Sina ELK

从运维到服务之路

@craftsman-凌霄

关于我

- Weibo:@craftsman-凌霄
- Wechat:lx900905
- 2013年7月入职新浪
- 前渣浪MySQL DBA，大数据工程师
- 现在还在渣浪，又跑去为微博多媒体下载和新浪ELK服务的建设搬砖了。

Agenda

- 运维一个50+的ELK集群
- 构建自动化&平台化之路
- 提供深入业务体系的产品

运维一个50+的ELK集群

运维一个50+的ELK集群

- 架构演进之路
- 工具介绍

架构演进之路

第一阶段

FILE

- 日志推送实时性
- 计算节点存储空间

第二阶段

Rsyslog

- 高峰期上游日志堆积
- 单次推送，服务解耦

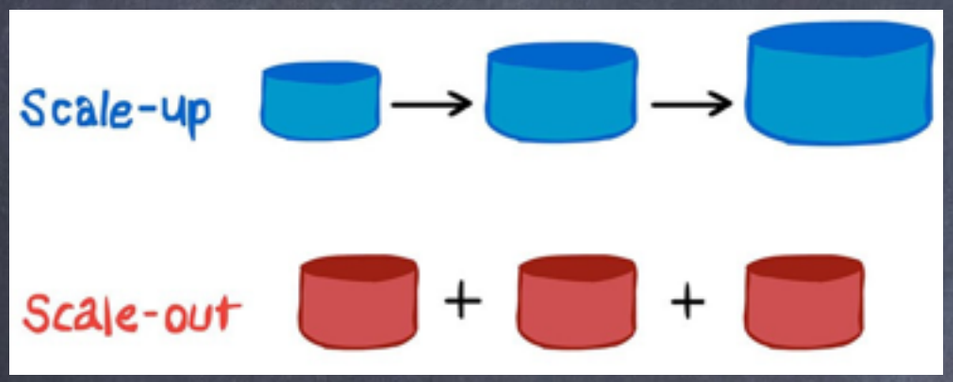
第三阶段

Kafka

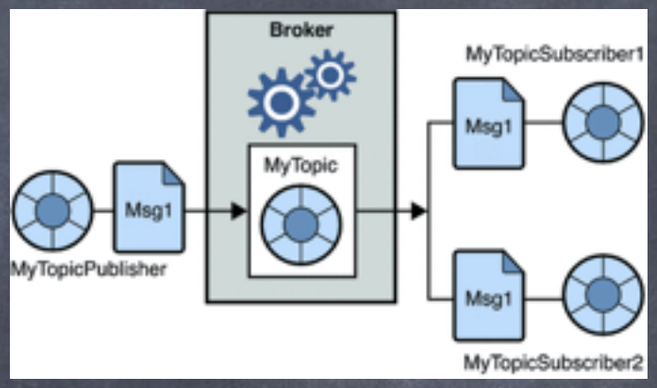
Why Kafka?

重要的事情：超高的吞吐！超高的吞吐！超高的吞吐！

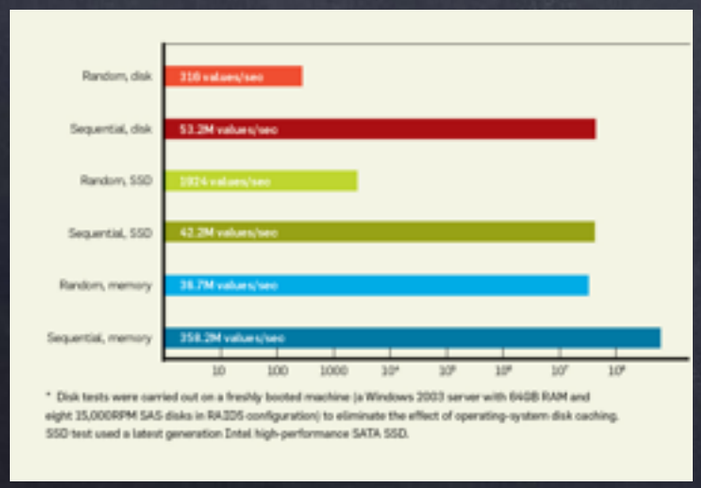
1、性能可扩展性



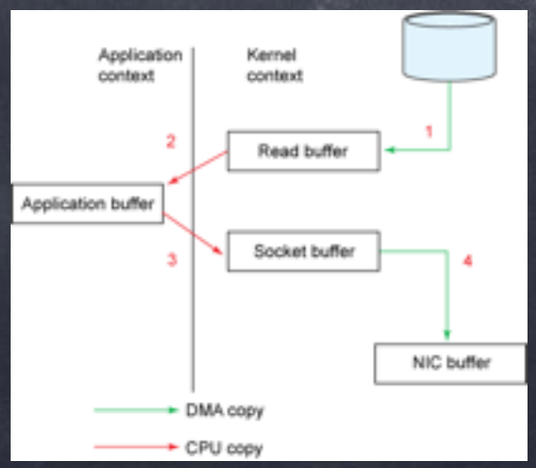
2、基于Topic的pub/sub

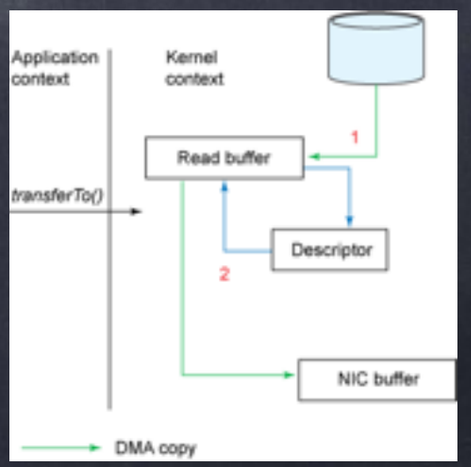


3、硬盘顺序写有多快?



4、Zero-Copy





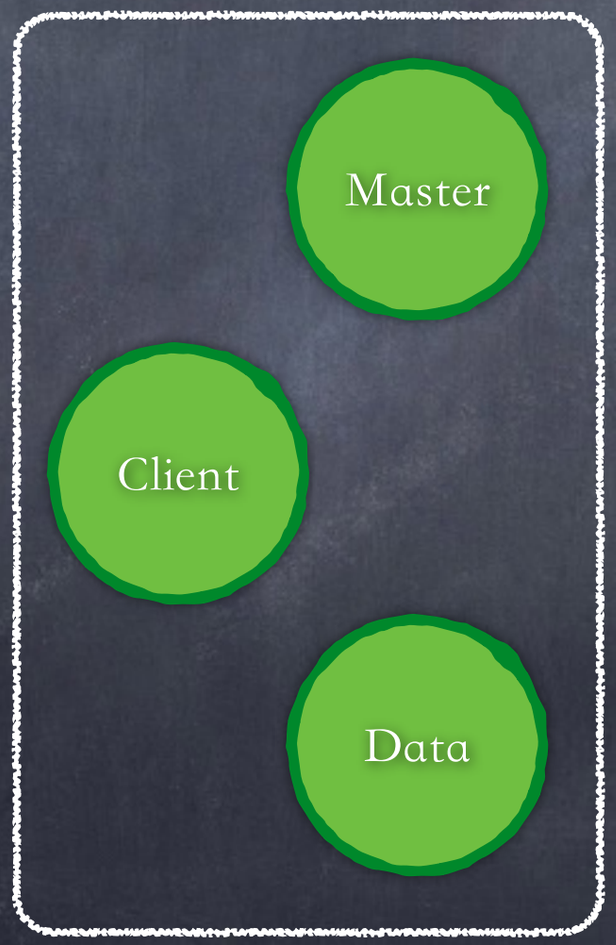
架构演进之路

- 支持更为丰富的计算模式
- 计算迁移，固定纬度预分析
- 统计结果长久保存
- 问题转换，提升并发（altp->oltp）

架构演进之路

第一阶段:

第二阶段:



一、Data

- 负责集群数据存储
- fetch集群中存储的数据

二、Master

- 集群状态管理
- 单独部署，管理节点稳定
- 奇数部署

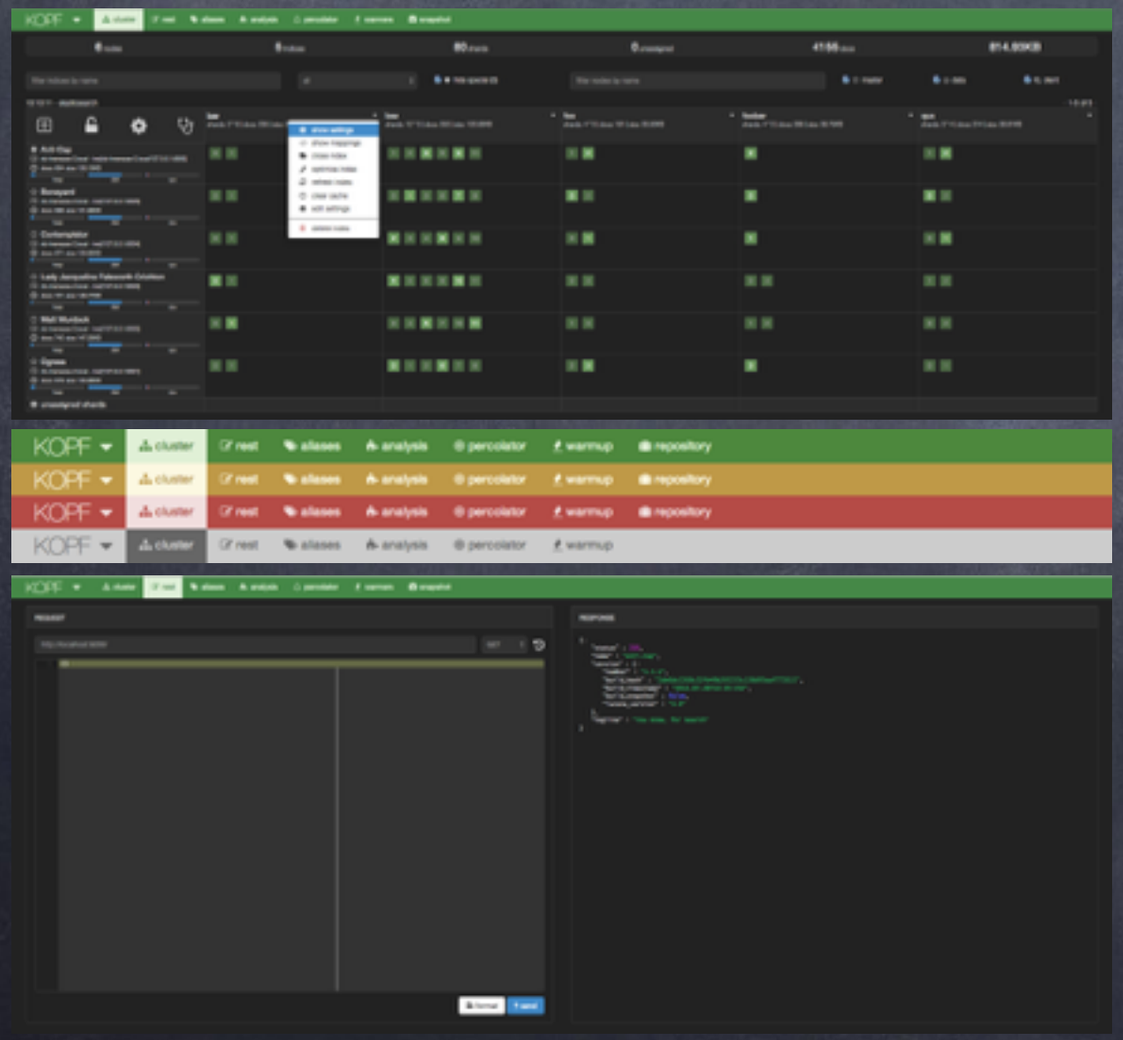
三、Client

- 处理HTTP请求处理分发（读写）
- 处理查询请求时的数据聚合

工具介绍

KOPF

Elasticsearch集群可视化管理工具



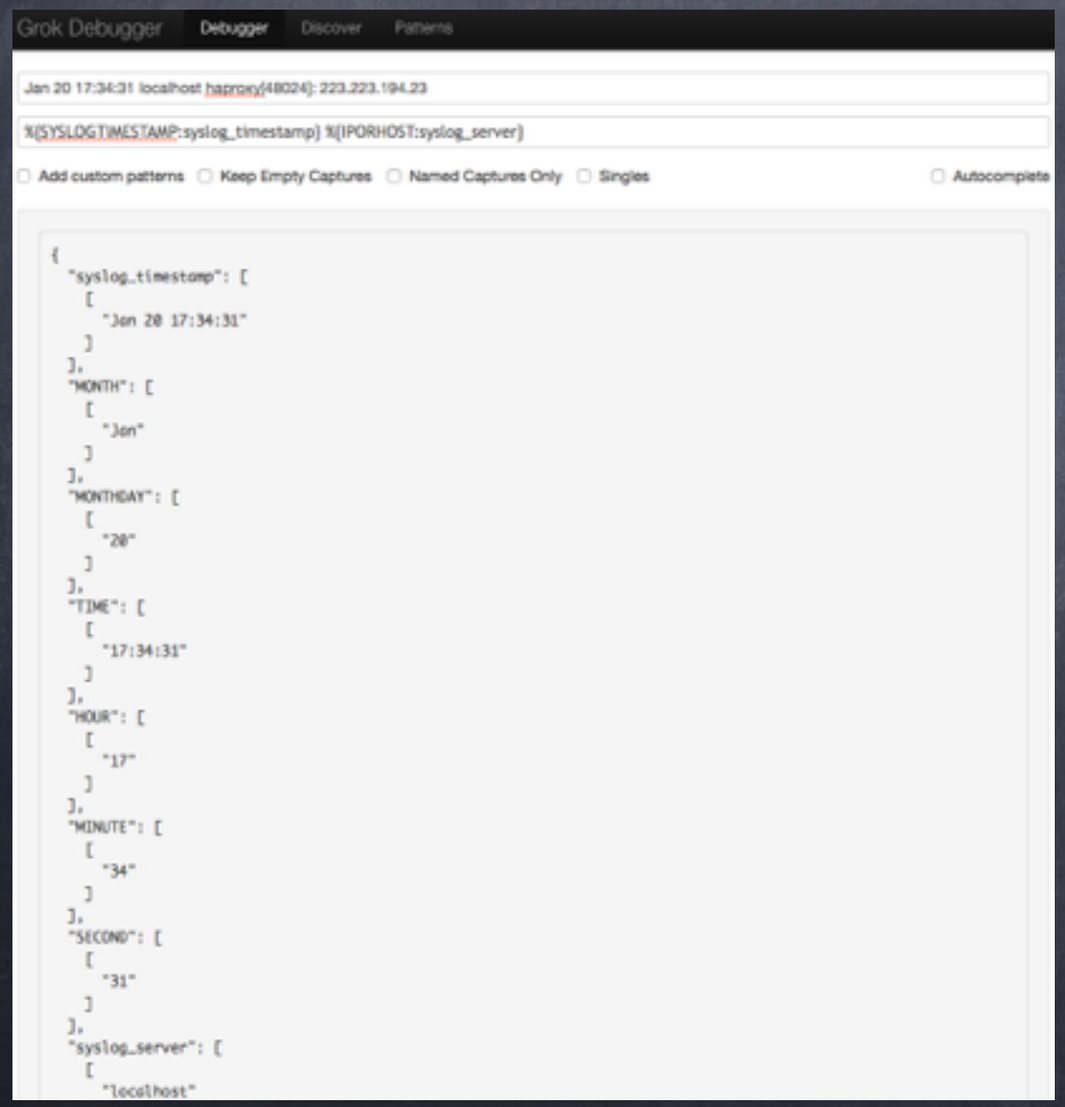
bigdesk

Elasticsearch节点性能调优工具

工具介绍

Gork Debugger

在线Logstash Grok 语法测试工具



Curtor

Elasticsearch索引管理工具

```
import elasticsearch
import curator

client = elasticsearch.Elasticsearch()

curator.close_indices(client, ['logstash-2014.08.16','logstash-2014.08.17'])
curator.disable_bloom_filter(client, 'logstash-2014.08.31')
curator.optimize_index(client, 'logstash-2014.08.31')
curator.delete(client, ['logstash-2014.07.16', 'logstash-2014.07.17'])
```

```
$ curator.py -h
usage: curator.py [-h] [-v] [--host HOST] [--port PORT] [-t TIMEOUT]
                  [-p PREFIX] [-s SEPARATOR] [-C CURATION_STYLE]
                  [-T TIME_UNIT] [-d DELETE_OLDER] [-c CLOSE_OLDER]
                  [-b BLOOM_OLDER] [-g DISK_SPACE]
                  [--max_num_segments MAX_NUM_SEGMENTS] [-o OPTIMIZE] [-n]
                  [-D] [-l LOG_FILE]

Curator for Elasticsearch indices. Can delete (by space or time), close,
disable bloom filters and optimize (forceMerge) your indices.

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program version number and exit
  --host HOST           Elasticsearch host. Default: localhost
  --port PORT           Elasticsearch port. Default: 9200
  -t TIMEOUT, --timeout TIMEOUT
                        Elasticsearch timeout. Default: 30
  -p PREFIX, --prefix PREFIX
                        Prefix for the indices. Indices that do not have this
                        prefix are skipped. Default: logstash-
  -s SEPARATOR, --separator SEPARATOR
                        Time unit separator. Default: .
  -C CURATION_STYLE, --curation-style CURATION_STYLE
```

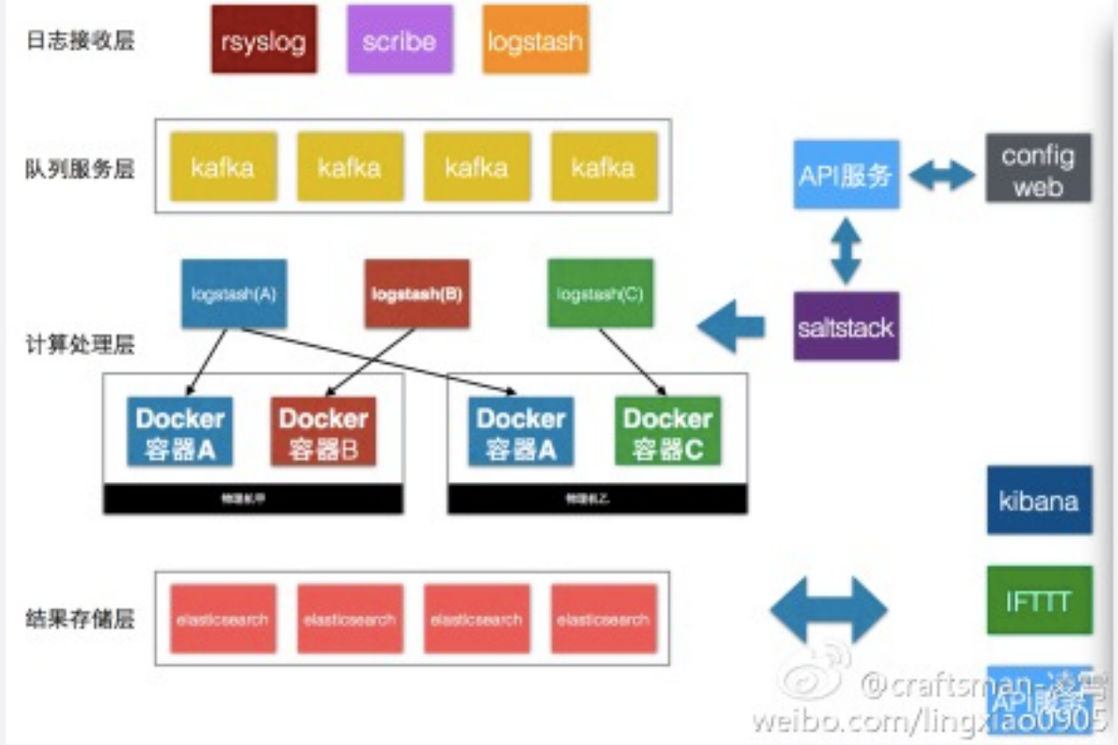
构建自动化&平台化之路

构建自动化&平台化之路

那一天，我们接入了5个业务
那一天，我们处理了一晚上故障
那一天，我们才刚刚起步
那一天，构思着未来的服务
我在工位的发了这条微博

梦想还是要有的，
万一实现了呢！

#ELK服务化#用kafka队列作为统一的日志入口，让用户自助的配置logstash的配置文件，实现业务级的资源隔离。提供分析结果的展示，可定制逻辑的报警，以及查询API服务。@ARGV @陈杰要骑车 @晓梦 @姑娘今年您贵姓@平凡的香草 @DBA陶会祥 @geda @邱春武



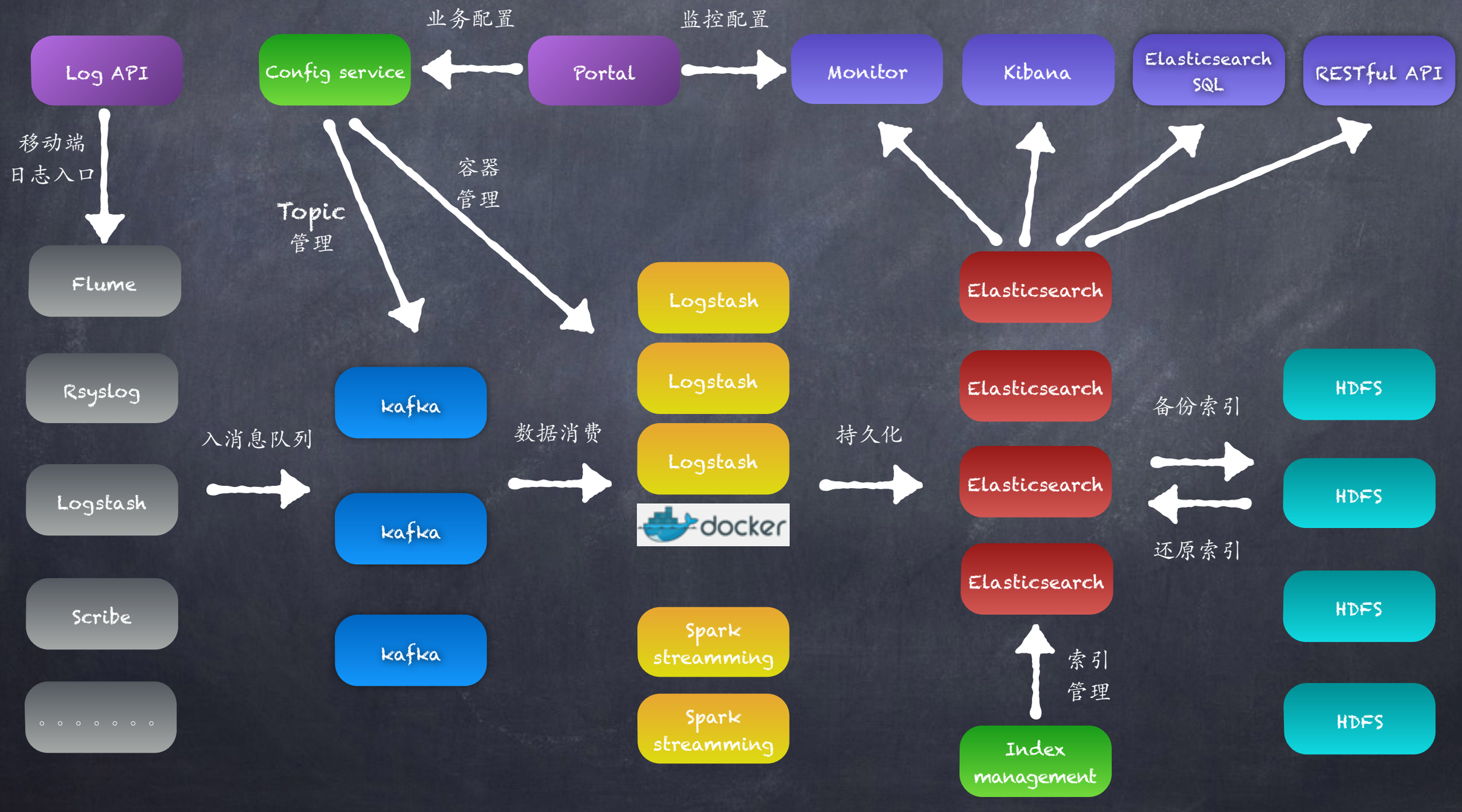
2014-9-28 20:49 来自 微博 weibo.com

阅读 4140　推广　转发 5　评论 2　1

构建自动化&平台化之路

- 整体架构介绍
- 日志格式协商
- 数据管理系统
- 移动端日志服务
- 服务docker化

整体架构介绍


Log API
移动端
日志入口
Flume
Rsyslog
Logstash
Scribe
。。。。。。。
Config service
业务配置
Portal
监控配置
Monitor
Kibana
Elasticsearch
SQL
RESTful API
Topic
管理
容器
管理
入消息队列
kafka
kafka
kafka
数据消费
Logstash
Logstash
Logstash
docker
Spark
streamming
Spark
streamming
持久化
Elasticsearch
Elasticsearch
Elasticsearch
Elasticsearch
索引
管理
Index
management
备份索引
还原索引
HDFS
HDFS
HDFS
HDFS

日志格式协商

1、日志格式协商

2、解析后返回格式

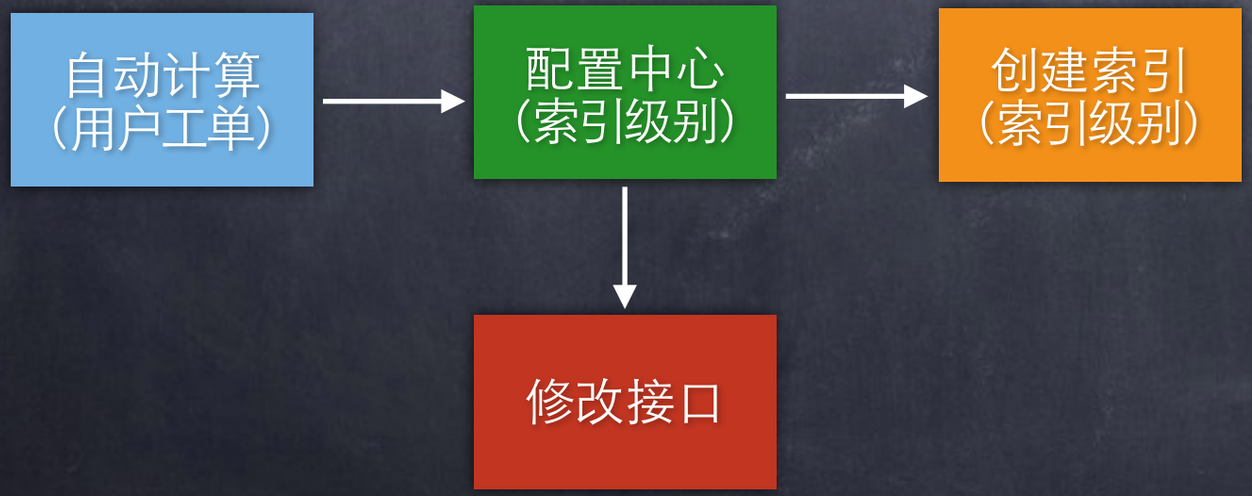
3、使用场景

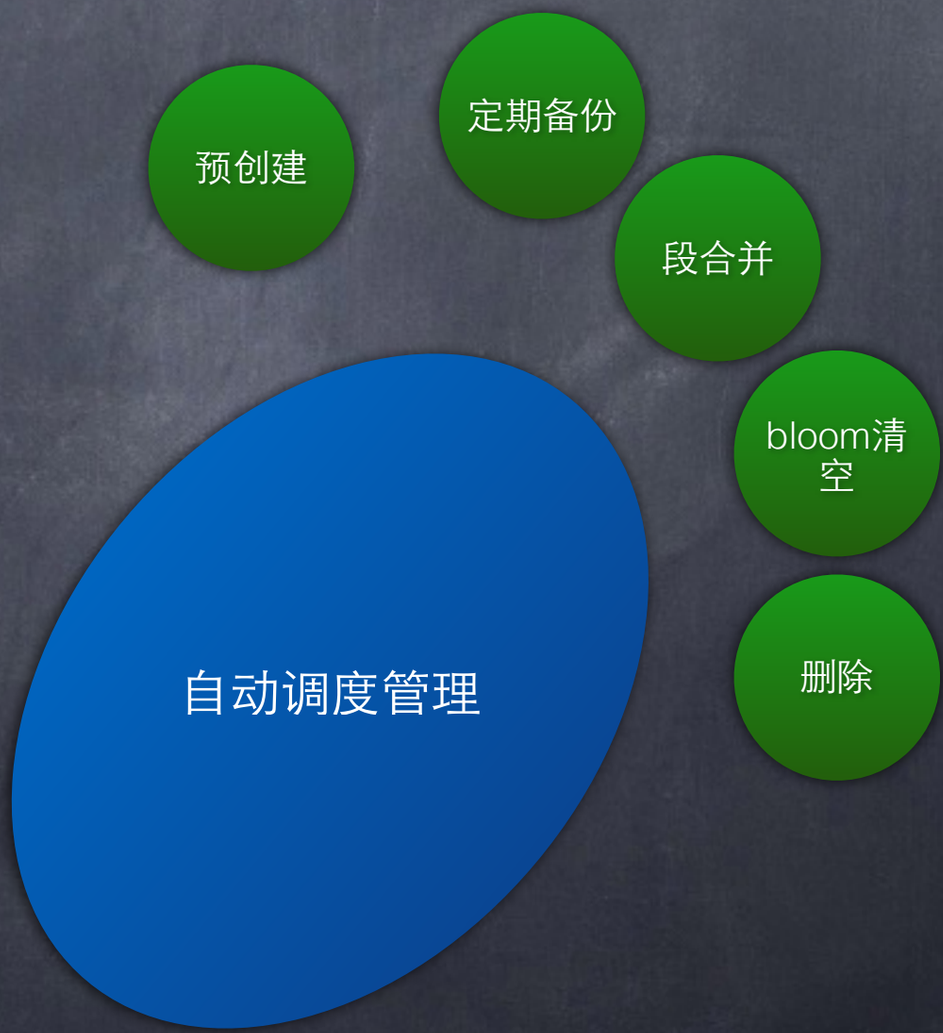
数据管理系统

1、mapping&setting

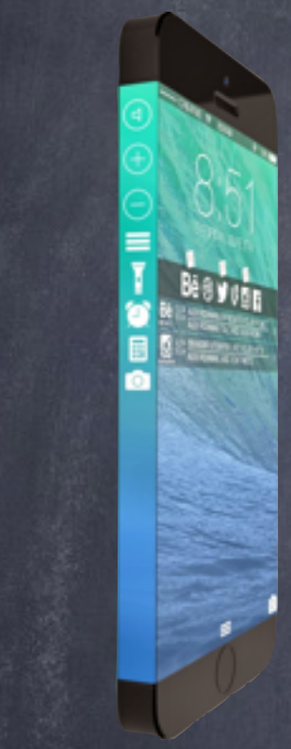
2、index management

template enough?
one index，one choose!

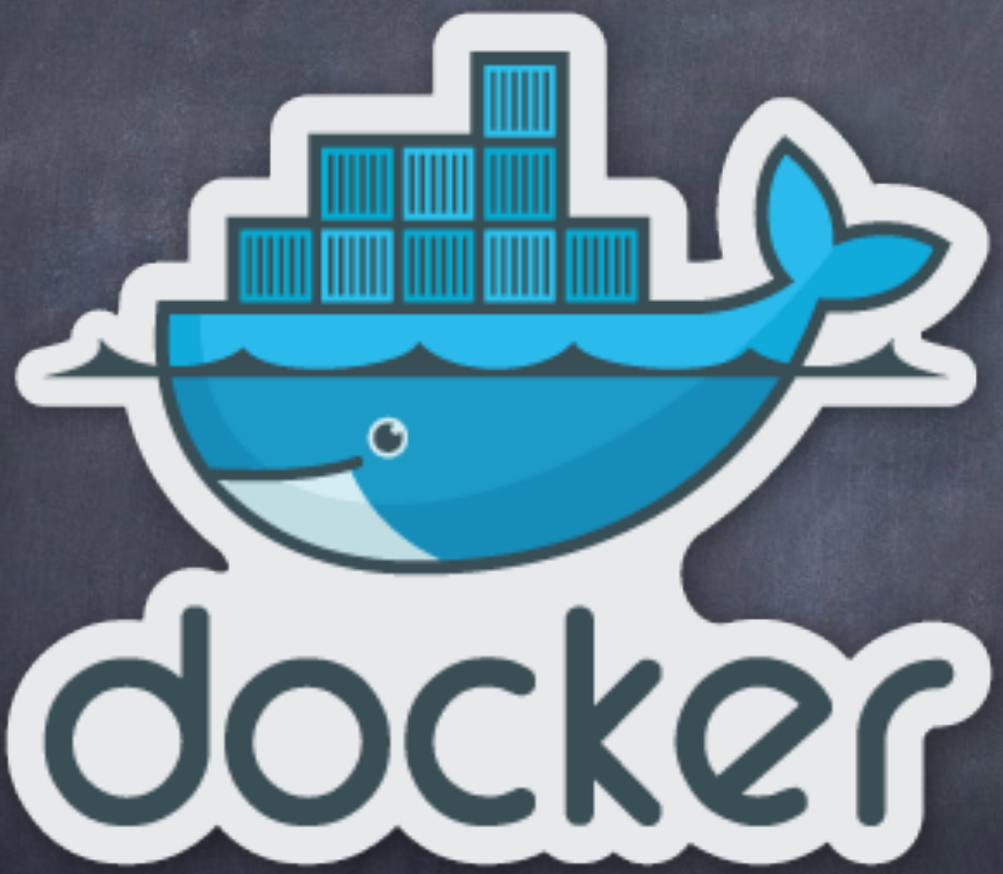




移动端日志服务



服务docker化



- Nginx
- Flume
- Logstash
- Kibana

提供深入业务体系的产品

提供深入业务体系的产品

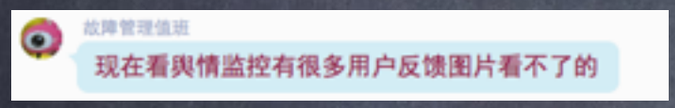
- ELK服务使用介绍
- 用户信息投诉管理
- 业务报警&报警分析
- CDN自动调度系统

ELK服务使用介绍

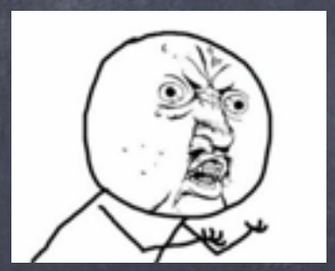
数据库平台
秒拍视频
成本中心
弹性计算平台
动态应用平台
故障管理组
微博图片
sinawatch
数据服务平台
新闻静态池
业务保障部
原生视频
微盘
小咖秀
新闻中心
新浪&微博通行证
新浪视频
微博主站
SAE
基础技术
Sinaedge
新浪&微博安全中心
数据智能平台

用户投诉信息管理

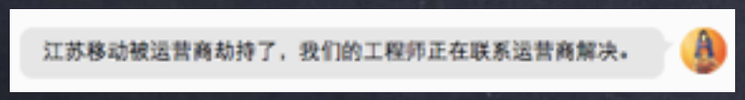
原来是这样的。

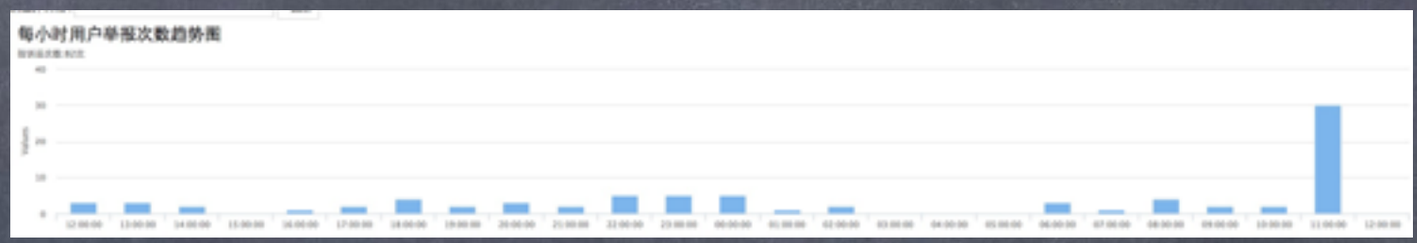


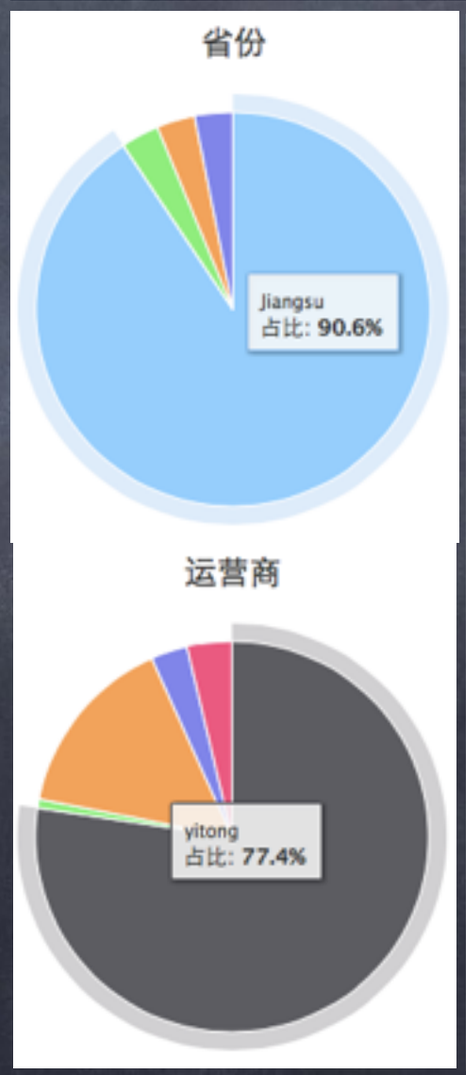
几分钟后一大波
uid发过来了。



后来呢？



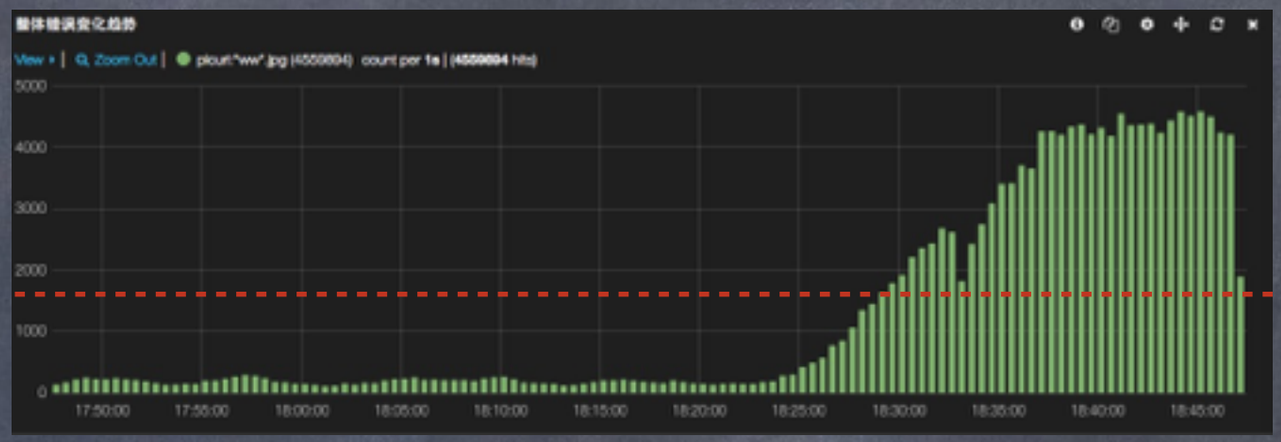




业务报警&报警分析

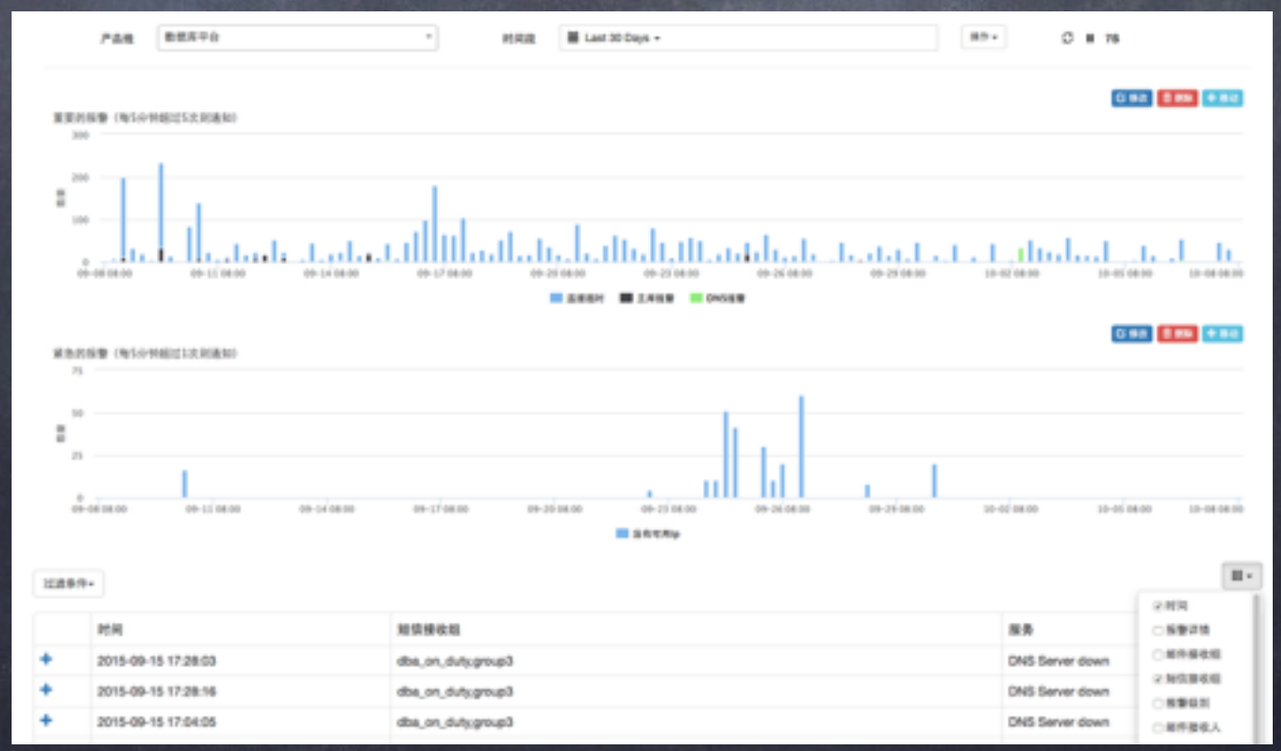
投诉?
毕竟too late!

业务报警



告警阀值

报警分析



CDN自动调度系统

天津爆炸　国庆阅兵　元旦春节

按照质量/成本的自建和商业CDN全局调度

节点宕机　网络问题　机房故障

实现调度层面的故障发现，服务failover

Thanks