# 告警功能调研

## 告警的作用

告警是运维工作最重要的一个信息数据，运维人员更新告警去响应处理对应的故障点，是整个运维流程中的吹哨者。

## **告警的需求**

用户对告警的需求无非就两个字快、准

从告警时序上来分析：主要可分为事前告警、事中告警、事后告警

事前告警一般为 预测类告警，主要由AI基于历史指标数据分析出预测告警事件

事中/事后告警主要为 对已发生的指标做阈值判定是否为告警。而阈值判断方法有N多种，在此不做详细深入

## **告警来源**

告警来源分为内部产生和外部接入

外部接入：主要指第三方运维或业务系统产生的告警接入进来

## **告警痛点**

海量告警无法确定哪种有用，哪种无用，是否需要重复告警。

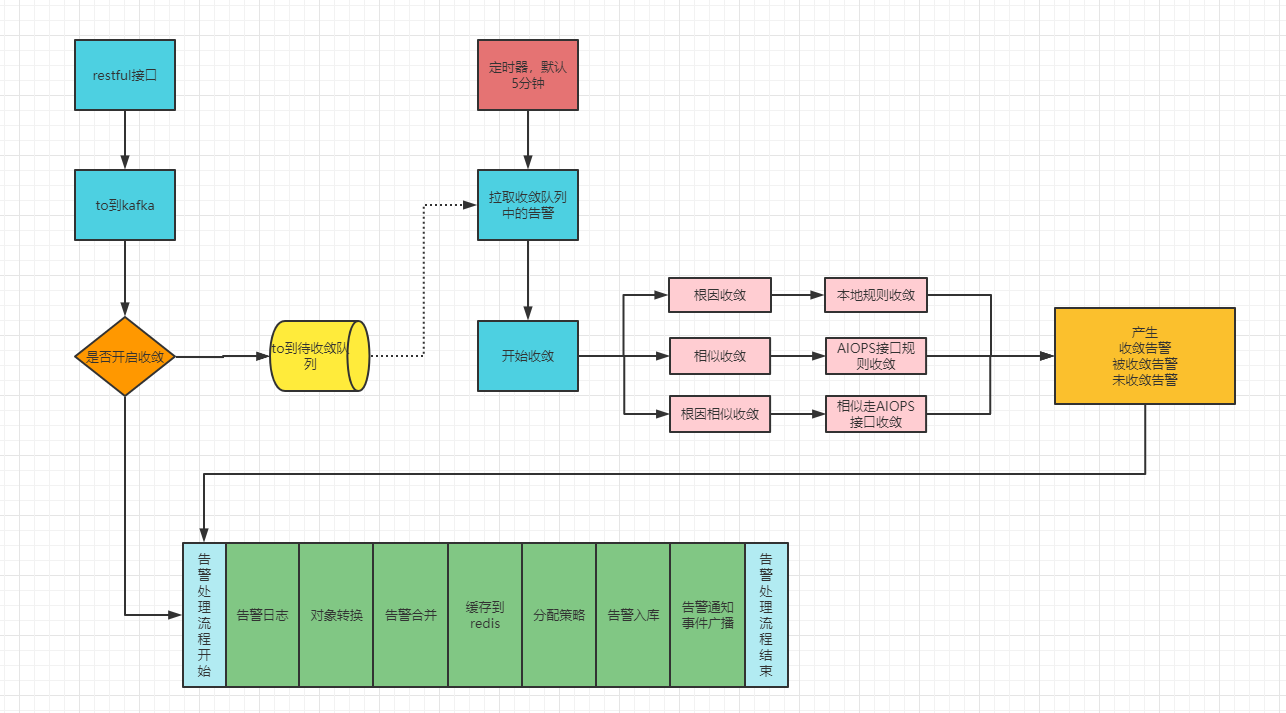
告警风暴

告警抑制

告警升级

## **当前告警收敛缺陷及优化方案**

当前收敛的流程图



收敛流程弊端。

1. 收敛延时滞后。影响告警快速提醒。且告警收敛效果与告警延时互斥。虽然我们有多间隔。
2. 收敛策略不能编排。当前收敛策略是固定的，先按相似收敛，没有相似走根因。
3. 相似收敛走AIOPS接口引响收敛效率。可将相似收敛规则同步至本地直接走本地规则收敛，类似根因收敛规则。

收敛规则弊端

相似收敛：当前相似是根据模板相似收敛。导致对告警内容要求过高

面对海量的告警，所以将告警进行收敛，只报告紧急的、严重的告警。

所以基于一些专家设定的规则、或AI分析出规则进行收敛

指标相似性规则

文本相似性规则

根因规则

完全相同规则(合并)

调用链关系收敛

amdb拓扑结构收敛

优先及规则

以上内容参考或引用

少年，你的告警量可以更少些！

<https://cloud.tencent.com/developer/article/1004636>

告警平台设计及告警收敛通用解决方案

<https://www.sohu.com/a/465035422_494937>

腾迅万亿告警是如何做到全、准、快的

http://www.360doc.com/content/17/0819/17/34701069\_680430317.shtml