

## 安装步骤

此安装环境为 centos 7.2

1. 安装 java 至少 1.8 版本(最好 1.9 或者更高)
  - linux 查看 java 版本
  - java -version
  - yum install java 默认 1.8 可以使用
2. 先安装 elasticsearch 我安装的 7.5(版本需要和后面的统一)
  - 下载地址: <https://www.elastic.co/cn/downloads/>
  - 建立一个文件夹 elk
  - 解压 tar -zxvf elasticsearch
  - 修改配置文件

在 config 目录下的 elasticsearch.yml 文件中你可以设置 es 服务的端口号以及网络 ip 等

```
network.host: 0.0.0.0
# custom config
node.name: "node-1"
discovery.seed_hosts: ["127.0.0.1", "[:,1]"]
cluster.initial_master_nodes: ["node-1"]
# 开启跨域访问支持, 默认为 false
http.cors.enabled: true
#跨域访问允许的域名地址, (允许所有域名) 以上使用正则
http.cors.allow-origin: /*/
```

启动:

进入 bin 目录下  
./elasticsearch

注意事项:

1. 请用普通用户启动个否则报错
2. 给此用户这个目录的最大权限

切换到 root 账户

编辑 /etc/sysctl.conf 追加以下内容

```
vm.max_map_count=655360
```

保存后, 执行:

```
sysctl -p
```

浏览器输入 222.229.27.225:9200 访问一下

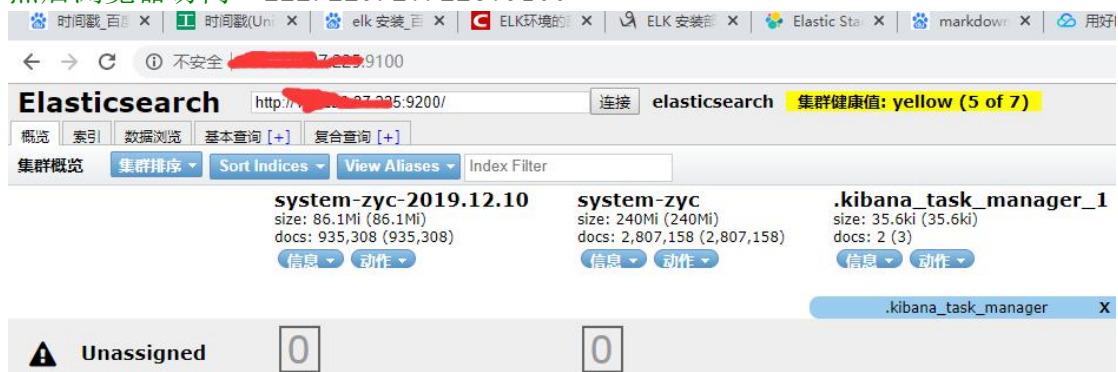
```
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "7hyy5ANOS1Su_KQUySVEEw",
  "version" : {
    "number" : "7.5.0",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "e9ccaed468e2fac2275a3761849cbee64b39519f",
    "build_date" : "2019-11-26T01:06:52.518245Z",
    "build_snapshot" : false,
    "lucene_version" : "8.3.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

出现这个数据为正常 安装成功

安装 elasticsearch-head 插件： 很重要，也很有必要方便看 es 的数据

```
# yum install -y npm
# git clone git://github.com/mobz/elasticsearch-head.git
# cd elasticsearch-head
# npm install
# npm run start
检查端口是否起来
netstat -antp |grep 9100
浏览器访问测试是否正常
```

然后浏览器访问 222.229.27.225:9100



会看着这个 证明成功

### 3 安装 kibana

下载地址: <https://www.elastic.co/cn/downloads/>

注意:版本和上面一致

```
tar -zxvf kibana
```

```
cd kibana
```

```
./bin/kibana 启动
```

注意:

请用普通用户启动个否则报错

如果重启可以

```
ps -ef | grep node
```

```
[zyc@VM_0_15_centos bin]$ ps -ef | grep node
zyc      5036  4984 13 19:56 pts/2    00:00:15 ./../node/bin/node ./../src/cli
zyc      5450  4984  0 19:59 pts/2    00:00:00 grep --color=auto node
[zyc@VM_0_15_centos bin]$
```

Kill 进程 id

`./bin/kibana` 启动

#### 4 安装 logstash

下载地址: <https://www.elastic.co/cn/downloads/>

注意:版本和上面一致

```
tar -zxvf logstash
```

`config/logstash.conf` 配置文件

```
input {
  file {
    path => "/zyc/log/*.log"
    start_position => beginning
  }
}
```

```
output {
  elasticsearch {
    hosts => ["123.333.22.225:9200"]
    index => "system-zyc"
    #user => "elastic"
    #password => "changeme"
  }
}
```

```
input {
  file {
    path => "/zyc/log/*.log"
    start_position =>beginning
  }
}

output {
  elasticsearch {
    hosts => ["192.168.1.225:9200"]
    index => "system-zyc"
    #user => "elastic"
    #password => "changeme"
  }
}
~
~
~
```

启动

```
./logstash -f /zyc/elk/logstash-7.5.0/config/logstash.conf
```

5.