

TechNeo 技术沙龙第21期——运维新挑战

大型企业智能运维探索与实践

中油瑞飞 孙 杰



微信扫码收听演讲音频

目录



构建新IT运维
管理体系



全景业务
服务管理



日志采集
监控股警



知识库
故障自治



01

构建新IT运维管理体系



微信扫码收听演讲音频

传统运维软件逐渐不适应运维需求



事后

所有的运维软件大多是事后报警，此时损失已经造成，晚了！



零散

一种软件监控一类设备，无法提供整体的运维监控解决方案



单一

针对不同的用户提供的是相同的界面和视图，不能满足用户不同岗位、不同业务的运维要求



“弱智”

智能化程度差，以监控和报表为主，不具备大数据关联分析和深度数据挖掘功能



无用

由于无法发挥实质性的作用，且运行时间长之后性能影响显著，最终被弃用。



传统运维存在的突出问题



数据分散，不利于故障分析和问题跟踪

- 不同的数据存储在不同的运维系统中，无法关联
- 数据格式、时间戳等各不相同，不利于问题排查



要的功能没有，没用的数据重复采集，影响正常业务

- 每个运维软件都有特长部分，同时也采集其他数据，造成重复影响
- 有些甚至相互影响，干扰正常业务运行

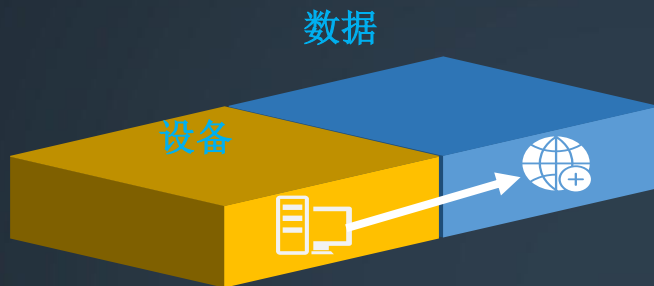


投资浪费，增加运维压力

- 采购多种运维软件，在功能上、设备上存在投资浪费
- 没有减轻运维压力，还增加了多种软件的维护工作



运维技术在持续升级



以**设备**为中心的维护

升级为

以**数据**为中心的运营

升级的3个原因：

技术进步

运维事故

运维压力

	人工	工具	自动化	智能
现状	目前大量的用户采用人工运维方式，包括自行运维、外包运维、原厂维保等	一些用户开始尝试自主开发工具、外购工具或者利用其他软件的附带工具进行运维	大部分互联网用户使用自动化运维；仅少量传统用户尝试自动化运维	很多客户开始探索使用大数据进行智能运维管理，并获得惊人收获
前景	人艰不拆	“弱智” “无用”	实施不易	未来趋势



运维应**做到**

无论云上云下，保障业务系统稳定运行都是最重要的工作。

- 通过部署智能运维系统，能够显著提升运维效率，大大增强运维团队的能力和价值；
- 通过部署智能运维系统，能够显著增加运维透明度，使管理和运维人员增加主动权和掌控力；
- ✨ 通过部署智能运维系统，能够显著降低故障频率，使运维更省心。

维护 -> 运营

帮助用户将以设备为中心的维护
升级为以数据为中心的**运营**。

“活着” -> 健康

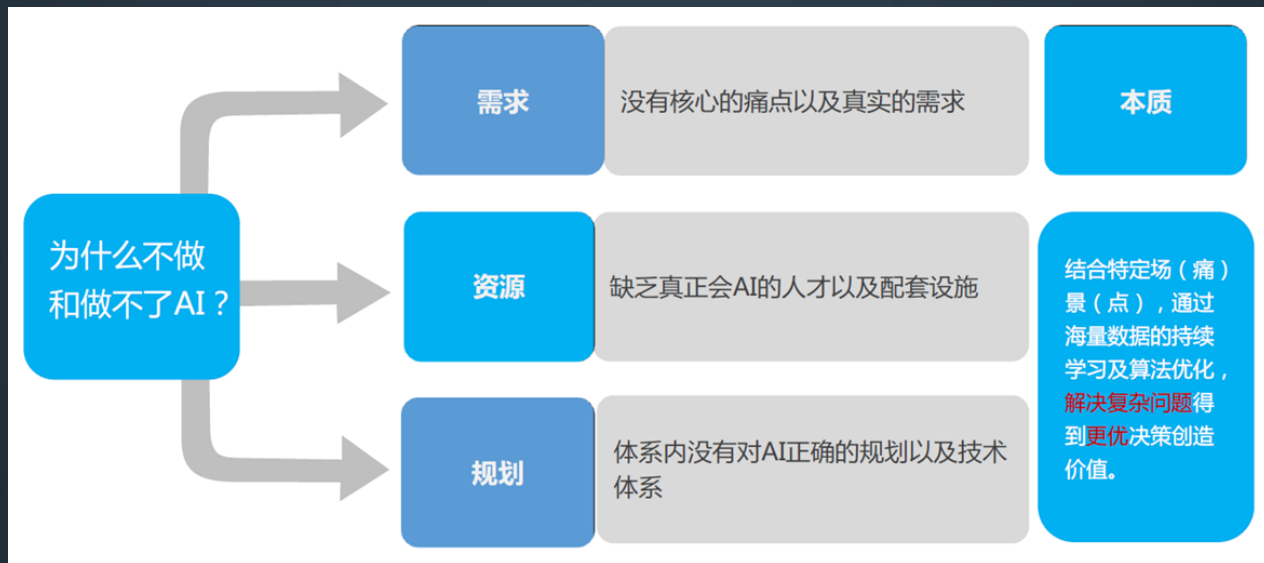
将运维质量的标准，从保证系统“活着”，升级为
确保系统始终运行在**最佳状态**。

合规 -> 敏捷

将用户的运维管理，从满足流程要求的合规管理，升级为以
事件响应为特点的**敏捷管理**。



AIOps：即Algorithmic IT Operations，是由Gartner定义的新类别，基于算法的IT运维。通俗来说，就是将人工智能数据科学和算法用于传统运维领域，基于已有的运维数据（日志、监控信息、应用信息等），通过机器学习的方式来进一步解决自动化运维所未能解决的问题，提高系统的智能化、稳定性、降低IT成本，并提高企业的竞争力。



科学规划、分阶段实现

NHTSA	L0	L1	L2	L3	L4	
SAE	L0	L1	L2	L3	L4	L5
	无自动化	驾驶支持	部分自动化	有条件自动化	高度自动化	完全自动化
功能	夜视 行人检测 交通标志识别 盲点检测 并线辅助 后排路口交通警报 车道偏离警告	自适应巡航驾驶系统 自动紧急制动 停车辅助系统 前向碰撞预警系统 车身电子稳定系统	车道保持辅助系统	拥挤辅助驾驶	停车场自动泊车	
特征	传感探测和决策警报	单一功能（以上之一）	组合功能（L1/L2组合）	特定条件 部分任务	特定条件 全部任务	全部条件 全部任务

一级

• 尝试应用：开始尝试应用AI能力，还无较成熟单点应用

二级

• 单点应用：具备单场景AI运维能力，初步形成供内部使用的学件

三级

• 串联应用：有由多个单场景AI运维模块串联起来的流程化AI运维能力

四级

• 能力完备：主要运维场景均已实现流程化免干预AI运维能力

五级

• 终极AIOPS：有中枢AI，可以在成本、质量、效率间从容不同生命周期对三个方面不同的指标要求，实现多目标下



02

全景业务服务管理



微信扫码收听演讲音频

IT业务服务管理—特点

监控的粒度细

01

04

易用性

面向业务管理

02

05

数据全面

面向用户管理

03

06

扩充性



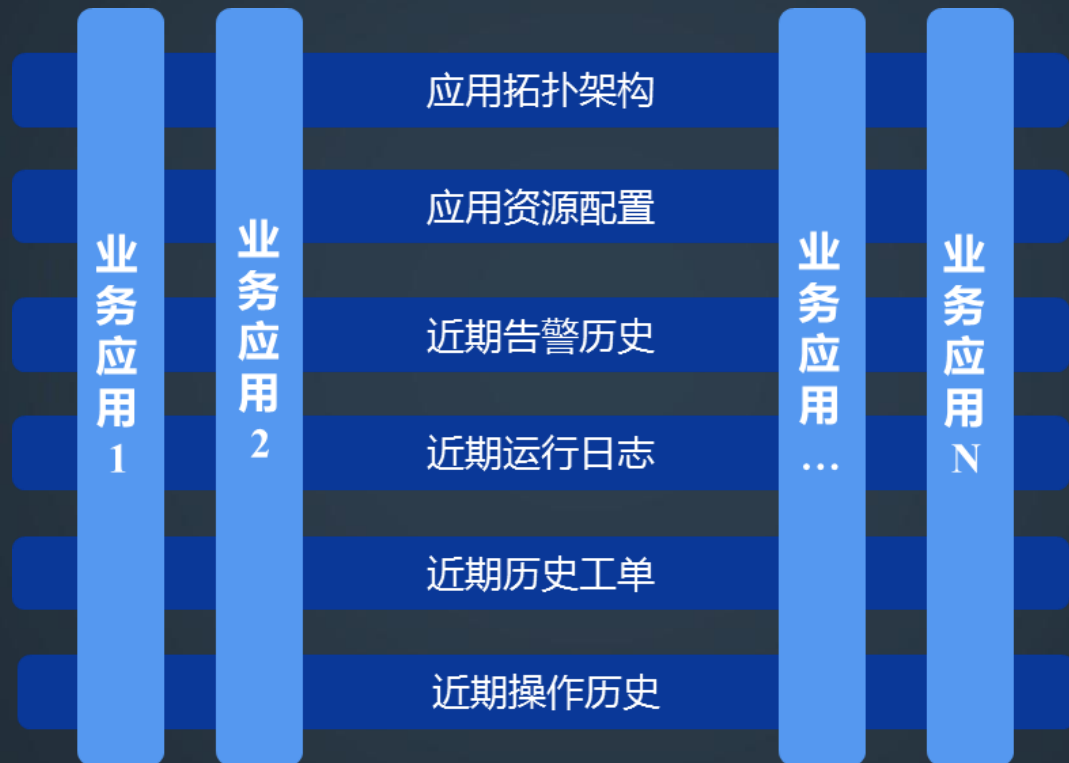
业务视角管理资源的视图



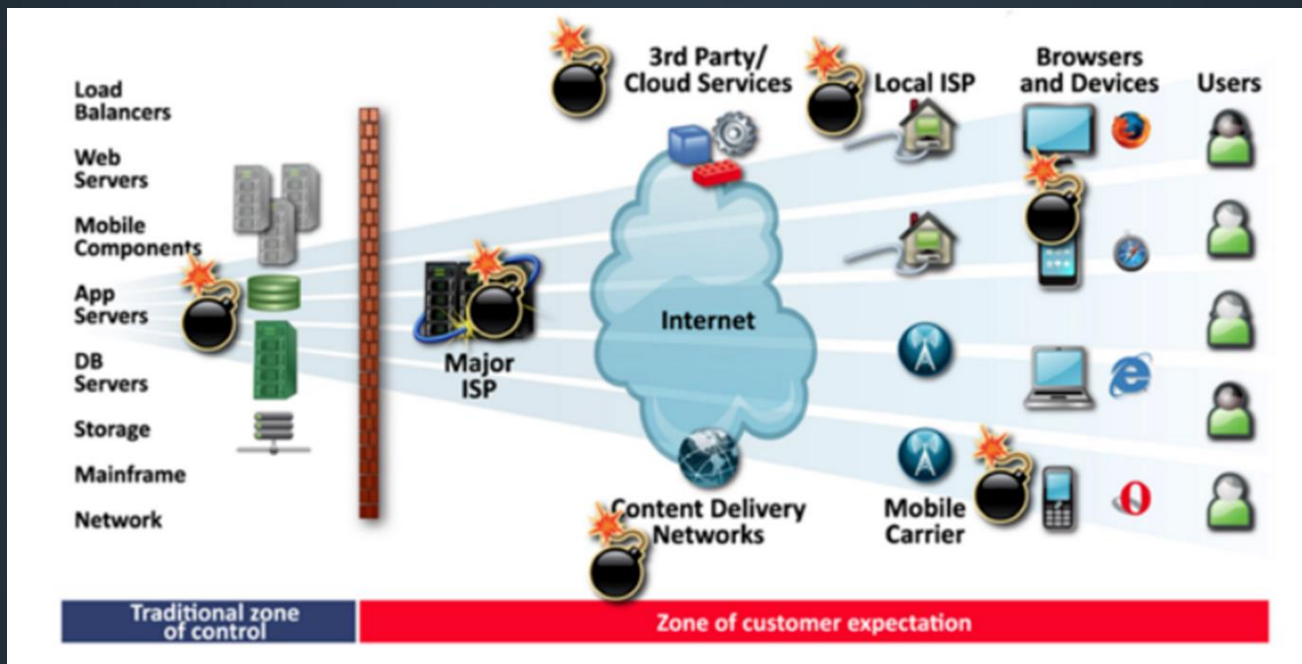
- 从业务的视角进行 IT 基础资源的管理与维护，一旦某个资源发生故障或者问题，都可以从业务视图中直观地了解到这个资源的故障将影响什么业务，影响哪些服务，进而了解到影响哪些用户。



业务视角的全方位分析



业务应用性能监控---发现瓶颈和故障



- 数据采集：
- 1、客户端：主动式探测和被动式监测
- 2、服务端：旁路监听和应用探针



几种技术的对比

位置	方式	技术	侵入式	竞品对标	网络问题定位	全样本	代码级定位	后端服务监控
客户端	主动	基于自动化测试的拨测	--	○	○	--	--	--
	被动	浏览器嵌码	○	--	--	○	--	--
		App嵌码	○	--	○	○	○	--
服务端	被动	旁路监听	--	--	○	○	--	○
		应用探针	○	--	--	○	○	○



业务问题整体诊断分析



03

大数据日志采集与监控告警



微信扫码收听演讲音频

基于大数据平台的日志采集分析

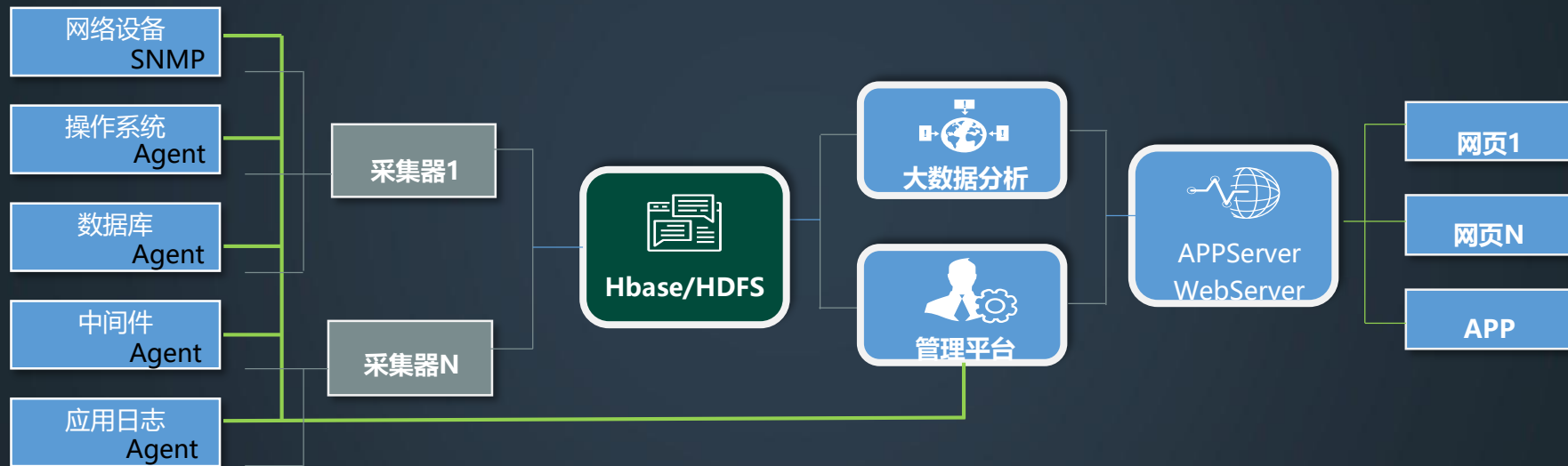
基于大数据平台，提供日志采集和聚合处理

日志关联分析帮助准确全面定位，提升效能和满意度

智能预测与预警，为精细管理，科学决策提供量化依据



各种日志的采集分析



跨层采集与监控

T1 设备层

对机房内的各种设备进行监控，如：交换机、路由器、安全设备、服务器、UPS、精密空调等，实现物理层的实时监控和数据采集。

T2 系统层

以系统作为单位，对数据中心的主机(Linux主机和X86服务器)、操作系统(LINUX/Winwdos)、数据库(Oracle、Mysql等主流)、中间件、存储系统、应用软件API、HTTP端口、备份系统、容灾系统、数据同步系统，虚拟化系统，云平台进行实时监控、预警分析和故障定位。

T3 业务层

在条件许可的情况下，采集一定的业务数据，如用户数、连接数、业务并发量、日志量等等，通过多维关联和分析，对未来的业务运行进行分析和预测。



整个数据中心范围内的配置变更跟踪

基础架构

- 操作系统和硬件
- DNS 和路由
- 文件级详细信息
- 物理网络
- 资源池
- 虚拟网络
- 快照详细信息
- 存储（SAN、NFS、分布式...）
- 高级功能（资源自动平衡...）
- 高级设置
- 安全配置文件
- 日志

运营

- 操作系统数据
- 硬件数据
- Cron 作业
- 设备驱动程序
- 存储（配额、空间、文件系统）
- 事件日志设置
- 文件系统
- 网络连接
- 流程
- 注册表
- 服务/导出服务
- 软件清单
- 系统启动
- 用户服务
- WMI

Active Directory 和安全性

- 帐户
- 组
- 帐户策略
- 审核策略
- 目录权限
- 目录审核设置
- 事件日志和 (ng) Syslog 配置与事件
- 补丁程序
- 注册表项权限
- 服务帐户
- 共享和权限
- 用户权限

应用

- Active Directory
- IIS
- SQL Server
- Exchange
- Oracle
- Apache
- Tomcat
- Redis
- Mysql
- mongodb



资产配置管理-CMDB的数据管理

关键动作：整合、调和、同步、映射和可视化

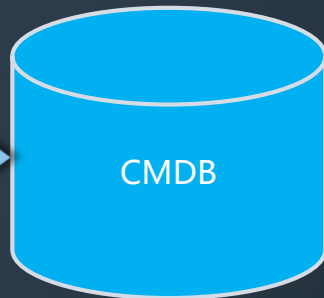


自动发现



录入、导入

数据处理

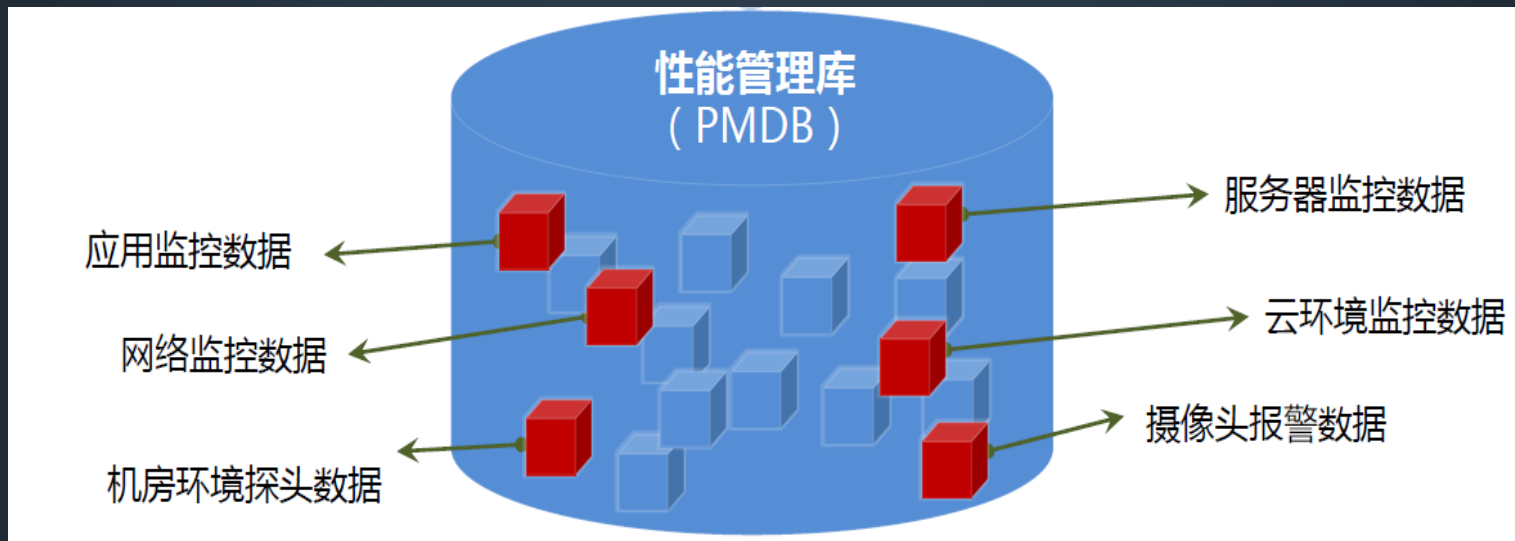


变更管理

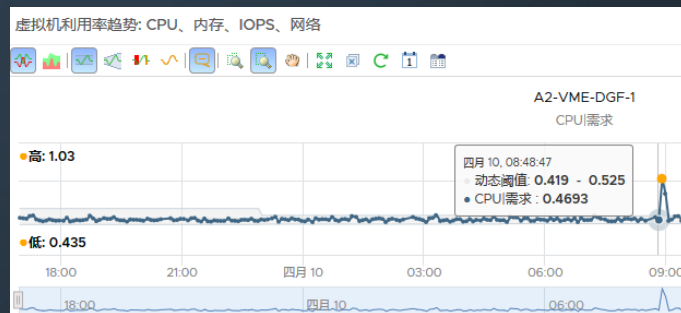
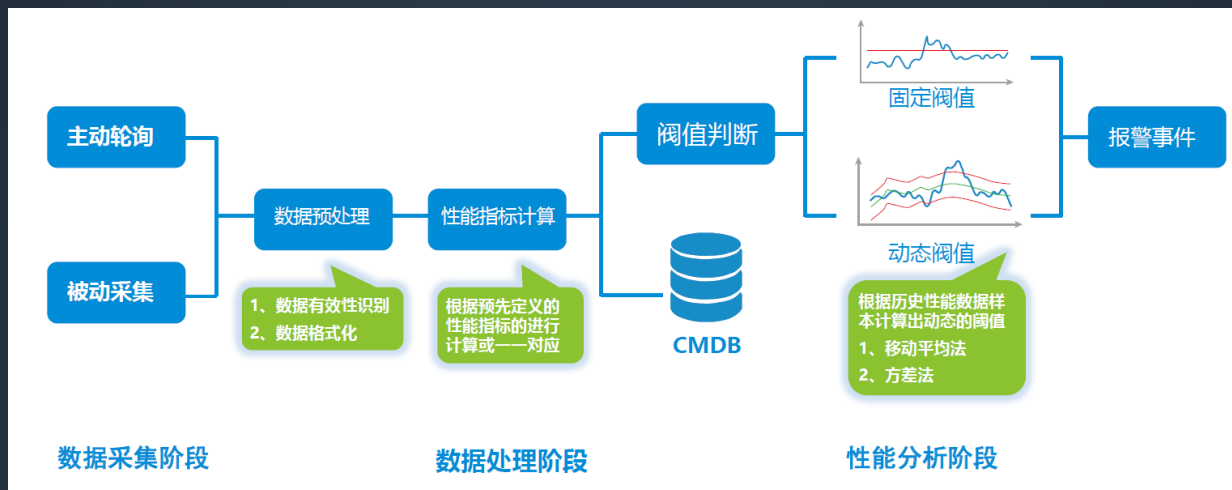


微信扫码收听演讲音频

数据大集中--PMDB



数据统一分析引擎和智能阈值



日志处理的几个问题

✦ 日志没有集中处理

- 登陆每一台服务器，使用脚本命令或程序查看

✦ 日志被删除

- 磁盘满了删日志
- 黑客删除日志，抹除入侵痕迹

✦ 日志只做事后追查

- 没有实时监控、分析

✦ 使用数据库存储日志

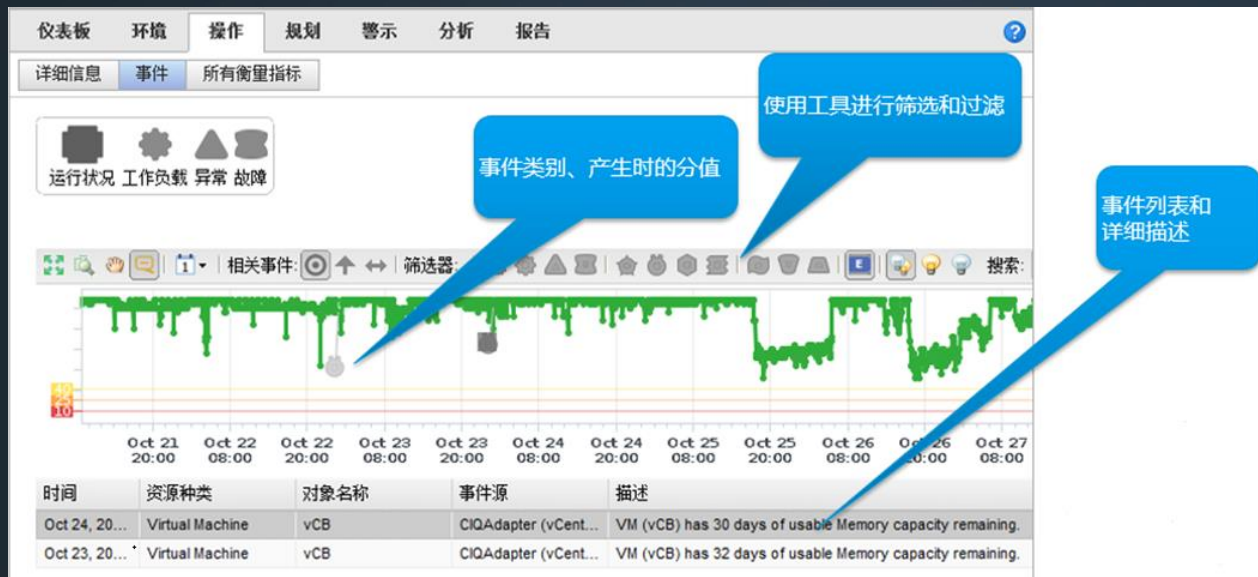
- 无法适应TB级海量日志
- 数据库的schema无法适应千变万化的日志格式
- 无法提供全文检索

The screenshot displays the Splunk Search & Reporting interface. At the top, the search bar contains the keyword 'mount'. Below the search bar, a summary bar indicates '32 个事件 (18/04/10 17:14:44.000 之前)' and '无事件采样'. The main results area shows a list of events with columns for '时间' (Time) and '事件' (Event). The events are filtered by 'source = alert_CP7PV1DB.log' and 'sourcetype = alert2'. The interface also includes a sidebar with filters for '隐藏字段' (Hidden Fields) and '感兴趣的字段' (Fields of Interest).

时间	事件
17/08/02 11:04:41.000	... 1 line omitted ... ALTER DATABASE MOUNT Successful mount of redo thread 1, with mount id 2058585929 Database mounted in Exclusive Mode Lost write protection disabled Completed: ALTER DATABASE MOUNT 显示所有 6 行 host = LAPTOP-GFN15LH2 ; source = alert_CP7PV1DB.log ; sourcetype = alert2
17/08/02 11:04:41.000	... 1 line omitted ... ALTER DATABASE MOUNT Successful mount of redo thread 1, with mount id 2058585929 Database mounted in Exclusive Mode Lost write protection disabled Completed: ALTER DATABASE MOUNT 显示所有 6 行 host = LAPTOP-GFN15LH2 ; source = alert_CP7PV1DB.log ; sourcetype = oraclealert
17/02/24 9:07:39.000	... 1 line omitted ... ALTER DATABASE MOUNT Successful mount of redo thread 1, with mount id 2044408539 Database mounted in Exclusive Mode Lost write protection disabled Completed: ALTER DATABASE MOUNT 显示所有 6 行 host = LAPTOP-GFN15LH2 ; source = alert_CP7PV1DB.log ; sourcetype = al
17/02/24 9:07:39.000	... 1 line omitted ... ALTER DATABASE MOUNT Successful mount of redo thread 1, with mount id 2044408539 Database mounted in Exclusive Mode Lost write protection disabled Completed: ALTER DATABASE MOUNT 显示所有 6 行



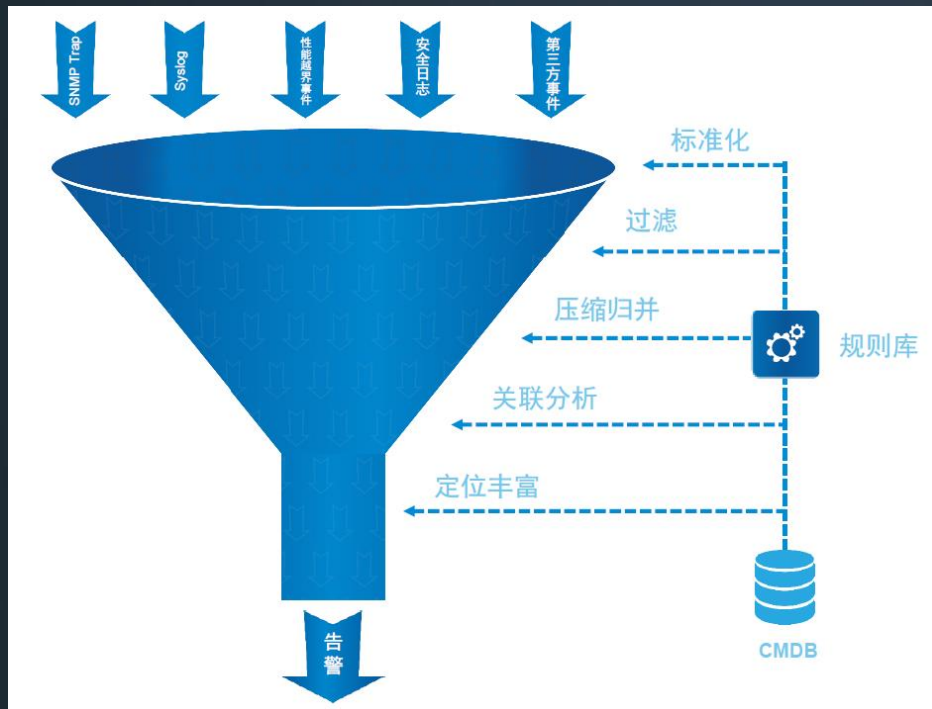
事件和时序关联分析



事件诊断一直是运维领域一个很重要的工作，事件和时序数据的相关性不仅可以为事件诊断提供很好的启发，而且在帮助进行根因分析等都能提供很好的线索。



数据汇聚处理：高性能事件分析引擎



- ◆ 高性能规则引擎
- ◆ 3600条事件/分
- ◆ 数据导入通道
- ◆ 全量HDFS
- ◆ 增量Kafka
- ◆ 数据分析的应用
- ◆ 开源算法的选择
- ◆ DataIDE
- ◆ 阿里云数加 (MaxCompute)
- ◆ StreamCompute



AIOps数据平台能力体系



04

知识库与故障自治管理



短信告警8000条/天

单人最高750条/天

邮件最多900封/天



如何从错综复杂的运维数据中形成知识库

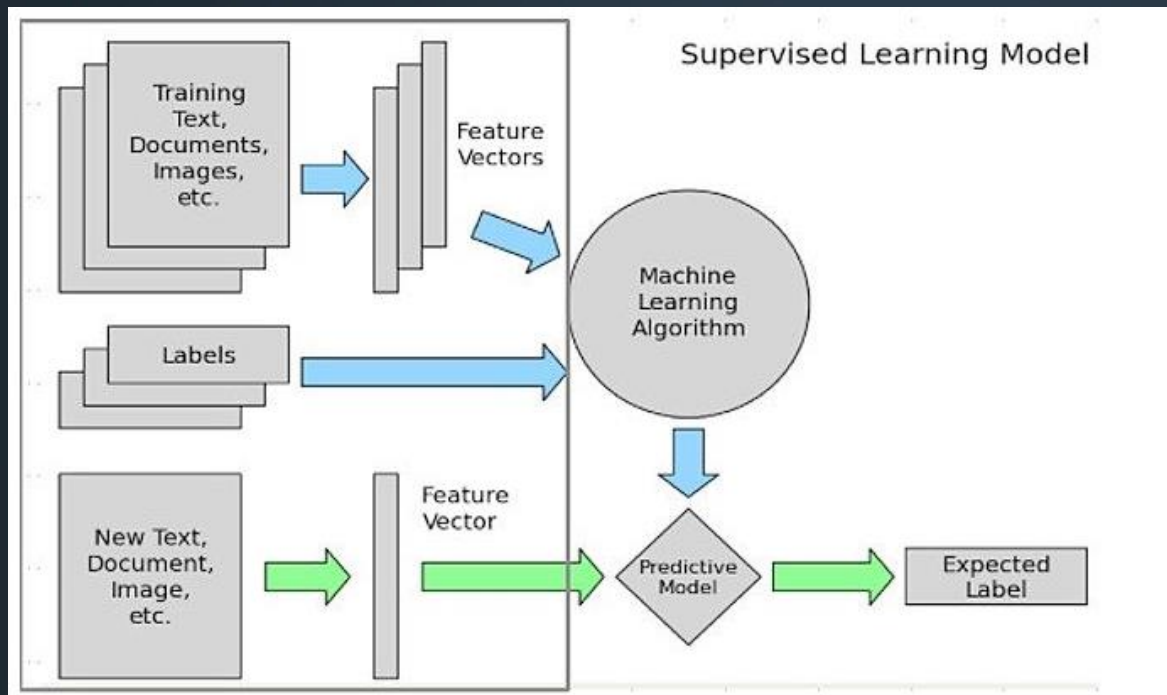


要实现的目标



IT运维管理化繁为简





◆ 数据

◆ 标注

◆ 工具

◆ 应用



策略知识库的构建 — 深

基于架构
基于经验
基于概率



收敛告警事件

基于规范
基于分工

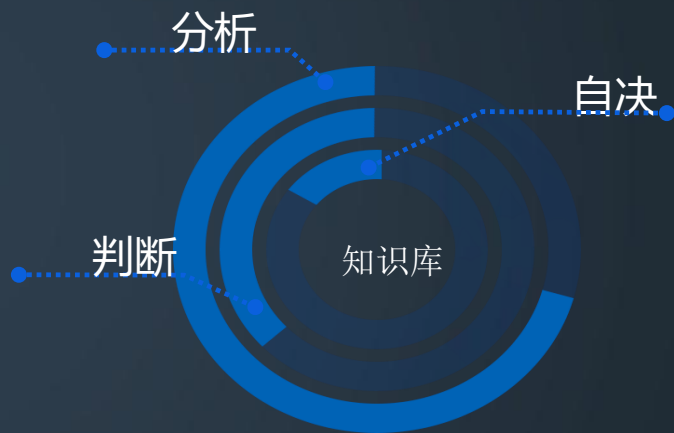


产生告警事件

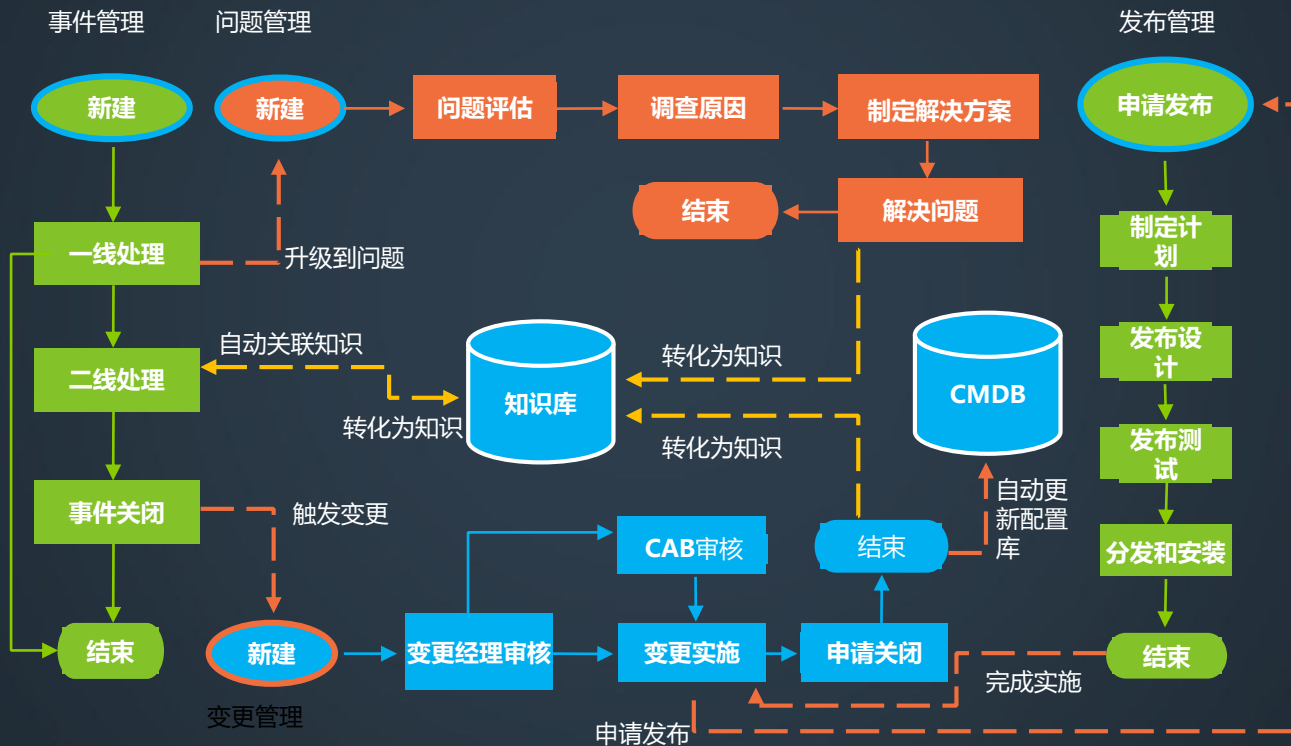
基于数据
基于模型



提高事件处理能力



企业内部知识库构建



AIOps的应用场景分析

效率提升方向

智能变更
智能问答
智能决策
容量预测

质量保障方向

异常检测
故障诊断
故障预测
故障自愈

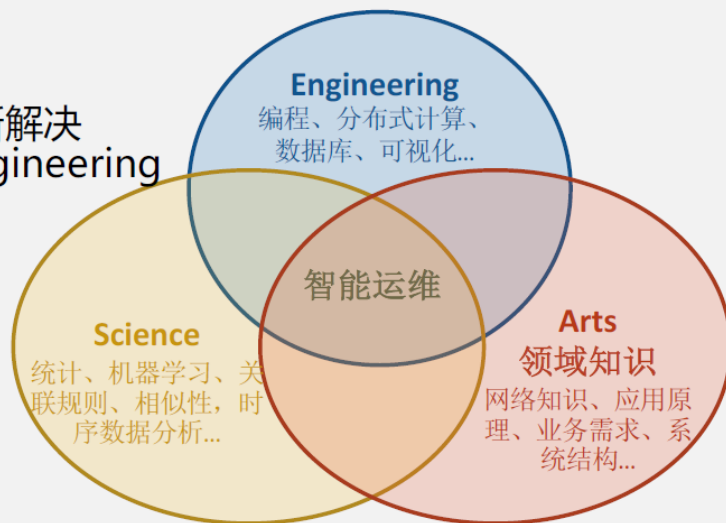
成本管理方向

成本优化
资源优化
容量规划
性能优化



减少对人的依赖，信任机器，实现自判自断自决

技术正在逐渐解决
Science+Engineering
的问题



技术可能永远也无法代替领域专家（艺术家），但是可以为领域专家提供更好的工具

智能运维的终极可行目标:


1. 日常工作都能自动完成
2. 运维人员能够独立进行数据分析




感谢观看

Thank you for watching

 xjsunjie@126.com

 hopexjlg

 北京



微信扫码收听演讲音频