杭州ELK部署方案

2017-9-12

|  |  |  |  |
| --- | --- | --- | --- |
| **作者** | **版本** | **时间** | **内容** |
| 卢鹏 | V1.0.0 | 2017-9-11 | 创建 |
|  |  |  |  |
|  |  |  |  |

[1 概述 4](#_Toc493002889)

[2 服务器 4](#_Toc493002890)

[3 组件描述 4](#_Toc493002891)

[4 组件安装 5](#_Toc493002892)

[**4.1** **Elasticsearch** 5](#_Toc493002893)

[**4.1.1.** **JVM设置** 5](#_Toc493002894)

[**4.1.2.** **句柄设置** 5](#_Toc493002895)

[**4.1.3.** **内存设置** 5](#_Toc493002896)

[**4.1.4.** **线程设置** 5](#_Toc493002897)

[**4.1.5.** **Elasticsearch安装** 5](#_Toc493002898)

[**4.1.6.** **Head插件安装（可选）** 5](#_Toc493002899)

[**4.1.7.** **Bigdesk插件安装（可选）** 7](#_Toc493002900)

[**4.2** **Kibana** 8](#_Toc493002901)

[**4.3** **Kafka** 8](#_Toc493002902)

[**4.4** **Logstash** 8](#_Toc493002903)

[5 组件配置 8](#_Toc493002904)

[**5.1.** **Logstash(Server)** 8](#_Toc493002905)

[**5.2.** **Logstash(Client)** 9](#_Toc493002906)

[6 常用命令 10](#_Toc493002907)

# 概述

该手册用于描述杭州机房ELK各服务器使用分布以及相关配置。

# 服务器

|  |  |  |  |
| --- | --- | --- | --- |
| IP | 配置 | 用途 | 备注 |
| 172.30.130.161 | 64核+128G+1.5T | Elasticsearch | 另外安装有oracle |
| 172.30.130.245 | 64核+128G+1000G | Elasticsearch  Kafka  Logstash  Kibana | Kibana可以直接通过5601端口访问。 |
| 172.30.130.246 | 64核+128G+1000G | Elasticsearch  Kafka  Logstash  Kibana | Kibana不能直接通过5601端口访问，因配置有baseBath,用于nginx代理。 |

# 组件描述

|  |  |  |
| --- | --- | --- |
| 组件 | 版本 | 备注 |
| JAVA | 1.8.0\_131 |  |
| Elasticsearch | 5.5.1 |  |
| Logstash | 5.5.1 | 充当采集端client和服务端server |
| Kafka | 2.11-0.10.0.1 |  |

注：ELK5.x各组件需要java1.8+环境编译。

# 组件安装

安装顺序不分前后，java环境为1.8或更高，启动顺序按照Elasticsearch,Kibana,Zookeeper(Kafka安装自带),Kafka,Logstash-server,Logstash-client依次执行。

1. **Elasticsearch**
2. **句柄、内存、线程设置**

用root用户修改/etc/security/limits.conf ，新增

\* soft nofile 65535

\* hard nofile 65535

\* soft memlock unlimited

\* hard memlock unlimited

\* soft nproc 2048

\* hard nproc 4096

执行service sshd restart使生效

1. **JVM线程设置**

用root用户修改/etc/sysctl.conf ，新增

vm.max\_map\_count=262144

执行sysctl –p使生效

1. **Elasticsearch安装**

直接用unzip命令解压zip包即可。

1. **Head插件安装（可选）**

* 获取head,执行

git clone git://github.com/mobz/elasticsearch-head

* 下载nodejs 并安装，执行

wget https://nodejs.org/dist/latest/[node-v8.3.0-linux-x64.tar.gz](https://nodejs.org/dist/latest/node-v8.3.0-linux-x64.tar.gz)

tar -zxvf softset/node-v8.3.0-linux-x64.tar.gz

* 配置环境变量

vim /etc/profile

export NODE\_HOME=/opt/aspire/product/elk/node-v8.3.0-linux-x64/

export PATH=$PATH:$NODE\_HOME/bin

其中的NODE\_HOME路径根据实际路径配置，执行source /etc/profile使生效

* 验证是否安装成功



* grunt安装

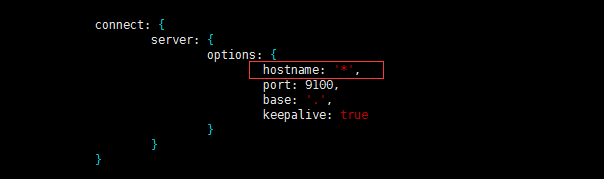
cd到elasticsearch-head目录下，执行

npm install grunt -save

npm install phantomjs-prebuilt@2.1.14 --ignore-scripts

npm install

修改elasticsearch-head下Gruntfile.js文件，增加hostname属性，设置为\*，如下：



* grunt启动

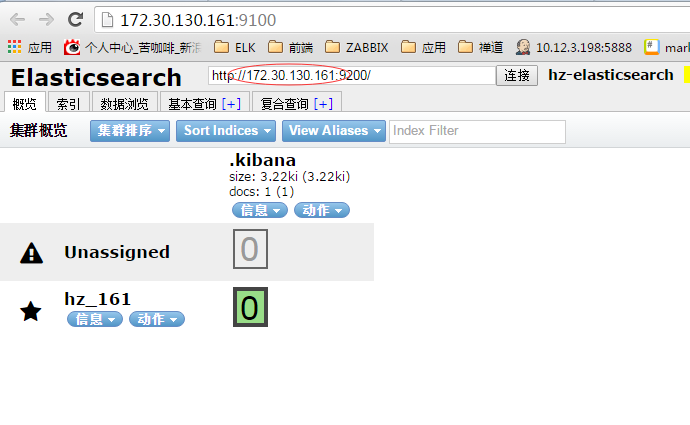
在elasticsearch-head目录下执行

cd /node\_modules/grunt/bin

nohup ./grunt server &

* 访问head

Elasticseach启动后才能访问head,地址：<http://IP:9100>,效果如下：



注意修改图标椭圆标识出的地址，在elasticsearch.yml中必须配置以下属性，否则head前台页面点连接无反应：

|  |
| --- |
| http.cors.enabled: true  http.cors.allow-origin: "\*" |

1. **Bigdesk插件安装（可选）**

* 获取bigdesk,执行

git clone https://github.com/hlstudio/bigdesk

* 启动bigdesk

cd bigdesk-master/\_site

nohup python -m SimpleHTTPServer 9000 &

* 访问bigdesk

Elasticseach启动后才能访问bigdesk,地址为: http://IP:9000 /\_site/#nodes

注意在elasticsearch.yml中必须配置以下属性，否则bigdesk前台页面点connect无反应：

|  |
| --- |
| http.cors.enabled: true  http.cors.allow-origin: "\*" |

1. **Kibana**

直接用tar命令解压tar包即可。

1. **Kafka**

直接用tar命令解压tar包即可。

1. **Logstash**

直接用tar命令解压tar包即可。

# 组件配置

因为ELK各组件的配置依据于服务器配置，随时可调整，完整配置此处暂略，仅提供logstash服务端server和采集端client基本配置。

1. **Logstash(Server)**

用于解析日志，部署在172.30.130.245和172.30.130.246上，组成消费者集群。

在config文件夹下创建conf.d文件夹，在conf.d中创建fromkafka.conf文件，配置内容如下：

|  |
| --- |
| input{  kafka{  bootstrap\_servers =>"172.30.130.245:9092,172.30.130.246:9092"  topics => ["yhzx\_topic"]  group\_id => "yhzx\_consumer"  consumer\_threads => 8  }  }  filter{  #filte用于解析以及过滤日志，依据实际日志接入而定。  }  output{  elasticsearch {  hosts => ["172.30.130.245:9200","172.30.130.246:9200"]  index => "ums-yhzx-%{+YYYY-MM-dd}"  flush\_size => 20000  idle\_flush\_time => 5  }  #stdout { codec => rubydebug }  } |

启动命令：nohup ./logstash -f ../config/conf.d/fromkafka.conf &

1. **Logstash(Client)**

用于采集日志，部署在业务主机上。

在config文件夹下创建conf.d文件夹，在conf.d中创建tokafka.conf文件，配置内容如下：

|  |
| --- |
| input{  file {  path => ["/opt/oneday/log/\*.log", "/opt/oneday/log/\*.txt"] #修改日志路径  start\_position => "end"  codec=>plain{charset=>"GBK"}  }  }  output{  kafka{  bootstrap\_servers =>"172.30.130.245:9092,172.30.130.246:9092"  topic\_id => "yhzx\_topic"  compression\_type => "snappy"  }  } |

修改实际日志路径保存即可，启动命令：nohup ./logstash -f ../config/conf.d/tokafka.conf &

# 常用命令

* Kafka topic列表

bin/kafka-topics.sh --zookeeper 172.30.130.245:2181 --list

* Kafka topic删除

bin/kafka-topics.sh --delete --zookeeper 172.30.130.245:2181 --topic yhzx\_topic

* Kafka topic分区描述

bin/kafka-topics.sh --zookeeper 172.30.130.245:2181 –describe

* Kafka topic分区扩展

bin /kafka-topics.sh --zookeeper 172.30.130.245:2181 -alter --partitions 16 --topic yhzx\_topic

* Kafka消费情况查询

bin/kafka-consumer-groups.sh --group yhzx\_consumer --describe --zookeeper 172.30.130.245:2181