GOPS 2021
Shenzhen

GOPS 全球运维大会

2021 -XOPS 风向标

深圳站

中国·深圳

指导单位：

主办单位：

时间：2021年5月21日-22日

GOPS 2021
shenzhen

基于智能运维算法的异常检测应用

王厦

王厦

综合运维架构师

资深专家，自动化智能运维工具平台建设项目负责人，负责监控、自动化、运维大数据分析、CMDB、智能运维等项目的建设。

目录
CONTENTS

背景

01

问题与挑战

业务创新

1）智能选股
2）智能打新
3）理财规划
4）策略交易

技术演进

1）分布式架构
2）微服务
3）大数据
4）人工智能

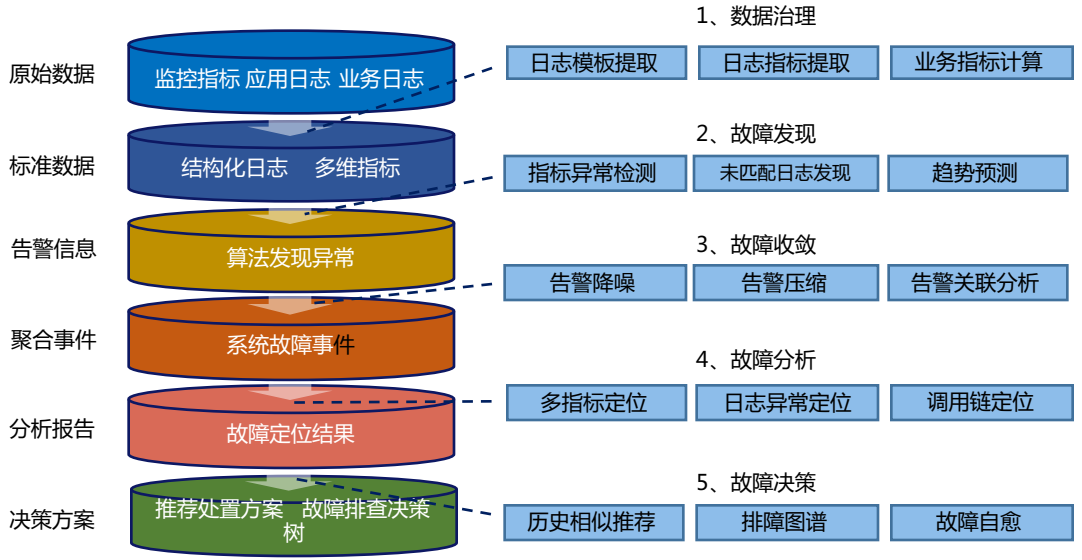
运维支撑

1）软硬件数量激增
2）应用和架构复杂化
3）频繁的变更
4）调用链显著增长
5）运维数据井喷

智能运维建设目标

数据化　智能化　自动化

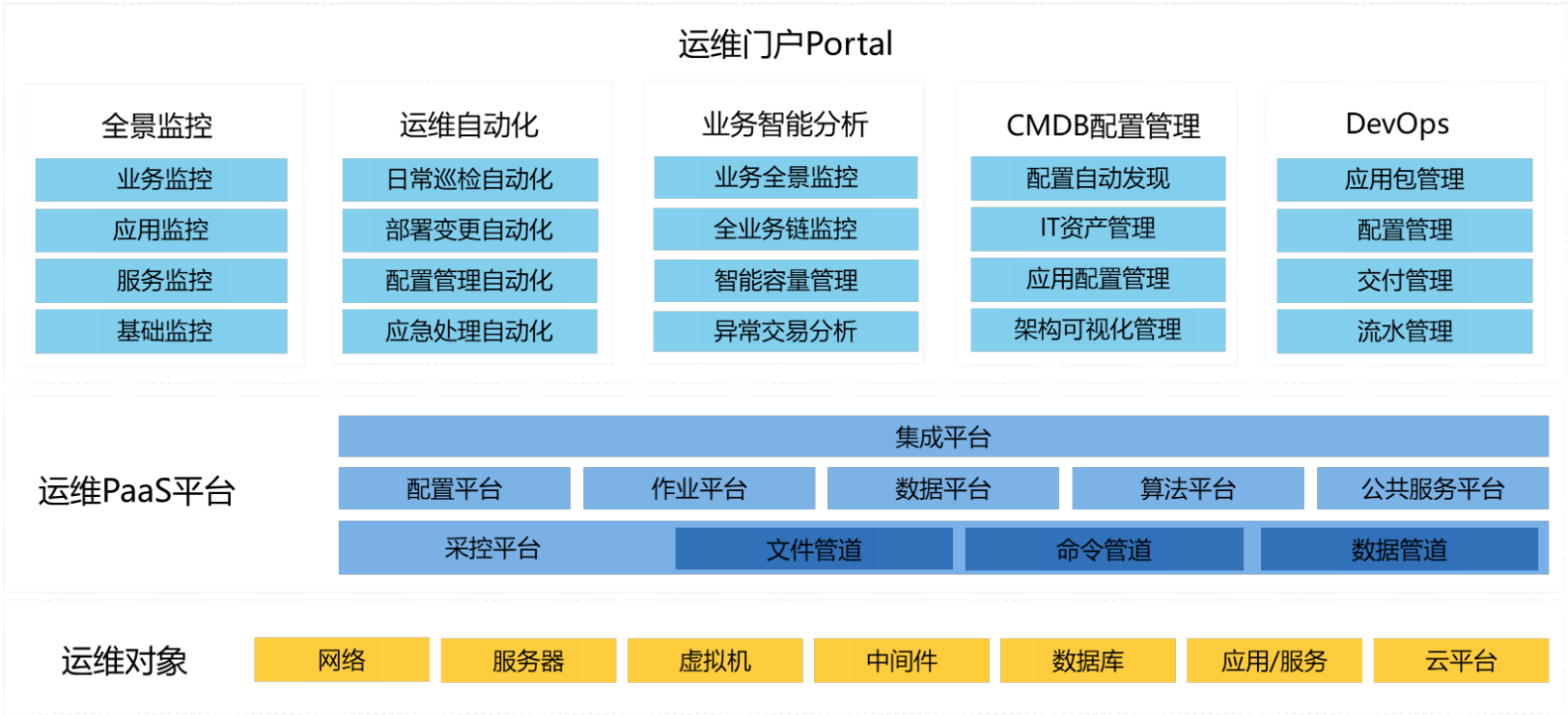
基于指标、日志、知识图谱等运维大数据，结合单指标异常检测、日志聚类分析、日志异常检测等各类智能运维算法，实时分析海量运维数据、感知应用系统状态变化，协助运维人员快速分析定位、做出决策。



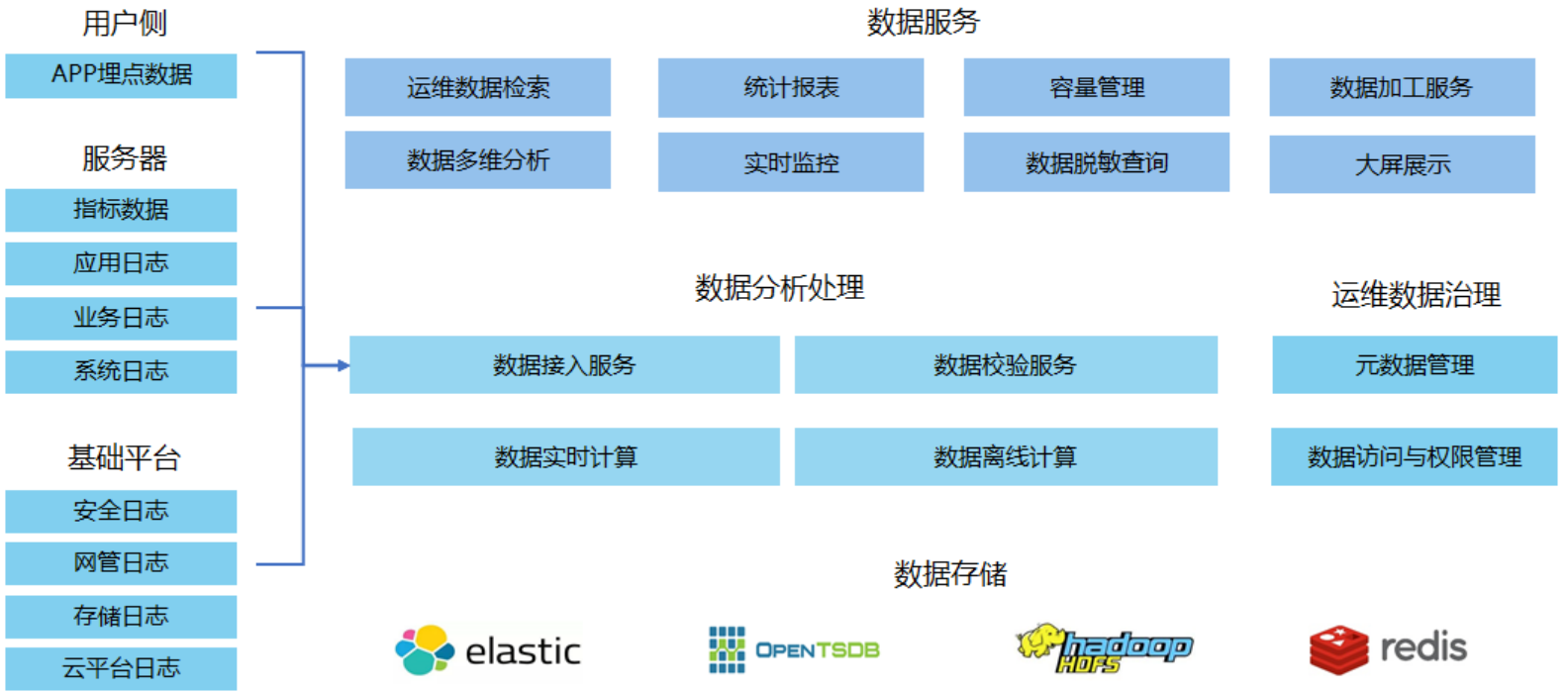
落地实践

02

智能运维体系架构


运维门户Portal
全景监控
业务监控
应用监控
服务监控
基础监控
运维自动化
日常巡检自动化
部署变更自动化
配置管理自动化
应急处理自动化
业务智能分析
业务全景监控
全业务链监控
智能容量管理
异常交易分析
CMDB配置管理
配置自动发现
IT资产管理
应用配置管理
架构可视化管理
DevOps
应用包管理
配置管理
交付管理
流水管理
运维PaaS平台
集成平台
配置平台
作业平台
数据平台
算法平台
公共服务平台
采控平台
文件管道
命令管道
数据管道
运维对象
网络
服务器
虚拟机
中间件
数据库
应用/服务
云平台

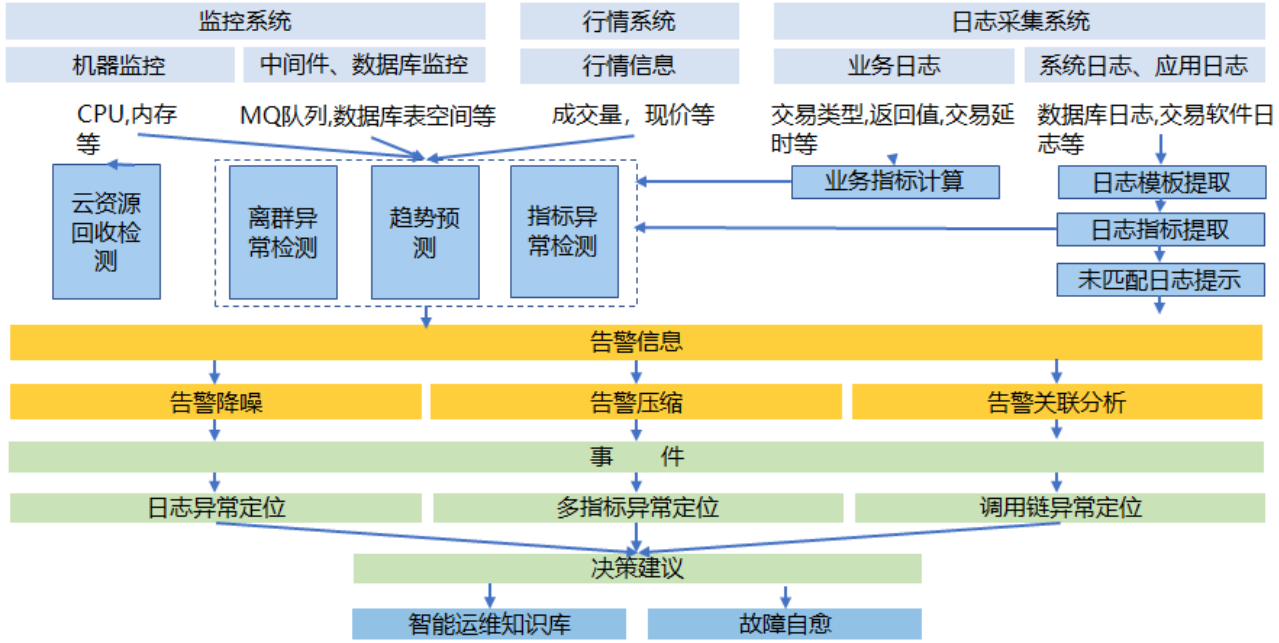
统一的数据服务


用户侧
APP埋点数据
服务器
指标数据
应用日志
业务日志
系统日志
基础平台
安全日志
网管日志
存储日志
云平台日志
数据服务
运维数据检索
统计报表
容量管理
数据加工服务
数据多维分析
实时监控
数据脱敏查询
大屏展示
数据分析处理
数据接入服务
数据校验服务
数据实时计算
数据离线计算
运维数据治理
元数据管理
数据访问与权限管理
数据存储
elastic
OPENTSDB
hadoop HDFS
redis

智能运维算法

编排算法，组合出适用的各类运维场景

原子算法可供多个场景复用，降低开发成本。



单指标异常检测

固定阈值监控存在的问题

固定

无法随着业务变化自动调整阈值

误报

完全依赖人工经验，部分指标阈值设置不合理

漏报

固定阈值触发前的突变无法检测到

业务指标监控难

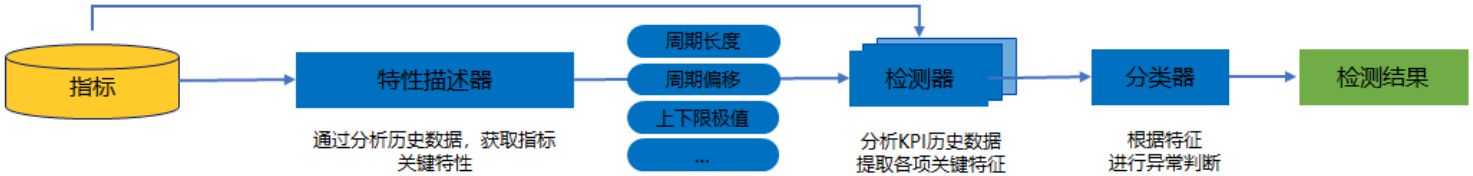
对于周期性指标，难以设置阈值监控

配置工作量大

管理员需要分析每个指标的特性后进行配置，成千上万的指标工作量大

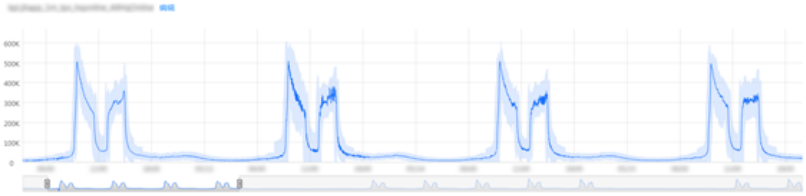
单指标异常检测

- **目标：**通过对各类关键业务指标异常情况的实时检测、告警，及时感知业务波动
- **数据：**交易量、在线人数、错误数、成功率、响应时间等
- **已应用系统：**10+　**查准率：**90%+



异常情况

正常情况



单指标异常检测

➢ 算法主要的特点

异常检测结果准确、及时

单指标异常检测服务使用的是多种无监督机器学习算法的组合，从数学原理上具备比基线阈值等相对简单的统计学方法更加准确、更早发现问题的能力

服务无需人工阈值调整

单指标异常检测服务所使用的算法可以随数据的更新和增长自我学习优化，自动调节敏感度

适用的多种检测指标，算法通用性高、适用性强

自动提取时序曲线的多种特征，适配最优算法，可支持网络场景下多种指标（如延迟、丢包）的检测。

开箱即用

隐藏复杂参数，自动敏感度调整，无需任何复杂配置和标注

日志异常检测

- **背景：**系统日志格式多样，归类设置告警困难；线上发生异常时，打印的大量错误日志难以阅读。
- **目标：**通过日志的相似性进行聚类，对日志模板的频率变化进行检测，将未匹配日志及频率改变的日志进行告警提示，辅助运维人员快速定位异常。
- **数据：**应用日志、系统日志、业务日志...已接入包括4个重保系统在内的12个重要系统，日检测量1T+。

效果及价值

03

应用推广及效果

1. 日志异常检测

   - 完成12个重要系统、25种日志的接入工作，日常分析数据量达1TB以上。

2. 指标异常检测

   - 完成12个重要系统、涉及指标类型包括耗时、请求数、主机指标等，业务指标效果较好。

有效预警机制

- 形成良好的预警-通知-排查-反馈闭环机制

01 有效预警通过微信、短信实时通知系统管理员
每天由专人及时在“重点系统保障群”将重要告警通知到相关管理员，避免管理员遗漏告警信息

02 管理员收到通知后，及时进行排查和处理

03 管理员在“重点系统保障群”中反馈处理情况及问题原因

04 收到管理员反馈后，进行问题记录与收集，有助于智能算法的后续优化

效果及价值

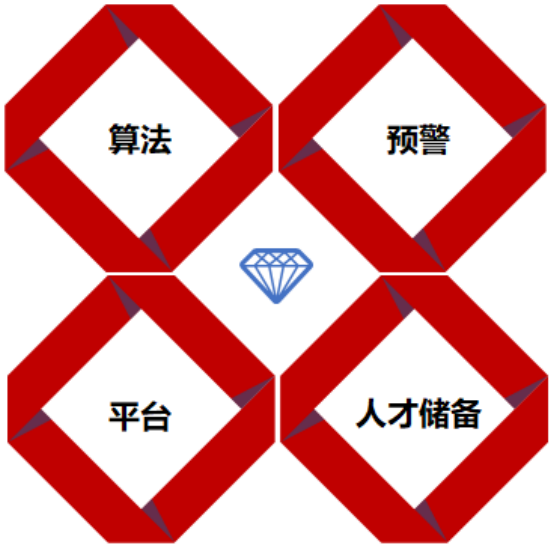
覆盖多个重要系统

指标异常检测已覆盖12个重要系统，接入处理1万多指标；日志异常检测已应用于25种日志，每日分析日志量1T以上。

基于此算法研究的课题，2020年5月评选获得深交所“AI赋能券商运维：智能运维场景落地实践”2019年度优秀课题一等奖。

促进智能运维平台建设

促进建设证券IT智能运维平台：综合集成多种前沿技术；算法和运行环境需分离，环境必须平台化，以便适应新的问题场景、新算法的引入和扩展；应用互联网思维变革传统的IT运维模式；在技术创新上勇于开拓，加快步伐；努力提升团队效能，打造高效高质量的IT运维。



故障提前预警

本应用主要集中在故障发现和提前预警，通过单指标异常检测、离群指标异常检测、日志异常检测的方式，已帮助运维管理员多次第一时间感知系统异常波动，并通过日志快速定位到问题，减少业务中断几率、缩短业务中断时间。收到运维管理员的一致好评。

促进运维转型

未来的运维不仅仅是自动化+人工经验判断，更多的是需要运维人员从各种数据当中分析出潜在风险隐患和业务价值，因此智能运维能够很好的帮助运维人员建立起数据利用的思维习惯，用数据来衡量运维，用数据来促进工作提升。

Thanks

高效运维社区

开放运维联盟

荣誉出品