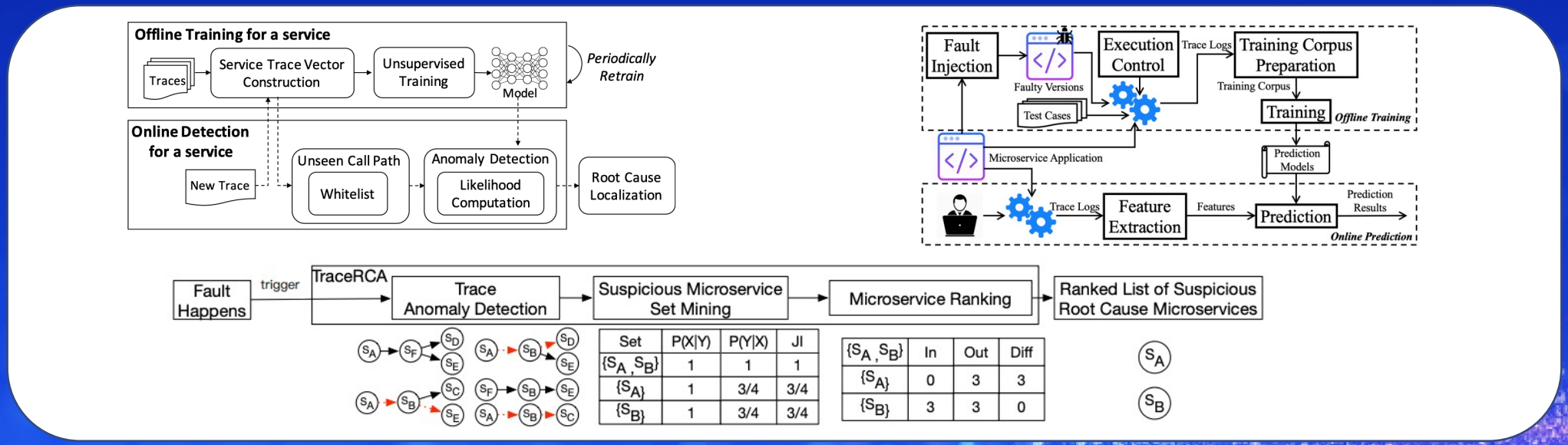
触发告警

17日18:20起，某业务系统【连续登陆失败次数超限】模板数量突增，产生多个日志告警

管理员查看告警详情及原始日志后排查发现原因为某次变更所致，及时进行回退，防止了故障进一步恶化。

AIOps应用： 调用链分析与异常检测

- Unsupervised Anomaly Detection on Microservice Tracesthrough Graph VAE, WWW 2023
- TraceCRL: Contrastive Representation Learning for MicroserviceTrace Analysis, FSE 2022
- Practical Root Cause Localization for Microservice Systems via Trace Analysis, IWQoS 2021
- Unsupervised Detection of Microservice Trace Anomalies through Service-Level Deep Bayesian Networks, ISSRE 2020
- Latent Error Prediction and Fault Localization for Microservice Applications by Learning from System Trace Logs, ESEC/FSE 2019

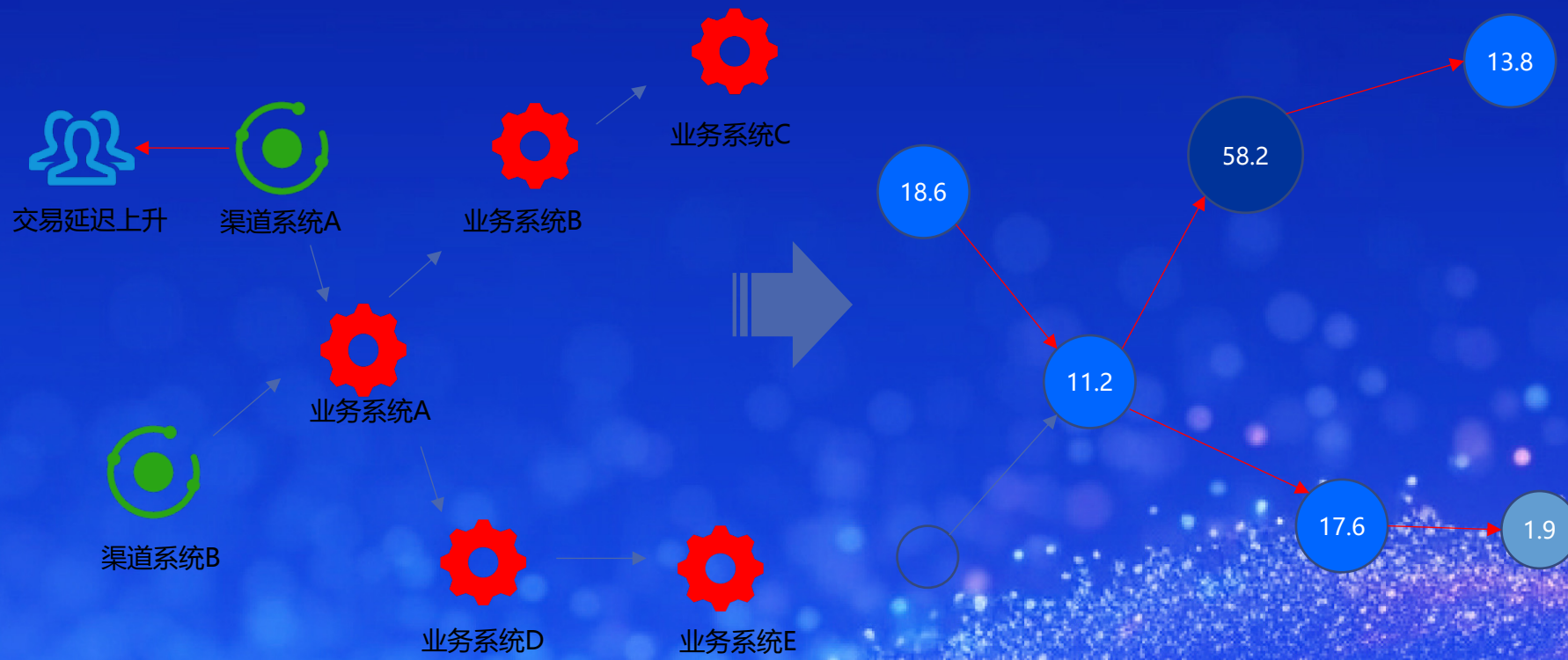


调用链根源系统定位

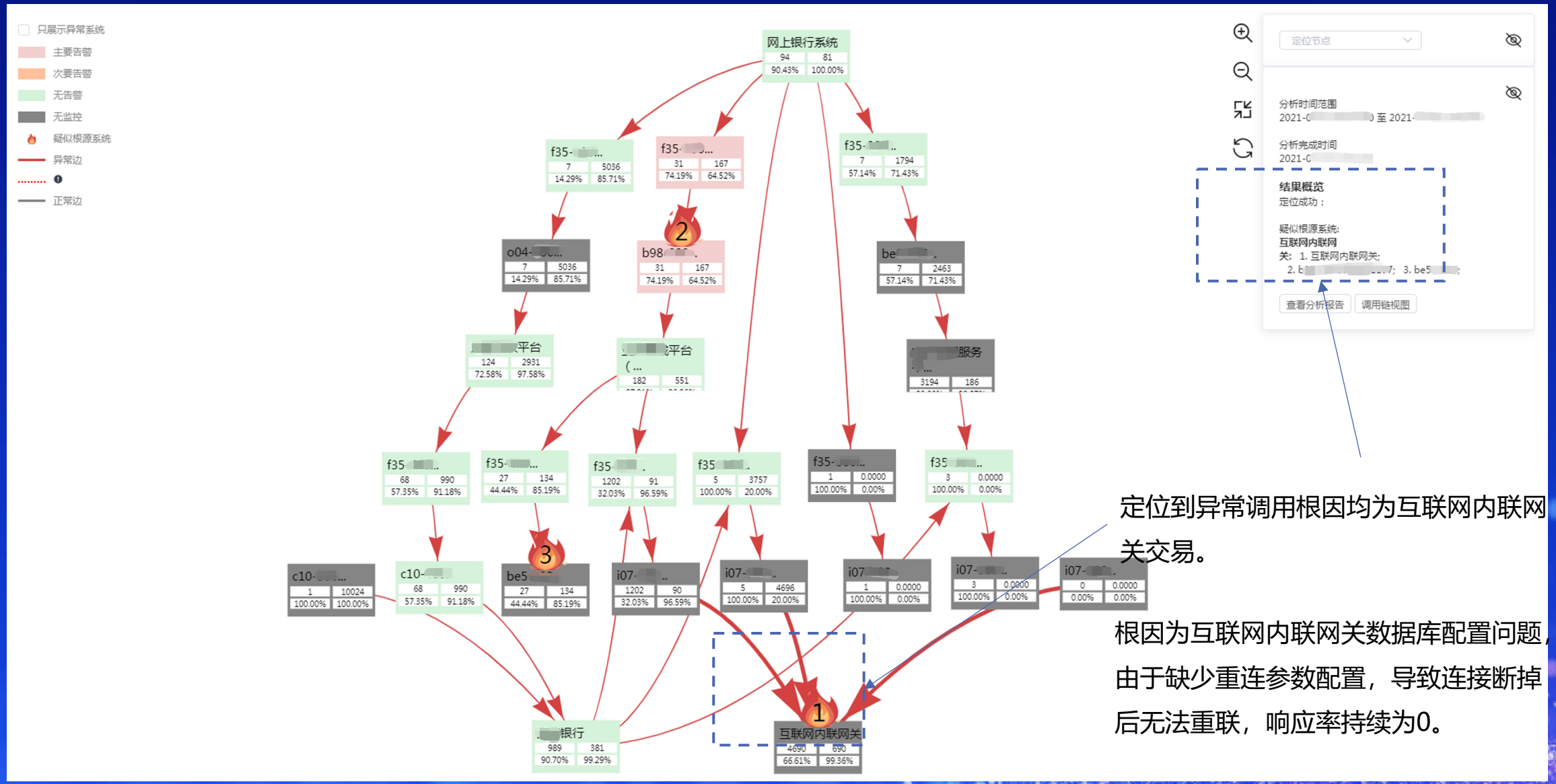
在大型系统中，为了完成一个确定的任务，需要多个系统或服务之间的相互调用。因此故障发生时，许多系统或服务可能会同时产生告警，对于多层次的系统架构导致故障定位愈发困难，如何**在大面积故障中**找到存在于多系统架构内的**故障产生的根本原因**？调用链根因定位系统利用系统或服务间的调用链数据，定位故障的可能根源，解决运维人员需要逐个排查的痛点。

构建骨架图	确定传播方向	定位排序
根据节点间调用边的异常情况构建骨架图	根据报警类型和节点间调用关系确定直接故障传播关系及方向	根据故障传播图拓扑结构及权值信息计算节点的根因概率并排序

- 自动产生系统关系图，无需人工配置
- <1分钟定为根源系统



调用链根源系统定位案例

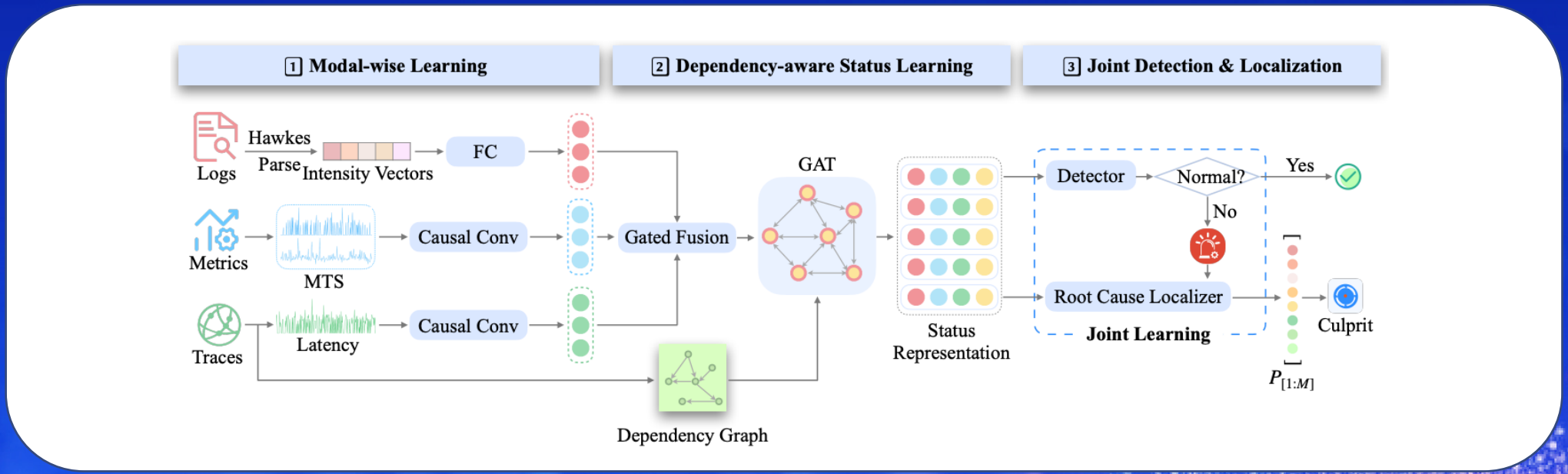


定位到异常调用根因均为互联网内联网关交易。

根因为互联网内联网关数据库配置问题，由于缺少重连参数配置，导致连接断掉后无法重联，响应率持续为0。

AIOps应用： 根因定位

- Robust Failure Diagnosis of Microservice System through Multimodal Data, TSE 2023
- Eadro: An End-to-End Troubleshooting Frameworkfor Microservices on Multi-source Data, ICSE 2023
- Actionable and Interpretable Fault Localizationfor Recurring Failures in Online Service Systems, ECSE 2022
- MicroHECL: High-Efficient Root CauseLocalization in Large-Scale Microservice Systems, ICSE 2021
- MicroRank: End-to-End Latency Issue Localization withExtended Spectrum Analysis in Microservice Environments, WWW 2021
- AutoMAP: Diagnose Your Microservice-based Web ApplicationsAutomatically, WWW 2020



业务明细多维定位

当检测到某个交易型指标出现异常的时候，通过多维定位可以从交易明细中**快速准确定位出哪个交易维度**导致了异常。

某个指标平均响应时间上升

多维交易明细

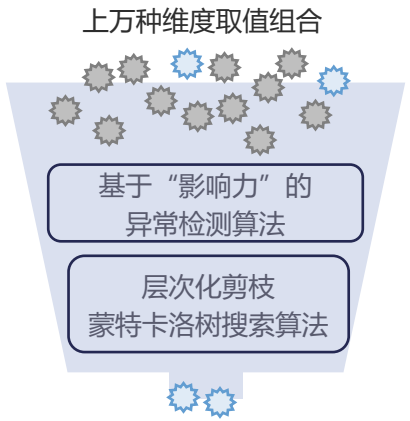
- 某个网络的问题?
- 某个客户端版本
- 新上线的版本bug?
- 某个城市或者ISP网络故障?

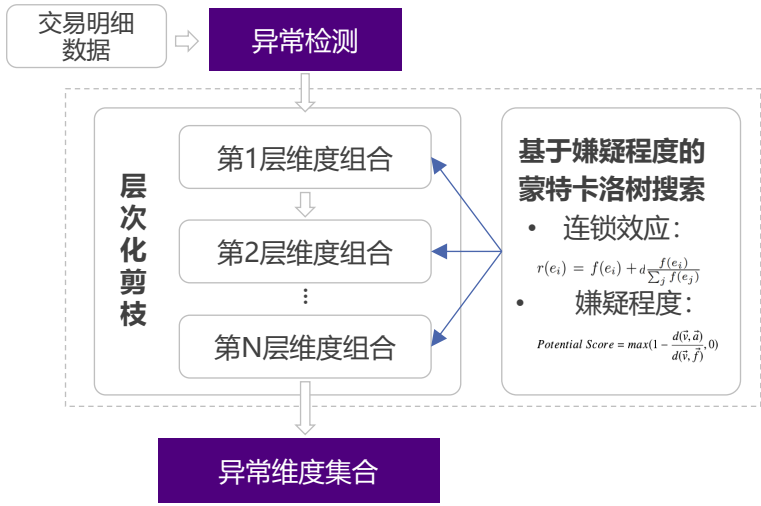
维度数据

省份、城市、网段、IP、ISP、客户端版本等

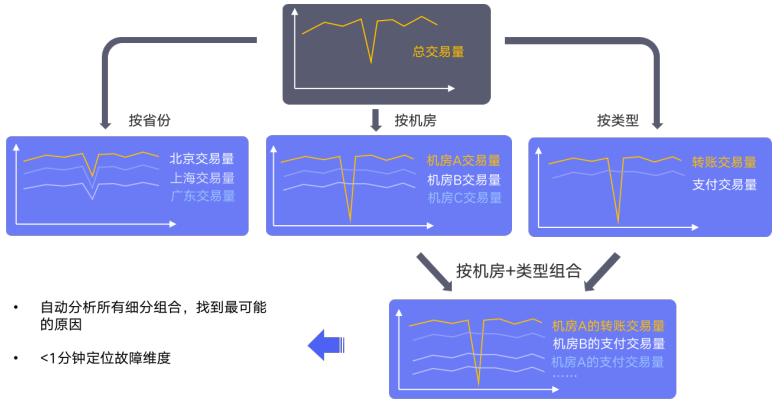
数据对接

业务监控工具、日志管理工具等





传统业务明细定位	AIOps业务明细多维定位
手工写大量查询语句，枚举所有维度组合，进行排障	自动遍历所有维度组合进行进行智能剪枝，无须人工干预
只能参考当前维度组合的绝对值，无法感知异常情况	准确地参考历史数据对所有维度组合进行异常评估



机器指标定位

机器指标定位场景有助于快速准确进行故障定界，**定位到是由底层哪个基础组件引发的问题**，从而快速进行止损和修复。如果不是因为基础组件引起的问题，通过定位结果可以首先排除IT基础设施层面的可能性。

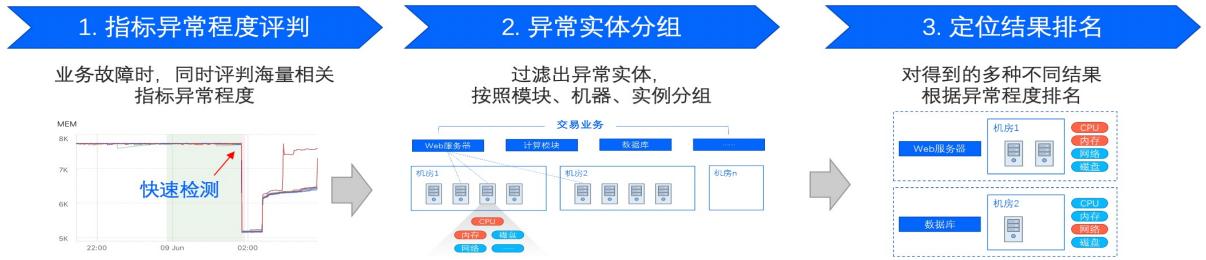
覆盖对象

- 主机、数据库、中间件、网络设备等

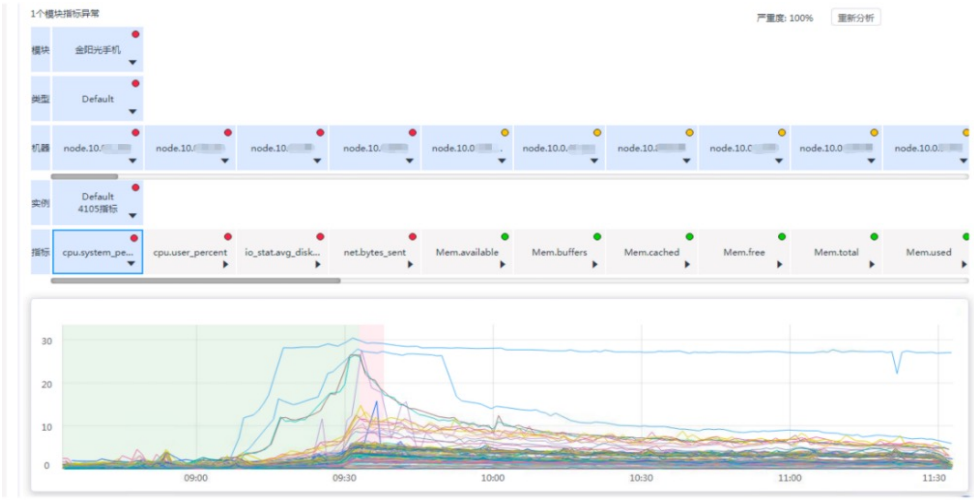
数据对接

- 基础监控工具
- 数据库监控工具
- 网络监控工具等

业务出现问题 → 依赖大量模块 → 多组件、多操作系统 → 海量对象和指标 哪些是问题所在?



传统基础设施定位	AIOps机器指标定位
各基础组件管理员逐一排查监控视图	智能故障定界，快速缩小问题排查范围
手工逐个检查基础设施监控对象及其指标	自动对海量指标做批量扫描，找出可疑对象和指标
基于经验对基础组件异常程度排序不够准确	基于算法对各组件指标异常程度进行准确排序



机器指标定位案例

传统固定阈值

- 未发现某查询功能号的指标异常
- 未发现该系统下的主机层面异常

智能运维平台

- 2020年X月X日发现网交系统某查询功能号响应时间异常升高
- 迅速定位到两台主机指标存在大幅波动

异常描述：

- 在交易时段内，网交系统某查询类功能号出现响应缓慢的情况，而历史同期却没有响应时间增加的问题

故障原因及影响：

- 网交系统所在主机集群的两台主机的CPU和IO指标在故障同一时间存在大幅异常波动，导致网交系统整体平均响应时间增加

故障处理：

- 更换这两台主机后未再复现上述问题

案例价值：

- 通过业务指标异常检测场景发现传统监控工具固定阈值未发现的异常事件，并在众多基础组件中准确定位出两台主机的问题，为管理员提供关键的故障定界线索，及时恢复系统正常运行状态

运维大模型OpsEval在线评测基准
http://opseval.cstcloud.cn

17350题

客观题 17000题
主观题 350道

中英双语
8中任务场景
3个能力分层

14单位

必示科技
国泰君安
华为
基石数据
联想集团
南开大学
日志易
上海银行
中国科学院
清华大学
腾讯
中兴通信
中亦科技
Zabbix中国宏时数据

5行业

互联网
通信
云计算
金融
证券

8场景

有线网络运维
5G网络通信
数据库运维
混合云建设和运维
金融IT运维
金融信创运维
证券信息系统
日志分析能力

* 排名不分先后，拼音序

OpsEval 离线评测基准 & 运维大语言模型

2023年12月16日

Model	Zero-shot				3-shot			
	Naive	SC	CoT	CoT+SC	Naive	SC	CoT	CoT+SC
GPT-4	/				/	/	**88.70**	/
Yi-34B-Chat	57.75				67.78	68.37	78.80	**80.06**
Qwen-72B-Chat	70.41				70.32	70.32	70.13	70.22
GPT-3.5-turbo	66.60	66.80	69.60	72.00	68.30	68.30	70.90	**72.50**
LLaMA-2-70B	55.80				55.00	56.20	66.80	**67.20**
DevOps-Model-14B-Chat	30.69				**63.85**	61.96	41.15	44.01
Qwen-14B-Chat	43.22				**62.60**	59.70	50.58	55.88
LLaMA-2-13B	41.80	46.50	53.10	58.70	53.30	53.00	56.80	**61.00**
LLaMA-2-7B	39.50	40.00	45.40	49.50	48.20	46.80	52.00	**55.20**
Qwen-7B-Chat	45.90				**52.10**	51.00	48.30	49.80
Baichuan2-13B-Chat	37.90				**51.90**	51.60	44.50	47.45
Mistral-7B	29.27				**47.22**	**47.22**	45.58	45.58
ChatGLM3-6B	42.66	42.66	44.83	**44.96**	40.78	40.78	43.58	43.66

第一梯队

第二梯队

第三梯队

2024年1月11日

Model	Zero-shot				3-shot			
	Naive	SC	CoT	CoT+SC	Naive	SC	CoT	CoT+SC
GPT-4	/				/	/	**88.70**	/
Yi-34B-Chat	57.75				67.78	68.37	78.80	**80.06**
Qwen-72B-Chat	70.41	70.50	72.38	**72.56**	70.32	70.32	70.13	70.22
GPT-3.5-turbo	66.60				68.30	68.30	70.90	**72.50**
ERNIE-Bot-4.0	61.15				60.00	60.00	70.00	**70.00**
LLaMA-2-70B	55.80				55.00	56.20	66.80	**67.20**
DevOps-Model-14B-Chat	30.69	30.59	55.77	63.63	**63.85**	61.96	41.15	44.01
Qwen-14B-Chat	43.22	47.81	56.63	59.40	**62.60**	59.70	50.58	55.88
LLaMA-2-13B	41.80				53.30	53.00	56.80	**61.00**
LLaMA-2-7B	39.50				48.20	46.80	52.00	**55.20**
Qwen-7B-Chat	45.90				**52.10**	51.00	48.30	49.80
Baichuan2-13B-Chat	37.90	38.30	42.70	46.60	**51.90**	51.60	44.50	47.45
Mistral-7B	29.27	29.27	46.30	46.30	**47.22**	**47.22**	45.58	45.58

第一梯队

第二梯队

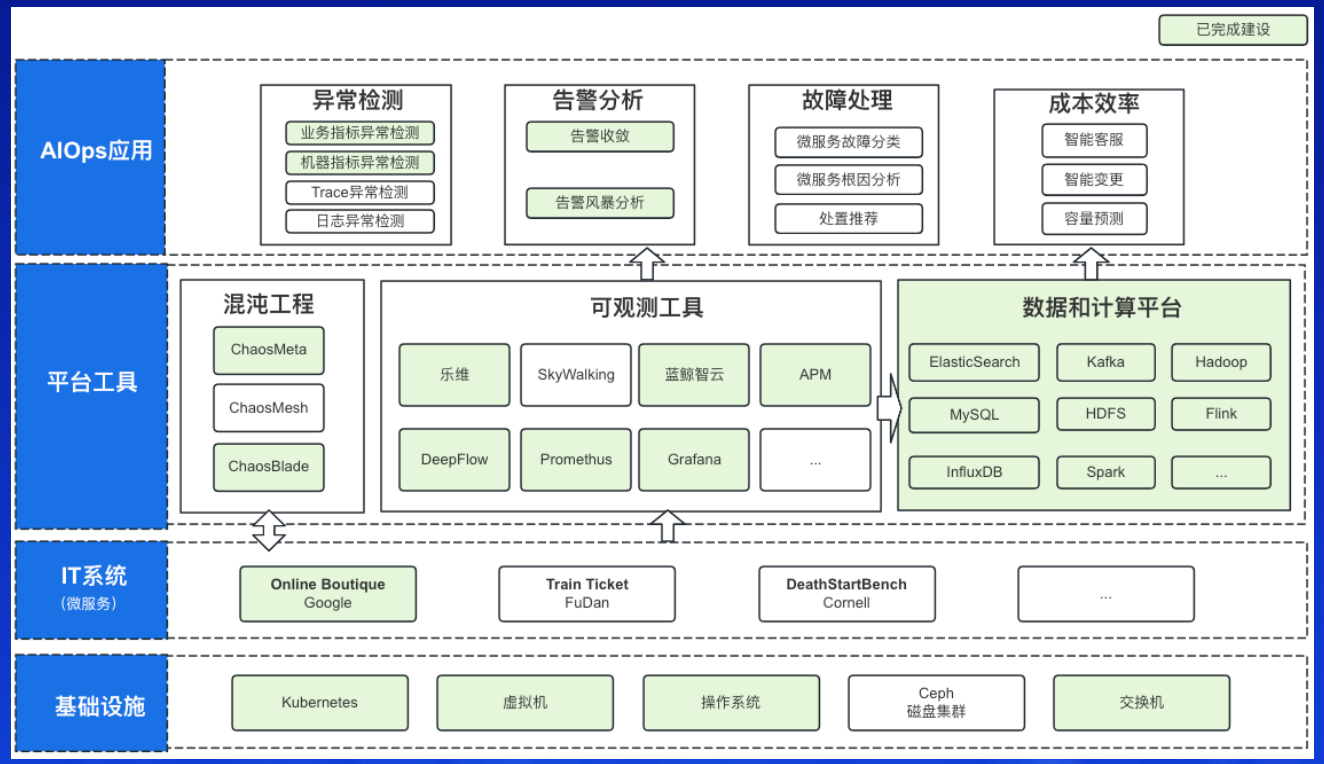
第三梯队

- 模型新增：文心一言、混元、某AIOps模型（未公开），模型 X 评测基准
- RAG评估数据和方法（进行中）
- 运维大语言模型OpsGLM（智谱AI参与OpenAIOps，基于ChatGLM训练迭代）

总结

智能运维产、学、研平台

真实系统、真实数据、真实应用



个人成员：

1. 获取到真实IT系统运维数据，包括指标、日志、调用链等，可用于学术研究、产品测试等场景

专家成员：

1. 作为在线评测基准的建设者，可以发布自己的系统，供社区用户使用
   - IT系统
   - 混沌工程工具
   - 可观测性工具
   - AIOps应用
2. 发布运维场景和评测标准，吸引社区的人贡献解决方案
   - 异常检测
   - 根因定位
   - 告警分析
   - ...
3. 参与实时打榜，在社区公布自己算法、系统排名

在线评测基准后续规划

社区专家成员

社区个人成员

L1层 运维大语言模型

人机协同群聊 ChatOps

L0层 底座通用大语言模型

离线评测基准样题库

AIOps Live Benchmark

微服务	流量模拟智能体	故障注入智能体
可观测性智能体	异常检测智能体	故障定位智能体
…	…	…

2024届CCF 国际AIOps挑战赛

「基于检索增强的运维知识问答挑战赛」

比赛数据提供：ZTE中兴

首次采用大模型检索增强（RAG）技术，基于5G领域运维技术文档，探索如何结合领域私有技术文档进行高效私域知识问答。揭示在通用大语言模型基座下，垂直领域知识问答面临的领域知识缺失，公私域知识冲突，多模态图表并存等一系列挑战。

挑战赛官网：https://competition.aiops-challenge.com/home/competition

报名方式

点击参加比赛按钮

报名网页二维码

魔搭资源问卷：https://wj.qq.com/s2/14445887/d084/
智谱资源问卷：https://wj.qq.com/s2/14630018/lqve/

组队完成填写**魔搭资源问卷**，如果参加赛道二，还需要填写**智谱资源问卷**。

CCF AIOps挑战赛社区全面升级为 CCF OpenAIOps社区

CCF 国际AIOps挑战赛

OpenAIOps

CCF OpenAIOps社区是一个AIOps开源社区及创新平台， 由中国计算机学会(CCF)、清华大学、南开大学、中科院、国防科大、必示科技等单位共同发起，致力于通过开放的社区合作与群体智慧协同创新，构建AIOps开源创新技术及软件，推动AIOps生态繁荣发展。

汇聚AIOps数据、语料、知识、大模型、算法、源代码、离线评测基准及榜单、在线评测基准及榜单、Demo、智能体、推理算力平台、文档、讨论区、竞赛、黑客马拉松、沙龙、研讨会、专家、问答应用、问答API

- 如果你主要关注人工智能和机器学习，尤其是在预训练模型和这些领域的专业社区方面，Hugging Face是一个比GitHub更好的选择
- 如果你主要关注AIOps, 那么OpenAIOps社区将是比Hugging Face 和 GitHub更好的选择

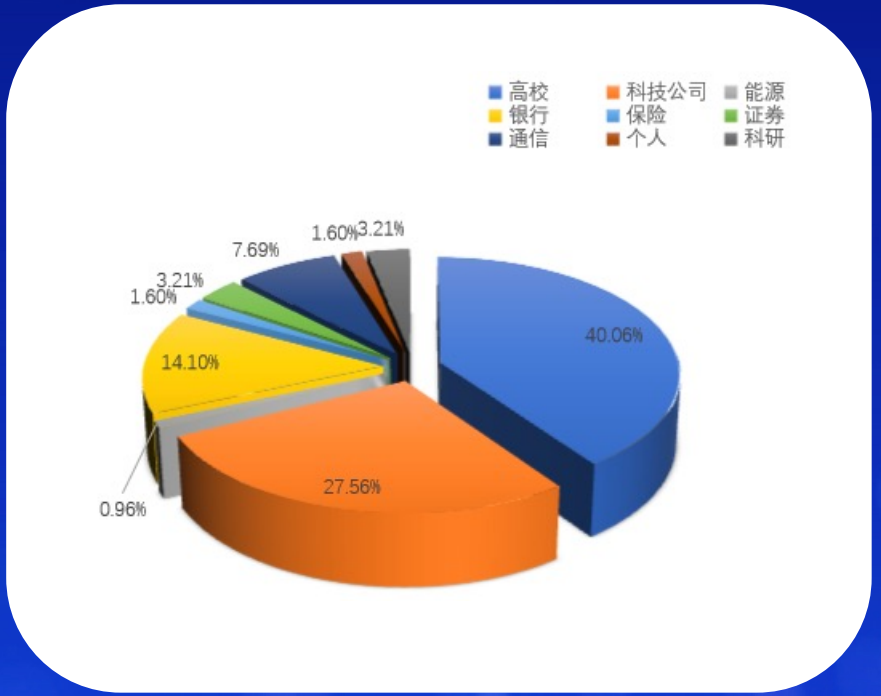
智能运维领域最大的垂直社区

AIOps领域最大的垂直社区之一

- 8个官方微信群，共计3200余人
- 持续交流AIOps观点、技术趋势、痛点和方案

社区活跃账号，分享硬核干货

- 微信公众号关注量20000+
- 发表文章67篇，优质内容平均阅读量2-3K，阅读峰值8K+
- 过去六年活动覆盖人数15W+



社区辐射圈层广泛，涵盖产学研用各界行业代表

2024年第一批工作组

- 活动竞赛专家工作组
  - 高频不定期线上研讨
  - 线下小型沙龙
  - 线下大型活动
  - AIOps挑战赛

  →
  - 活动策划、筹办
  - 场地、赞助
  - 挑战赛：
    - 提供赛题、数据
    - 成为竞赛TPC，参与竞赛

- 运维大模型评测专家组（72人）
- 运维大模型训练专家组（41人）

  →
  - 参与离线评测基准工作
    - 华为、中兴、腾讯、智谱AI等14家企业已参与

- 在线评测基准专家组（59人）

  →
  - 参与在线评测基准的建设和维护
  - 发布新的问题和评测标准

- 线上资源专家工作组

  →
  - 课程、视频、论坛、综述文章等

OpenAIOps社区网站（ https://www.aiops.cn/ ）

总计访客**7400+**人次，总点击**46000+**次

CCF OpenAIOps 社区参与方式

个人成员

联系“OpenAIOps社区助手”微信号加入“OpenAIOps社区群”

关注“OpenAIOps”公众号

访问 http://www.aiops.cn

收益：消费社区资源

责任：积极对社区提出反馈、积极参与社区活动

专家成员

（单位或个人身份均可）

责任：为社区贡献至少一项资源，或参与至少一个工作组

收益：
- **贡献度较高的成员将获得CCF致谢证书、活动优先参会发言权、推理算力消费费用减免**
- **资源优先试用权**

已参与社区的专家成员：

华为、中兴、腾讯、蚂蚁、智谱AI、信通院、中国电信、新华三、联想集团、浦发银行、国泰君安、上海银行、广发证券、南天、中亦科技、广通优云、日志易、乐维、Zabbix中国宏时数据、基石数据、亿阳信通、云杉网络等

科技生态圈峰会 + 深度研习

——1000 + 技术团队的共同选择

KEYLINK ing

K+峰会

上海站
K+全球软件研发行业创新峰会
时间：2024.06.21-22

敦煌站
K+思考周®研习社
时间：2024.10.17-19

香港站
K+思考周®研习社
时间：2024.11.10-12

K+峰会详情

AiDD峰会

上海站
AI+研发数字峰会
时间：2024.05.17-18

北京站
AI+研发数字峰会
时间：2024.08.16-17

深圳站
AI+研发数字峰会
时间：2024.11.08-09

AiDD峰会详情

AiDD

THANKS