易宝集团
YEEPAY GROUP

基于ELK的智能监控

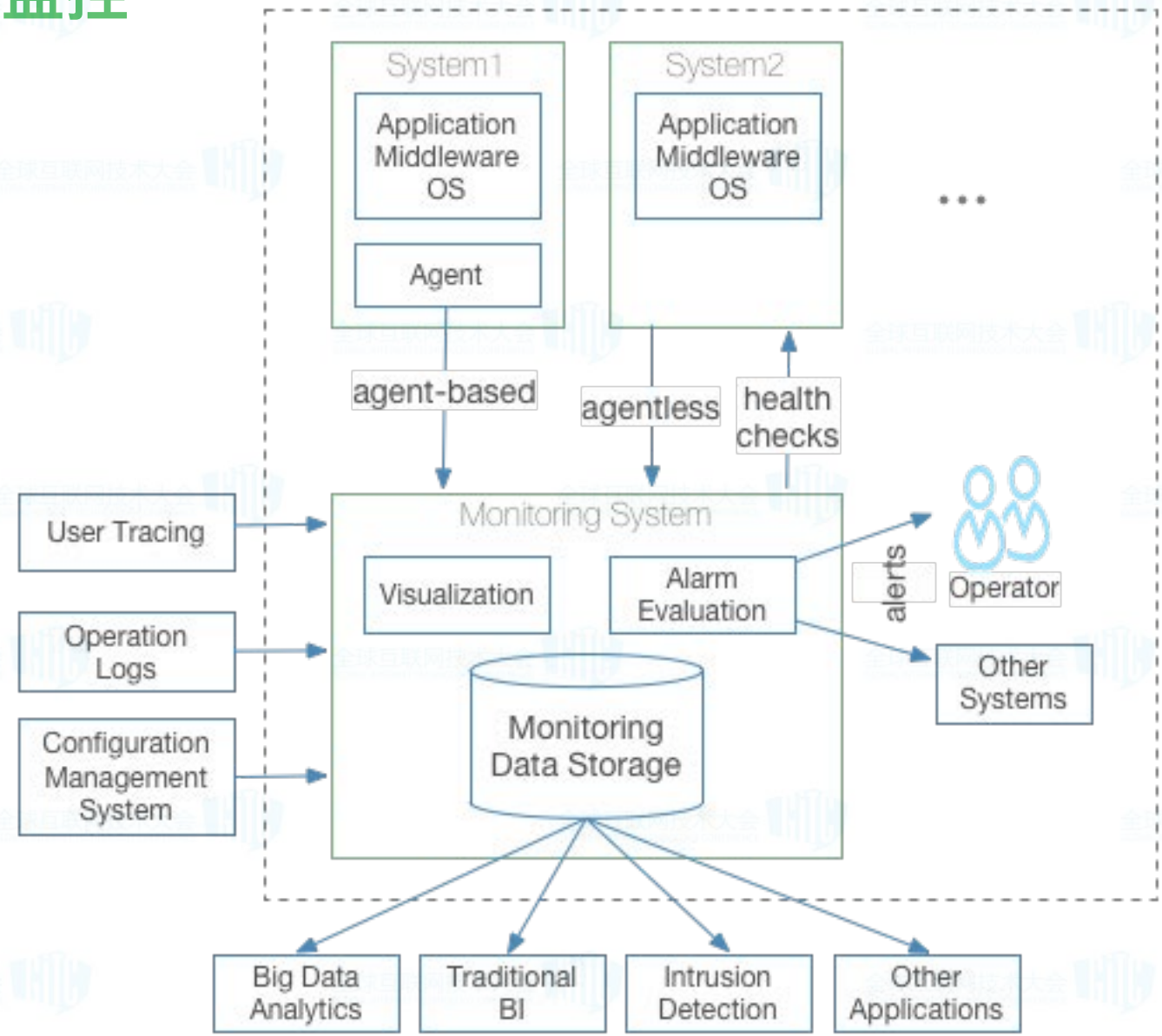
刘　斌

2016.11.24

项目背景

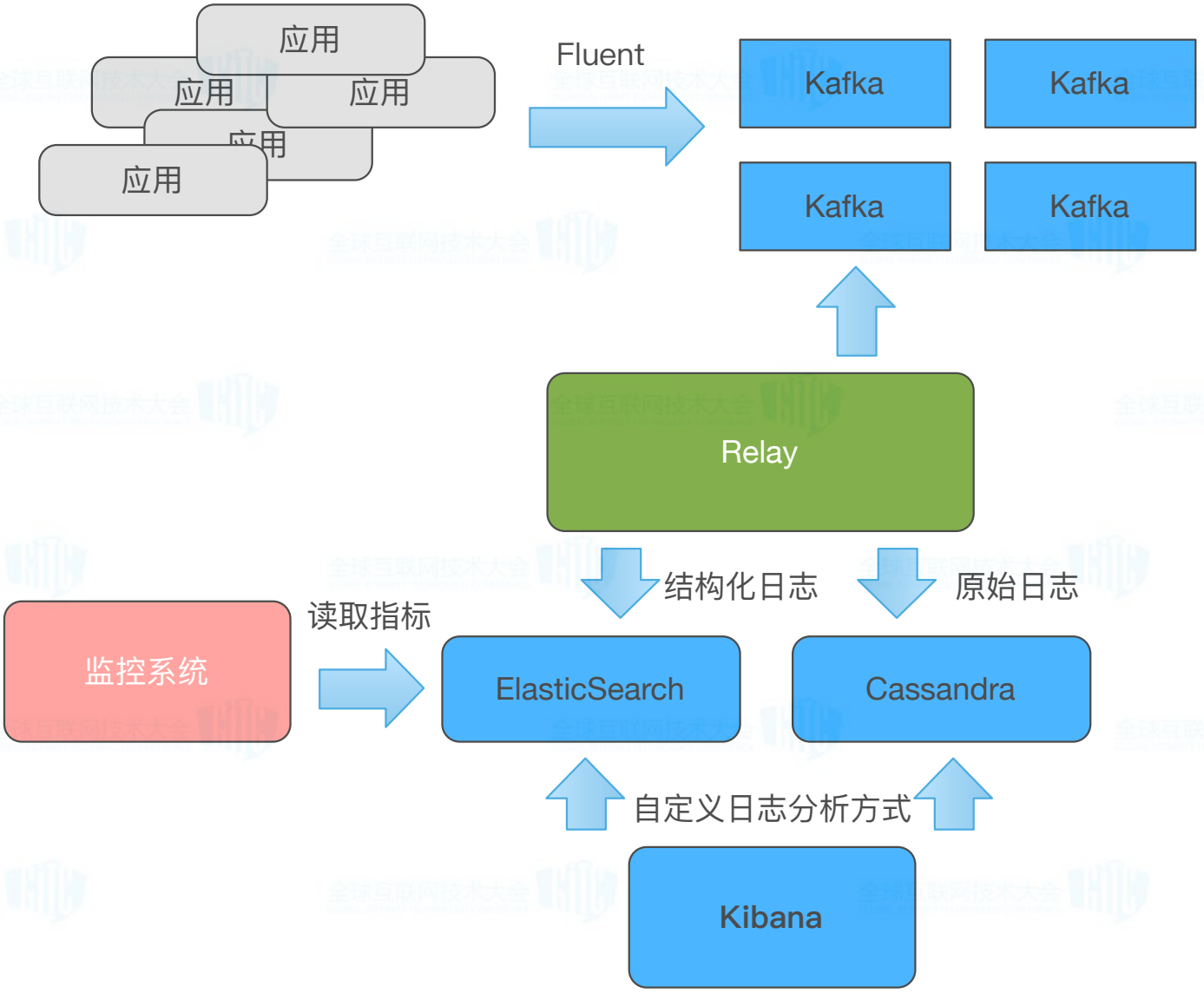
- 原有监控指标分散、相互割裂
- 产品运营和开发人员无法参与到监控数据的分析和规则的设定（DevOps）
- 正在建设日志中心（Centralized Logging），需要实际的应用来展现日志中心的能力

关于监控



图片来自《DevOps, A software Architect's Perspective》

基于ELK的实现


应用
应用
应用
应用
Fluent
Kafka
Kafka
Kafka
Kafka
Relay
结构化日志
原始日志
监控系统
读取指标
ElasticSearch
Cassandra
自定义日志分析方式
Kibana

期望的使用方式

易宝集团 YEEPAY GROUP

提取所需的日志

配置图形

生成监控指标

配置报警规则

将所配图形组合到一个仪表盘中，对比查看

Kibana与监控系统互通

将filter或filter的一部分用通配符替换

Query Search

```
{"index":"nopay-monitor-*","query":{"query_string":{"query":"*","analyze_wildcard":true}},
"filter":[],"size":0}
```

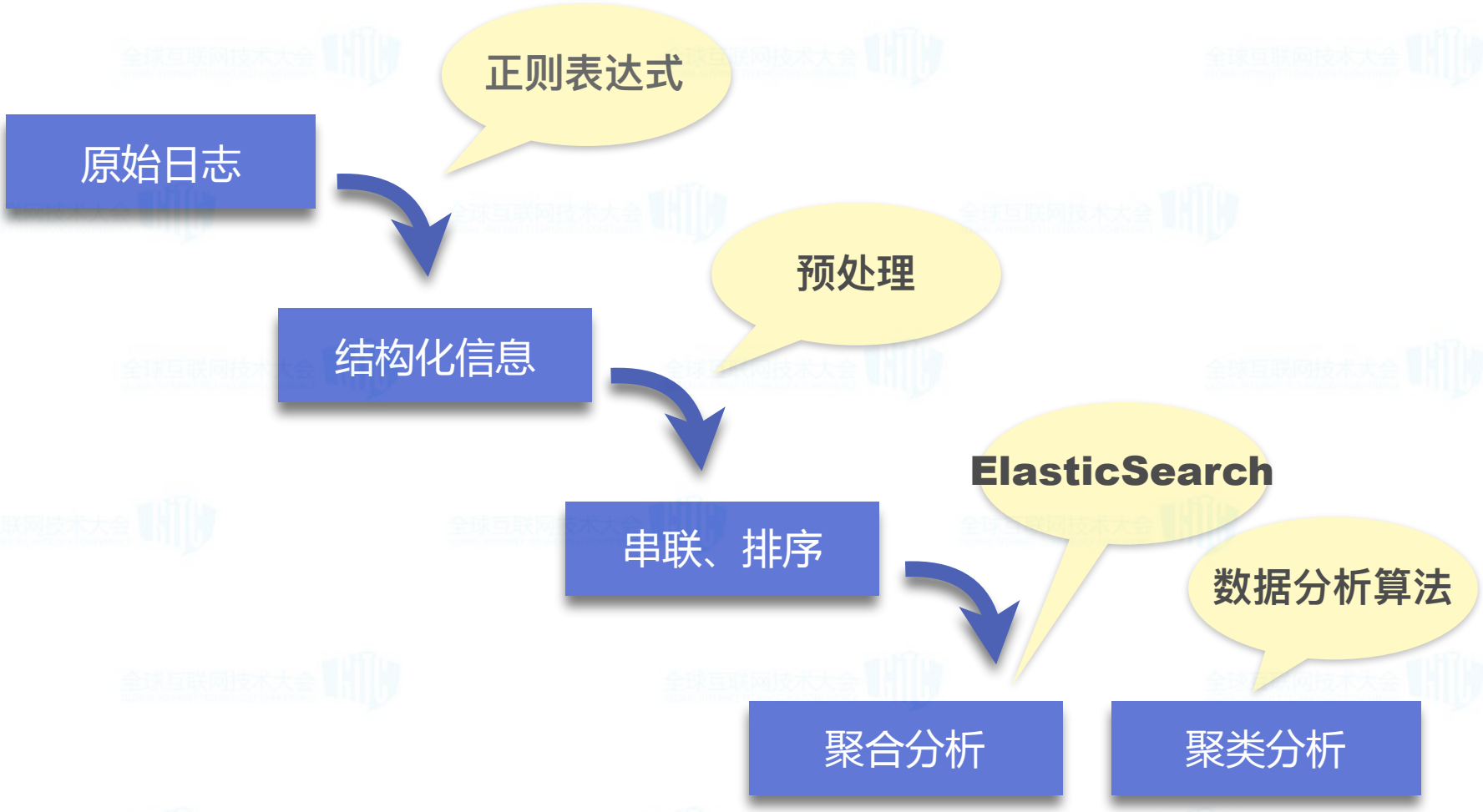
visState

```
[{"id":"1","type":"sum","schema":"metric","params":{"field":"isReq"}},
{"id":"2","type":"sum","schema":"metric","params":{"field":"realSuccess"}},
{"id":"3","type":"date_histogram","schema":"segment",.....
```

aggDSL

```
{"3":{"date_histogram":{"field":"TIME","interval":"1m","pre_zone":"+08:00",
"pre_zone_adjust_large_interval":true,"min_doc_count":1,
"extended_bounds":{"min":1452130064252,"max":1452133664252}},
"aggs":{"4":{"filters":{"filters":{"eventType:\"bankChannelSuccess\" AND customerNumber:\"@@\"
AND bankCode:\"HX\"":{"query":{"query_string":{"query":"eventType:\"bankChannelSuccess\"
AND customerNumber:\"@@\" AND bankCode:\"HX\"",
"analyze_wildcard":true}}}}},"aggs":{"1":{"sum":{"field":"isReq"}},
```

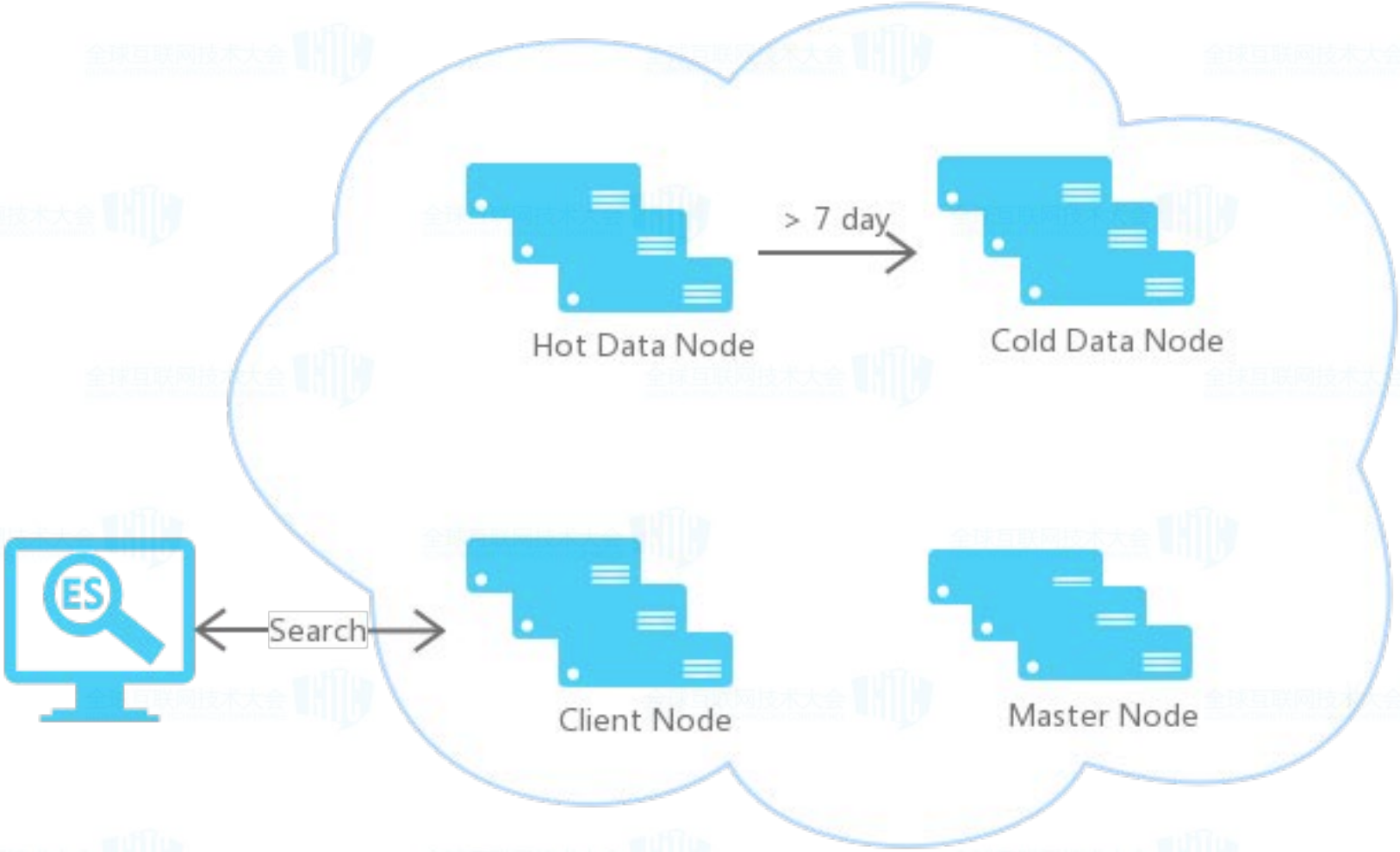
自主分析



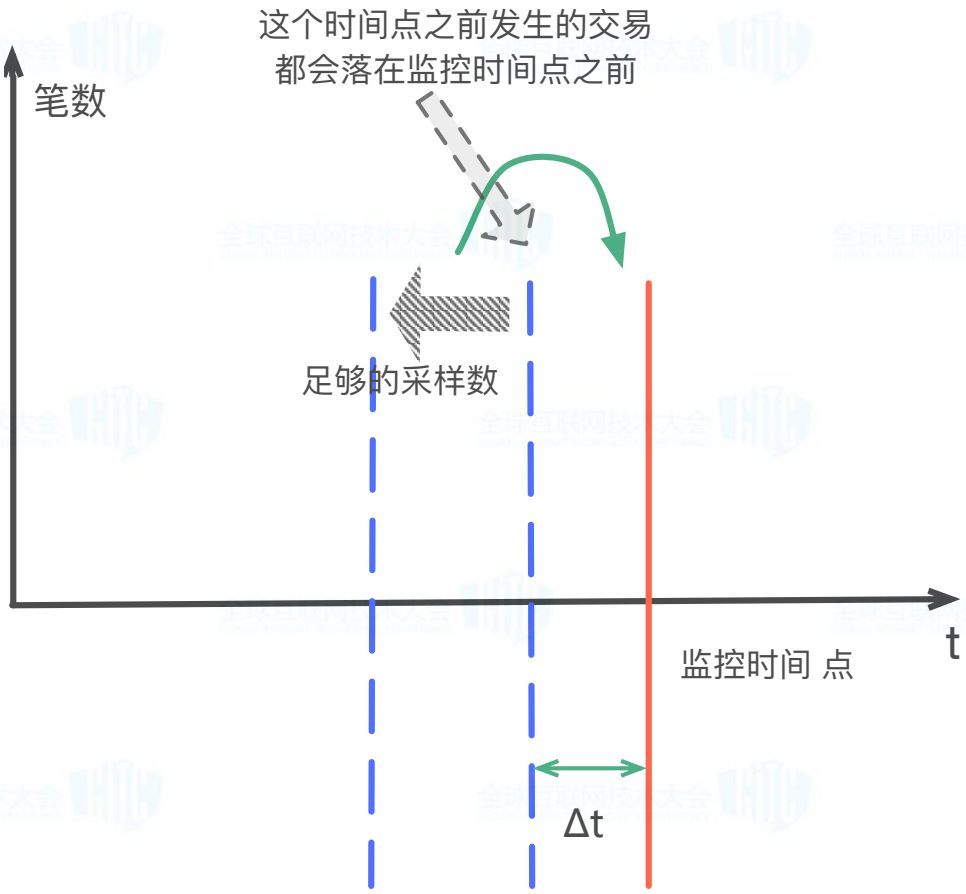
稳定的日志同步-I


同步
网关
kafka队列
kafka队列
kafka队列
Fluent4j
Fluent4j
Fluent4j
横向扩展

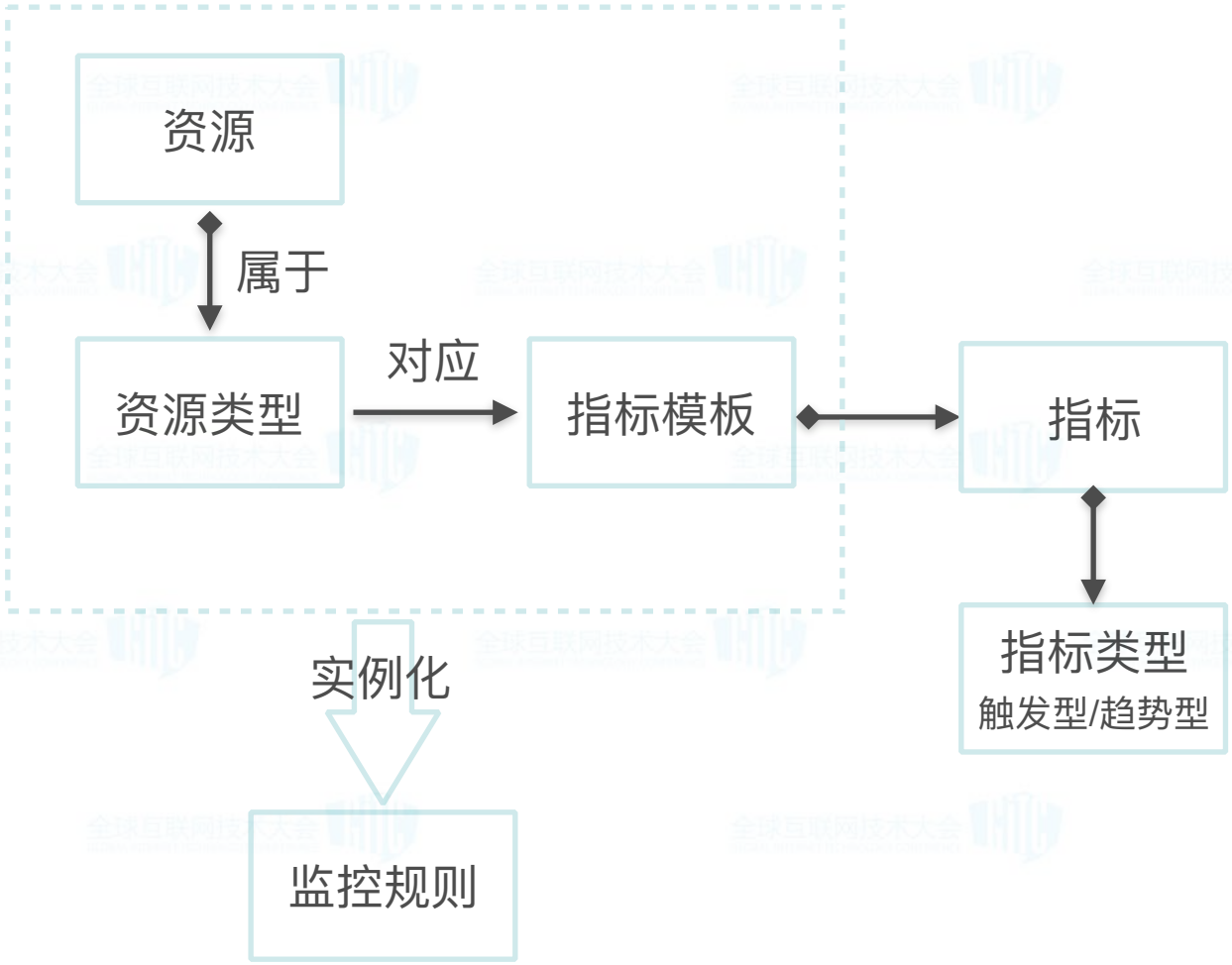
稳定的日志同步-II


> 7 day
Hot Data Node
Cold Data Node
ES
Search
Client Node
Master Node

业务事件串联



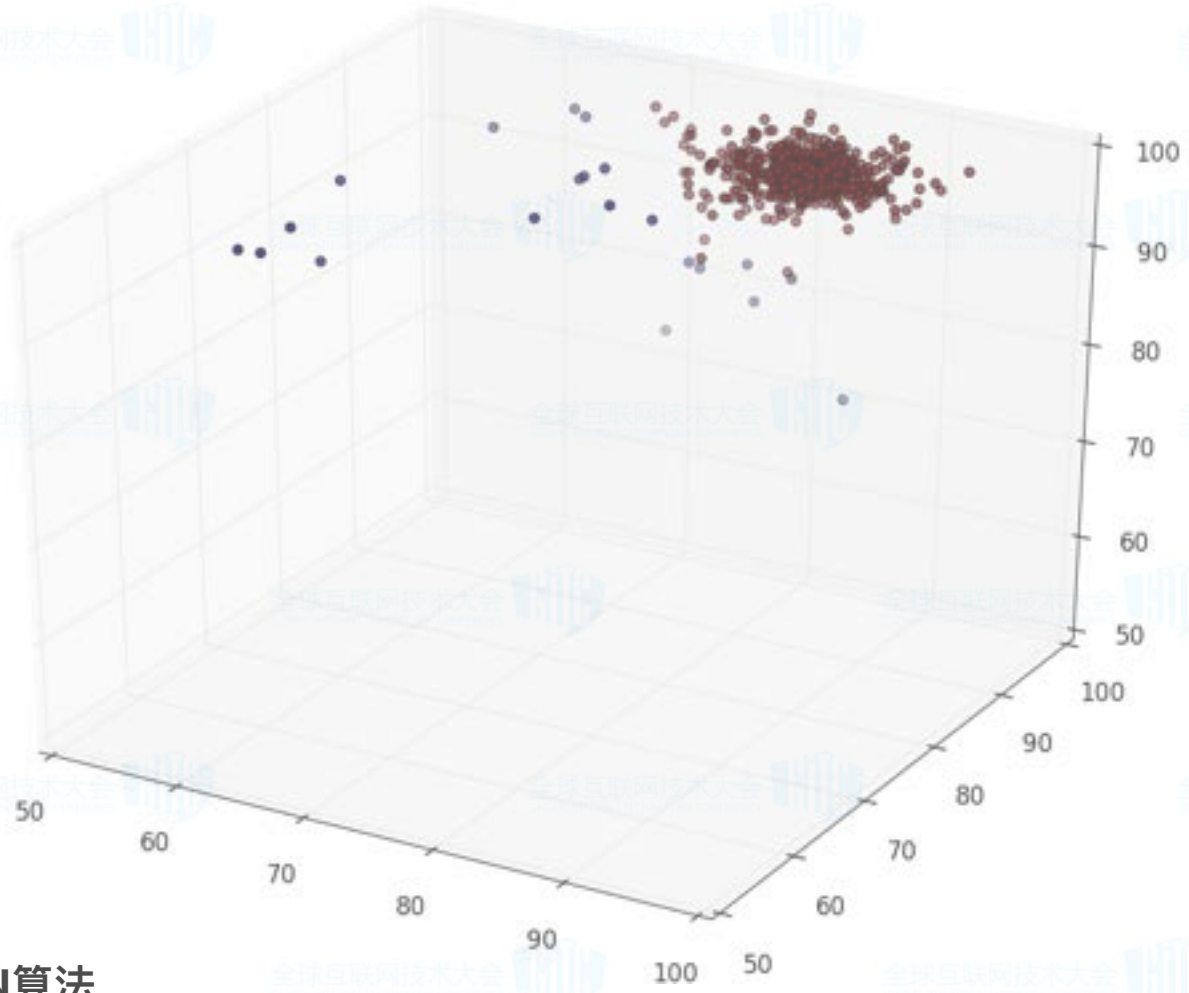
监控规则领域模型



复合监控

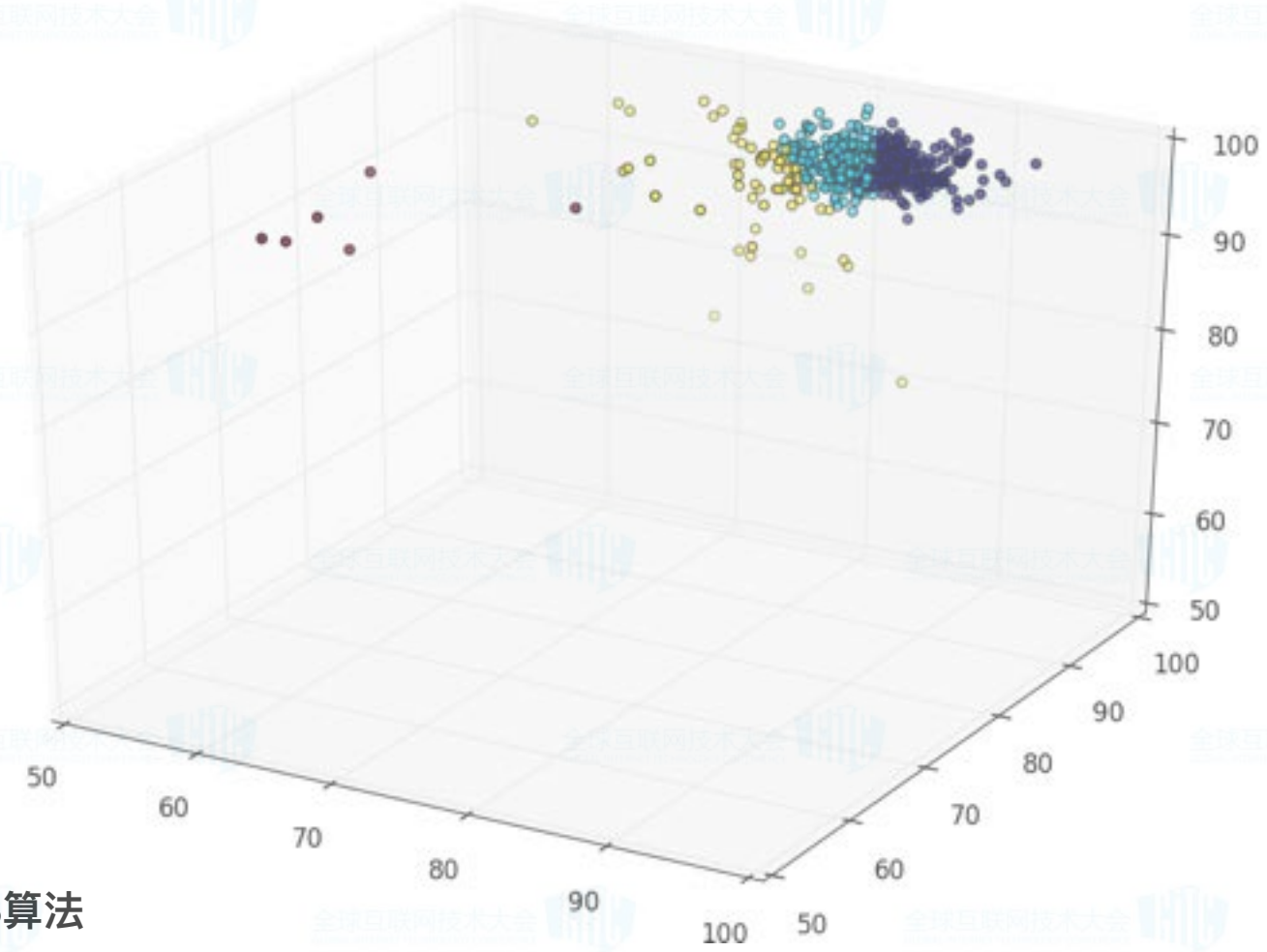
- 横向：连续的成功率的趋势
- 纵向：关联指标变化的相关性分析
- 聚类分析

复合监控——聚类分析



DBSCAN算法

复合监控——聚类分析

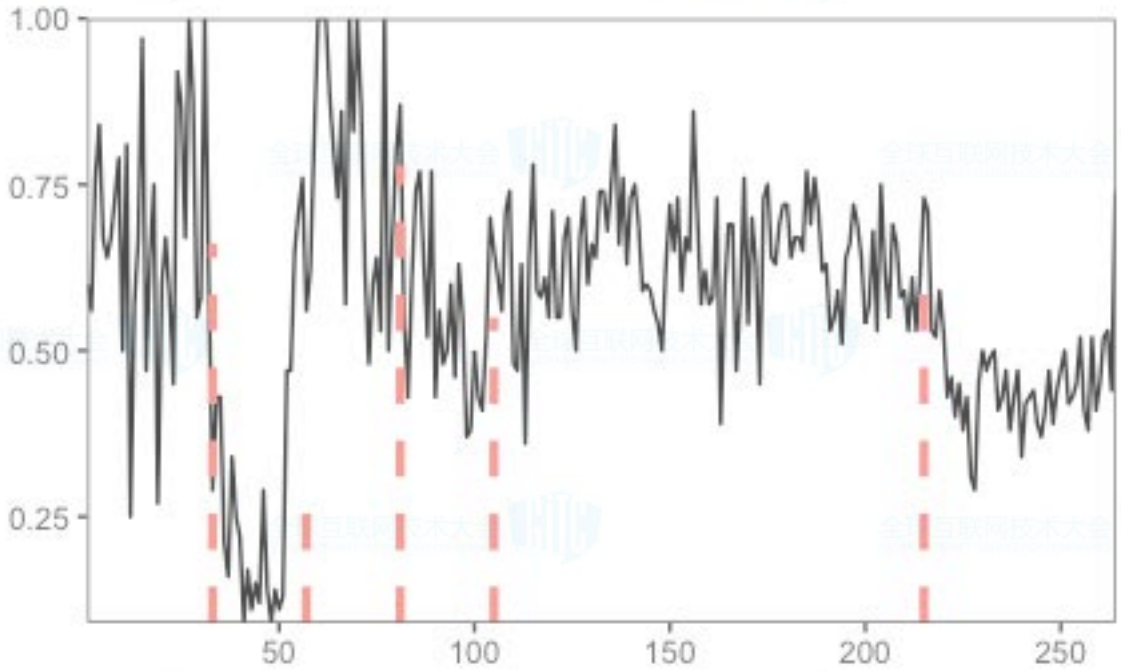


KMEANS算法

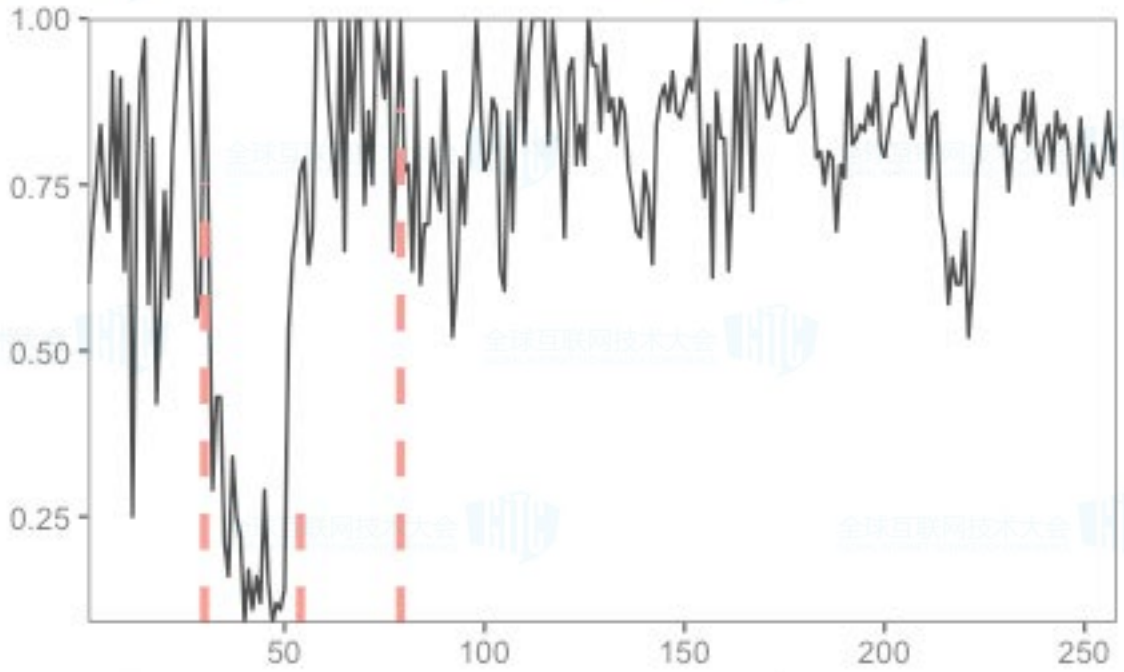
智能监控

- 整体成功率报警，可能是整体出问题了，也可能是各别商户出问题了
- 哪个异常突然增多了

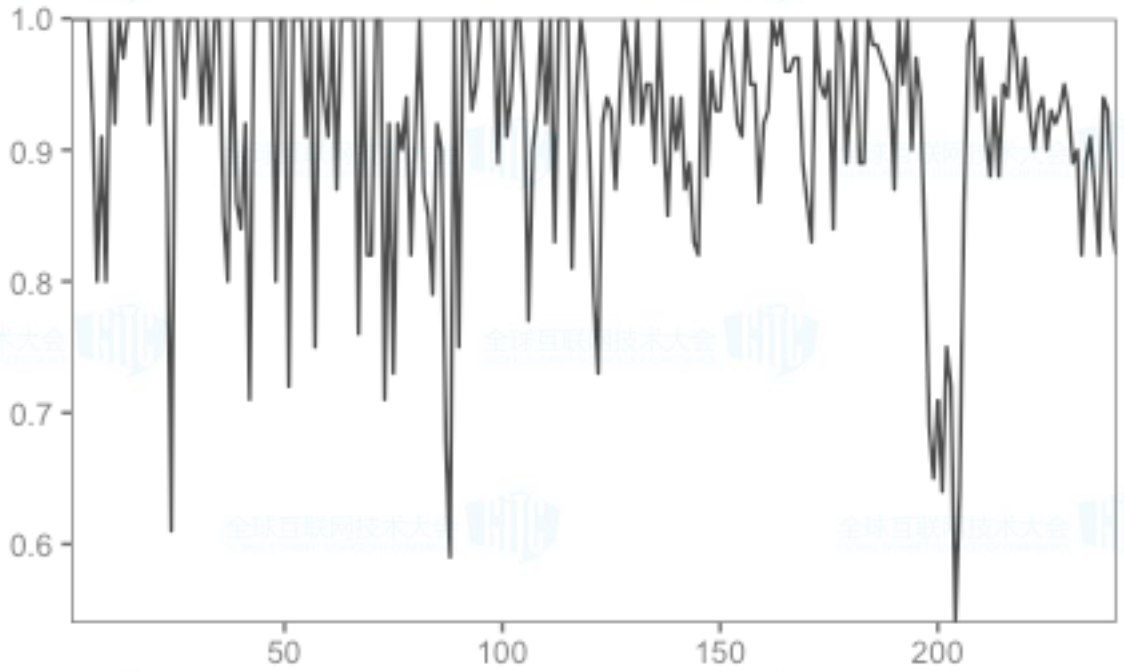
用BreakoutDetection排除单个干扰因素



用BreakoutDetection排除单个干扰因素



用BreakoutDetection排除单个干扰因素



后续要做

- 容量评估经验值
- 智能生成正则表达式

Thank You!