

Docker部署ELK

ELK是指Elasticsearch、Kibana、Logstash这三种服务搭建的日志收集系统，官方网站：<https://www.elastic.co/cn/downloads/>。

ELK中各个服务的作用：

- Elasticsearch：用于存储收集到的日志信息；
- Logstash：用于收集日志，SpringBoot应用整合了Logstash以后会把日志发送给Logstash,Logstash再把日志转发给Elasticsearch；
- Kibana：通过Web端的可视化界面来查看日志。

安装参考：

- <https://www.elastic.co/guide/en/elasticsearch/reference/7.6/docker.html>
- <https://www.elastic.co/guide/en/kibana/7.6/docker.html>
- <https://www.elastic.co/guide/en/logstash/7.6/docker.html>

1 准备目录

在home目录下面创建elk目录

```
1 mkdir /home/elk
2 cd /home/elk
3 mkdir logstash elasticsearch elasticsearch/data elasticsearch/plugins
4 # 修改数据目录访问权限
5 chmod 777 elasticsearch/data/
```

将资源目录下面的logstash.conf上传到logstash目录下面。

在生产环境中在Docker中运行Elasticsearch时适用以下要求和建议，参考下面链接：

<https://www.elastic.co/guide/en/elasticsearch/reference/7.6/docker.html#docker-prod-prerequisites>

2 开放端口

```
1 # 开放端口
2 firewall-cmd \
3 --add-port 9200/tcp \
4 --add-port 9300/tcp \
5 --add-port=4560-4563/tcp \
6 --add-port=5601/tcp \
7 --permanent
8 # 重新加载防火墙
9 firewall-cmd --reload
```

3 服务编排

执行命令 `vi docker-compose.yml` 创建服务编排文件，然后在文件中写入下列内容后保存。

当然你也可以使用资源目录中提供yaml文件直接上传到elk目录即可，然后跳过本步骤。

```
1 version: '3'
2 services:
3   elasticsearch:
4     image: docker.elastic.co/elasticsearch/elasticsearch:7.6.2
5     container_name: elasticsearch
6     environment:
7       - "cluster.name=elasticsearch"
8       - "discovery.type=single-node"
9       - "ES_JAVA_OPTS=-Xms256m -Xmx256m"
10      - TZ=Asia/Shanghai
11     volumes:
12       - /home/elk/elasticsearch/plugins:/usr/share/elasticsearch/plugins
13       - /home/elk/elasticsearch/data:/usr/share/elasticsearch/data
14     ports:
15       - 9200:9200
16       - 9300:9300
17   kibana:
18     image: docker.elastic.co/kibana/kibana:7.6.2
19     container_name: kibana
20     links:
21       - elasticsearch:es
22     depends_on:
23       - elasticsearch
24     environment:
25       - "elasticsearch.hosts=http://es:9200"
26       - "JAVA_OPTS=-Xms256m -Xmx256m"
27       - TZ=Asia/Shanghai
28     ports:
29       - 5601:5601
30   logstash:
31     image: docker.elastic.co/logstash/logstash:7.6.2
32     container_name: logstash
33     environment:
34       - "LS_JAVA_OPTS=-Xms256m -Xmx256m"
35       - TZ=Asia/Shanghai
36     volumes:
37       - /home/elk/logstash/logstash.conf:/usr/share/logstash/pipeline/logstash.conf
38     depends_on:
39       - elasticsearch
40     links:
41       - elasticsearch:es
42     ports:
43       - 4560:4560
44       - 4561:4561
45       - 4562:4562
46       - 4563:4563
```

4 启动服务

执行命令`docker-compose up`。

首次启动会拉取镜像，效果如下图所示。

```

[root@localhost elk]# pwd
/home/elk
[root@localhost elk]# ls
docker-compose.yml  elasticsearch  logstash
[root@localhost elk]# docker-compose up
[+] Running 0/10
  ⚙️ elasticsearch Pulling
     ⚙️ c808caf183b6 Pulling fs layer
     ⚙️ d6caf8e15a64 Pulling fs layer
     ⚙️ b0ba5f324e82 Pulling fs layer
     ⚙️ d7e8c1e99b9a Waiting
     ⚙️ 85c4d6c81438 Waiting
     ⚙️ 3119218fac98 Waiting
     ⚙️ 914accf214bb Waiting
  ⚙️ kibana Pulling
  ⚙️ logstash Pulling

```

如果启动过程没有看到明显的错误，那么表示服务器启动成功，接下来访问一下elasticsearch和kibana。

首先访问elasticsearch，访问地址：<http://ip:9200> 如果看了类似下图所示的结果表示elasticsearch启动成功。

←
→
↻
⚠️ 不安全 | 192.168.85.128:9200

```

1 // 20220830205055
2 // http://192.168.85.128:9200/
3
4 {
5   "name": "8dcc0141ee33",
6   "cluster_name": "elasticsearch",
7   "cluster_uuid": "p941EIV5Tj-AMZ7MSQ19mQ",
8   "version": {
9     "number": "7.6.2",
10    "build_flavor": "default",
11    "build_type": "docker",
12    "build_hash": "ef48eb35cf30adf4db14086e8aab07ef6fb113f",
13    "build_date": "2020-03-26T06:34:37.794943Z",
14    "build_snapshot": false,
15    "lucene_version": "8.4.0",
16    "minimum_wire_compatibility_version": "6.8.0",
17    "minimum_index_compatibility_version": "6.0.0-beta1"
18  },
19   "tagline": "You Know, for Search"
20 }

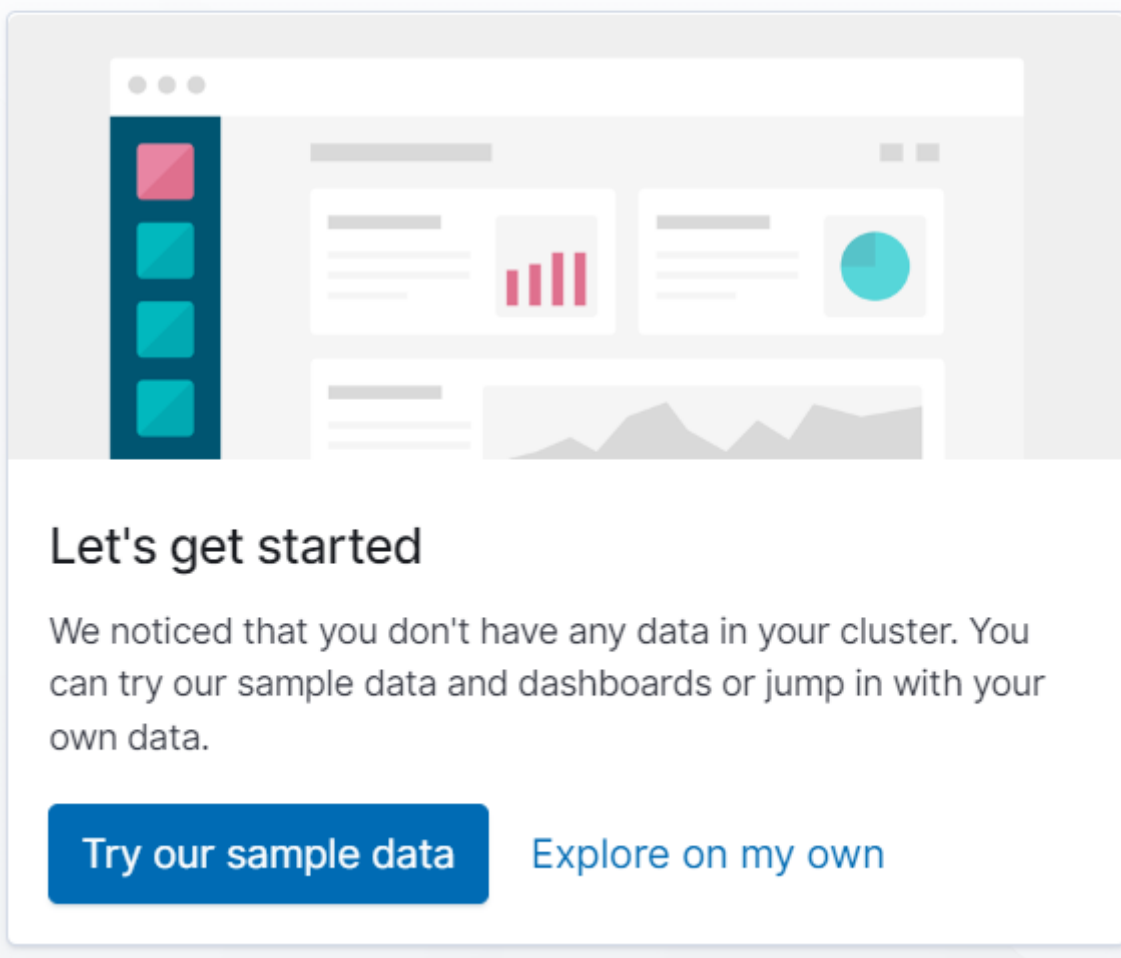
```

接下来在访问kibana，访问地址：<http://ip:5601> 如果看了类似下图所示的结果表示kibana启动成功。



Welcome to Kibana

Your window into the Elastic Stack



然后Ctrl + C结束前台启动，成功停止效果如下图所示

```
": "gzip, deflate", "accept-language": "zh-CN, zh;q=0.9"}, "
responseTime": 710, "contentLength": 9}, "message": "POST /ap
^CGracefully stopping... (press Ctrl+C again to force)
[+] Running 3/3
# Container logstash      Stopped
# Container kibana        Stopped
# Container elasticsearch Stopped
canceled
[root@localhost elk]#
```

执行后台启动，使用命令docker-compose up -d，启动成功如下图所示

```
canceled
[root@localhost elk]# docker-compose up -d
[+] Running 3/3
  # Container elasticsearch   Started
  # Container kibana          Started
  # Container logstash        Started
[root@localhost elk]#
```

使用docker ps 指令查看进程

```
[root@localhost elk]# docker ps
```

CONTAINER ID	IMAGE	NAMES	COMMAND	CREATED	STATUS
6cdb48e6609a	docker.elastic.co/kibana/kibana:7.6.2	kibana	"/usr/local/bin/dumb..."	37 seconds ago	Up 35 seconds
7f7d3a428846	docker.elastic.co/logstash/logstash:7.6.2	logstash	"/usr/local/bin/dock..."	37 seconds ago	Up 34 seconds
-4563/tcp, 9600/tcp	docker.elastic.co/elasticsearch/elasticsearch:7.6.2	elasticsearch	"/usr/local/bin/dock..."	37 seconds ago	Up 36 seconds
3b533a0963d6	tcp, :::9300->9300/tcp				

5 安装插件

5.1 安装IK分词插件

讲入elasticsearch容器

```
1 docker exec -it elasticsearch /bin/bash
```

执行插件安装命令

```
1 elasticsearch-plugin install https://release.infinilabs.com/analysis-ik/stable/elasticsearch-analysis-ik-7.6.2.zip
```

安装完成效果如下图所示

```
[root@3b533a0963d6 elasticsearch]# elasticsearch-plugin install https://github.com/medcl
-> Installing https://github.com/medcl/elasticsearch-analysis-ik/releases/download/v7.6.1
-> Downloading https://github.com/medcl/elasticsearch-analysis-ik/releases/download/v7.6.1
[=====] 100%??
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      WARNING: plugin requires additional permissions      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
* java.net.SocketPermission * connect,resolve
See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html
for descriptions of what these permissions allow and the associated risks.

Continue with installation? [y/N]y
-> Installed analysis-ik
[root@3b533a0963d6 elasticsearch]#
```

执行exit退出容器

```
Continue with installation? [y/N]y
-> Installed analysis-ik
[root@3b533a0963d6 elasticsearch]# exit
exit
[root@localhost elk]#
```

5.2 安装json_lines插件

进入logstash容器

```
1 docker exec -it logstash /bin/bash
```

执行插件安装命令

```
1 logstash-plugin install logstash-codec-json_lines
```

安装成功可以看到如下图所示的效果

```
[root@localhost elk]# docker exec -it logstash /bin/bash
bash-4.2$ logstash-plugin install logstash-codec-json_lines
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by com.headius.backport9.modules.Module
WARNING: Please consider reporting this to the maintainers of com.headius.
WARNING: Use --illegal-access=warn to enable warnings of further illegal r
WARNING: All illegal access operations will be denied in a future release
Validating logstash-codec-json_lines
Installing logstash-codec-json_lines
Installation successful
bash-4.2$ █
```

执行exit退出容器。

```
Installing logstash-codec-json_lines
Installation successful
bash-4.2$ exit
exit
[root@localhost elk]# █
```

5.3 重启服务

所有插件安装完成统一重启一下服务。

```
[root@localhost elk]# docker-compose restart
[+] Running 3/3
 # Container elasticsearch Started
 # Container logstash Started
 # Container kibana Started
[root@localhost elk]# █
```