搭建ELK环境

建立日期：2020年7月31日

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 变更原因 | 变更内容简述 | 编制/修订者 | 适用范围 | 发布日期 |
| V1.0 | 建立 |  | 陈文华 | 测试、开发 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

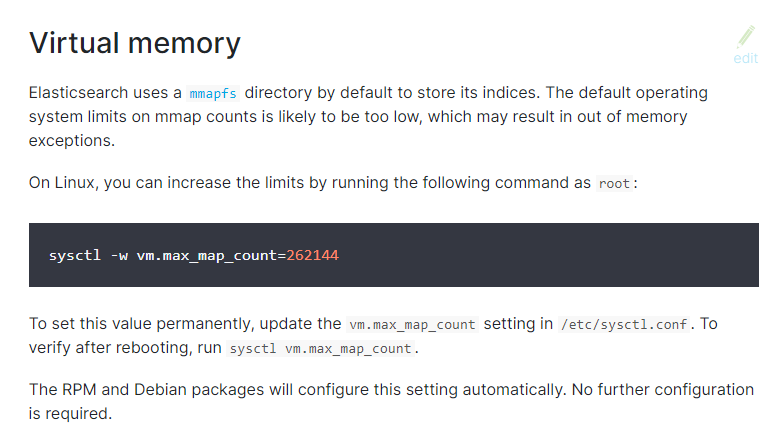
## 环境准备

1、增加内存

sysctl -w vm.max\_map\_count=262144

官网原因解释

<https://www.elastic.co/guide/en/elasticsearch/reference/current/vm-max-map-count.html>



2、创建ELK Docker Compose文件存储路径

mkdir -p /platform/elk

3、在该目录下创建elk.yml配置文件

cd /platform/elk

vim elk.yml

内容如下

version: '3'

services:

elasticsearch:

image: elasticsearch:6.4.1

container\_name: elasticsearch

restart: always

environment:

- cluster.name=elasticsearch

- xpack.security.enabled=false

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

- node.name=elasticsearch\_node\_1

- "TZ=Asia/Shanghai"

volumes:

- /platform/elasticsearch/data:/usr/share/elasticsearch/data

- /platform/elasticsearch/logs:/usr/share/elasticsearch/logs

- /platform/elasticsearch/elasticsearch.yml:/usr/share/elasticsearch/config/elasticsearch.yml

ports:

- 9200:9200

- 9300:9300

kibana:

image: kibana:6.4.1

container\_name: kibana

links:

- elasticsearch:es

depends\_on:

- elasticsearch

environment:

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

ports:

- 5601:5601

logstash:

image: logstash:6.4.1

container\_name: logstash

volumes:

- /platform/logstash/logstash-platform.conf:/usr/share/logstash/pipeline/logstash.conf

depends\_on:

- elasticsearch

links:

- elasticsearch:es

ports:

- 4560:4560

4、创建挂载目录

mkdir -p /platform/elasticsearch/data

mkdir -p /platform/elasticsearch/logs

mkdir -p /platform/logstash

5、目录授权

chmod 777 -R /platform/elasticsearch

6、创建Elasticsearch配置文件elasticsearch.yml

touch /platform/elasticsearch/elasticsearch.yml

添加如下内容

http.host: 0.0.0.0

http.cors.enabled: true

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

transport.host: 0.0.0.0

7、创建Logstash配置文件logstash-platform.conf

touch /platform/logstash/logstash-platform.conf

添加以下内容

input {

tcp {

mode => "server"

host => "0.0.0.0"

port => 4560

codec => json\_lines

}

}

output {

elasticsearch {

hosts => "es:9200"

index => "platform-logstash-%{+YYYY.MM.dd}"

}

}

8、创建ELK容器

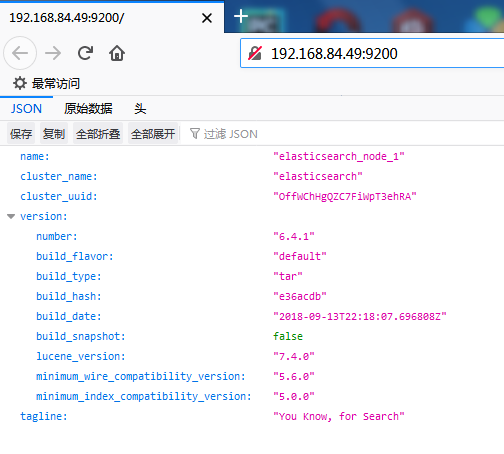
docker-compose -f elk.yml up -d

9、查看容器运行情况

docker ps -a

浏览器访问：

<http://192.168.84.49:9200/>



## Logstash中安装json\_lines插件

使用如下命令进入到Logstash容器中

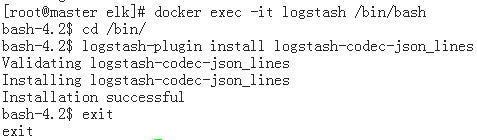
docker exec -it logstash /bin/bash

切换到/bin目录，安装json\_lines插件，然后退出

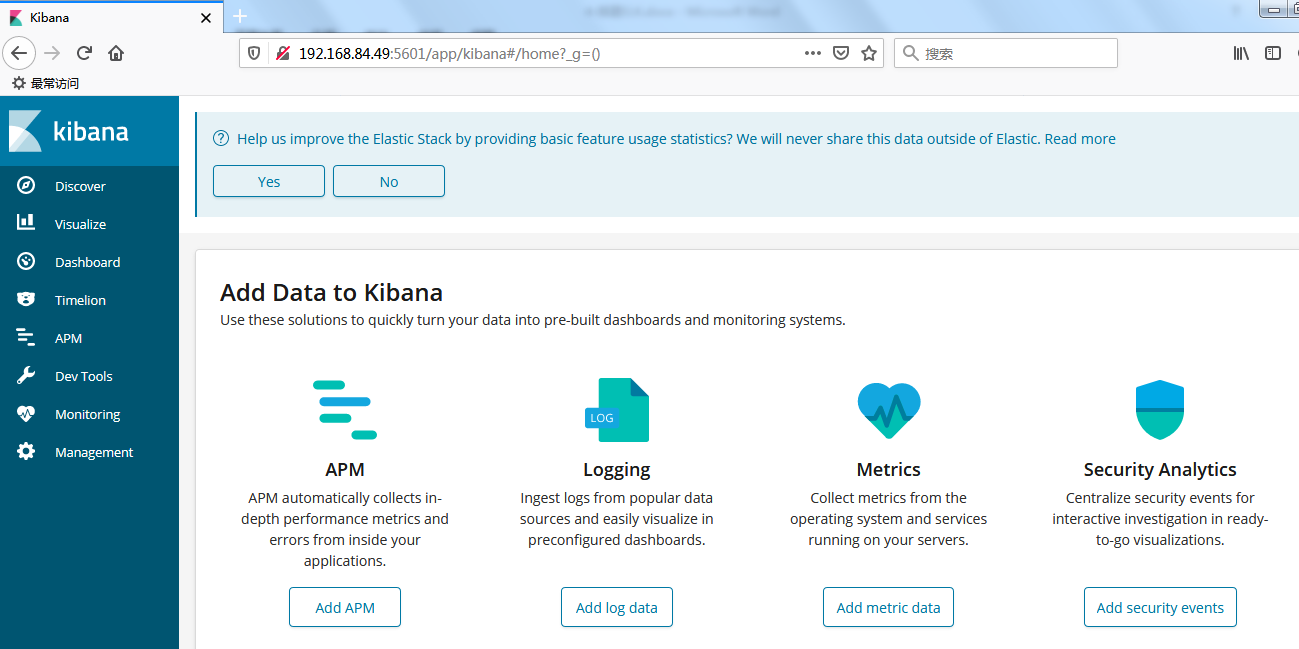
cd /bin/

logstash-plugin install logstash-codec-json\_lines

exit



浏览器访问<http://192.168.84.49:5601>



## 增加日志配置

1. auth、gateway、system模块里引入Logstash依赖

<dependency>

<groupId>net.logstash.logback</groupId>

<artifactId>logstash-logback-encoder</artifactId>

<version>6.1</version>

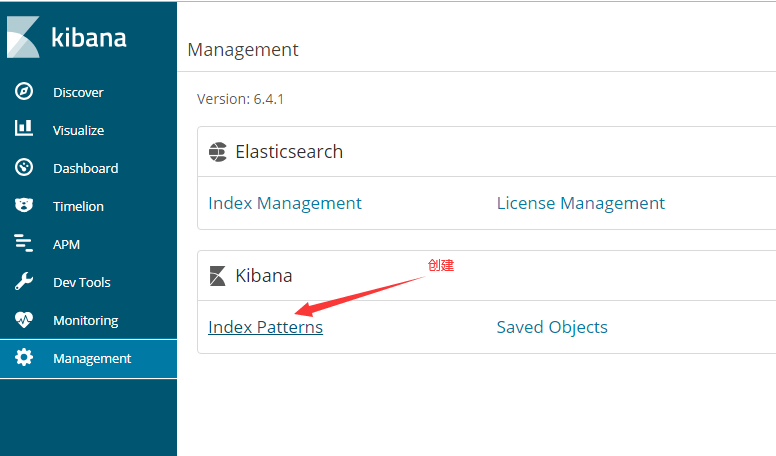
</dependency>

1. 在日志配置文件logback-spring.xml里添加配置

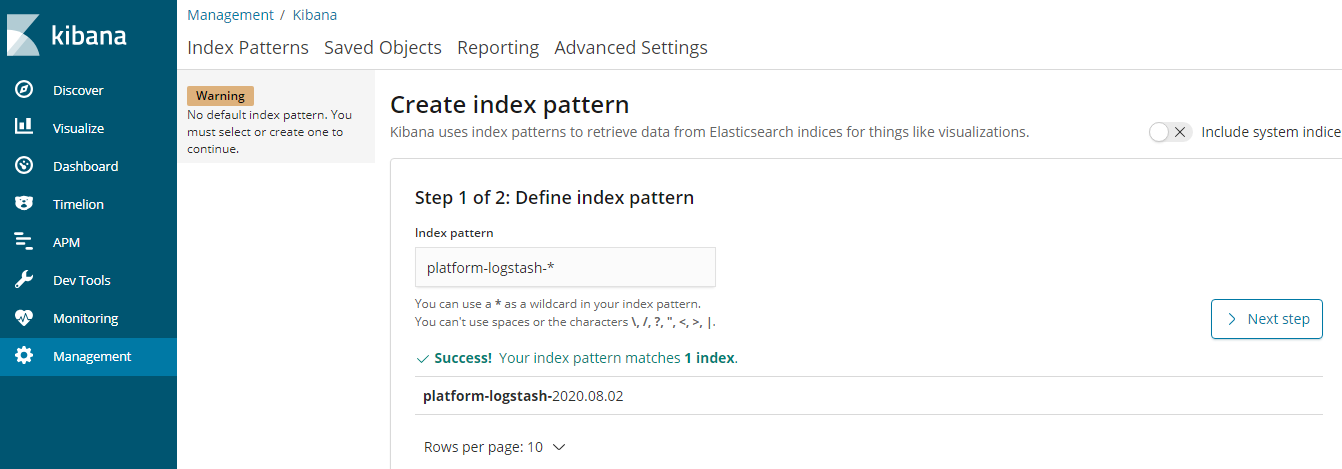
<**appender name="logstash" class="net.logstash.logback.appender.LogstashTcpSocketAppender"**>  
 <**destination**>192.168.84.49:4560</**destination**>  
 <**encoder charset="UTF-8" class="net.logstash.logback.encoder.LogstashEncoder"**/>  
</**appender**>

<**root level="info"**>  
 <**appender-ref ref="logstash"** />  
</**root**>

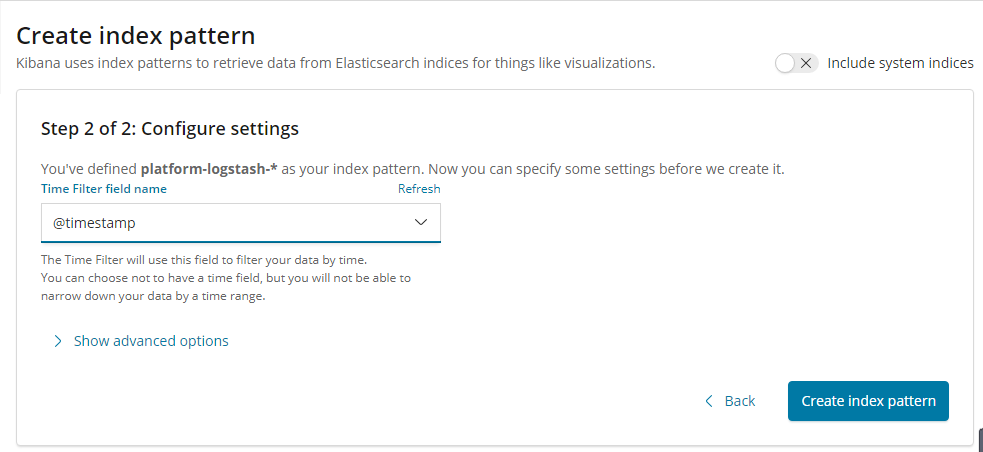
3、启动系统，创建Index Patterns



4、输入在logstash配置文件logstash-platform.conf里output.index指定的值platform-logstash-\*



5、点击Next step，在下拉框里选择@timestamp然后点击Create Index Pattern按钮完成创建。



6、Discover界面查看日志

