新浪实时日志分析服务进化

Better ELK

高英举(@Gary的影响力)

http://garyelephant.me

Contents

- 服务介绍
- 技术架构
- Do Better
  - 提升服务质量
  - 增强易用性
  - 提供新功能
- 我们经历过的坑和坎儿
- 未来努力方向

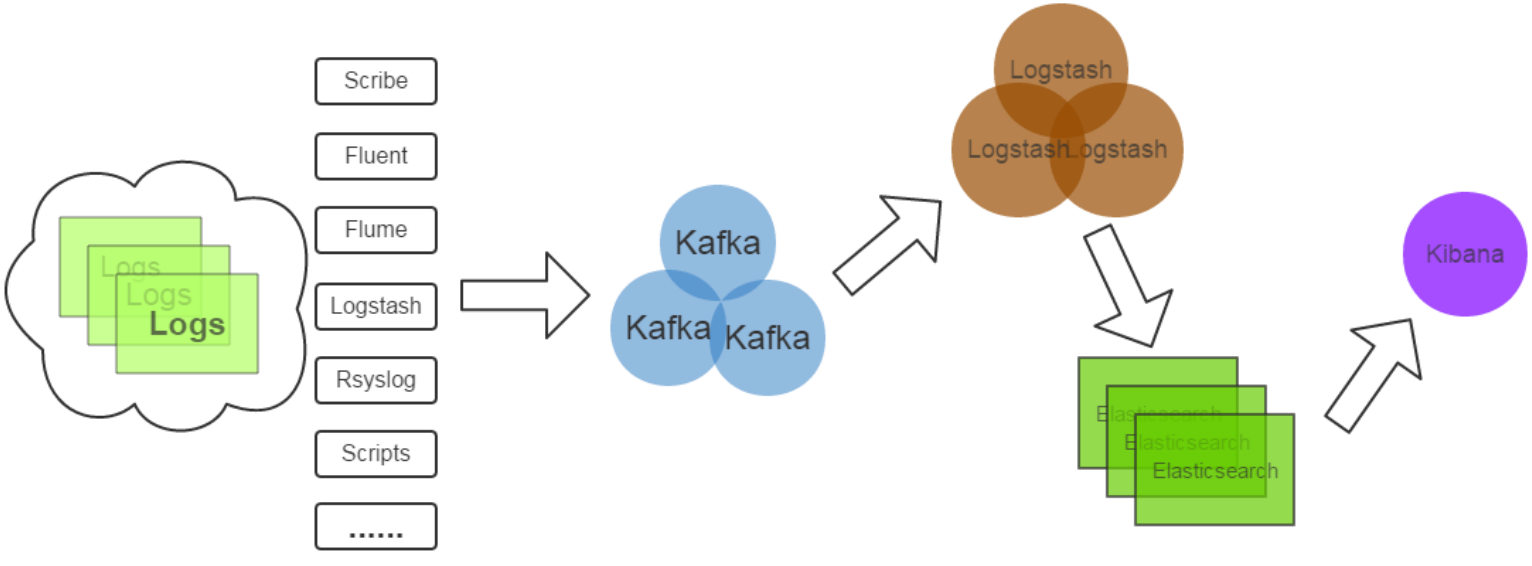
实时日志分析服务介绍

服务内容：实时的日志搜索和统计

已有用户：微博图片下载，微博视频，微盘，
秒拍，云存储，SCE, CDN……

规模：每天35亿条日志，2TB

技术架构


Logs
Logs
Logs
Scribe
Fluent
Flume
Logstash
Rsyslog
Scripts
.....
Kafka
Kafka
Kafka
Logstash
Logstash
Logstash
Elasticsearch
Elasticsearch
Elasticsearch
Kibana

技术架构

数据流：

(1) 用户日志--> Kafka --> Logstash --> Elasticsearch --> Kibana

(2) 用户日志--> Kafka --> Logstash --> Elasticsearch --> API Clients

技术架构

- Kafka:接收用户日志的消息队列
- Logstash：将日志解析为json输出给Elasticsearch
- Elasticsearch：实时日志分析服务的核心技术，一个schemaless，实时的数据存储服务，通过index组织数据，兼具强大的搜索和统计功能。
- Kibana：基于Elasticsearch的数据可视化组件，超强的数据可视化能力是众多公司选择ELK stack的重要原因。

Better ELK,More Than ELK

在ELK的基础上为用户提供更好的服务

Do Better & More

- 提升服务质量
- 增强易用性
- 提供新功能

提升服务质量

- Elasticsearch优化
- Logstash优化
- ES Index管理系统
- 数据备份
- 监控报警

Elasticsearch优化

- System Level
  - 关闭swap
  - max open files
  - Jdk1.8
- App Level
  - ES_HEAP_SIZE
  - 调整shard, replica数
  - String默认not_analyzed
  - 使用doc_values
  - 定制index template

Logstash优化

- 使用supervisord管理logstash
- 调大 filter worker number(-w)
- 减少使用非官方插件和logstash-filter-ruby

Es Index管理系统

- 定期Create Index
- 定期Optimize Index
- 定期Close Index
- 定期Delete Index
- 定期Snapshot Index to Hdfs

Crontab is not enough, We Use Celery!

监控报警

- System Level 使用公司内部的Sinawatch服务
  - 磁盘满，坏
  - 宕机
  - Load, Mem
- App Level(, Logstash, Kibana, Kafka, Celery) 自己开发+用开源产品
  - Es:JVM Heap Usage, node number, bulk reject rate
  - Logstash,Kibana: service status
  - Kafka: topic consumer offset lag
  - Celery: Flower

增强易用性

我们面临的易用性难题：

- IP解析成地区、ISP信息不准，完全没有参考意义
- 用户日志接入流程复杂，沟通困难。
- 部分数据可视化需求得不到满足，Kibana配置难度大

如何增强易用性：

新浪IP库+ logstash-filter-geoip2

用户日志接入自动化+Es Index管理自动化

官方Kibana 3 -> 三斗Kibana 3 -> 官方Kibana 4

提供新功能

- 中文分词功能

中文分词功能

Es standard analyzer中文分词：

”美国打伊拉克“—>"美"，”国“，”打“，”伊“，”拉“，”克“

ik analyzer 中文分词：

”美国打伊拉克“—>”美国“，”打“，”伊拉克“

我们经历过的坑和坎儿

- elasticsearch 进程JVM Heap High Usage(>90%)
- Elasticsearch Query DSL, Facets, Aggs学习困惑
- logstash不工作
- Kibana没有用户的概念，不同用户的数据无法隔离
- 与用户沟通成本高

未来努力方向

- 日志接入全自动化：即点即用
- 完整的用户服务web系统
- 用户数据层面的报警
- 服务性能优化
- 数据安全/用户隔离
- 内部组件容器化：docker