# AIOps

1. 数据源
   1. 日志：K-V的半结构化文本信息，可以用列簇式数据模型管理
      1. 网络日志
      2. 系统日志
      3. 应用程序日志
   2. 数据库数据：一般通过关系型数据表进行存储，也可以用于关联查询
      1. 系统的事务处理
      2. 分析型数据仓库中存储的各种信息
   3. 配置信息：K-V键值对或可嵌套的键值文档类数据，可以通过结构化文档数据模型管理
      1. 软件配置
      2. 用户信息
      3. 参数状态
   4. 拓扑和跟踪：复杂网络上的关系信息，可以通过图数据模型管理
      1. 软硬件系统的物理、逻辑关系
      2. 应用程序的调用关系
      3. 数据流向关系
   5. 监控指标：时序型数据，可以通过时序型数据模型管理
      1. 系统指标
      2. 应用指标
      3. 业务指标
   6. 其他信息
      1. API数据
      2. 客户关系数据
      3. ITSM流程数据
      4. 社交媒体数据
2. 主要功能点
   1. 告警消噪
      1. 目标
         1. 告警合并
         2. 告警抑制、告警收敛
      2. 方法
         1. 时序数据的聚类与分类
         2. 节假日误告消噪
         3. 基于NLP的告警日志简化
         4. 告警日志聚类
   2. 根因分析：事后的定位
      1. 目标
         1. 跨系统追踪和关联分析
         2. 分析故障的根本原因
      2. 方法
         1. 基于可解释、有监督机器学习的归因
            1. 决策树等（实践）
            2. CNN等（学术）
         2. 基于无监督的异常检测
            1. 基于能量或信息量最小化的归因（Boltzman机）
            2. 基于条件概率模型的归因
         3. 基于知识的故障分析
            1. 故障树分析
            2. 故障知识图谱
         4. 基于图的故障传播分析
            1. 图随机游走
            2. 图排序

基于时序行为异常关联TBAC

基于距离排名DBR

* + - * 1. 状态迭代
  1. 异常检测：事前的预测
     1. 目标
        1. 发现异常指标
        2. 发现网络中的异常节点、边、子图
        3. 事件(event)或突变(change)检测
     2. 方法
        1. 截面数据异常检测（静态异常指标）
           1. 基于密度或分布估计方法

典型性和离心率数据分析TEDA

核密度估计

递归密度估计RDE

* + - * 1. 基于信息量的方法

多项式相对熵MRE

* + - 1. 时间序列异常检测（动态异常指标）
         1. 异常分类

空间异常

明显偏离历史异常记录

上下文异常（条件异常）

细微的异常，通常发生在特定的时序上下文中，本身取值可能在正常范围内

概念漂移

该观测点之后数据的统计特征发生了变化或偏移

* + - * 1. 方法

基于时间序列建模残差：ARMA等

基于统计分布模型的距离异常检测，核密度估计，k维树等

基于贝叶斯法则的参数变化检验

贝叶斯在线突变点检验

随机过程(？)

RNNs，LSTM，分层时序记忆网络HTM等

* + - 1. 基于静态图的异常检测（异常节点、边、子图）
         1. 基于社区检测的方法
         2. 基于压缩的方法
         3. 基于矩阵分解的方法
         4. 基于概率模型的方法
         5. 基于表示学习的方法
      2. 基于动态图的异常检测（异常节点、边、子图、事件、突变）
         1. 基于社区检测的方法

异常顶点检测

异常子图检测

突变检测

* + - * 1. 基于压缩的方法

异常边检测

突变检测

* + - * 1. 矩阵或张量分解方法

异常顶点检测

事件检测

突变检测

* + - * 1. 基于距离测度的方法

异常边检测

异常子图检测

事件检测

* + - * 1. 基于概率模型的方法

异常顶点检测

异常边检测

异常子图检测

事件检测

* 1. 故障运维知识图谱
     1. 目标
        1. 累计运维专家经验
        2. 实现知识融合的告警消噪、异常检测、根因分析
  2. 指标统一监控
     1. 目标
        1. 在已知故障传播路径的条件下，选择有限的监控指标和节点，实现特定目标下的系统监控
        2. 去阈值或动态阈值
     2. 方法
        1. outbreak detection
        2. 基于统计量的统一去阈值管理
        3. 动态阈值策略

1. 市场
   1. IBM、BMC、ITOM
      1. 传统IT场景下的IT资源管理、IT服务管理、IT 自动化等需求，
      2. 针对的用户群体也是以L1/L2级运维工程师为主
   2. Moogsoft、Splunk、Cloudwise
      1. 适合数字化和混合IT场景
   3. 灵犀
      1. 数据增强
         1. **数据汇聚：**首先我们需要把摄入的数据能够汇集到统一的位置，保证能够通过统一的方式能够在需要时访问到。
         2. **数据过滤：**缺失值填充、字段过滤、事件去重、告警降噪、规则引擎等多种预制处理单元和自定义过滤接口可以有效提升数据过滤的效率
         3. **数据规范化：**数据规范化确保从许多不同来源收集的数据能被置于统一的格式，然后允许各种算法模型使用AI 来关联这些数据
         4. **数据充实：**数据充实的定义是将第三方数据与现有的第一方数据数据进行关联和合并。
         5. **数据分类：**最后，为了给各种机器学习和人工智能算法做好数据准备，AIOps数据平台还需要提供完成特征工程的能力。
      2. 事件关联
         1. **基于时间的相关性分析：**通过检查事件之前或与事件同时发生的事情来寻找事件的时间和顺序的关系。
         2. **基于规则的相关性分析：**将事件与具有特定变量值的规则进行比较，如交易类型或客户城市。
         3. **基于模式的相关性分析：**结合了基于时间和基于规则的技术，不需要为每个变量确定取值，而是允许足够的不确定性，只寻找符合定义模式的事件。
         4. **基于拓扑结构的相关性分析：**这种方法基于网络拓扑结构，构建软硬件的物理和逻辑知识图谱，如服务器、集线器、网络上的节点，以及对它们如何相互连接的理解。
         5. **基于特定领域的相关性分析：**这种方法从专注于 IT 运营的某一方面（例如网络性能、应用性能和计算基础设施）的监控系统中获取事件数据，并将事件关联起来。
         6. **基于历史的相关性分析：**将新事件与历史事件进行比较，看它们是否匹配。
         7. **基于编码簿相关性分析：**将事件和告警编码为一个庞大的矩阵，并将事件映射到告警。
   4. 必示、擎创、云智慧、擎创、听云、华为
   5. 微众
      1. 异常发现
         1. 定义业务黄金指标（交易量、业务成功率、系统成功率、单位时间交易平均耗时）
            1. 识图：对微众银行“关键产品黄金生命指标曲线”进行自动检测，无需人工设置阀值，系统自己计算阀值区间，自动告警

基于LSTM与高斯分布的检测，这个算法主要用于交易量和时延的检测。大部分的曲线突变都能准确检测到，但算法的死角在于小幅度长时间的缓慢变化容易被漏掉。

基于k-means算法的特征检测，主要用于填补第一种算法的盲区,在交易量缓慢变化的案例效果较好。

基于概率密度的检测，主要用于业务成功率和系统成功率的曲线，因为成功率曲线的背后隐藏着无数的可能，需要用一个更接近本质的量来衡量异常的程度。

* + - 1. 对黄金指标进行算法结合规则的检测
         1. Knowing: 曝光交易路径，将服务治理的数据旁路出一份，根据业务流水号，时间点将各条零散的数据组成交易树，对交易树进行实时检测并针对中断情况进行告警

获取需要处理的流水号对应的原始消息列表

将原始消息转化为消息对

消息对转化为树节点

树节点转化为链路

合并链路生成交易树

* + 1. 根因分析
       1. 消息总线的消息日志为基础，基于算法生成交易链路
       2. 异常时绘制故障交易链路图
       3. 定位中断子系统，然后以中断子系统为圆心，使用知识图谱算法发散式根因挖掘
       4. 历史异常事件的数据也导入知识图谱，修正知识图谱中的专家经验
       5. 从运维管理的角度进行异常识别和根因定位标记，不断迭代修订基础模型数据
  1. 百度
     1. 监控报警
        1. 从两个方面进行了合并，按部署架构合并和跨部署架构的合并
        2. 按部署架构合并主要基于配置管理系统的基础关联关系
        3. 跨部署架构合并则依赖上下游关系和离线的策略挖掘
     2. 异常检测
        1. 实现了算法和模型分离
        2. 迭代周期从月缩短到日
        3. 验证算法策略的平台分为了离线环境、近线环境、在线环境，使算法在一个可靠的数据环境中验证。
  2. 美团
     1. Alfred
        1. 故障发现-Horae（美团服务运维部与交易系统平台部共建项目）
        2. 告警触达-告警中心
        3. 故障定位-雷达
        4. 故障恢复-雷达预案
     2. 即时物流业务的AIOps
        1. 容量评估
        2. 弹性设计
        3. 故障诊断
           1. 故障检测
           2. 根因分析
           3. 故障收敛
           4. 链路监控
           5. 故障拓扑展示
           6. 告警升级
           7. 对故障进行相对完整的标记、运营、管理、跟踪
        4. 风险防范
        5. 应用
           1. 端到端链路监控
           2. 失败率监控的动态阀值
  3. 腾讯
     1. 主要场景
        1. 内存存储智能降冷
           1. 痛点：社交网络业务，用户规模大，又有大量的访问，这样就导致团队喜欢用内存型的KV存储。上线的时候，请求量可能很高，但是随着时间的推移，他的数据量不断地增长，访问密度反而在下降，对的成本造成很大的压力。
           2. 方案：特征抽取-->基于机器学习进行降冷条目预测
           3. 效果：数据进行了一个下沉，把接近 90% 的数据，下沉到硬盘上，我们的访问量并没有下降，SS D数据没有造成访问压力，可以看到下沉和下降是非常精准的。而且这里面的数据延迟和成功率几乎没有变化
        2. 统一监控去阈值
           1. 痛点：监控有两种情况，一种是成功率的监控，它应该是一个直线，正常应该在 100% 左右，但它会往下掉。第二个就是类似于一个累计性的曲线，或者 CPU 的曲线，这个曲线监控其实是非常的千变万化的。如何设置统一监控，减少人工阈值
           2. 方案

成功率监控：基于3sigma原则筛选初始样本-->孤立森林等筛选异常样本-->规则筛选

曲线监控：区间采样的3igma原则筛选初始样本-->统计判别异常样本-->多项式拟合-->孤立森林等筛选异常样本-->人工标准，训练模型实现自动筛选

* + - 1. ROOT智能根源异常分析
         1. 痛点：原先的方案是基于规则的

先降维关系

然后列出统一模块的所有路径

把告警出现叠加在模块上

设置一个人为定义的面积算法

从面积的大小，就判定哪个模块是异常的根源

* + - * 1. 方案：Apriori频繁项集+皮尔逊相关系数定位根源告警
      1. 织云全自动扩容
         1. 方案:核心是平衡木模块，使得所有设备的负载趋于一致
      2. 多维下钻智能分析
      3. 频繁项集关联告警智能分析
      4. 变更体检智能机报告
      5. 操作工具智能客服