海量业务日志多维度实时监控实践

百度运维部

王达心

2015.8

About Me

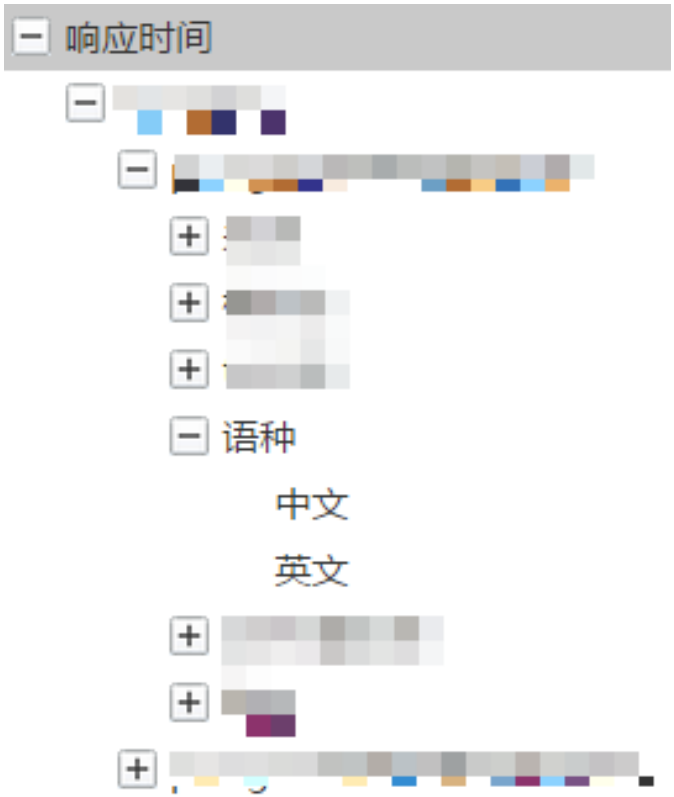
- 2008加入百度运维部，从事监控系统工作
- 2011~2013，新浪，分布式MySQL
- 2013~至今，重回老地方
- 个人信条：大道至简

Baidu 百度

The Problem

百度一下，你就知道

99.99%



- 数据计算：海量实时
- 异常检测：明察秋毫
- 根因定位：统筹全局
- SaaS化：即插即用

What's ELK

logstash

elasticsearch

Kibana

- Logstash：Collect, Enrich & Transport Data
- Elasticsearch：Search & Analyze Data in Real Time
- Kibana：Explore & Visualize Your Data

Baidu 百度

WOW~

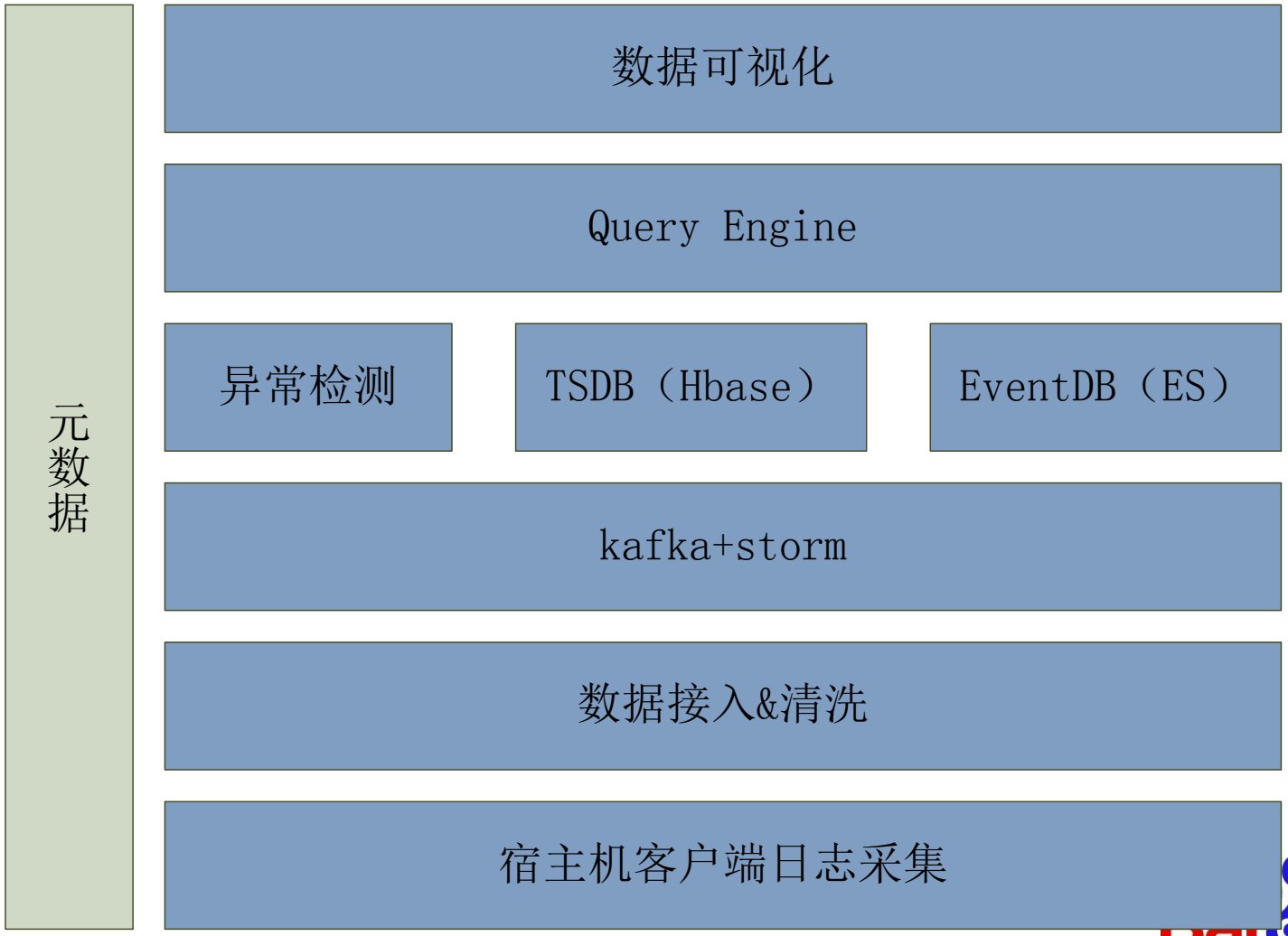
然并...

Enhanced by Storm?

- 为大规模日志实时分析而生
- 需要外围其他设施配套
- 直接跟ELK配合的问题
  - Logstash消耗单机较多资源
  - 原始日志全量集中处理成本极高
  - 一条日志可能参与Storm多个计算，elasticsearch查询时不能区分，会重复计算

Baidu 百度

我们的解决方案


元数据
数据可视化
Query Engine
异常检测
TSDB（Hbase）
EventDB（ES）
kafka+storm
数据接入&清洗
宿主机客户端日志采集

数据模型

- 数据属性
  - PRODUCT，产品线（数据隔离空间）
  - CLUSTER，某个服务集群，如模块
  - METRIC，指标，如PV、响应时间、错误数
  - VALUE，支持统计值：sum/cnt/max/min
  - TAGS，维度，如API、IDC、地域、来源等
- 可任选多个维度对某个指标聚合
- 维度可以有派生关系，如城市->省份、IP->省份

设计细节

- 客户端
  - 通用，使用正则从文本日志中提取结构化数据
  - 高性能，比logstash快10倍+
- 数据ETL
  - 可根据用户配置、平台元数据做维度派生，如：用户IP -> 所属地域
- 分层、分片聚合
  1. 客户端本地初步聚合，单机传输量至少降低一个数量级
  2. 各IDC内Storm实时聚合单机数据
  3. 多IDC汇总，由存储系统在查询时完成
- 外围指标派生计算
  - 例：命中率=命中数/请求总数

基于Hbase的时间序列数据存储（TSDB）

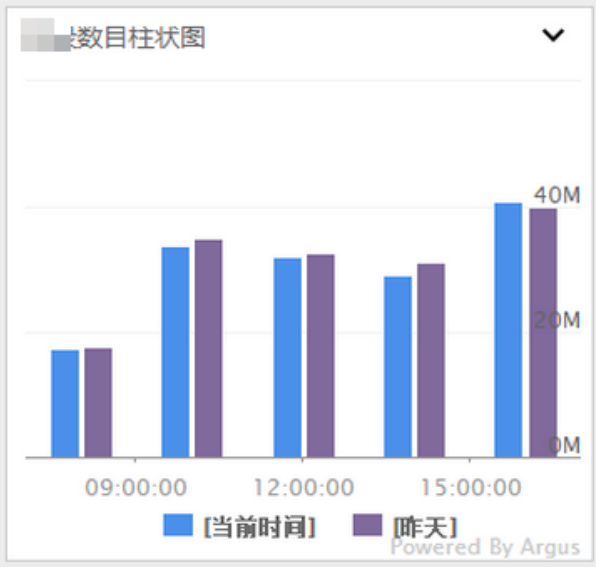
- 时序数据特性
  - 随机写，顺序读，写多读少，读写特性正交
  - 头大身小
- Hbase特性
  - 将随机写在一定程度上转化为顺序写
  - column可以自由扩展
- 存储结构设计
  - 按日期分表
  - 每小时一行
  - Rowkey设计：<entity_id> <metric_id> <timestamp_hour>
  - 列名：timestamp_offset

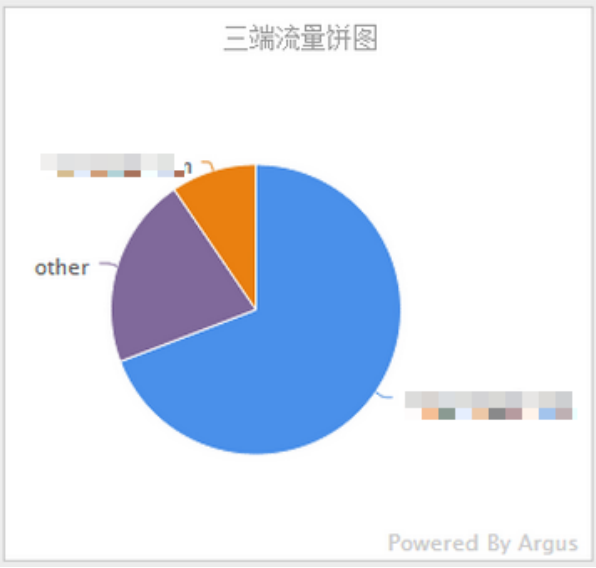
Key / Column	+0	+10	+20	…	+3590
0x0103713076829384**1292148000**	82.12	78.01	84. 56	…	89.42

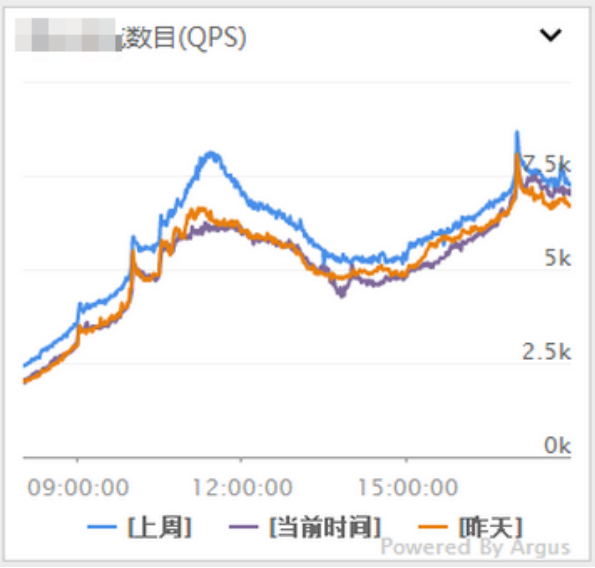
TSDB几个细节

- 支持追加同一时间点数据
  - 场景：部分数据延迟到达，前期部分计算已存储。
  - 解决方案：利用Hbase多版本机制，保存多份，查询时merge成一份。
- 查询时聚合
  - 场景：数据查询周期与生成周期不一致，比如生成周期为1分钟，需要查5分钟粒度的数据。
  - 解决方案：查询接口支持指定peroid，计算好返回给用户。
- 实时抽样
  - 场景：原始数据量巨大，长期数据需要抽样存储，并且尽量保证数据精度。
  - 解决方案：上游写入方用一致性hash选择TSDB节点，TSDB在内存中增量计算数据的sum、cnt、max、min，定期生成10分钟、60分钟抽样值。

可视化——图表







接口可用性报表(2015-08-05 08:00:00|2015-08-05 18:00:00)　　设置　刷新

维度	pv	pv_lost	response_time	499	5xx	接口列表
	37,018	--	0.2073	1	--	100%
	84,733	2	0.2914	3,621	1	99.9976%
	14,364	2	0.4487	15	2	99.986%
/web	167,581	9	0.1526	33,829	2	99.9946%

Baidu 百度

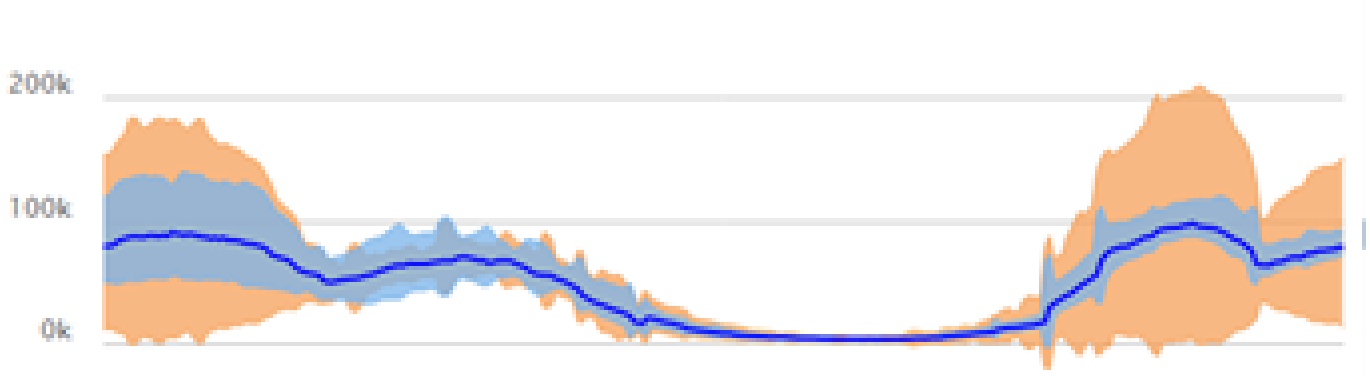
可视化配置

```
{
  "title": "浏览数目趋势图",
  "aggrNames": [
    {
      "product": "on[redacted]",
      "scope": "ignore",
      "dimensions": [
        {
          "name": "noah_namespace",
          "values": ["grou[redacted]all"]
        }
      ],
      "metrics": ["qps=#{oo_pv}/60"],
      "period": "60",
      "statistics": "sum",
      "times": ["before(2h)"],
      "contrast":["1w", "1d"],
      "legend": ""
    }
  ]
}
```

Baidu 百度

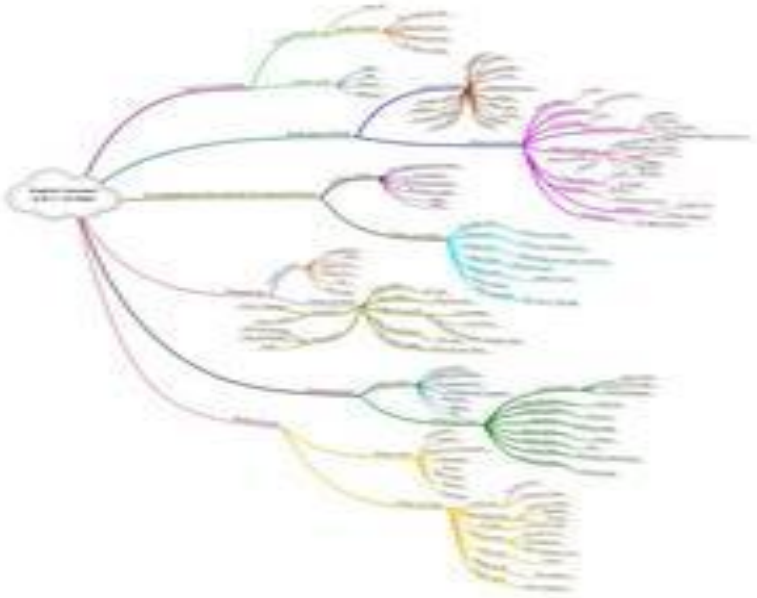
异常检测

- 流量波动监控的难题
  - 波动大
  - 简单同环比误报多
- 数据pattern自学习



多维度故障根因定位

- 系统平均响应时间突增，问题在哪？
- 数十个模块，成千上万维度
- 多维度细分，根据变化幅度、权重等排序



SaaS化

- 用户仅需提交配置即可使用服务
- 平台按用户分配资源，软隔离
- 业务应用：搜索、广告、糯米、地图、手机百度…
- 系统TPS: 100W+
- 日处理原始日志量：数百TB

Q&A

: daxin11