# [docker搭建单机ELK](https://www.cnblogs.com/lz0925/p/12018209.html)

yum -y install epel-release

yum -y install python-pip

// 更新pip

pip install --upgrade pip

// 安装docker-compoes，如已安装，跳过

pip install docker-compose

// 下载elasticsearch，logstash，kibana， 自es5开始，一般三个软件的版本都保持一致了。

docker pull docker.elastic.co/elasticsearch/elasticsearch:7.1.1 && docker pull docker.elastic.co/logstash/logstash:7.1.1 && docker pull docker.elastic.co/kibana/kibana:7.1.1

**配置**

* 我们建立一个目录，用来存放yml文件（docker-compose启动一组编排过的容器时使用）

mkdir -p /root/elk

cd /root/elk

vim docker-compose.yml

* docker-compose.yml文件内容如下

version: '3'

services:

elasticsearch:

image: docker.elastic.co/elasticsearch/elasticsearch:7.1.1

container\_name: elasticsearch7.1.1

environment:

- node.name=node-41 # 节点名称，集群模式下每个节点名称唯一

- network.publish\_host=172.168.50.41 # 用于集群内各机器间通信,对外使用，其他机器访问本机器的es服务，一般为本机宿主机IP

- network.host=0.0.0.0 # 设置绑定的ip地址，可以是ipv4或ipv6的，默认为0.0.0.0，即本机

- discovery.seed\_hosts=172.168.50.40,172.168.50.240,172.168.50.41 # es7.0之后新增的写法，写入候选主节点的设备地址，在开启服务后，如果master挂了，哪些可以被投票选为主节点

- cluster.initial\_master\_nodes=172.168.50.40,172.168.50.240,172.168.50.41 # es7.0之后新增的配置，初始化一个新的集群时需要此配置来选举master

- cluster.name=es-cluster # 集群名称，相同名称为一个集群， 三个es节点须一致

# - http.cors.enabled=true # 是否支持跨域，是：true // 这里设置不起作用，但是可以将此文件映射到宿主机进行修改，然后重启，解决跨域

# - http.cors.allow-origin="\*" # 表示支持所有域名 // 这里设置不起作用，但是可以将此文件映射到宿主机进行修改，然后重启，解决跨域

- bootstrap.memory\_lock=true # 内存交换的选项，官网建议为true

- "ES\_JAVA\_OPTS=-Xms512m -Xmx512m" # 设置内存，如内存不足，可以尝试调低点

#- discovery.type=single-node # 是否启用单节点模式，如果启用，上面这些环境配置，只保留两个内存的选项即可。

ulimits: # 栈内存的上限

memlock:

soft: -1 # 不限制

hard: -1 # 不限制

volumes:

- esdata:/usr/share/elasticsearch/data

- /root/elk/elasticsearch.yml:/usr/share/elasticsearch/config/elasticsearch.yml

hostname: elasticsearch

restart: always

ports:

- 9200:9200

- 9300:9300

kibana:

image: docker.elastic.co/kibana/kibana:7.1.1

container\_name: kibana7.1.1

environment:

- elasticsearch.hosts=http://elasticsearch:9200

hostname: kibana

depends\_on:

- elasticsearch

restart: always

ports:

- 5601:5601

logstash:

image: docker.elastic.co/logstash/logstash:7.1.1

container\_name: logstash7.1.1

hostname: logstash

restart: always

depends\_on:

- elasticsearch

ports:

- 9600:9600

- 5044:5044

volumes:

esdata:

driver: local

* 在当前目录，启动elk

docker-compose up -d

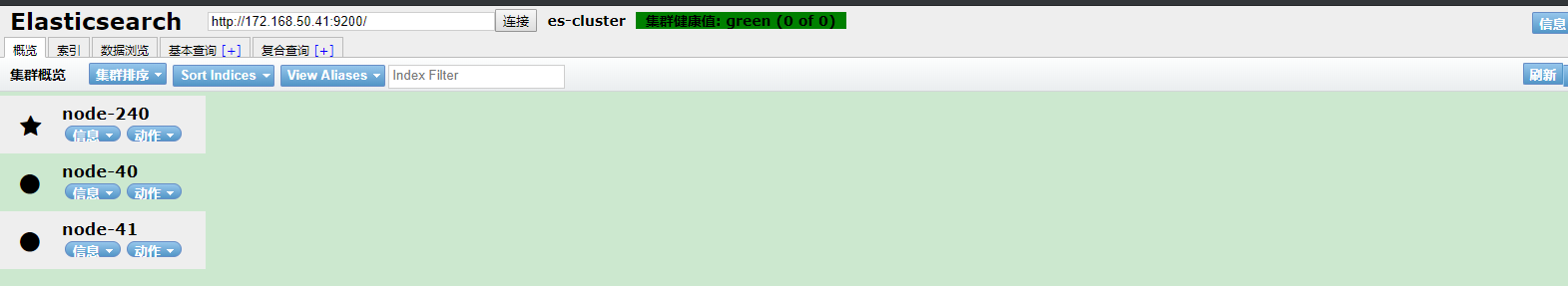
* 出现done表示成功，docker-compose logs 查看日志（分别输出elk三个服务的日志）执行docker ps可以看到三个服务的运行状态
* 在浏览器输入http://IP:5601/
* 可以使用head监控es

// 拉取镜像

docker pull mobz/elasticsearch-head:5

// 启动

docker run -d --name es\_admin -p 9100:9100 mobz/elasticsearch-head:5

* 在浏览器输入http://IP:9100  
  
* 注意，IP地址要使用你es所在服务器的地址，然后点击连接，出现类似的显示说明，没问题，我这里是三个节点，你应该只有一个节点。
* 如果点击连接没有反应，F12查看network是403，或者200，但是console中提示跨域，那么你需要设置跨域，下面说两个方法

方法1： 直接进入容器中，使用 docker exec -it 容器ID /bin/bash ，进入后修改/usr/share/elasticsearch/config/elasticsearch.yml文件，

加入以下两行：

http.cors.enabled: true

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

方法2：将容器中的es配置文件映射到宿主机，然后加入以上两行配置重启即可，映射文件就不说了，如果不会，参考