DAMS

中国数据资产管理峰会

CHINA DATA ASSET MANAGEMENT SUMMIT

传统企业ITOA运维与实践

演讲人：轻维软件有限公司 CEO 宋辉

IT 已经成为我们生活的一部份

光鲜的背后，是无数运维人员7*24的保障

英国遭遇大面积网络故障 两大机场所有航班取消

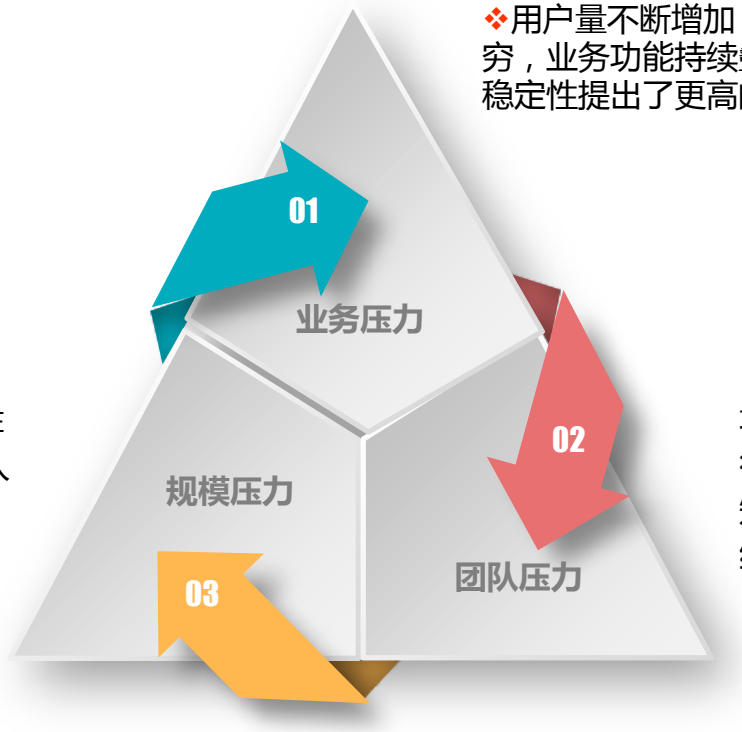
互联网　央视　2017-05-27 23:10　196 评论　分享

（原标题：遭遇罕见大面积网络故障 英航取消两大机场所有航班）

但随着信息化的不断深入，运维面临越来越大的压力

大数据时代的运维面临“**业务、规模、团队**”三大问题多种压力：不断提升的用户体验要求；应用交付周期越来越短；数据中心规模不断增长；大量分布式、开源架构引入；各种新技术层出不穷；团队人员能力增长缓慢且流动性大等。在种种压力影响下，运维团队需站在承前启后的时间节点主动寻求变革。

❖用户量不断增加，营销活动层出不穷，业务功能持续叠加对系统响应与稳定性提出了更高的要求



❖数据中心分区域建设，海量设备持续接入，去IOE X86化，分布式架构的引入使得系统规模成倍的上涨

❖流程化、规范化、集中化人员培训后虽然人才培养效率已经有很大提升，但初级人员吸收理论知识转化为实践经验依然与团队维护压力存在一定的距离

这些问题随时可以把我们打扒在地上

IT软硬件体量庞大，增长迅速

软硬件厂家众多，数量庞大，管理分散，协调困难

故障定位分析难

现网业务复杂，涉及业务部门及系统众多，问题核查定位耗时费力，过程冗长

运维数据量庞大

机器很多，操作很多，日志种类多， 数量从G级单位上升到PB级单位，传统方式处理效率低下，无法沉淀

性能分析不深入

无有效分析手段进行深入的性能分析，导致解决问题延时，影响生产系统业务运行

自动化运维能力不足

简单重复的事“堆人”，难的事“堆专家”

牛人效应

运维处理重心依赖少量牛人及经验，少了牛人问题就很难处理甚至无法处理。且运维经验难以有留存并有效传递

故障处理全靠人工

人工依据经验逐条排查问题，受运维人员水平所限，难于快速精确定位与处理，且耗时长，可能延误处理问题最佳时机。

被动运维

运维总是被动救火，不能将风险扼杀在故障发生之前

我们一直在改变，一直在努力

运维迈入智能化时代

运维发展

用ssh+exp代替了手工登录服务器维护的模式。

脚本时代

工具时代

以chef/puppet配置工具为代表，把运维的能力变成一个个的工具能力。

运维工具能力平台化，进一步固化运维的常见场景。

平台时代

运维不仅仅是技术革新的受益者，更应该是贡献者。

智能时代

- 事件（海量数据智能总结归档）自动处理
- 不可预知故障，依托智能算法提前预判，提前预警，主动性介入，真正做到运维“保健”化
- 常规工作（上线、部署、容量预估等）平台化
- 解放人来做技术革命的贡献者

机器学习

结合机器学习，构建智能分析预测模型池，为生产系统运维提供依据，动态结合监控体系实现智能运维.

大数据

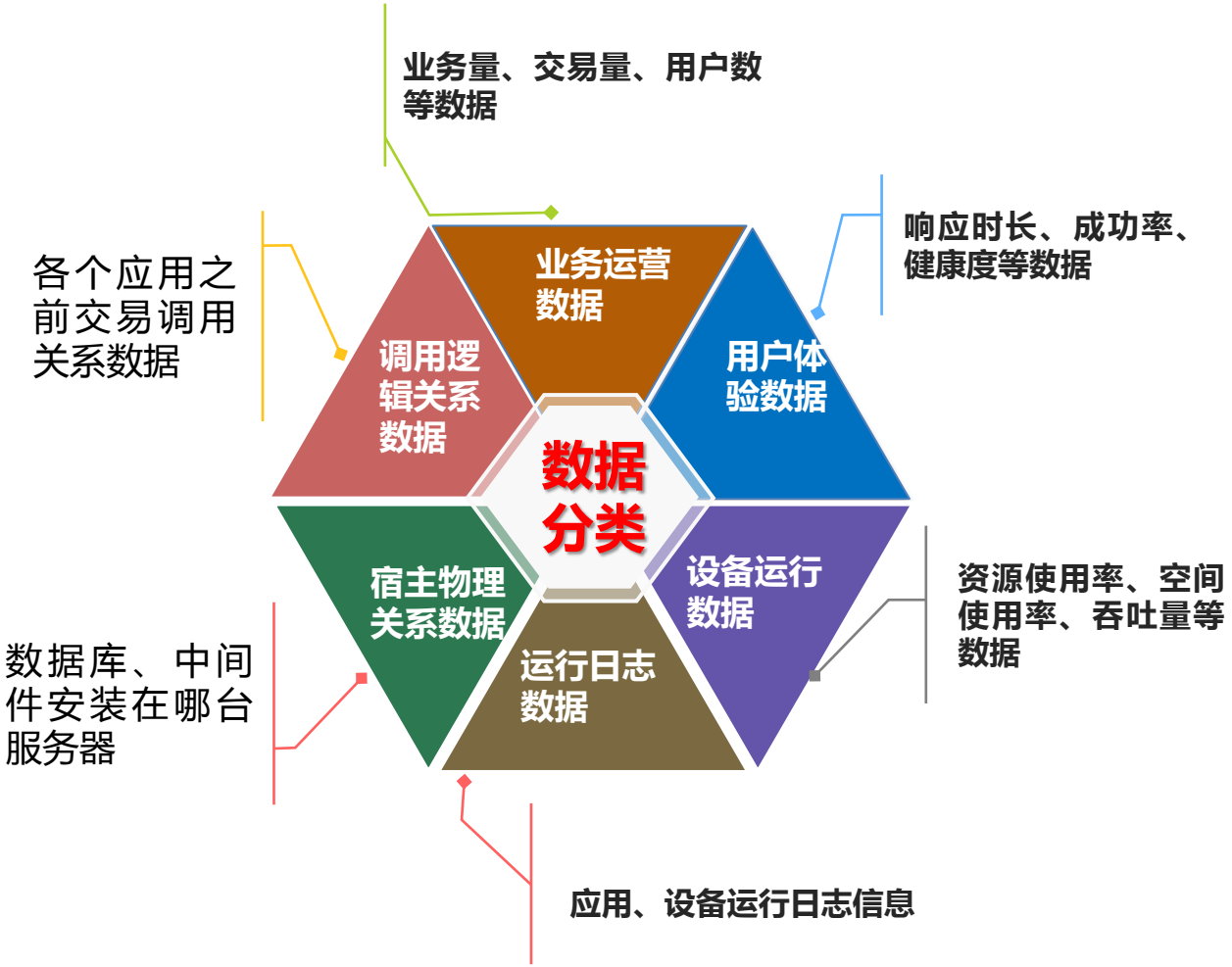
新时代运营商体量庞大，需要完善的监控运维体系，实现对数据中心环境的整体深度监控，高度自动化运维能力

人工智能

基于变更/故障/异常分析/预测等各个运维场景，都可以找到智能化的模型/具体实现。IT大数据分析提供实时的变更和调度智能决策能力。

智能时代离不开数据

与运维相关的数据分类


业务量、交易量、用户数等数据
响应时长、成功率、健康度等数据
各个应用之前交易调用关系数据
业务运营数据
调用逻辑关系数据
用户体验数据
数据分类
宿主物理关系数据
设备运行数据
运行日志数据
资源使用率、空间使用率、吞吐量等数据
数据库、中间件安装在哪台服务器
应用、设备运行日志信息

各种各样的数据如何采集？

使用不同方式可以获取不同数据，这些数据重叠交叉，这就是ITOA的价值

A 日志分析（日志数据、调用关系数据、业务运营数据）

-- IT系统自己产生的数据，包括客户端、服务器、网络设备、安全设备、应用程序、传感器产生的日志

B 抓包解码（调用关系数据、业务运营数据、用户体验数据）

-- 系统之间2~7层网络通信协议的数据，可通过网络端口镜像流量

C 应用探针（调用关系数据、业务运营数据、用户体验数据）

-- 是在 .NET、PHP、Java 字节码里插入代理程序，从字节码里统计函数调用

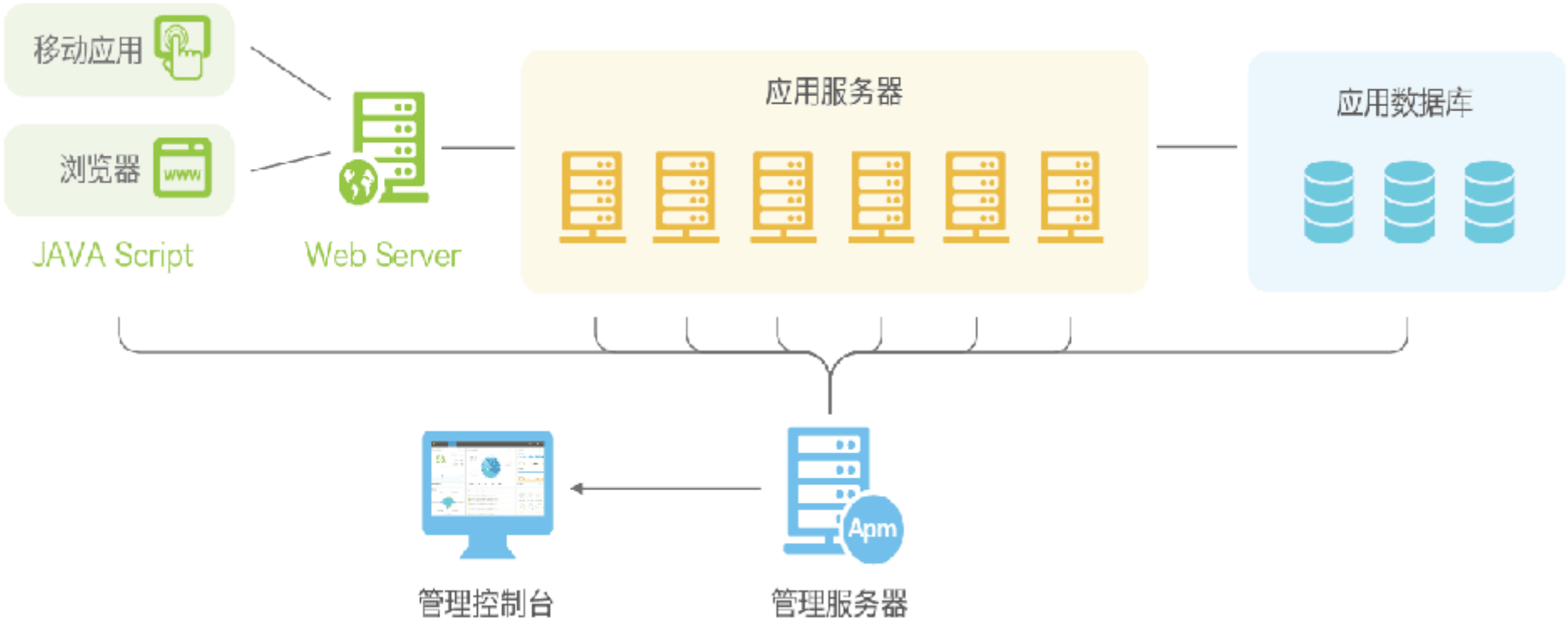
D 指标采集（设备运行数据、物理关系数据）

-- 监控采集到的数据库、主机、应用等运行状态及指标数据

E 外部拨测（用户体验数据）

-- 模拟用户请求检测系统，如 ICMP ping、HTTP GET等，能够从不同地点模拟客户端发起

通过植入应用探针，构建应用交易全链路数据分析能力

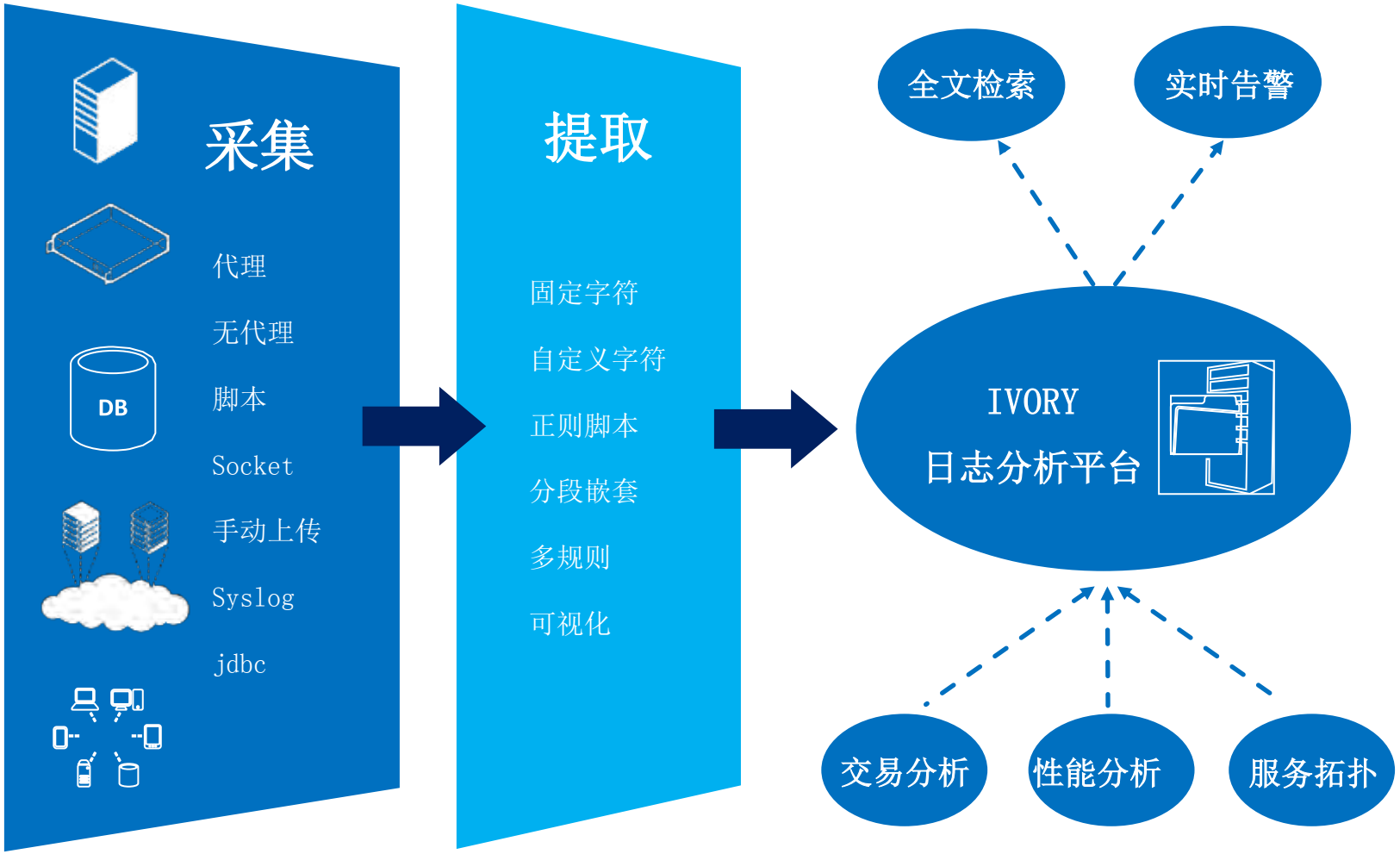


流览器 移动端 性能跟踪

代码诊断 系统拓扑 交易追踪 API监控

执行计划 性能分析 慢SQL跟踪

通过日志数据分析平台，构建应用端交易分析能力



基于日志分析的分析应用场景

某基金公司，为了保障系统稳定易方达利用日志对交易违规，交易故障，交易失败，接口异常和请求量等进行分析，对所有系统日志进行统一管控

设备运维

- ✓ 安全分析
- ✓ 故障分析

应用运维

- ✓ 应用性能分析
- ✓ 应用监控
- ✓ 故障分析定位

安全分析

- ✓ 操作日志分析
- ✓ 访问行为日志分析

利用监控、日志、APM等手段构建全面的关系自发现能力

物理关系自发现

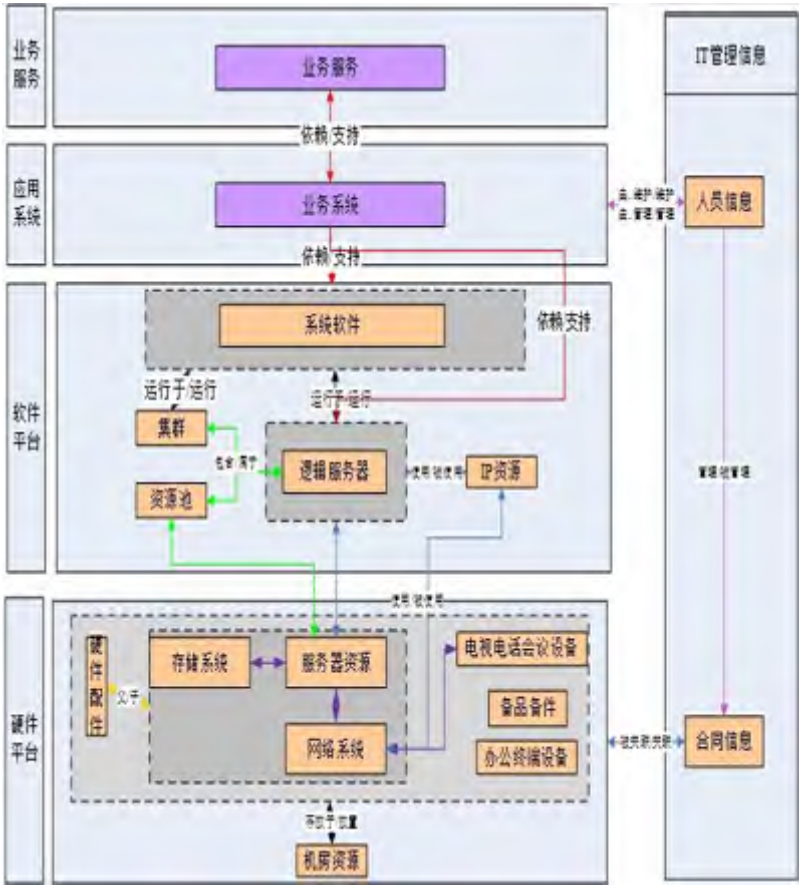
软件实例

操作系统

主机

资源池

存储、网络



逻辑关系自发现

应用

数据库

缓存

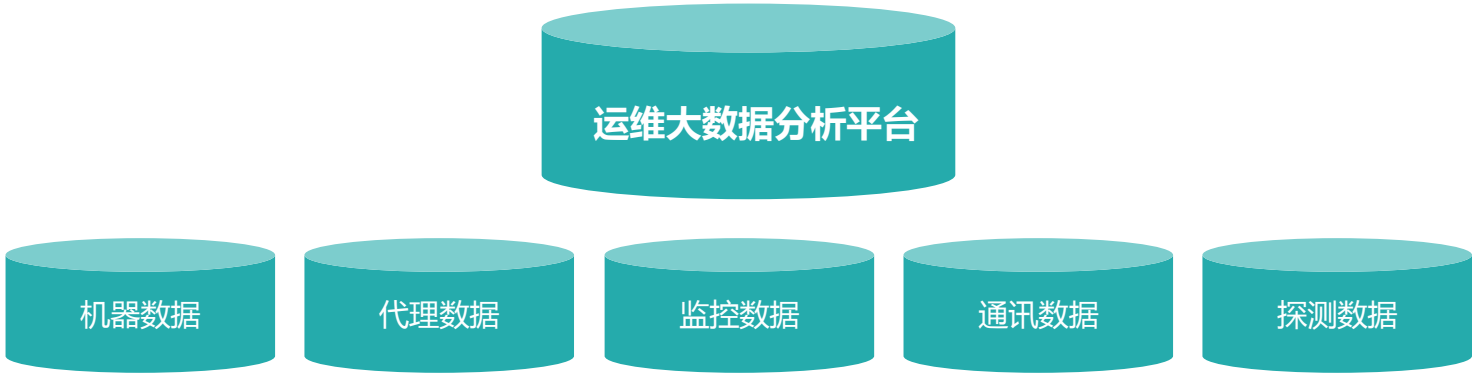
服务

运维大数据的价值

ITOA的价值，各种数据关联产生更大的价值

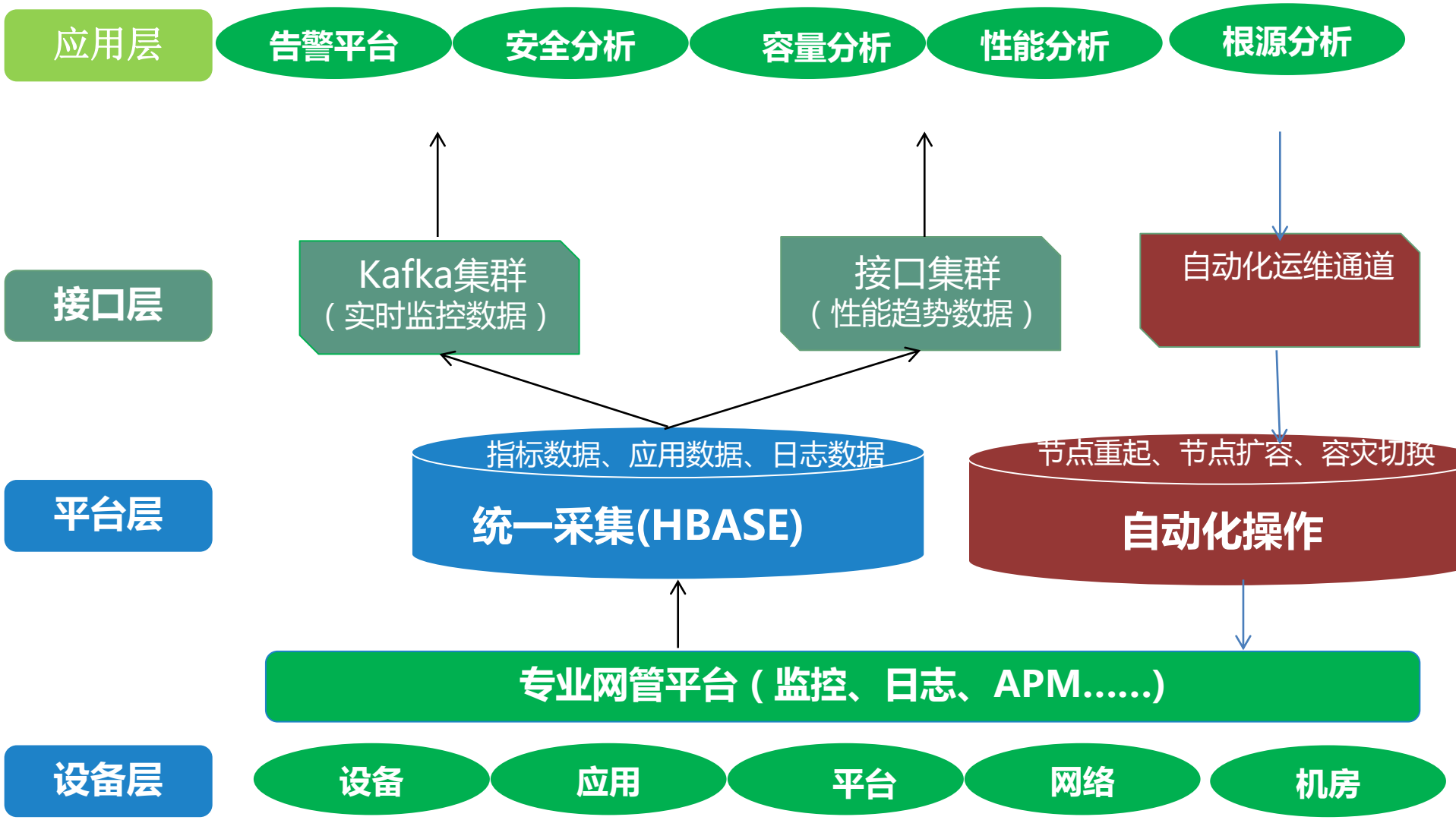
ROOT分析　性能基线分析　容量分析　告警阀值优化　基线偏离告警

安全事件分析　故障预测　容量预测　关联告警　事件关联分析



业务　应用　PaaS　数据库　IaaS　其他...

平台整体技术架构


应用层
告警平台
安全分析
容量分析
性能分析
根源分析
接口层
Kafka集群
（实时监控数据）
接口集群
（性能趋势数据）
自动化运维通道
平台层
指标数据、应用数据、日志数据
统一采集(HBASE)
节点重起、节点扩容、容灾切换
自动化操作
专业网管平台（监控、日志、APM……）
设备层
设备
应用
平台
网络
机房

应用场景分析

- 场景目标

问题闭环：发现 -> 决策分析-> 问题解决

异常检测	报警风暴	关联分析	故障定位	自愈、预测
■ 告警	■ 归一/归类	■ 单点关联 ■ 驱动关联 ■ 业务性关联 ■ 基础决策 ■ 算法关联	■ 关联定位 ■ 特征归类 ■ 强决策 ■ 算法预测 ■ 基线预测	■ 逻辑规律自愈 ■ 特征预测自愈

通过异常检测，判断指标数据趋势性问题

1.自回归模型（AR：Auto-regressive）
2.移动平均模型（MA：Moving-Average）
3.混合模型（ARMA）

数量型	增长型	扩散型	分布型	频率型
• 各类安全事件发生次数	• 各类安全事件的增长速度	• 各类安全事件涉及的IP地址数量	• 各类安全事件的IP地址熵	• 安全事件排名异常度

面向流量态势感知指标

整体流量指标	• 平均流量、平均包长 • 大包数量、小包数量、重传次数	分布类指标	• 源IP地址熵 • 目的IP地址熵
会话信息指标	• 平均TCP、UDP、ICMP...会话数 • 平均TCP、UDP、ICMP...会话长度	比例类指标	• SYN+ACK / SYN • RST / SYN
端口流量指标	• 各端口流量 • 各端口数据包数目	方差类指标	• TCP流大小方差 • UDP流大小方差
指示位指标	• TCP SYN、ACK+SYN、FIN、RST数目 • ICMP Echo、Reply、...数目...		

态势感知预测算法：非周期性指标预测+周期性态势预测模型

异常检查应用示例：指标动态基线告警

设备管理 > STNG3BOSS-IB4 > 触发器管理 > kernel使用率(vmstat) 60s为采集频率，超过基线上门限10%，请检查性能趋势情况 > 编辑

告警 | 依赖关系 | 预处理脚本

* 名称: kernel使用率(vmstat) 60s为采集频率，超过基线上门限10%，请检查性能趋势情况

默认规则 | 高级规则 | 基线告警

*表达式: {STNG3BOSS-IB4:system.run[vmstat 10 1 | tail -1 |awk '{print $15}'].last()}>

历史告警 > STNG3BOSS-IB4 > CPU使用率(vmstat)60s为采集频率，超过基线上门限10%，请检查性能趋势情况,触发值：41%

总览
1新网管-zabbix
1网管-zabbix
2网络设备
4A-VM物理机
4A-VM虚拟机
4A-存储
4A-平台
4A-湛江容灾平台
DNS维护组
ERP-测试环境
ERP服务器组

STNG3BOSS-IB4(10.252.177.49) 于 2017-07-02 22:18:00 至 2017-07-02 22:58:00 期间发生 31 次告警: CPU使用率(vmstat)60s为采集频率，超过基线上门限10%，请检查性能趋势情况,触发值：41% ：
目前 已恢复,影响业务系统:计费帐务子系统汕头区域,短信 无需下发

预处理动作信息

动作名称	描述	执行方式	操作
暂无数据			

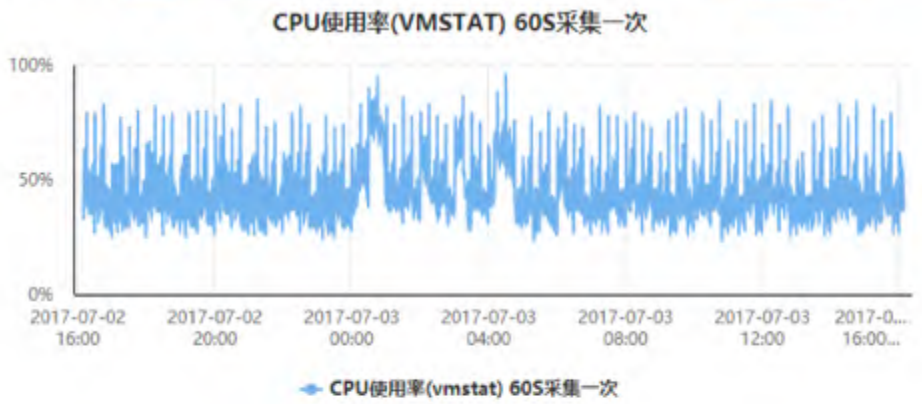
执行其他脚本

预处理记录

暂无数据

性能

图表 | 值 | 天 | 周 | 月 | 从 2017-07-02 16:09:08 至 2017-07-03 16:09:08 | 搜索

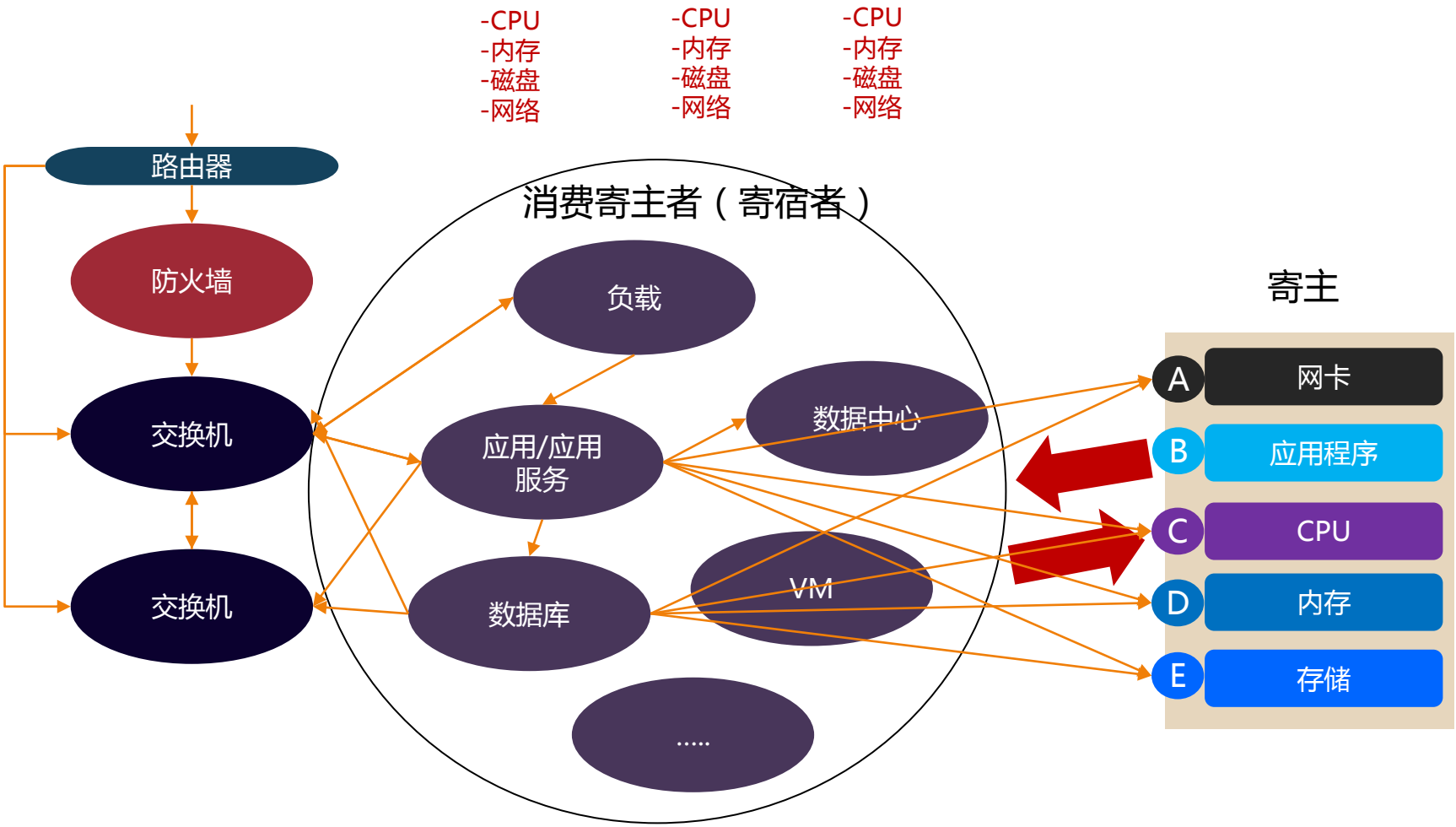


告警处理

处理动作： | 备注： | 确认

利用物理及逻辑关系进行关联分析与根因定位

1 路由器 - 防火墙 - 交换机 - 中间件 - 应用程序 - 数据库 - CPU – 内存 – 磁盘 – 网络



对指标进行分类、构建关系，进行关联分析及根因定位

根因分析

故障ROOT分析

告警短信：XX缓存硬件故障，影响XX、XX业务，可能原因为磁盘故障

架构分层原则：越底层的设备可能性越大

用户层

接入层

逻辑层

数据层

路径分析原则：当某个设备出现问题，属于这个调用链上的节点都可能出现告警，按访问顺序，最末端的可能性越大

时间面积原则：结合告警时间先后顺序，告警影响面积等权重分析

时间相关性

面积权重

关联分析：在一个视图上呈现点、线、面、立体的问题

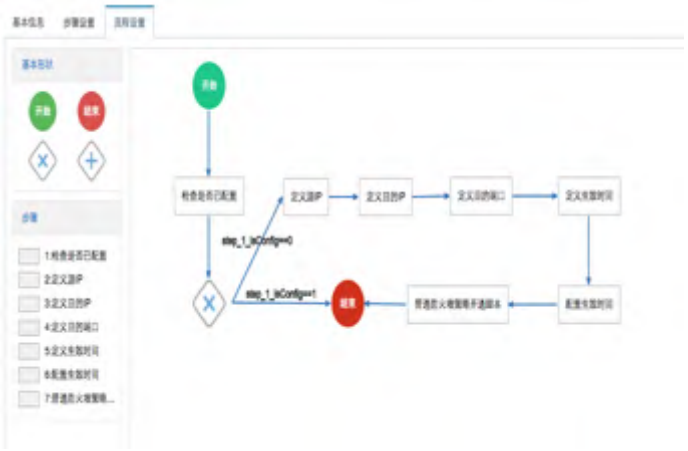
应用拓扑可视化

应用调用链分析

关联分析示例

隐患推荐-根因告警-影响度分析-深度钻取

故障自愈



问题 → 告警 → 问题根源 → 重起 / 扩容 / 退服 / 新增节点 / 容灾切换

整合的价值

提供整体运维解决方案，并基于此构建全面的自动化、智能化能力

平台自管理 帐号权限管理 流程管理

移动运维(APP)

大屏视图

个人门户

专业报表

定制场景应用

业务开通，网络开通， CHATOPS，应用部署、系统部署……

基于场景化的“统一运维管理”

智能监控告警	自动化运维	性能管理	大数据&AI
95%，10万+	自动化巡检	应用性能分析	机器学习
智能基线	自动化安装	用户体验分析	根因分析
智能告警预处理	任务编排/调度	用户行为分析	监控/性能/故障场景
可视化健康度	云资源管理	数据库性能分析	大数据安全&风险分析

统一采集 AGENT，SSH，SNMP，IPMI，SYSLOG，应用探针，日志……

统一控制 SALTSTACK，ANSIBLE，SHELL，SQL，PERL，API……

统一资源 CMDB（模型/自发现），集成指标库，集成操作库……

外系统接口

IT基础设施层

主机 存储 网络 基础软件 虚拟机 云平台

DAMS

中国数据资产管理峰会

CHINA DATA ASSET MANAGEMENT SUMMIT

THANK YOU !