ELK安装文档

软件环境：

Centos 7.X

EKL 6.3.2

JDK 1.8.0\_181

软件下载地址：

https://www.elastic.co/downloads

部署结构：

Server1、Server2、Server3：Elasticsearch 服务

Server1：Kibana

Server2：Logstash

# 一、Elasticsearch 安装

参考《ElasticSearch安装手册1.0.docx》

# 二、Kibana安装

## 1.解压：

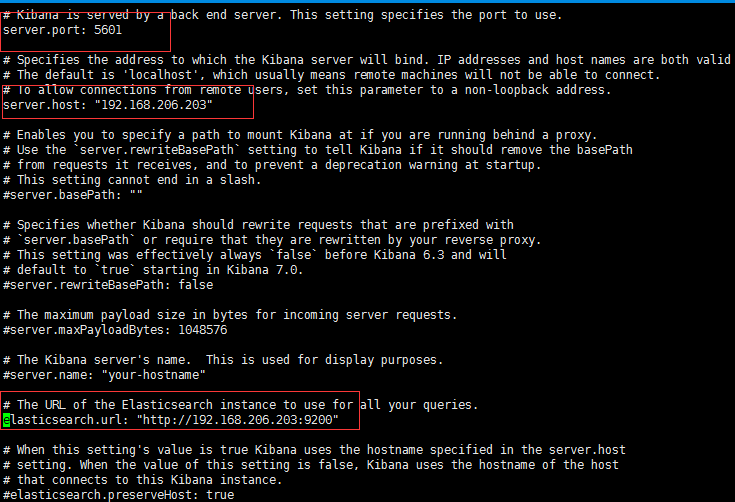
[root@iZwz90ct5msiflmndcqljmZ kibana]# tar zxvf kibana-6.3.2-linux-x86\_64.tar.gz

## 2.配置：

[root@iZwz90ct5msiflmndcqljmZ kibana]# cd kibana-6.3.2-linux-x86\_64

[root@iZwz90ct5msiflmndcqljmZ kibana-6.3.2-linux-x86\_64]# cd config/

[root@iZwz90ct5msiflmndcqljmZ config]# vi kibana.yml



主要修改选项：

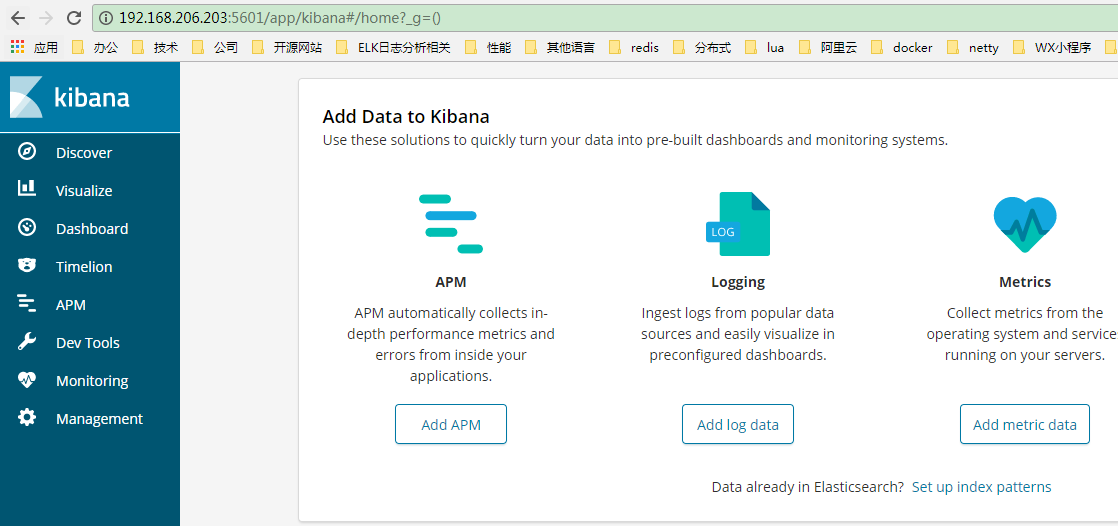
|  |
| --- |
| server.port: 5601 #开启默认端口5601  server.host: “ip” #站点地址 elasticsearch.url: http://es-ip:9200 #指向>elasticsearch服务的ip地址  kibana.index: “.kibana” |

## 3.启动

[root@iZwz90ct5msiflmndcqljmZ config]# cd ../bin/

后台启动：

[root@iZwz90ct5msiflmndcqljmZ bin]# nohup ./kibana &



# 三、Logstash安装

## 1.解压：

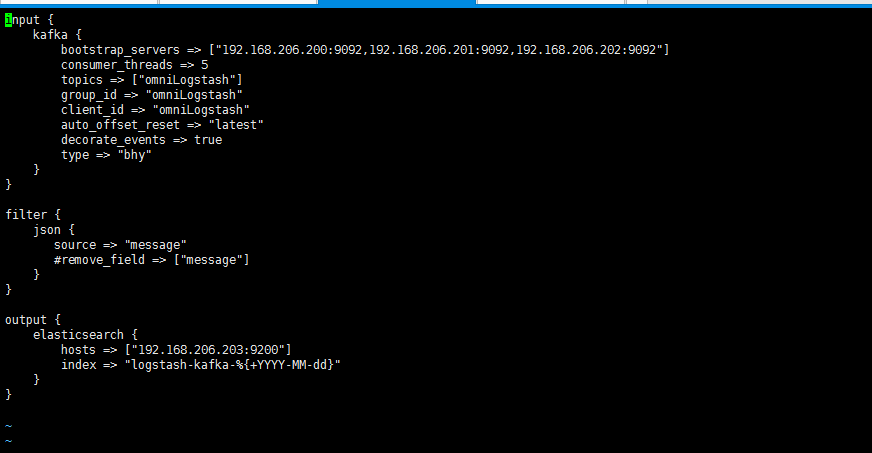
[root@iZwz90ct5msiflmndcqljmZ logstash]# tar logstash-6.3.2.tar.gz

## 2.配置conf：

[root@iZwz90ct5msiflmndcqljmZ logstash]# cd logstash-6.3.2

在conf目录下创建一个测试文件logstash-kafka

[root@iZwz90ct5msiflmndcqljmZ config]# vi logstash-kafka.conf



添加内容

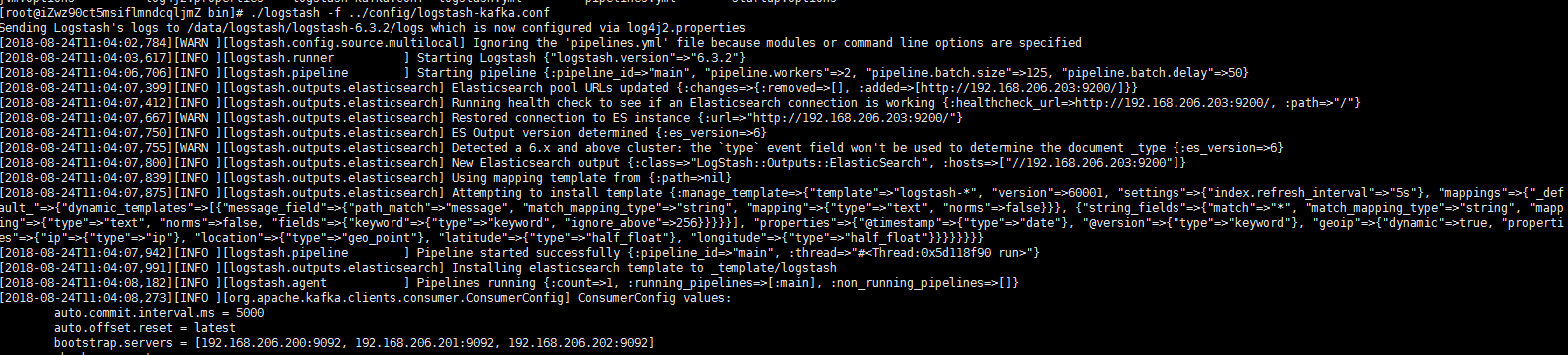
|  |
| --- |
| input {  kafka {  bootstrap\_servers => ["192.168.206.200:9092,192.168.206.201:9092,192.168.206.202:9092"]  consumer\_threads => 5  topics => ["omniLogstash"]  group\_id => "omniLogstash"  client\_id => "omniLogstash"  auto\_offset\_reset => "latest"  decorate\_events => true  type => "bhy"  }  }  filter {  json {  source => "message"  #remove\_field => ["message"]  }  }  output {  elasticsearch {  hosts => ["192.168.206.203:9200"]  index => "logstash-kafka-%{+YYYY-MM-dd}"  }  } |

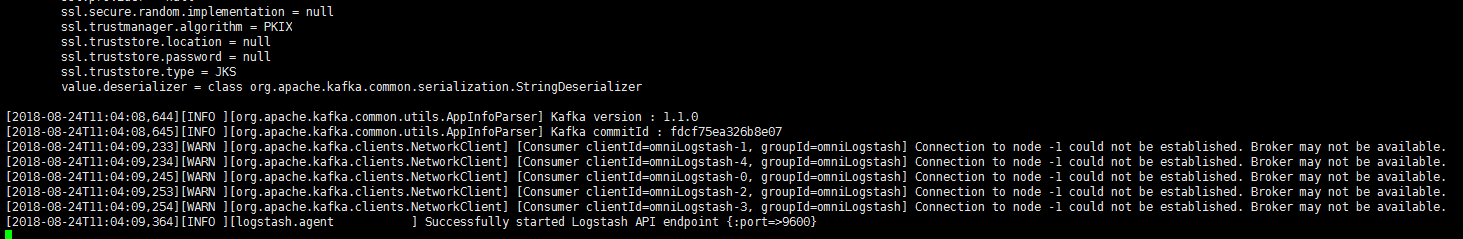
参考说明：

|  |
| --- |
| input {  kafka {  //kafka集群  bootstrap\_servers => ["192.168.206.200:9092,192.168.206.201:9092,192.168.206.202:9092"]  consumer\_threads => 5  topics => ["omniLogstash"]  group\_id => "omniLogstash"  client\_id => "omniLogstash"  auto\_offset\_reset => "latest" //从最新的偏移量开始消费  decorate\_events => true  type => "bhy" //所有插件通用属性,尤其在input里面配置多个数据源时很有用  }  }  filter {  // 对json格式数据进行转换  json {  source => "message"  #remove\_field => ["message"]  }  }  output {  // es配置，此处暂不能获取到appname  elasticsearch {  hosts => ["192.168.206.203:9200"]  index => "logstash-kafka-%{+YYYY-MM-dd}"  }  } |
|  |

## 3.启动

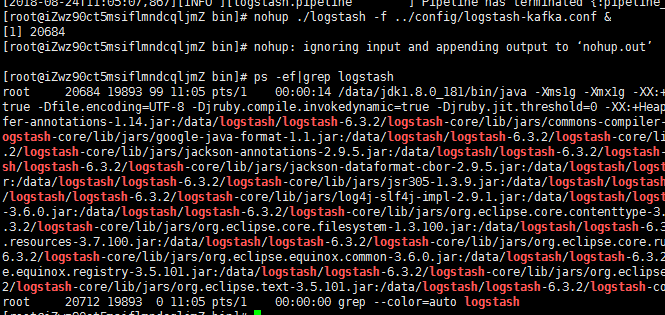
[root@iZwz90ct5msiflmndcqljmZ bin]# ./logstash -f ../config/logstash-kafka.conf





后台启动：

[root@iZwz90ct5msiflmndcqljmZ bin]# nohup ./logstash -f ../config/logstash-kafka.conf &



多个logstash同一台机器启动需要加上path选项

|  |
| --- |
| nohup ./logstash -w 2 -f ../config/logstash-kafka.conf --path.data=/data/logstashKafka &  -w 线程，一般跟CPU核数保持一致  -f  指定配置文件运行  --path.data 指定数据路径，解决多实例运行问题 |

# 三、FQA

## 3.1 logstash不消费kafka日志

Logstash -f logstash-kafka.conf --debug 模式启动

Debug启动发现打印了大量的如下日志：

Coordinator discovery failed, refreshing metadata

导致原因：

之前是由于手动创建了topic，使用了创建的topic命令进行创建消费者测试，导致logstash无法消费kafka的数据，另外也能是产生了很多脏数据导致。

解决方法：

我的解决方法：清空zk和kafka所有内容，重启zk和kafka

另外猜测：应该删除之前手动创建的topic即可(未实验)