**docker搭建ELK 7.1版本（出现的坑都有决绝方案）**

docker镜像地址： https://www.docker.elastic.co/#

首先安装docker-compose，使用pip安装docker-compose，因为pip可以自动对应版本问题

安装pip

yum -y install epel-release

yum -y install python-pip

确认版本

pip --version

更新pip

pip install --upgrade pip

1.

安装docker-compose

pip install docker-compose

1.

查看版本

docker-compose version

1.

下载elasticsearch

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

下载logstash

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

下载kibana

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

编写docker-compose.yml文件,在/opt/目录下新建一个elkDocker目录

mkdir /opt/elkDocker

1.

进入elkDocker目录

cd /opt/elkDocker

1.

新建docker-compose.yml文件

vi docker-compose.yml

version: '2.2'

services:

elasticsearch:

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

container\_name: elasticsearch7.1.1

environment:

- discovery.type=single-node

- "ES\_JAVA\_OPTS=-Xms512m -Xmx512m"

volumes:

- esdata:/usr/share/elasticsearch/data

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yml文件所在目录执行

docker-compose up -d

1.

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/

需要注意情况如下：

1.不要下载docker官方的镜像，最好使用 elastic官方仓库里的镜像

2.如果出现启动不成功，先把其他两个注释掉，一个一个服务单独运行试试

3.logstash需要监听elasticsearch服务，不然logstash会自动停掉

4.logstash和kibana可以不用设置关联 elasticsearch 的环境变量，官网文档说如果是docker镜像有默认设置

5.如果自己修改了服务名称或者端口要记得修改默认的设置

下面开始安装ElasticSearch-Head

拉取ElasticSearch-Head镜像

docker pull mobz/elasticsearch-head:5

1.

运行ElasticSearch-Head容器

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

1.

在浏览器输入http://IP:9100

注： 运行ElasticSearch-Head容器时如果出现报错如下：

docker: Error response from daemon: Conflict. The container name "/es\_admin" is already in use by container "a9a2a5c74ab3b2dc42c2260fad0b0b1dd6e7c768a5cfb2ddbb121eb2946a370c". You have to remove (or rename) that container to be able to reuse that name.

1.

则执行 docker container ls -all 查看CONTAINER ID 然后执行 docker rm id号

之后重新执行docker run -d --name es\_admin -p 9100:9100 mobz/elasticsearch-head:5 即可

注： Elasticsearch-head 连接不上Elasticsearch的原因和解决方案

1.修改elasticsearch-head下Gruntfile.js文件，内容如下：

connect: {

server: {

options: {

hostname: '0.0.0.0',

port: 9100,

base: '.',

keepalive: true

}

}

}

2.修改elasticsearch-head\_site\app.js 文件。this.base\_uri 改为下面的值。

this.base\_uri = this.config.base\_uri || this.prefs.get("app-base\_uri") || "http://localhost:9200";

编辑配置文件

vim /etc/elasticsearch/elasticsearch.yml

增加下面两项

http.cors.enabled: true

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

然后重启 elasticsearch ，访问  http://localhost:9100/ 就可以成功的连接上 9200 端口