## Docker24.0.7+ELK7.2.0

本地docker24.0.7部署搭建(Elasticsearch7.2.0+Logstsh7.2.0+Kibana7.2.0),实现日志监控链的自动化可视化分析环境

## 1安装

wget https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo -O /etc/yum.repos.d/docker-ce.repo

yum -y install docker版本 (docker-ce-19.03.10)

## 2 修改国内镜像源

vi /etc/docker/daemon.json

{

"registry-mirrors": ["https://mj9kvemk.mirror.aliyuncs.com"]

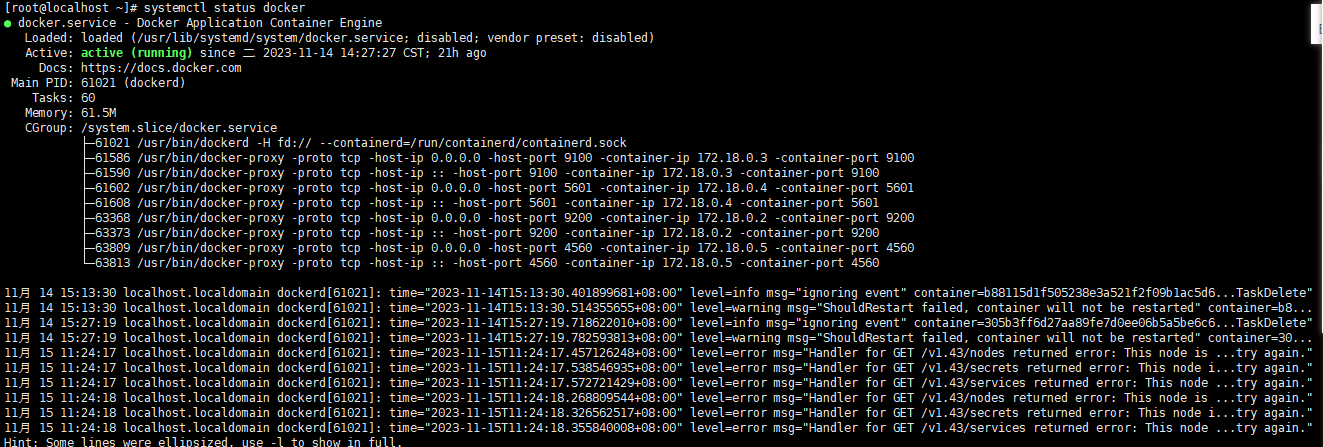
}

## 3 启动

systemctl start docker

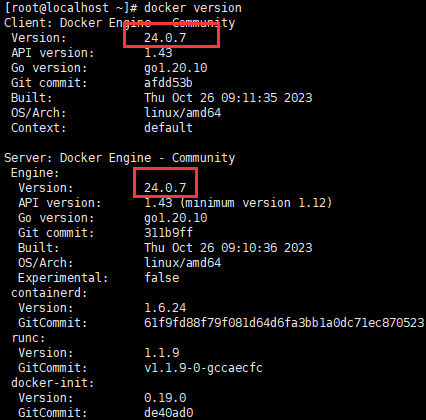
## 4查看状态

systemctl status docker



## 5查看版本

Docker version



**Docker-compose安装**

1.下载

Curl -L"https://github.com/docker/compose/releases/download/1.29.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

2.安装成功赋予权限

chmod +x /usr/local/bin/docker-compose

3.查看版本

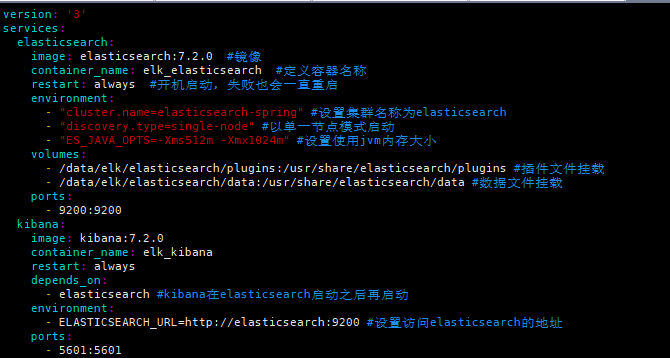
docker-compose --version

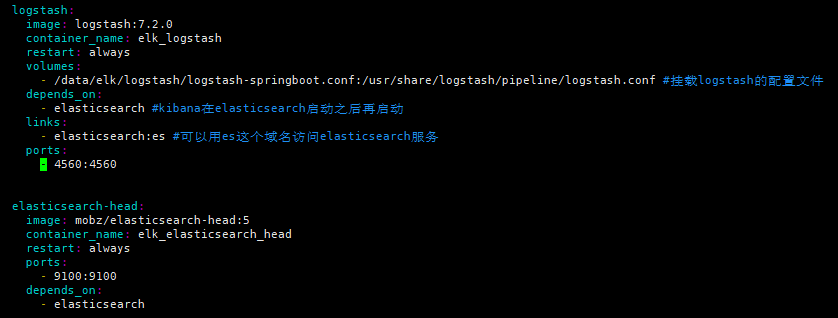


先创建文件夹

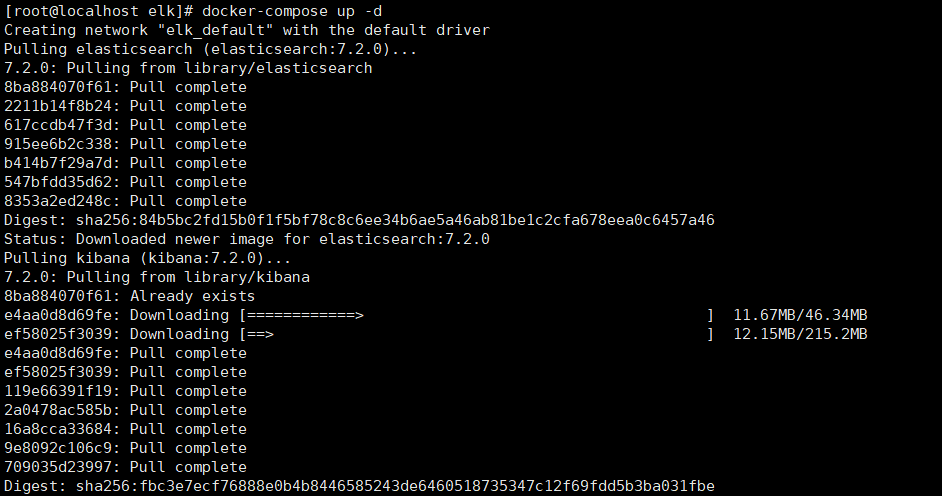
Mkdir /data/elk

在elk里面创建docker-compose.yml

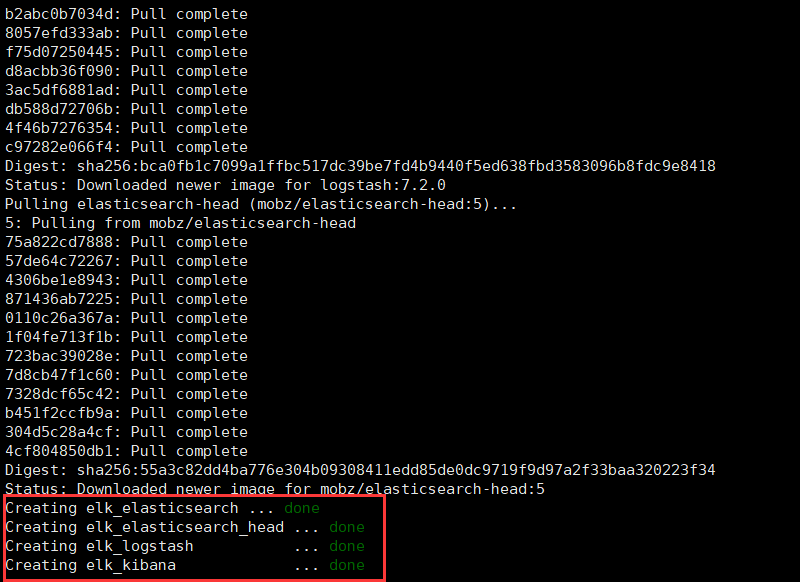


配置完 :wq

在elk文件里执行 docker-compose up -d

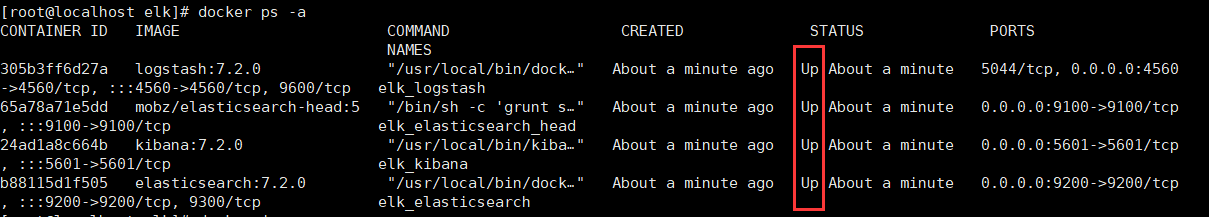


....



再执行

Docker ps -a 查看一下



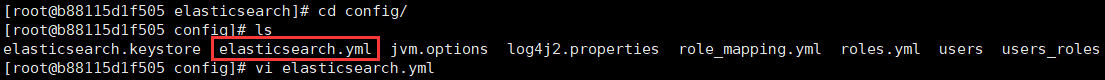
开始配置每个容器的文件

1. **Elasticsearch**

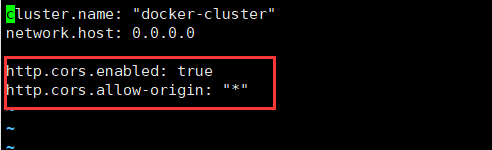
先进入elsticsearch容器内



进入文件夹 并修改文件



添加红框里面的文字



保存退出文件 并退出容器

再安装分词器（在宿主机上安装）

下载分词器

<https://github.com/medcl/elasticsearch-analysis-ik/releases/download/v7.2.0/elasticsearch-analysis-ik-7.2.0.zip>

# 解压后通过ftp上传到服务器下

# 将这个文件夹拷贝到elasticsearch中

docker cp /home/silence/elk/ik es:/usr/share/elasticsearch/plugins

# 查看是否拷贝成功，进入elasticsearch/plugins/ik中：

docker exec -it es /bin/bash

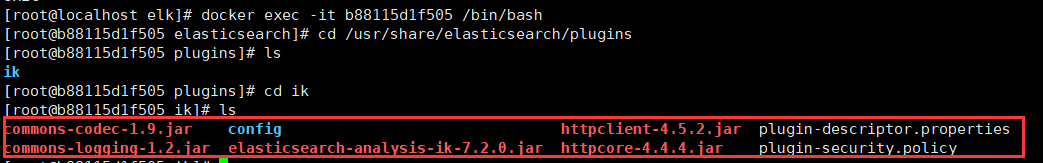
cd /usr/share/elasticsearch/plugins

ls

cd ik

Ls

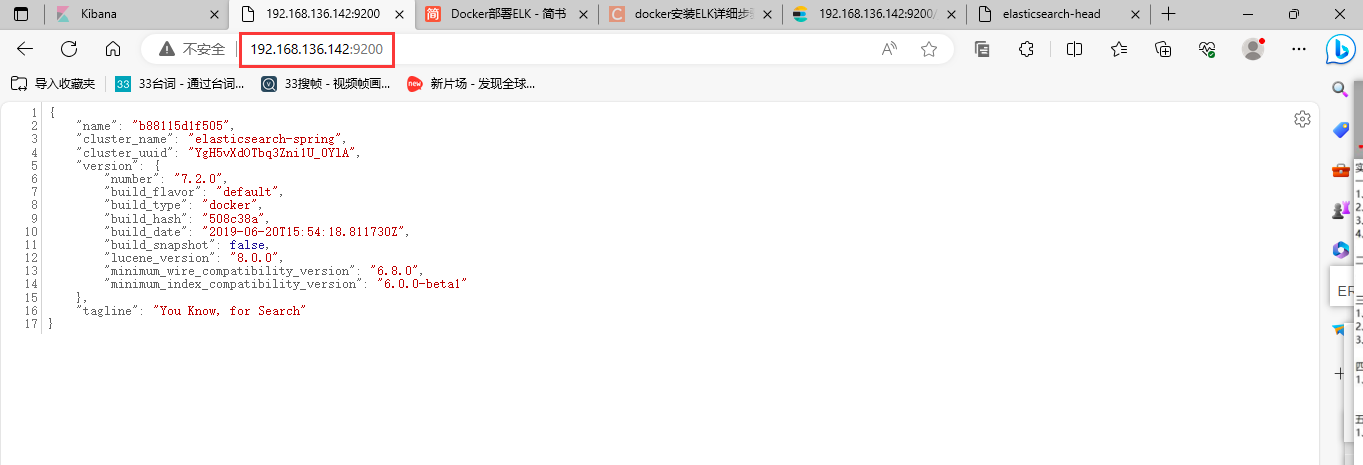
下图就是配置完的



再重启容器

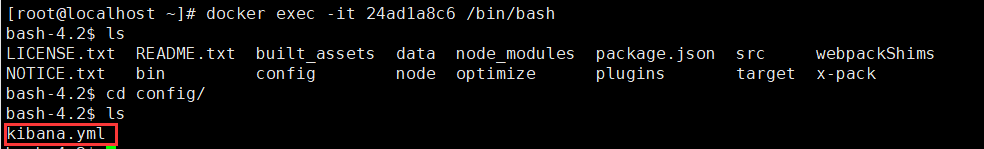


访问网页



**2.Kibana**

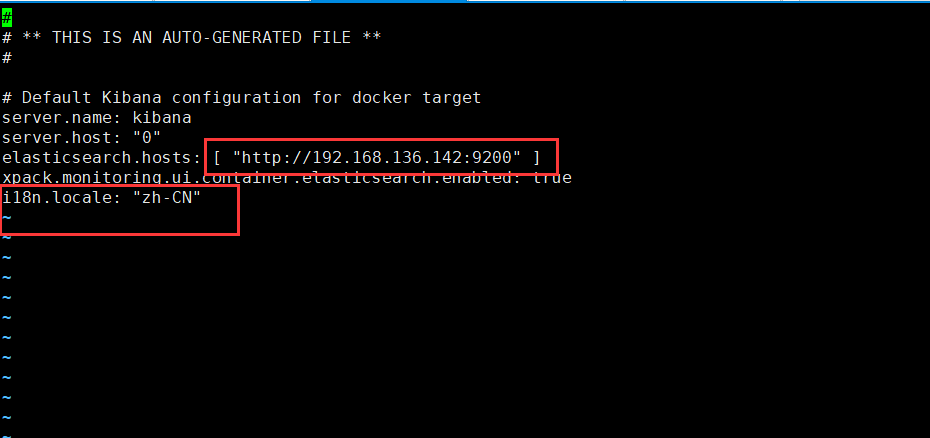
进入Kibana容器内修改配置文件



Ip 为自己虚拟机的ip端口 9200

后面加上中文配置

i18n.locale: "zh-CN"



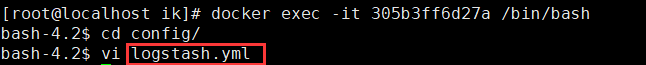
修改完配置文件重启容器



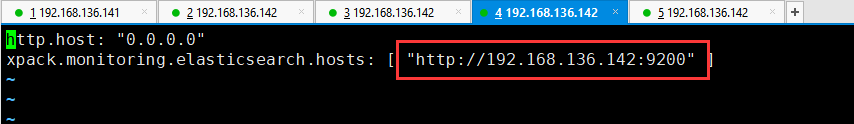
**3.logstash**

进入logstash容器中

修改logstash.yml文件

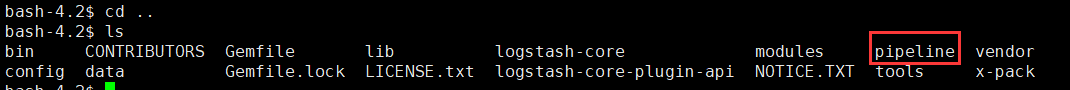


ip自己主机IP 端口elasticsearch的端口



修改完保存退出：wq

再去pipeline文件下配置文件



在pipeline里创建一个名为logstash.yml的文件

在里面写上以下内容



保存退出：wq

退出容器再重启容器Id 为 logstash的id



查看日志（logstash进程的id）

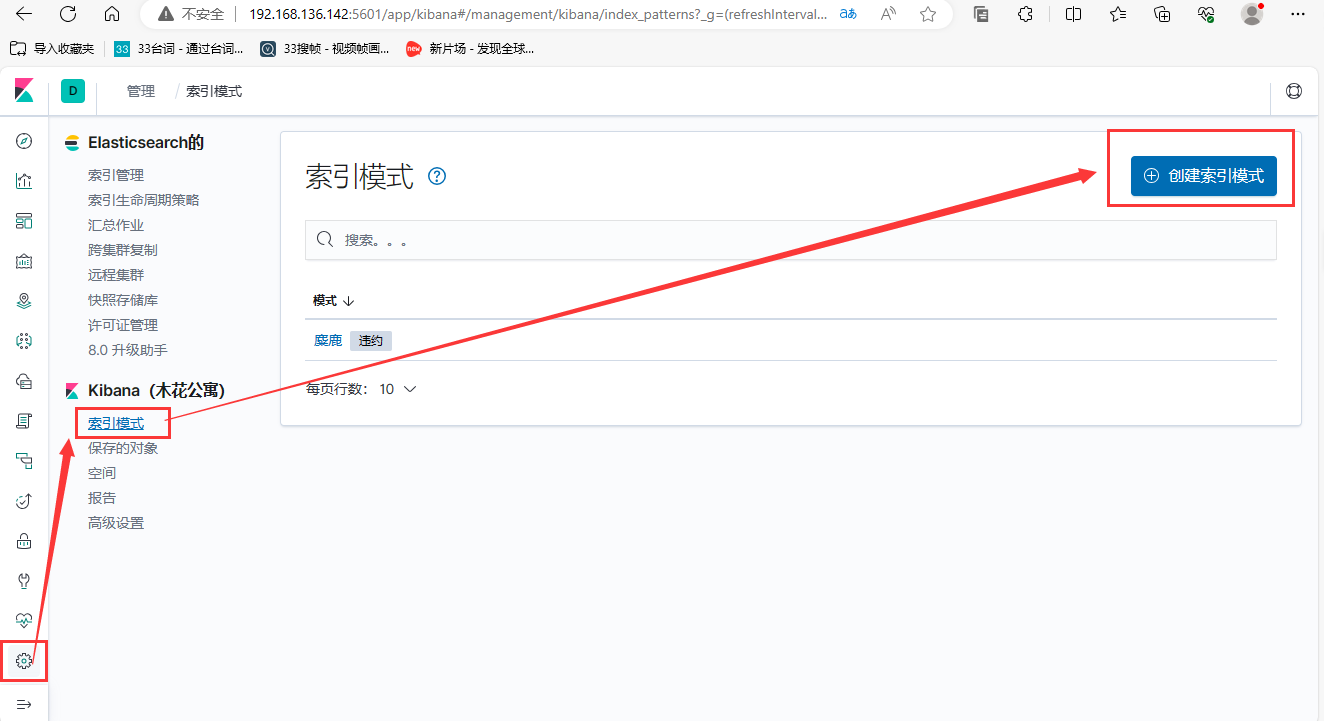


查看elasticsearch是否获取数据

[192.168.136.142:9200/\_cat/indices?v](http://192.168.136.142:9200/_cat/indices?v)

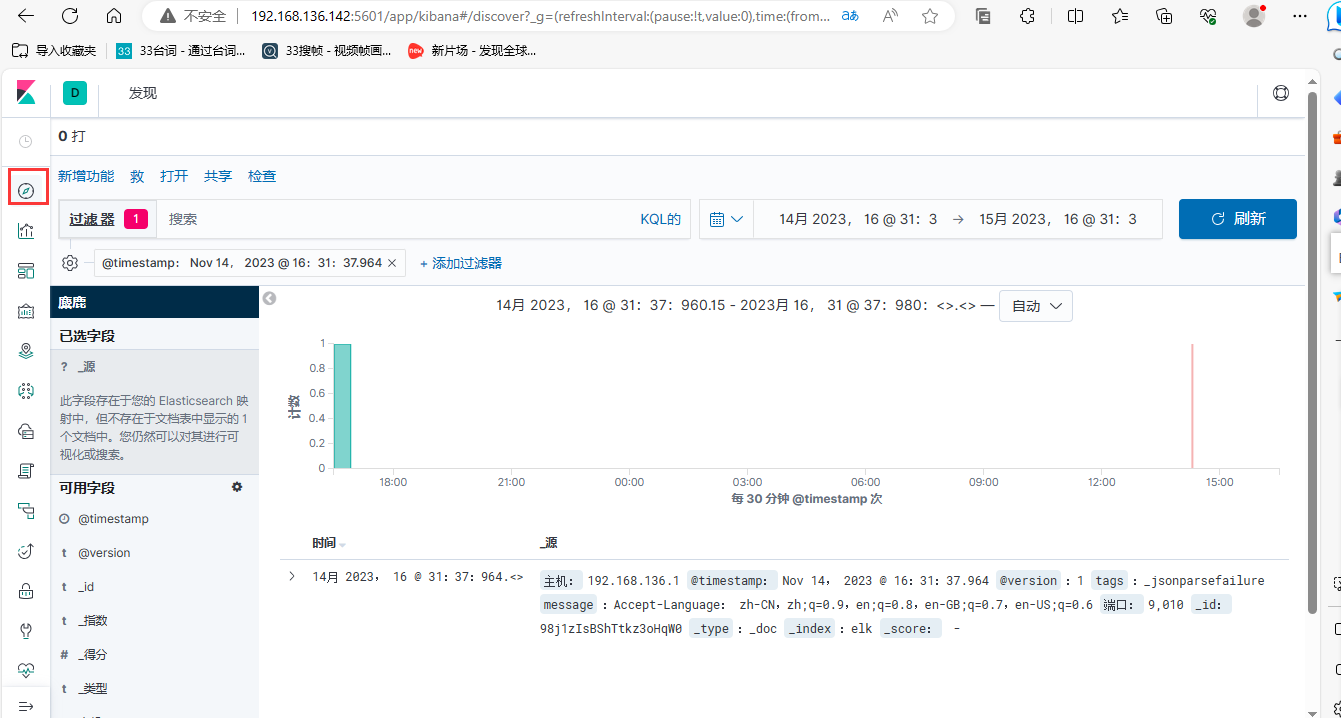


**Kibana 新建索引模式**





主页显示这个界面



最后查看一下elasticsearch-head的网页

192.168.136.142：9100

根据自己的IP写完显示这个界面即为成功

