



中国・深圳

指导单位:



Catig开版产业取款量 RPA产业推进方阵



OOPSA Open OPS Alliance

RPA时代

时间: 2021年5月21日-22日



为AIOps的普及而重生的"基础监控"

张建 腾讯IEG-基础监控平台负责人





张建

腾讯IEG-基础监控平台负责人

从事运维领域的工作有十多年,当前负责蓝鲸的监控、日志、自愈等产品,重点在解决运维线上问题的发现、定位、处理等核心诉求。

为AIOps的普及而重生的"基础监控"









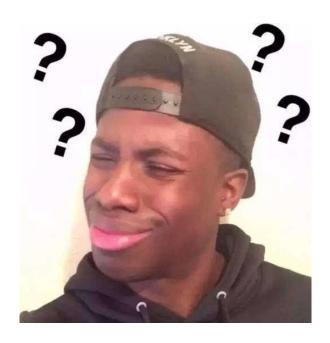


图论

信息论

自然语言处理

机器学习







- ① 为什么AIOps难普及?
- 2 如何保证数据质量
- 3 如何降低AIOps使用门槛
- 4 如何健全反馈和验证机制



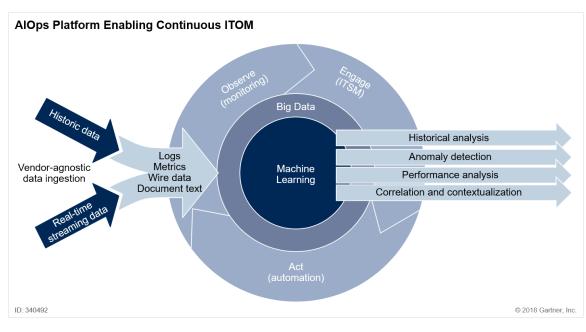
为什么AIOps难普及?

01

了解AIOps



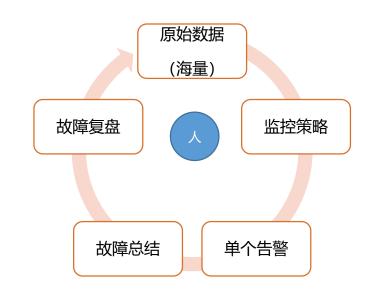
- 1. AlOps的特点
- 2. AIOps业界的情况
- 3. AIOps应用的案例
- 4. 为什么难普及?



AIOps的特点



传统运维,以人的经验单一策略为核心驱动。

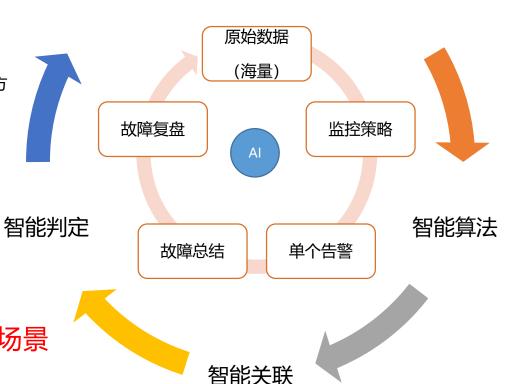


AIOps的特点



自动检测

智能运维,将AI应用于运维领域,基于已有的运维数据(日志、指标、事件等信息),通过机器学习的方式来解决人工或者单一规则无法完成的事情,涉及到很多运维场景,监控、效率、安全、成本等方向。

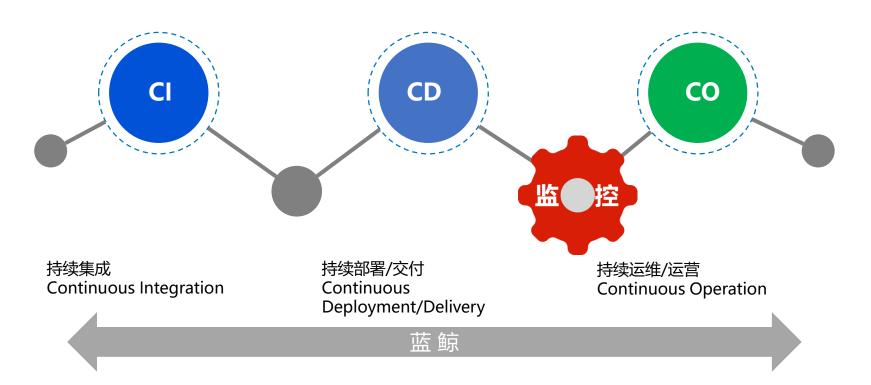


智能学习

监控只是AIOps中的一种应用场景

AIOps中监控的重要性

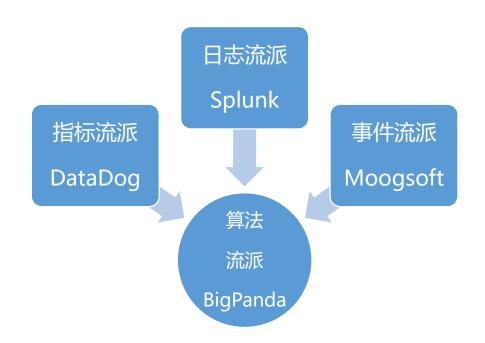




AIOps中监控的业界情况



- 切入的角度不一样
- •基础功能+智能分析
- 单一的数据无法发挥AI的能力
- 各个流派都有局限性



AIOps的应用案例

初阶: 纯手动接入

第一步:拥有大数据平台/技术

第二步:分析业务架构,想办法获取业务使用到的数据

第三步: 把数据接入大数据平台进行清洗, 打标签, 标准

化等

第四步:拥有AI建模能力,依据业务特性创建模型算法

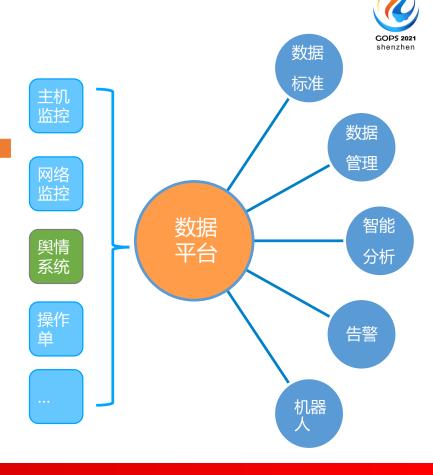
第五步:消费输出的内容进行告警,添加机器人等

进阶: 固化黄金指标自动接入

如何迁?

第三步:利用对同一类架构的业务的理解,抽象出黄金指标及保证相关的数据的稳定性,再提高模型算法的准确率,

封装成一键接入的服务。



为什么难普及?

> 数据质量难保证

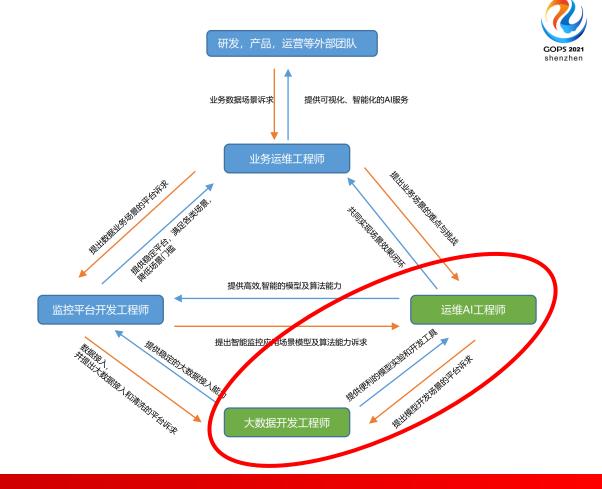
- 稳定性差
- 难识别
- 数据不全

▶ 使用门槛高

- 理解成本高
- 不可迁移
- 反智

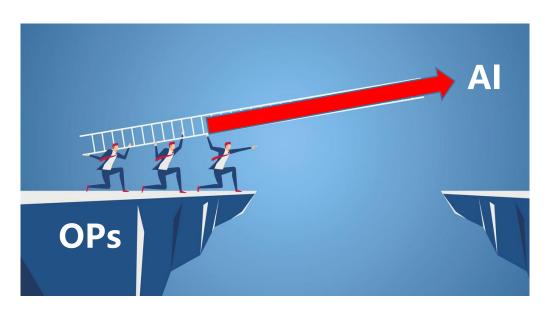
▶ 反馈和验证难

- 反馈少
- 无法自动验证



解决方案:基础监控重生-方法论产品化





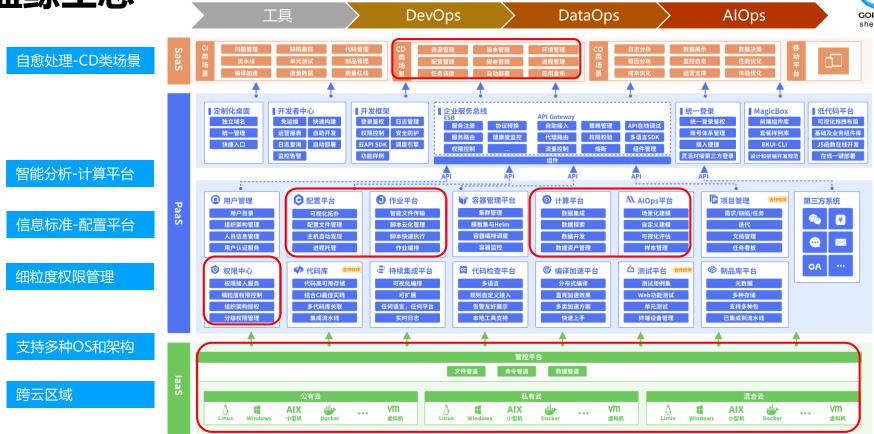
AI和Ops之间的鸿沟



AIOps三类用户

蓝鲸生态







如何保证数据质量

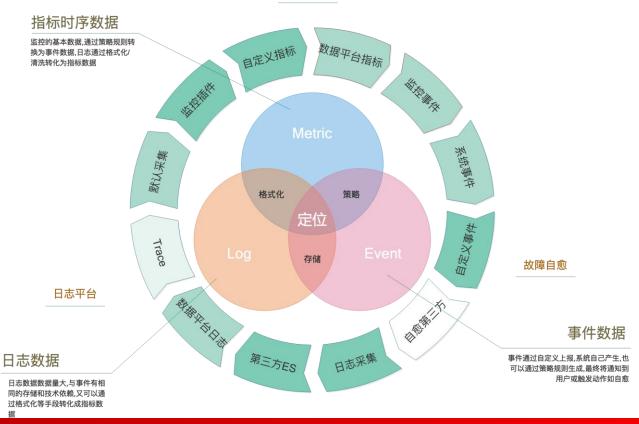
数据质量是最基本的保障-全,识,稳

02

数据质量-全

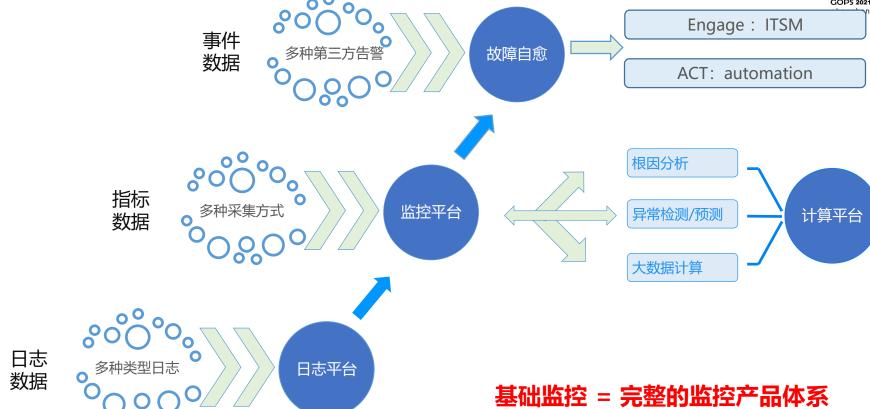






数据质量-全





数据质量-识



监控对象分层

Application移动端用户体验业务应

Service 服务

Host 主机

Data Center 数据中心 浏览器 移动端 业务应用 服务模块 组件

进程

容器

操作系统主机设备

云主机

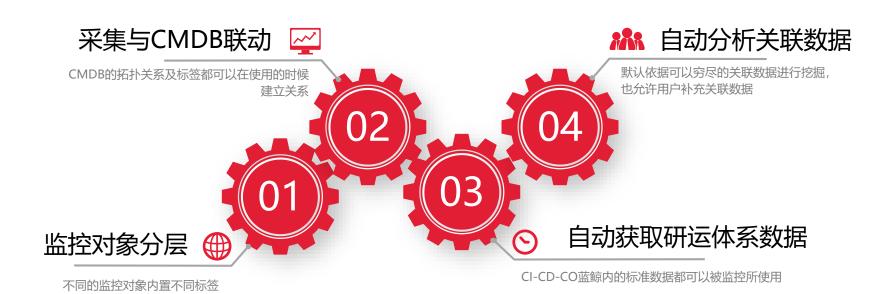
网络连接硬件设备

机房状态



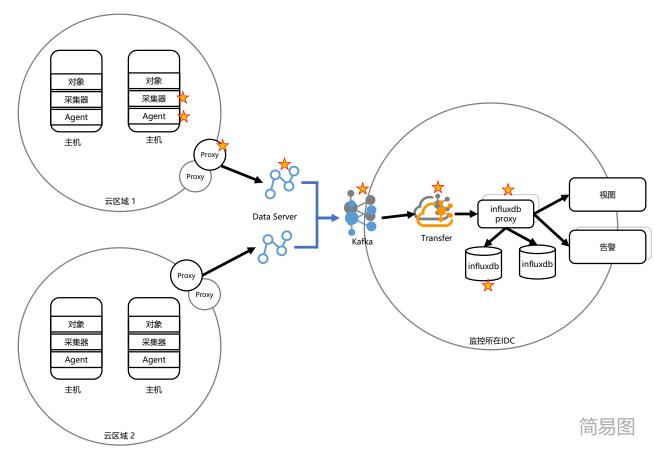
数据质量-识





数据质量-稳







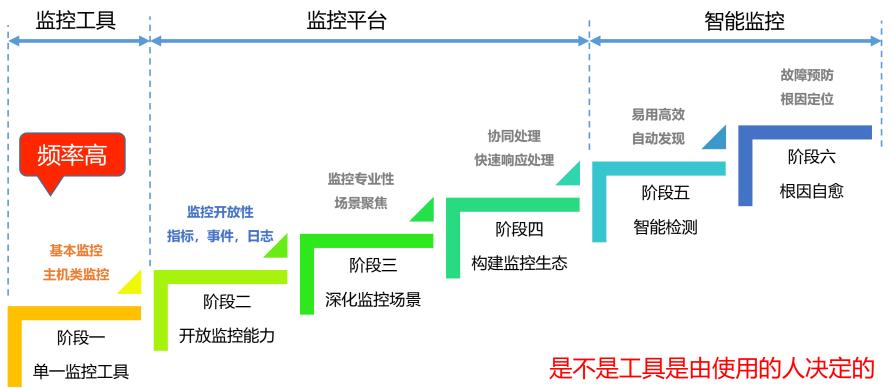
如何降低使用门槛

让AIOps更容易理解

03

监控产品解耦





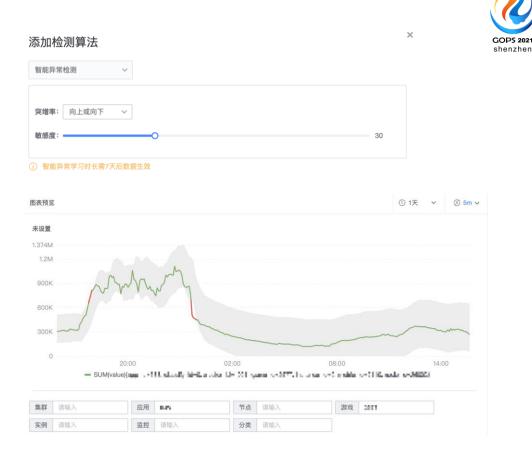




例:智能异常检测

添加检测算法





AIOps的三个阶段



	▲ 故障生成 - 根因分析											
		名称	原理	故障输出	产品输出	效果	配置成本	技术成本				
補助系	阶段一	○ 纯数据驱动	依赖的信息最少,只基于数据本身的时间,概 率,还有人工的规则,甚至是已知的层级关系进 行事件的分类	粗的故障分类	故障列表	一般	简单	低				
					根因推荐							
				概率的根因	人工规则输入							
控制系	阶段二	功能驱动	依赖拓扑结构,人工拓扑,trace链路	有拓扑关系的故障	人工拓扑输入	中 人工拓扑 影响效	高	高				
				有推导的影响范围	拓扑查看							
					告警通知的影响范围							
强攻系	阶段三	КРІ驱动	KPI定义,范围,人工权重 -> 根因定位优先级更 高	正向: KPI发生时,给出根因结论	高优先级的KPI告警	好 人工权重和范围 关联数据影响效果	很高	ф				
				ating to 100.000 at high sold participated FU	基于KPI的关联信息展示							
				反向:KPI关联的告警发生时,提前预警和验证 关系	提前预警配置和通知							
					Feedback							

阶段三: KPI驱动



指标?

KPI定义的方法论需要产品化

SaaS

在线/订单

用户接入质量

PaaS

应用质量

IaaS

(CPU/MEM/NET/DISK)

GOPS 全球运维大会2021·深圳站



如何建立有效反馈

有反馈才能够不断学习

04

评价反馈的重要性



无监督: 其实是更复杂的阈值策略

有监督: 更智能,但需要更多的评价反馈

数据接入

评价反馈

AI判断

矛盾: 运维容忍度很高

对比项	阿里-智能基线	百度-Noah	Yahoo-EGADS	Twitterβ	Skyline	Microsoft					
算法框架	曲线分类+无监 控+有监督	曲线分类+无监 控+有监督	无监督	无监督	无监控	无监控+有监督					
场景多样化	曲线从数据形态 及业务特性分别 分类,场景细	曲线分为3类, 分别适配不同的 无监督+有监督 算法	曲线分为3类, 适配不同的算法	无曲线分类,统 ——套餐算法	无曲线分类,统 ——套算法	曲线分为3类, 分别训练模型					
算法多样性	Bi-LSTM、统计 差别算法、 MAD、Multi- Gaussian Tail、 SMIQD、 SMAD、孤立森 林	统计判别算法、 逻辑回归、 LOESS局部回归、 ARIMA	Olympic模型、 EWMA、移动平 均、OLS、 ARIMA、状态 空间模型、超低 密度模型、 DBSCAN	STL、S-H-ESD 算法	统计判别算法、 MAD、EWMA、 OLS、HBOS、 KS检验	DBSCAN、 Spectral Residual、 CNN					
脏数据清洗	滤波器去噪+均 值补点	离群值剔+平滑	无	无	无	无					
特征工程	完善	完善	完善	无	无	无					
是否开源	否	是	是	是是		是					
人工标注	暂无	需要打标,并有 成熟的打标工具	暂无	暂无	暂无	需要打标,并有 成熟的打标工具					

发现阶段: 监控工具 日志平台 4% 采集 日志 原始 日志数据 自愈 时序数据 监控 收敛 告警 事件 策略 采集 异常点事件 标准 10% 原始 时序数据 系统数据 汇总通知 监控平台 100% 20% 误告 人为判断 网络监控工具 告警 事件 经验沉淀 50% 快速处理 解决 确 确定是 15% 定 一类问题 工单 根 1% 因 跟踪 复盘 确定是故 快速止损 长期跟进 故障中心 决 障 经验沉淀 经验沉淀

【后期】收尾和闭环阶段: 故障跟踪/知识库

【中期】 定位并协作处理阶段: 故障自愈

生态联动+AI赋能





- •指标异常检测
- •指标预测
- 离群检测
- •文本聚类

定位阶段

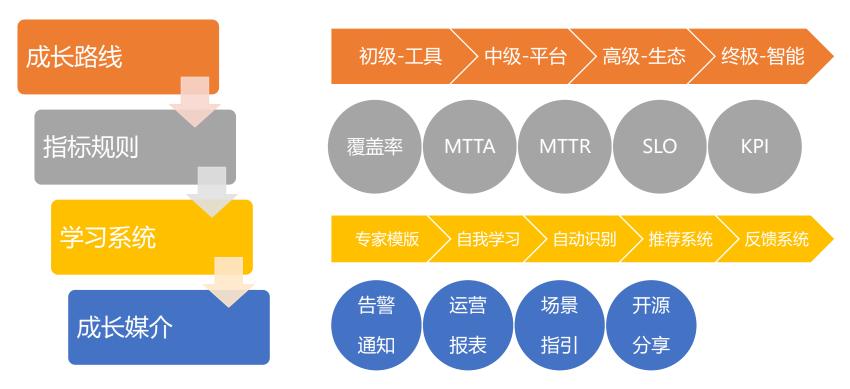
- •多维下钻分析
- •告警关联
- •告警智能摘要
- •根因定位

处理阶段

- 故障复盘分析
- 运维知识库
- 智能决策

养成类"游戏"

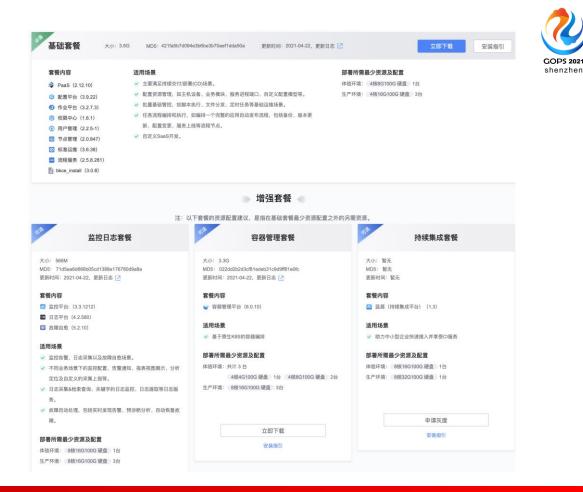




蓝鲸社区版6.0.3



https://bk.tencent.com/download/







Thanks

高效运维社区 开放运维联盟

荣誉出品