# ELK部署文档

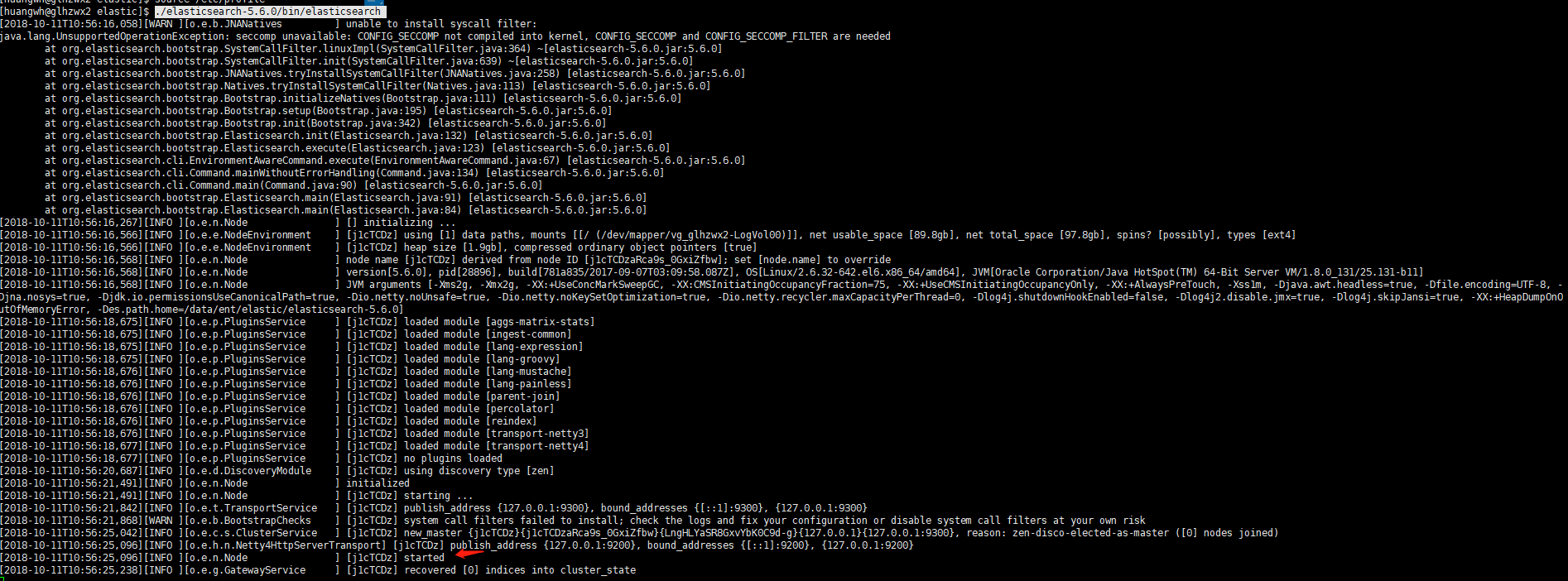
\*：elasticsearch，logstash需要jdk支持，5.6的es版本需要使用1.8的jdk版本，安装略。

## Elasticsearch

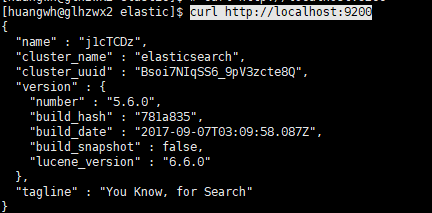
1. 将elasticsearch-5.6.0.tar.gz包上传至安装目录下；
2. tar -zxvf elasticsearch-5.6.0.tar.gz解压文件；
3. elasticsearch不能使用root权限启动，启动时需切换用户（假设用户elk）；
4. 切换后启动会报错，需切换root用户，给目录加权限；

chmod -R 777 elasticsearch-5.6.0

1. 切换回用户elk，启动:./elasticsearch-5.6.0/bin/elasticsearch，如下日志显示成功；



1. 测试。使用命令：curl [http://localhost:9200，显示基本信息则安装成功；](http://localhost:9200，显示基本信息则安装成功。)



1. 开放外部访问。

vim elasticsearch-5.6.0/config/elasticsearch.yml，添加：

network.host: {ip}

bootstrap.memory\_lock: false

bootstrap.system\_call\_filter: false

vim /etc/security/limits.conf，添加：

{用户名} hard nofile 65536

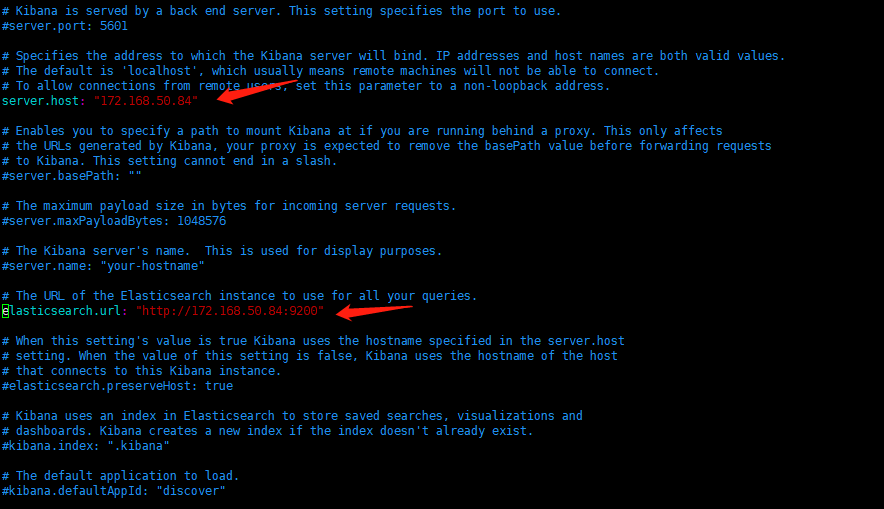
{用户名} soft nofile 65536

vim /etc/sysctl.conf，添加 vm.max\_map\_count=262144，执行生效：sysctl -p；

8、开放9200端口，重新启动，浏览器访问http://{ip}:9200,返回上面基本信息则安装成功。

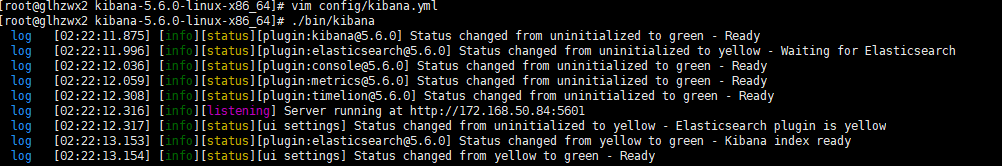
## Kibana

1. 将kibana-5.6.0-linux-x86\_64.tar.gz包上传至服务器安装目录下；
2. cd /data/ent/elastic, 进入安装目录；
3. tar -zxvf logstash-5.6.0.tar.gz，解压；
4. vim kibana-5.6.0-linux-x86\_64/config/kibana.yml,配置elasticsearch地址；



这边需要修改server.host(服务器地址)，elasticsearch.url(elasticsearch访问地址)两处；

1. 防火墙端口开放5601。
2. 执行命令：./bin/kibana；后台启动使用nohup命令；



1. 浏览器访问：<http://{ip}:5601>

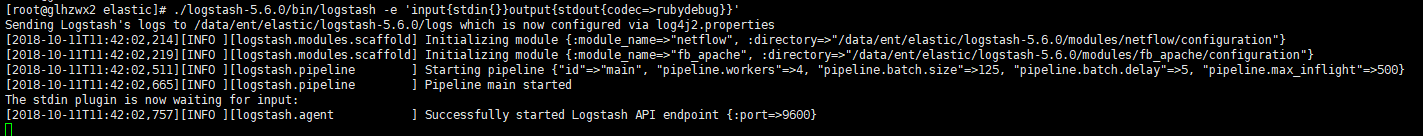
## Logstash

1、将logstash-5.6.0.tar.gz包上传至服务器安装目录下；

2、cd /data/ent/elastic, 进入安装目录；

3、tar -zxvf logstash-5.6.0.tar.gz，解压；

4、./logstash-5.6.0/bin/logstash -e 'input{stdin{}}output{stdout{codec=>rubydebug}}'启动测试；



1. 输入hello，返回如下则安装成功。

