日志监控分析平台

1. **架构**

Beats+Kafka+ strom +Logstash++ES+Kabina (实时或者自定义那个框架)+Graphi

参考：

<http://lxw1234.com/archives/2015/12/588.htm>

https://mp.weixin.qq.com/s/t-ktlzJsrpad1-YRuIakiw

<http://www.open-open.com/lib/view/open1456887784031.html>

<https://wenku.baidu.com/view/7053671fb9d528ea81c779b1.html>

Monitor

Elastic Search

Filebeat

Kibana

Logstash

kafka

…

JStorm

KSQL

Grafana

Graphite

canal

Zabbix-api

Alter(ding/we)

Mysql

Web

服务器部署（最小化分布式部署，用于后期扩展）：beats部署在各个应用服务器

Kafka 部署2台做集群(ZK集群复用)

Logstash+ES(2)+ Kibana 部署2台做集群(做高可用)

实时计算部分：2台虚机

**二．目的**

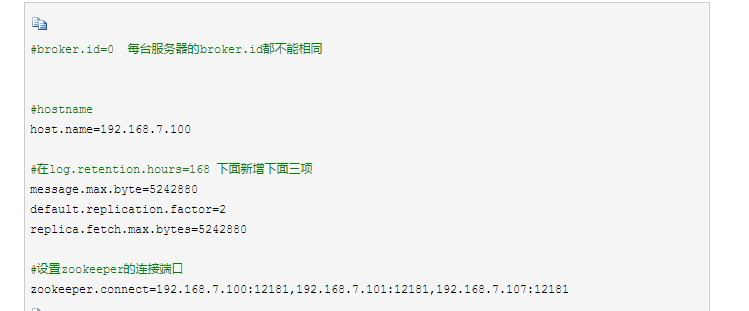
1. UV、PV、IP、用户ID、微店ID、商品ID、来源 URL、URL、停留时间、访问时间
2. 性能分析
3. 预警-错误日志，非200告警
4. 监控IO，监控disk 空间增长，预警
5. 错误日志告警
6. 自动扩容、安全防护、404错误要加入--验证系统（通过内网访问）
7. 内网访问业务检查系统--对各个业务、各个关键服务器进行1对1 检查
8. 监控重点url，重点dubbo调用，一旦发现缓慢，非200码，告警
9. 业务监控：订单、购物车，采用
10. 提供合并报表—曲线图
11. 通过zabbix api 开发，监控磁盘CPU情况，不要在安装新的了，唯一要确保的是要确保所有机器安装了，重要的监控模版，通过puppet来实现巡检功能
12. 静态文件排查
13. 订单大屏，负载大屏 JVM
14. 日志查询
15. 业务线日志分析预警,单ip请求次数并发次数过高！
16. 接口响应缓慢告警！
17. Storm 监控日志量，环比
18. PHP日志nginx日志
19. 所有日志纳入范围
20. 日志增量监控！限制预警，不要过于频繁
21. 实现系统大屏，业务大屏效果
22. **部署步骤**

**-----安装JDK 1.8**

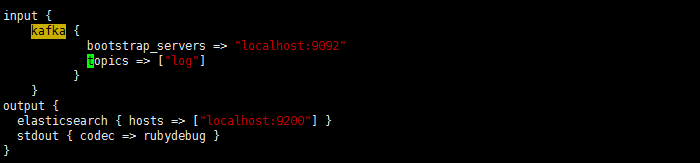
1. 安装beats，Filebeat Packetbeat Metricbeat Topbeat，DubboBeat（自行开发）

<https://www.elastic.co/guide/en/beats/libbeat/current/community-beats.html>

1. curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.6.1-x86\_64.rpm
2. sudo rpm -vi filebeat-5.6.1-x86\_64.rpm
3. /etc/init.d/filebeat start
4. 安装Kafka
5. wget <http://mirror.bit.edu.cn/apache/kafka/0.11.0.1/kafka_2.11-0.11.0.1.tgz>
6. 修改zk地址等



1. ./kafka-server-start.sh -daemon ../config/server.properties
2. 安装Logstash
3. wget <https://artifacts.elastic.co/downloads/logstash/logstash-5.6.2.zip>
4. unzip
5. 按照kafka input 插件：bin/logstash-plugin install logstash-input-kafka
6. 配置文件修改



1. 启动

bin/logstash -f config/logstash-simple.conf 注意config路径

Bin/logstash -f ../config/logstash-simple.conf

1. 安装ES
2. wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.6.1.zip>
3. unzip \*.zip
4. groupadd elk ; useradd -g elk es
5. ./bin/elasticsearch -d

注意：新建立用户组以及用户，不要用root

1. 按照kibana
2. wget <https://artifacts.elastic.co/downloads/kibana/kibana-5.6.1-linux-x86_64.tar.gz>
3. tar zxvf kibana-5.6.1-linux-x86\_64.tar.gz
4. config/kibana.yml
5. 启动：

bin/kibana

**四．生产环境部署**

1. 移除sysng

2. 通过agent收集

3. 提供部署工具：用于扩容！

4. 开发工具，复制相关elk信息到文本框可得到对应的文本文件下载！

**五．注意事项**

1. ES日志清理

2. HDFS

六．参考

<https://www.elastic.co/guide/en/beats/filebeat/current/configuring-howto-filebeat.html>

<https://www.elastic.co/guide/en/kibana/5.0/getting-started.html>

<https://www.elastic.co/guide/en/beats/filebeat/1.2/filebeat-template.html>

<http://suclogger.com/ES%E4%BD%BF%E7%94%A8filebeat%E6%94%B6%E9%9B%86nginx%E6%97%A5%E5%BF%97/>

<http://kafka.apache.org/quickstart>

[https://www.elastic.co/guide/en/logstash/current/config-examples.html\](https://www.elastic.co/guide/en/logstash/current/config-examples.html\\)

[https://www.elastic.co/guide/en/logstash/current/plugins-inputs-kafka.html#plugins-inputs-kafka](https://www.elastic.co/guide/en/logstash/current/plugins-inputs-kafka.html" \l "plugins-inputs-kafka)