centos7中使用docker搭建elk

创建文件夹mkdir /data/elk，在文件夹下创建docker-compose.yml文件，文件内容如下

version: '3'

services:

elasticsearch:

image: elasticsearch:7.2.0 #镜像

container\_name: elk\_elasticsearch #定义容器名称

restart: always #开机启动，失败也会一直重启

environment:

- discovery.type=single-node

ports:

- 9500:9200

kibana:

image: kibana:7.2.0

container\_name: elk\_kibana

restart: always

depends\_on:

- elasticsearch #kibana在elasticsearch启动之后再启动

environment:

- ELASTICSEARCH\_URL=http://elasticsearch:9500 #设置访问elasticsearch的地址

ports:

- 5601:5601

logstash:

image: logstash:7.2.0

container\_name: elk\_logstash

restart: always

volumes:

- /data/elk/logstash/logstash-springboot.conf:/usr/share/logstash/pipeline/logstash.conf #挂载logstash的配置文件

depends\_on:

- elasticsearch #kibana在elasticsearch启动之后再启动

links:

- elasticsearch:es #可以用es这个域名访问elasticsearch服务

ports:

- 4560:4560

elasticsearch-head:

image: mobz/elasticsearch-head:5

container\_name: elk\_elasticsearch\_head

restart: always

ports:

- 9100:9100

depends\_on:

- elasticsearch

在elk下创建logstash目录，进入目录创建logstash-springboot.conf文件，在文件内写入如下内容

input {

tcp {

mode => "server"

host => "0.0.0.0"

port => 5044

codec => json\_lines

}

}

output {

elasticsearch {

hosts => ["http://192.168.9.50:9500"]

index => "elk"

codec => "json"

}

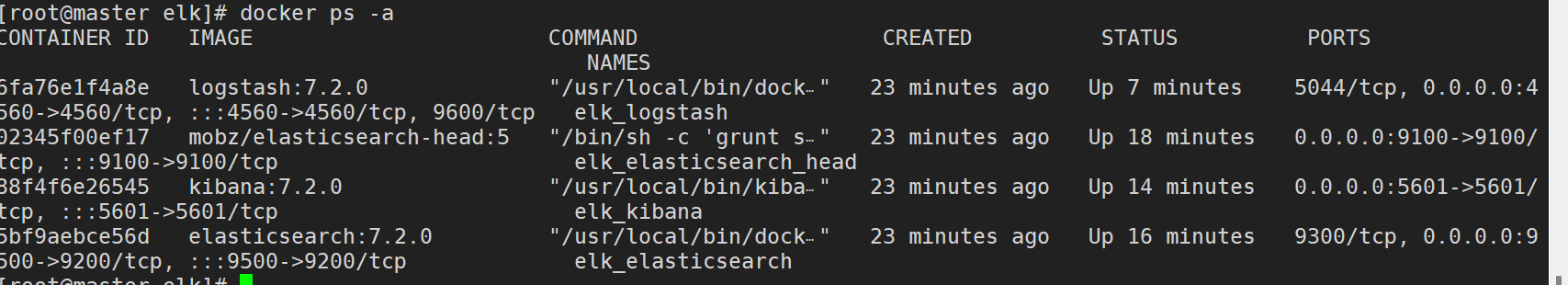
stdout {

codec => rubydebug

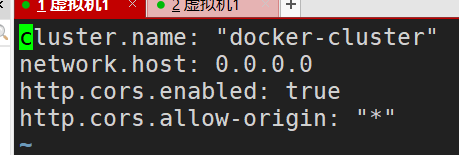
}

}

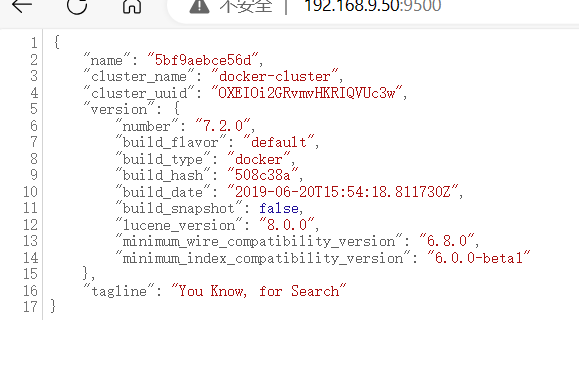
写入内容完毕后输入docker-compose up -d运行，查看容器状态，显示都在运行



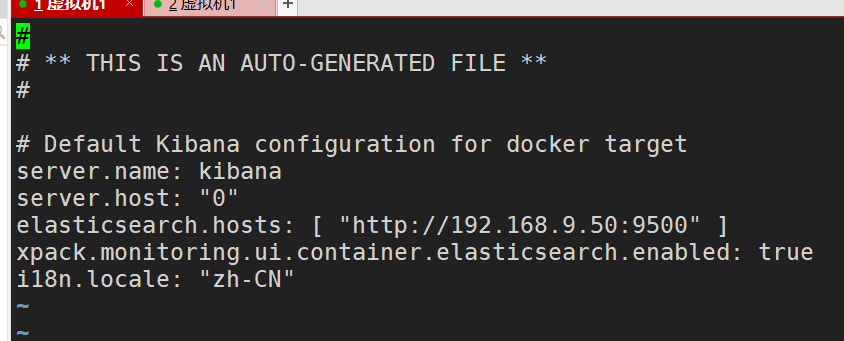
输入命令docker exec -it elk\_elasticsearch /bin/bash进入elk\_elasticsearch容器内部，输入 vi config/elasticsearch.yml编写文件，如下图



编写完毕后保存并重启容器，从本地访问192.168.9.50:9500成功，如下图

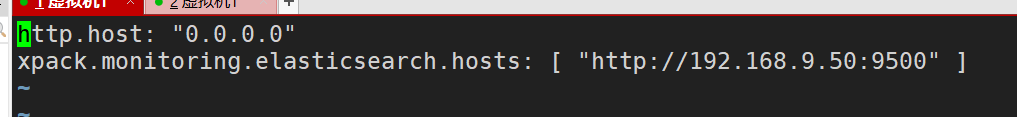


输入docker exec -it elk\_kibana /bin/bash进入kibana容器命令行，输入vi comfig/kibana.yml编辑文件，如下



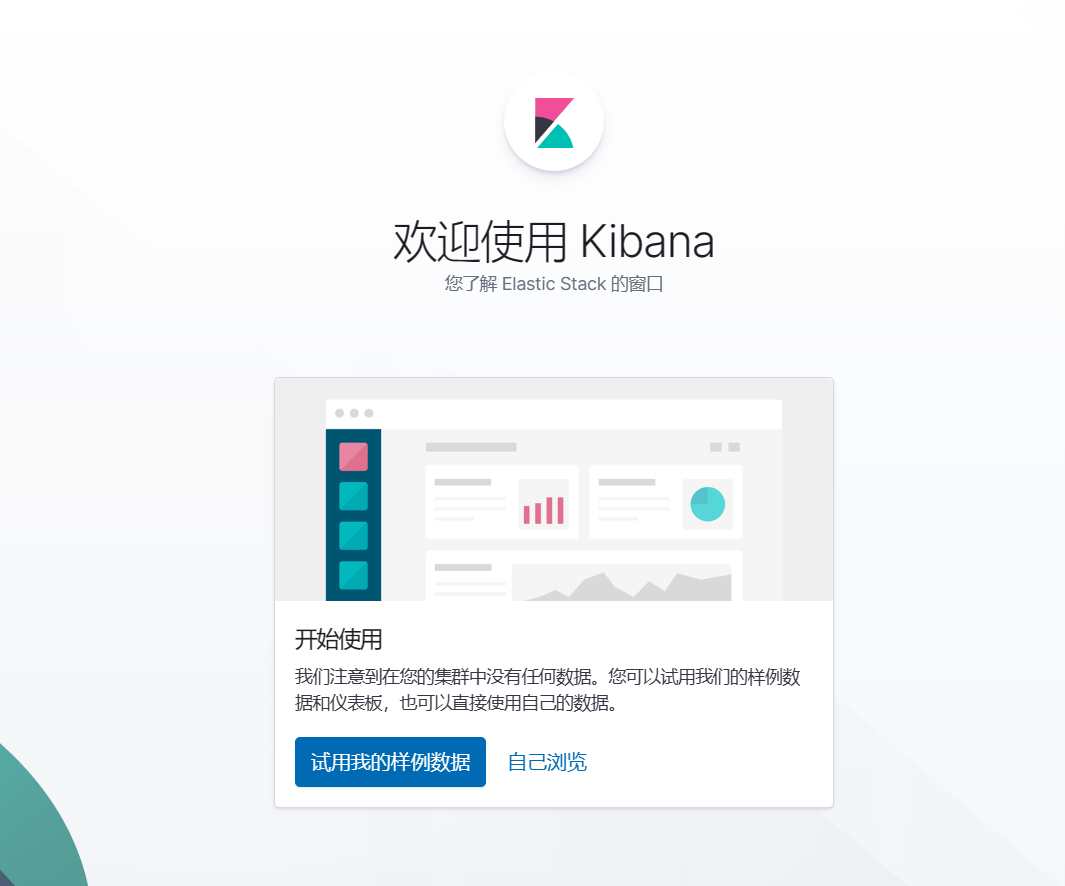
保存退出后重启容器

输入docker exec -it elk\_logstash /bin/bash进入logstash容器命令行，输入vi config/logstash.yml编辑文件，如下图



保存文件,退出命令行并重启容器

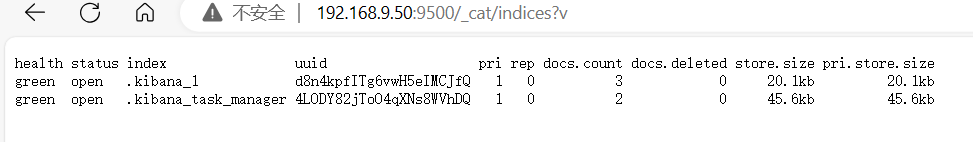
访问kibana界面



访问elasticsearch-head界面



输入http://localhost:9200/\_cat/indices?v查看es是否获取数据



根据教学文档，配置完成后途中应该显示elk索引，如下图所示实际配置完成之后无法显示elk索引

