**本次安装elk使用filebeat收集nginx日志信息发送到logstash进行过滤后发给elasticsearch添加索引再发送到kibana进行展示**

**Centots版本:7.4**

**Elk版本：7.4.1**

**关闭Selinux  
vi /etc/sysconfig/selinux**

SELINUX=disabled #需重启永久生效

保存退出

setenforce 0 #临时生效

关闭Firewalld

systemctl stop firewalld #关闭防火墙

systemctl disable firewalld #禁止开机自启

**安装elk机器设置一下参数：**

**vim /etc/security/limits.conf**

\* soft nofile 65536

\* hard nofile 65536

\* soft memlock unlimited

\* hard memlock unlimited

这里的\*代表的是所有用户名称，可以更换为指定用户名  
另：这里有个坑就是如果/etc/security/limits.d文件夹下的有配置文件，那么会覆盖刚才修改的文件，所以请确保该目录没有其它文件，如有请联系运维人员确认删除

**vim /etc/sysctl.conf**

vm.max\_map\_count=262144

vm.swappiness=0

这个参数的作用是告诉Linux内核尽少的使用swap分区，不等于禁用swap，通过少使用swap来提高性能。  
如果想立即生效而不是重启之后让sysctl.conf生效，请使用sysctl -p

##### **局部生效方式：（针对包管理器安装elasticsearch的形式）**

systemctl edit elasticsearch

此命令会在/etc/systemd/system下创建elasticsearch.service.d/override.conf文件

添加如下内容

[Service]

LimitMEMLOCK=infinity

保存，退出，执行如下命令生效

systemctl daemon-reload

**安装jdk.11.0.5,官网下载：**<https://www.oracle.com/technetwork/java/javase/downloads/jdk11-downloads-5066655.html>

tar xvf jdk-11.0.5\_linux-x64\_bin.tar.gz -C /usr/local/

mv /usr/local/jdk-11.0.5 /usr/local/jdk

**vim /etc/profile**

export JAVA\_HOME=/usr/local/jdk

Export CLASSPATH=.:$JAVA\_HOME/jre/lib/rt.jar:$JAVA\_HOME/lib/dt.jar:$JAVA\_HOME/lib/tools.jar

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

ln -s /usr/local/jdk/bin/java /bin/

**安装elasticsearch，在官网下载yum文件：**[https://www.elastic.co/guide/en/elasticsearch/reference/7.4/rpm.html#rpm-repo](https://www.elastic.co/guide/en/elasticsearch/reference/7.4/rpm.html" \l "rpm-repo)

yum install elasticsearch -y #安装elasticsearch

mkdir -p /data/elasticsearch/data #手动建数据索引文件夹

mkdir -p /data/elasticsearch/logs #手动建数据日志文件夹

chown elasticsearch: elasticsearch -R /data #修改elk文件夹属主与属组

**编辑elasticsearch配置文件  
vi /etc/elasticsearch/elasticsearch.yml**

#找到配置文件中的cluster.name，打开该配置并设置集群名称

cluster.name: elk

#找到配置文件中的node.name，打开该配置并设置节点名称

node.name: node1

#修改data存放的路径

path.data: /data/elasticsearch/data

#修改logs日志的路径

path.logs: /data/elasticsearch/logs

#配置内存使用用交换分区

bootstrap.memory\_lock: true

#监听的网络地址(一定要本地IP，不能用127.0.0.1 and localhost)

network.host: 0.0.0.0

#开启监听的端口

http.port: 9200

#增加新的参数，这样head插件可以访问es (5.x版本，如果没有可以自己手动加)

http.cors.enabled: true

http.cors.allow-origin: "\*"

#允许创建的索引

action.auto\_create\_index: "\*"

**保存，退出！**

**配置elastic内存**

vim /etc/elasticsearch/jvm.options 修改  
- Xms8g  
- Xmx8g

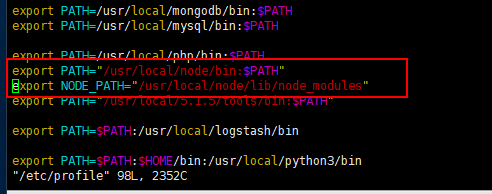
systemctl enable elasticsearch #设置开机启动elasticsearch服务

systemctl start elasticsearch #启动elasticsearch

**安装elasticsearch-head插件**

1.安装nodejs环境  
1)   **wget https://npm.taobao.org/mirrors/node/latest-v8.x/node-v8.10.0-linux-x64.tar.gz**  
2)   **tar -zxvf node-v8.10.0-linux-x64.tar.gz -C /usr/local/**

1. **mv /usr/local/node-v8.10.0-linux-x64/ /usr/local/node**  
   4)   **vim /etc/profile**5)   追加 export PATH=$PATH:/自定义路径/node-v4.4.7-linux-x64/bin 至文件最后

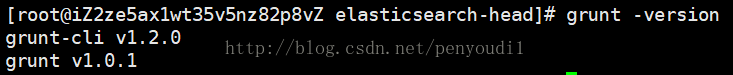


6)   source /etc/profile    重启配置文件命令  
测试  node --version  
 v8.10.0

IMG_256

IMG_258

2.安装grunt  
     1）安装grunt命令行工具grunt-cli      **npm install -g grunt-cli**    2）安装grunt及其插件                     **npm install grunt --save-dev**   
     测试命令：**grunt -version**



成功后执行下面的安装命令：

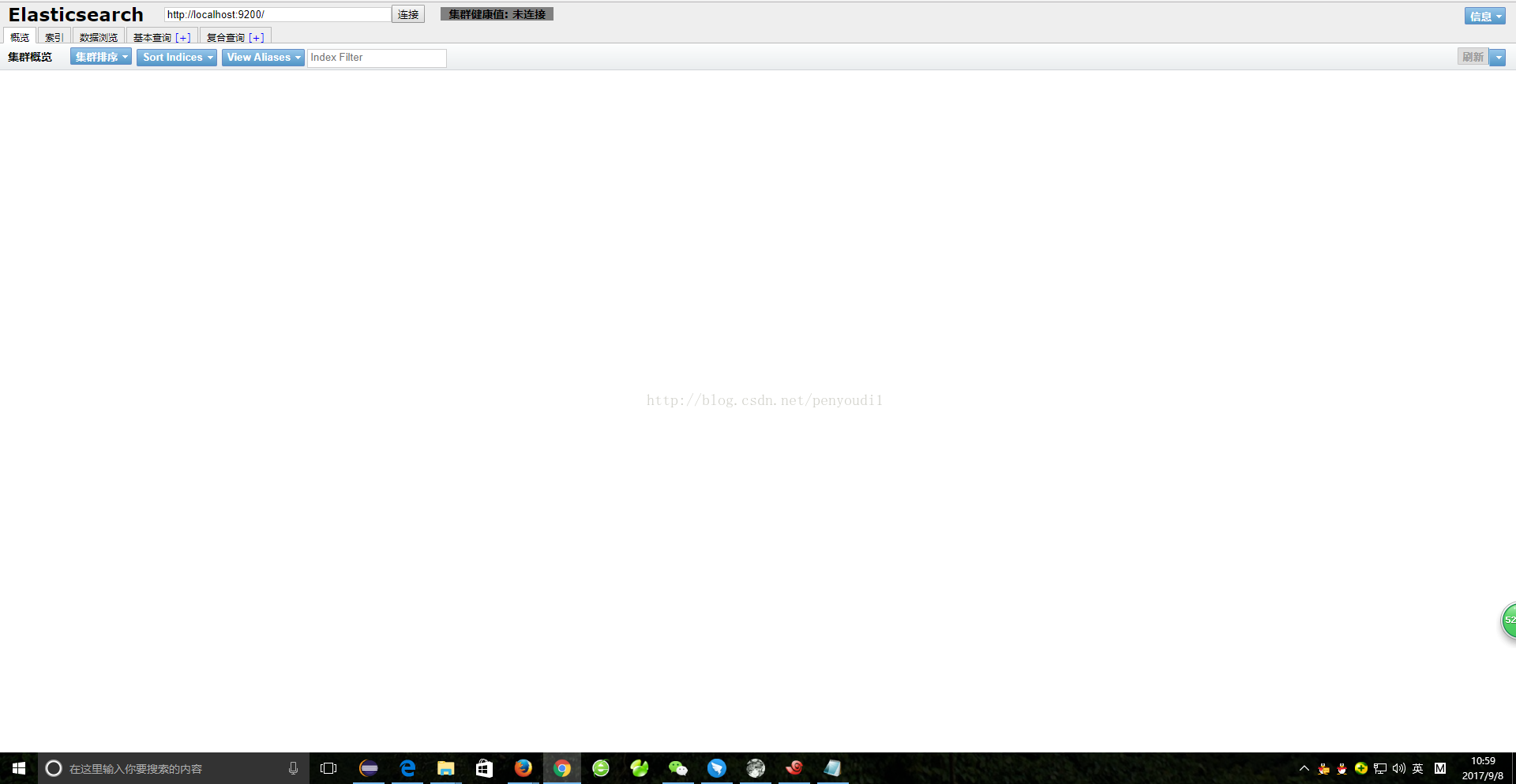
**git clone git://github.com/mobz/elasticsearch-head.git**    **mv elasticsearch-head /usr/local/head**

**cd /usr/local/head  
    npm install  
    npm install grunt --save**修改head下Gruntfile.js文件，默认监听在127.0.0.1下9200端口，



原文件中没有hostname,请按照图片中说明的添加，并将值改为0.0.0.0

然后 **cd /usr/local/head**

执行 **grunt server &**  
（&符号为可选，加上是后台运行）  
浏览器访问 http://ip地址:9100/

以上就是ElasticSearch-head插件安装的过程

**安装logstash，在官网下载yum源：**

[https://www.elastic.co/guide/en/logstash/7.4/installing-logstash.html#\_yum](https://www.elastic.co/guide/en/logstash/7.4/installing-logstash.html" \l "_yum)

yum install logstash -y #安装elasticsearch

**#Logstash.yml没有特殊需求就用默认的就好**

**配置Logstash内存**

vim /etc/logstash/jvm.options 修改  
- Xms8g  
- Xmx8g

**编辑接受规则后过滤的文件：**

**vim /etc/logstash/conf.d/log\_nginx.conf**

input {

beats {

host => "172.16.0.55"

port => "5044"

}

}

filter {

if [fields][log\_source] == "172.16.0.207-nginx"{

grok { #使用正则匹配解析日志字段

match => { "message" => "%{IPORHOST:agent\_ip} - - \[%{HTTPDATE:access\_time}\] \"%{WORD:http\_method} %{DATA:url} HTTP/%{NUMBER:http\_version}\" %{NUMBER:request\_status} %{NUMBER:body\_sent\_bytes} \"%{DATA:agent\_url}\" \"%{DATA:agent}\""

}

}

date { #使用date转换时间格式

match => ["access\_time", "dd/MMM/yyyy:HH:mm:ss Z"]

target => "logdate" #新生成转换时间格式后的字段

}

geoip { #配置geoip地理解析

source => "agent\_ip" #设置解析ip字段

target => "geo\_ip" #将geoip解析数据保存到一个字段

}

urldecode { #所有字段允许显示中文

all\_fields => true

}

}

}

output {

if [fields][log\_source] == "172.16.0.207-nginx"{

elasticsearch { #配置 elasticsearch服务地址

hosts => ["172.16.0.55:9200"]

index => "207-nginx-%{+YYYY.MM.dd}"

}

}

}  
**保存，退出**

systemctl enable logstash #设置开机启动logstash服务

systemctl start logstash #启动logstash

**安装kibana，在官网下载yum源：**

[https://www.elastic.co/guide/en/kibana/7.4/rpm.html#rpm-repo](https://www.elastic.co/guide/en/kibana/7.4/rpm.html" \l "rpm-repo)

yum install kibana -y #安装kibana

**编辑kibana配置文件**

**vim /etc/kibana/kibana.yml**

#服务端口

server.port: 5601

#服务监听ip

server.host: "0.0.0.0"

#连接elasticsearch服务地址

elasticsearch.hosts: ["http://172.16.0.55:9200"]

#kibana索引

kibana.index: ".kibana"

#设置显示中文

i18n.locale: "zh-CN"

**保存，退出！**

systemctl enable kibana #设置开机启动kibana服务

systemctl start kibana #启动kibana

**安装filebeat，在官网下载yum源：**[https://www.elastic.co/guide/en/beats/filebeat/7.4/setup-repositories.html#\_yum](https://www.elastic.co/guide/en/beats/filebeat/7.4/setup-repositories.html" \l "_yum)

yum install filebeat -y #安装filebeat

**编辑filebeat配置文件**

**vim /etc/filebeat/filebeat.yml**

filebeat.inputs:

- type: log #inputs类型，默认为log

enabled: true

paths:

- /var/log/nginx/access.log #此处是log日志服务器集中采集本地日志文件

fields:

log\_source: 172.16.0.207-nginx #添加字段标签

scan\_frequency: 10s #该参数指定Filebeat搜索新文件的频率

output.logstash:

hosts: ["172.16.0.55:5044"]

**保存，退出！**

systemctl enable filebeat #设置开机启动filebeat服务

systemctl start filebeat #启动filebeat