## 软件下载解压

### 1下载

在<https://www.elastic.co/>网站中搜索下面三个软件的压缩包。

logstash all plugins 7.6.1

elasticsearch 7.6.1

kibana 7.6.1

### 2解压

解压到/usr/local/ELK目录下

tar -xzvf elasticsearch-7.6.1.tar.gz

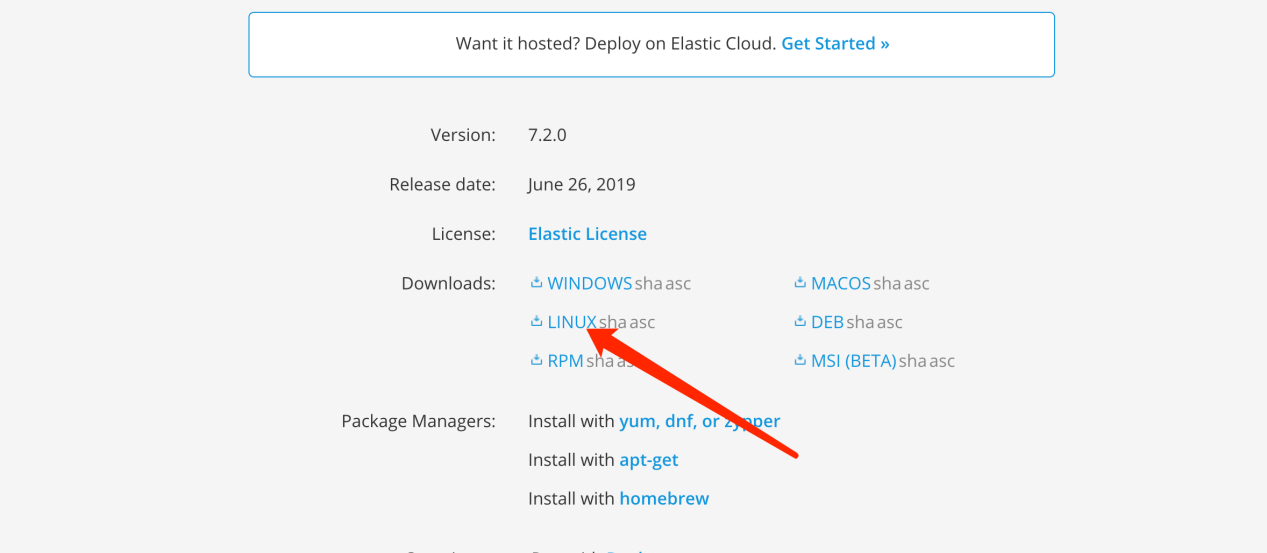
tar -xzvf logstash-all-plugins-7.6.1.tar.gz

tar -xzvf kibana-7.6.1-linux-x64.tar.gz

## Elasticsearch安装

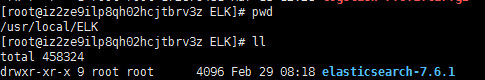
### 1、下载

<https://www.elastic.co/cn/downloads/elasticsearch>



### 2、解压

tar -xvf elasticsearch-7.6.1-linux-x86\_64.tar.gz



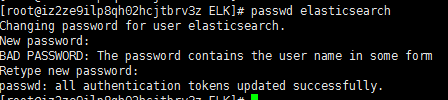
### 3、添加用户

#### 1）、创建用户：elasticsearch

adduser elasticsearch

#### 2）、创建用户密码，需要输入两次

passwd elasticsearch



#### 3）、将对应的文件夹权限赋给该用户

chown -R elasticsearch elasticsearch-7.6.1

#### 4）、切换至elasticsearch用户

su - elasticsearch

### 四、启动

./bin/elasticsearch -d



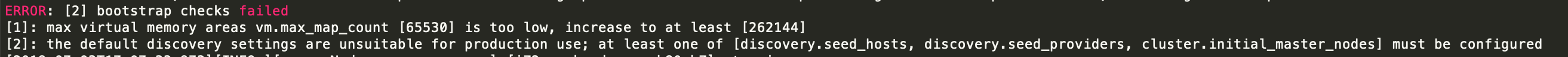
### 开启远程访问

elasticsearch.yml下的network.host:  0.0.0.0

cluster.initial\_master\_nodes: ["node-1"]

### 五、常见问题处理

#### 1



解决办法：

1、切换到root用户修改配置sysctl.conf

vi /etc/sysctl.conf

2、添加下面配置：

vm.max\_map\_count=655360

3、并执行命令：

sysctl -p

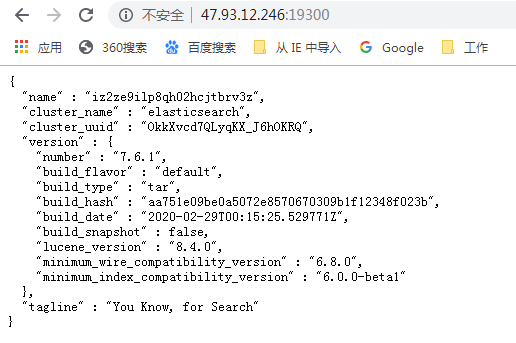
#### 2）bootstrap checks failed

[1]: the default discovery settings are unsuitable for production use; at least one of [discovery.seed\_hosts, discovery.seed\_providers, cluster.initial\_master\_nodes] must be configured

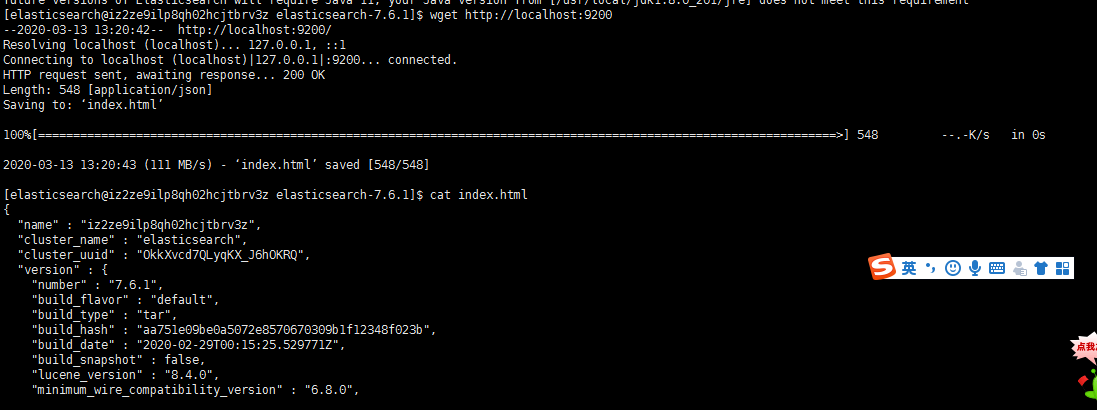
这时候继续编辑elasticsearch.yml文件，将 #cluster.initial\_master\_nodes: ["node-1", "node-2"] 修改为 cluster.initial\_master\_nodes: ["node-1"]，记得保存。

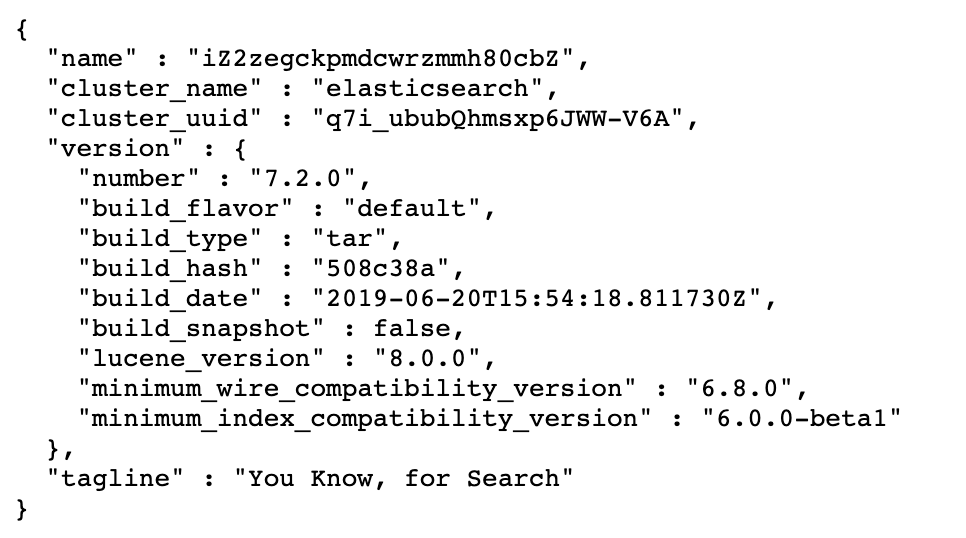
### 六、访问,安装成功

[http://ip:19300/](http://47.95.206.149:9200/)



或者





## Logstash安装

### 1、下载

在<https://www.elastic.co/>网站中搜索。

logstash-7.6.1.tar.gz

### 2、解压

解压到/usr/local/ELK目录下

tar -xzvf logstash-7.6.1.tar.gz

### 3、创建配置文件

logstash运行时需要使用配置文件，主要是用于定义内容的输入、输出、中间处理等。

创建配置文件所在目录，并编辑配置文件

cd /usr/local/ELK/logstash-7.6.1

vim logstash\_agent.conf

在配置文件logstash\_agent.conf添加如下内容：

**input {**

**stdin{}**

**}**

**output {**

**elasticsearch {**

**action => "index" # 在ES上操作index**

**hosts => "localhost:9200" # ES地址**

**index => "logstash--%{+YYYY-MM}" # 索引名**

**}**

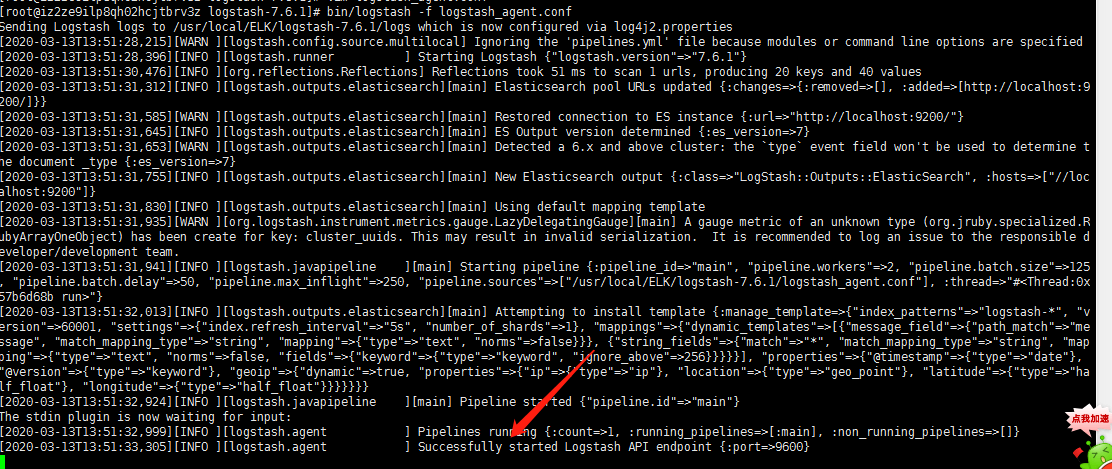
**}**

上面的配置主要是在logstash命令段输入日志信息，然后将日志输出到elasticsearch中。

ps：注意这里的index选项，我命名的是logstash--%{+YYYY-MM}，这个在后面的head插件和kibana中都会有所体现的。

### 4、启动

bin/logstash -f logstash\_agent.conf

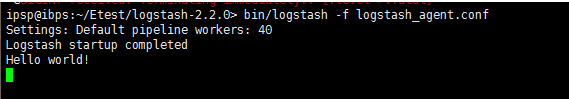


### 4、测试

通过上面的配置，我们已经可以在logstash命令端输入信息，然后通过head插件进行查看了：

前提要保证elasticsearch和logstash都正常启动（需要先启动elasticsearch，再启动logstash，不然elasticsearch会报错），head插件也已经正确安装！

我们输入Hello world！



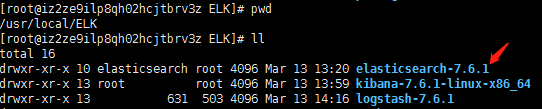
## kibnana安装

### 下载

wget https://artifacts.elastic.co/downloads/kibana/kibana-7.6.1-linux-x86\_64.tar.gz

### 解压

tar -xvf kibana-7.6.1-linux-x86\_64.tar.gz



### 授权

chown -R elasticsearch kibana-7.6.1-linux-x86\_64

### 修改端口(用默认端口不需要修改)

cd /usr/local/ELK/kibana-7.6.1-linux-x86\_64/config

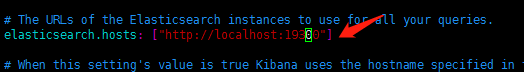
vim kibana.yml

修改如下内容

Kibana端口



Es端口（默认9200端口不用修改）



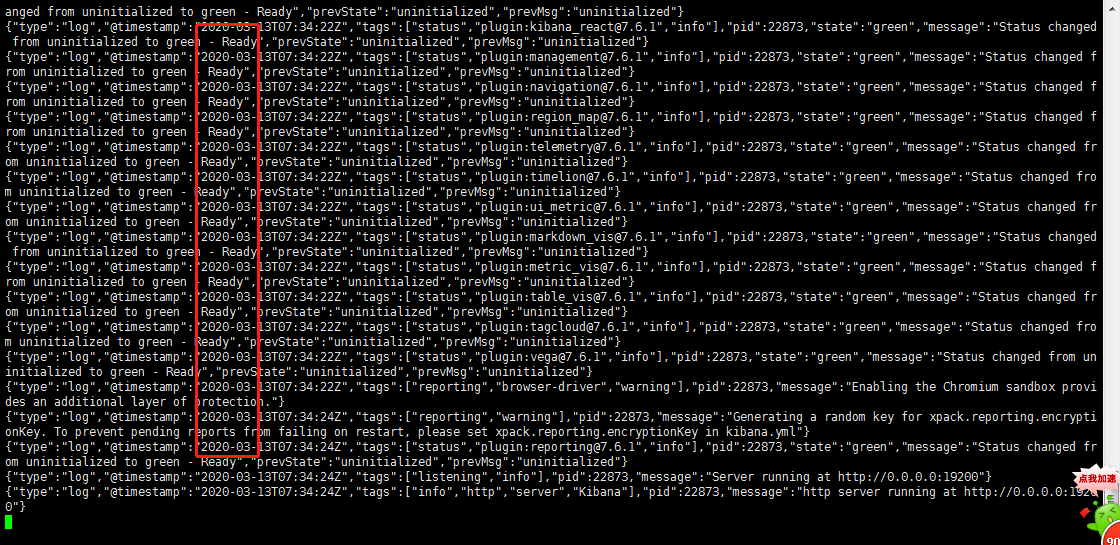
### 启动

su - elasticsearch

cd /usr/local/ELK/kibana-7.6.1-linux-x86\_64/bin/

nohup ./kibana &

查看日志



启动完成后，浏览器内输入"ip:端口"，这样就算是部署成功了

**问题**

kibana启动后通过jps或jobs找不到对应的PID

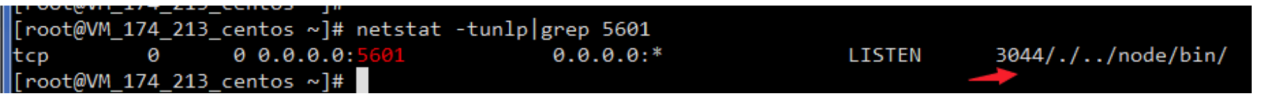
但是启动的时候却报：

{"type":"log","@timestamp":"2018-11-21T06:32:59Z","tags":["fatal"],"pid":22160,"message":"Port 5601 is already in use. Another instance of Kibana may be running!"}

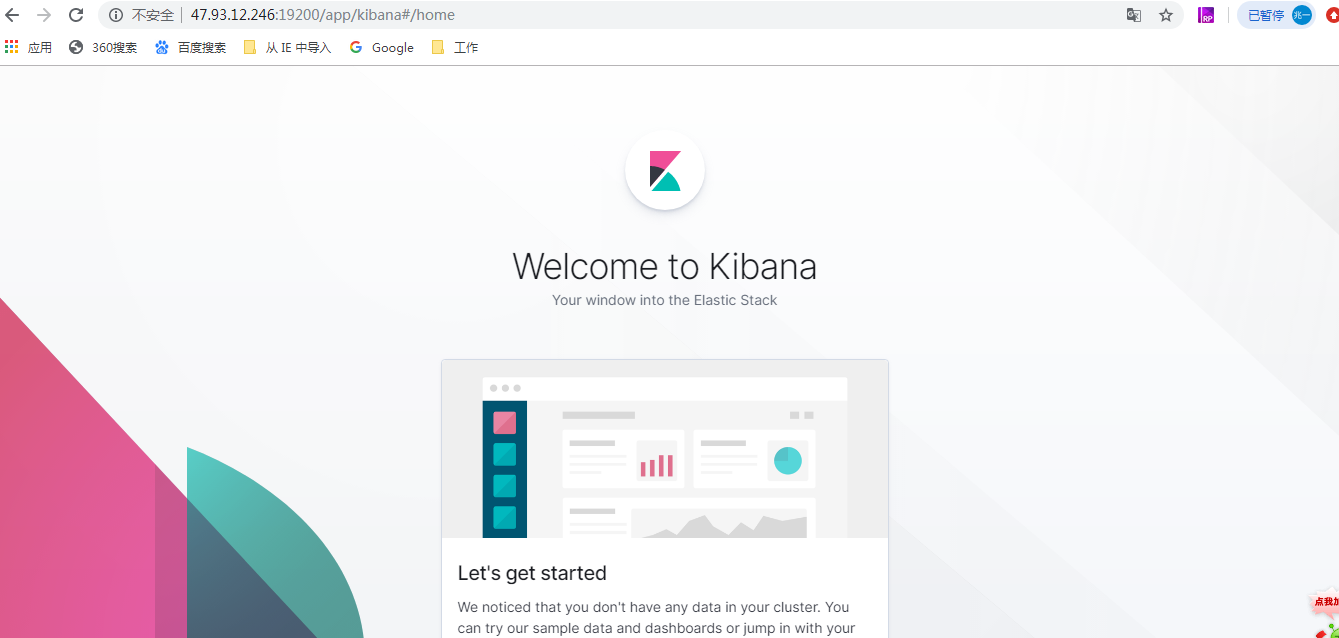
可以通过**ps -ef|grep node**

查找对应端口关闭

netstat -tunlp|grep端口号



### 查看



## 注意事项：

linux搭建kibana或者Elasticsearch 环境后，远程访问，被拒绝

解决办法：

1. 检查端口是否开放；

2. 修改config下面的配置文件，

因为Kibana 5.x 默认占用的地址是localhost(127.0.0.1)

将$KIBANA/config/kibaba.yml下的

server.host: "localhost" 更改为

server.host: "0.0.0.0" 就可以了

## springboot日志接入elk

### logstash\_agent.conf配置文件

input {

tcp {

port=> 19300

codec => "json"

}

}

output {

elasticsearch {

hosts => "127.0.0.1:9200"

index => "%{[appname]}-%{+YYYY.MM.dd}"

}

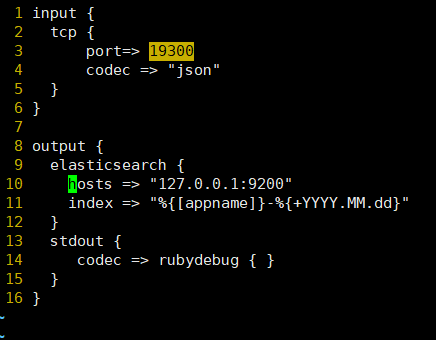
stdout {

codec => rubydebug { }

}

}

appname在logback-spring.xml中配置相应名称



### 启动logstash

挂起 bin/logstash -f logstash\_agent.conf & 或者bin/logstash -f logstash\_agent.conf



### pom.xml 修改

<dependency>

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

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

<version>5.3</version>

</dependency>

### logback-spring.xml配置

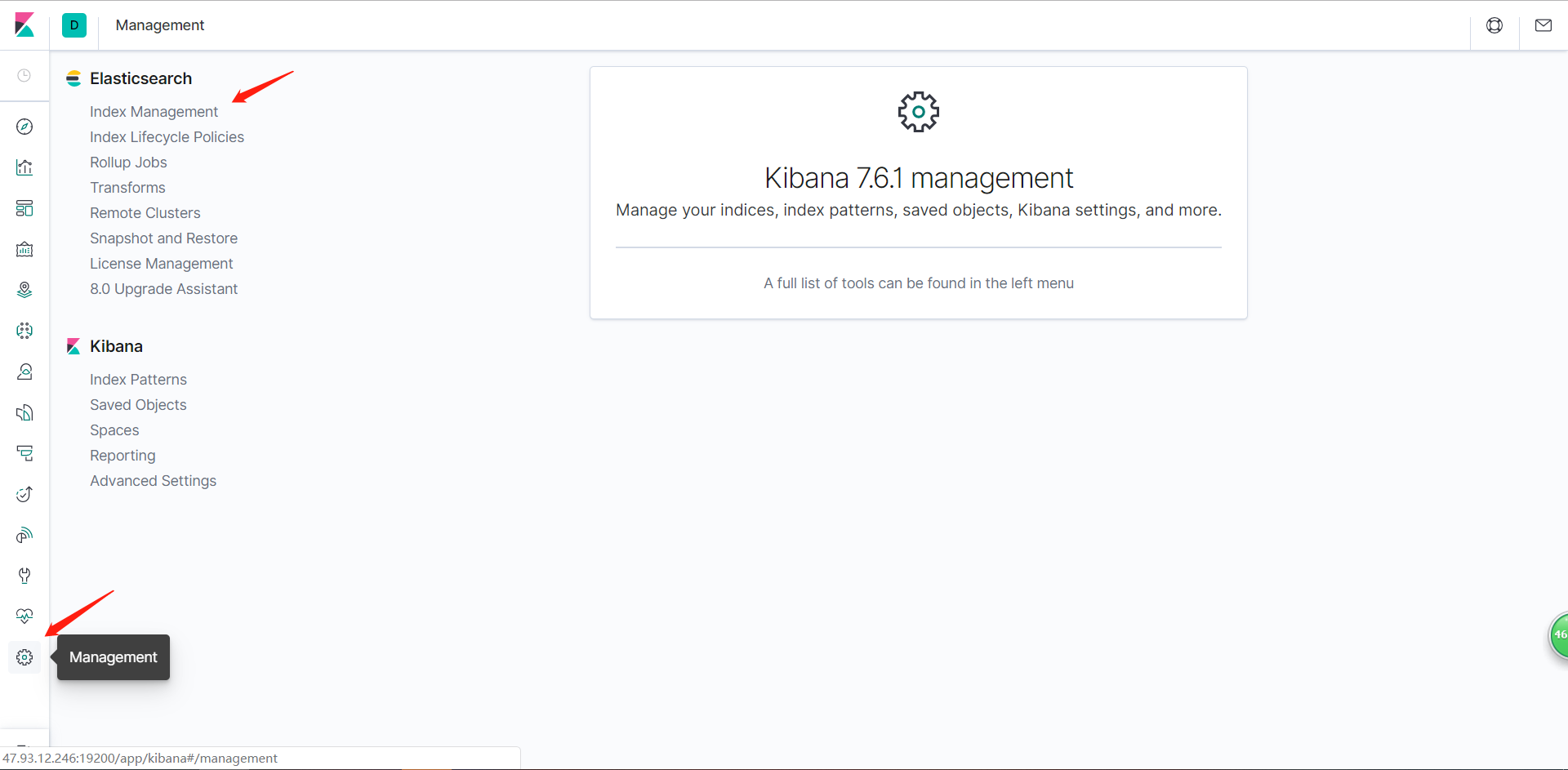
配置访问的logstash日志收集端口和项目名称

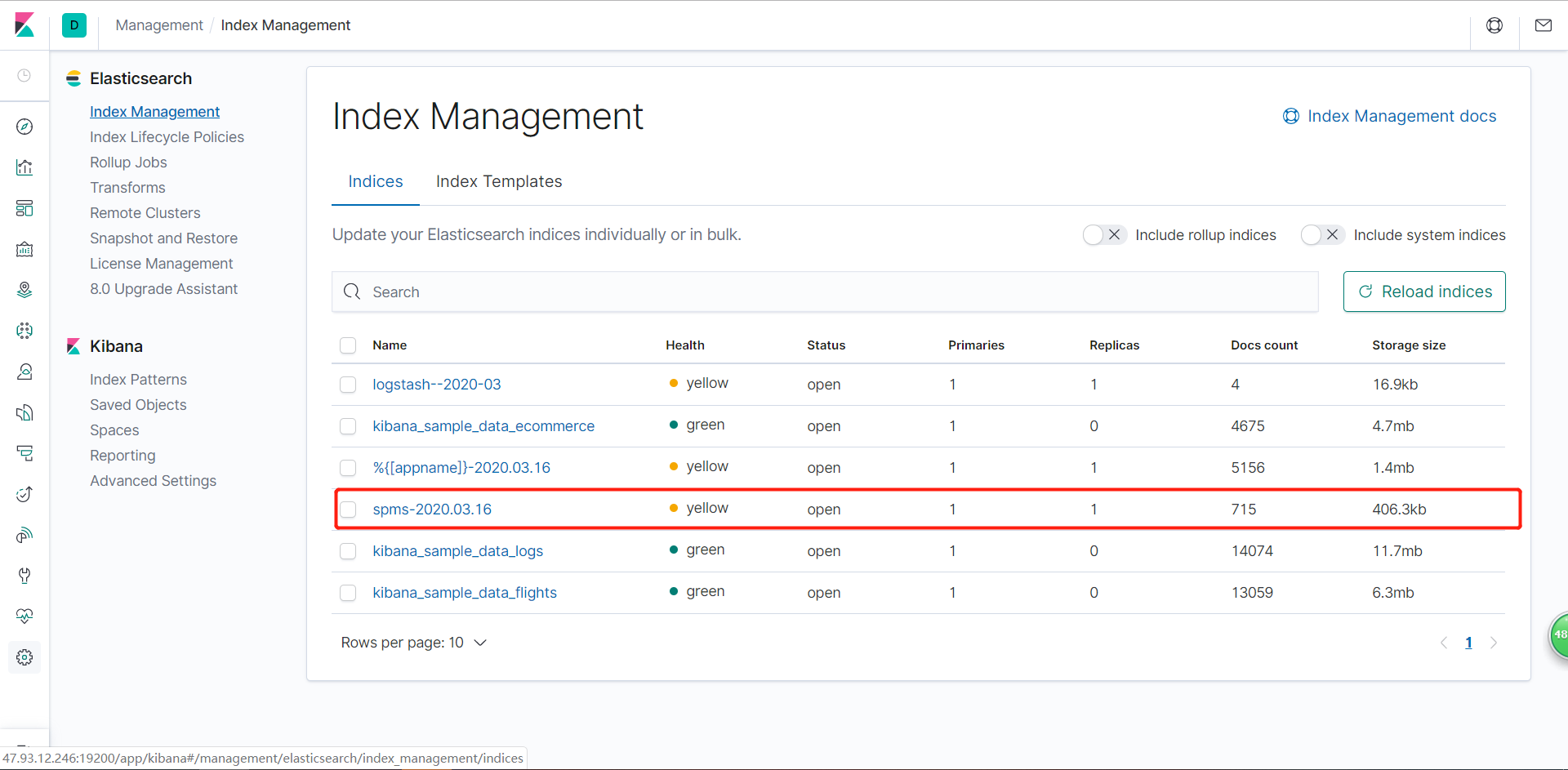




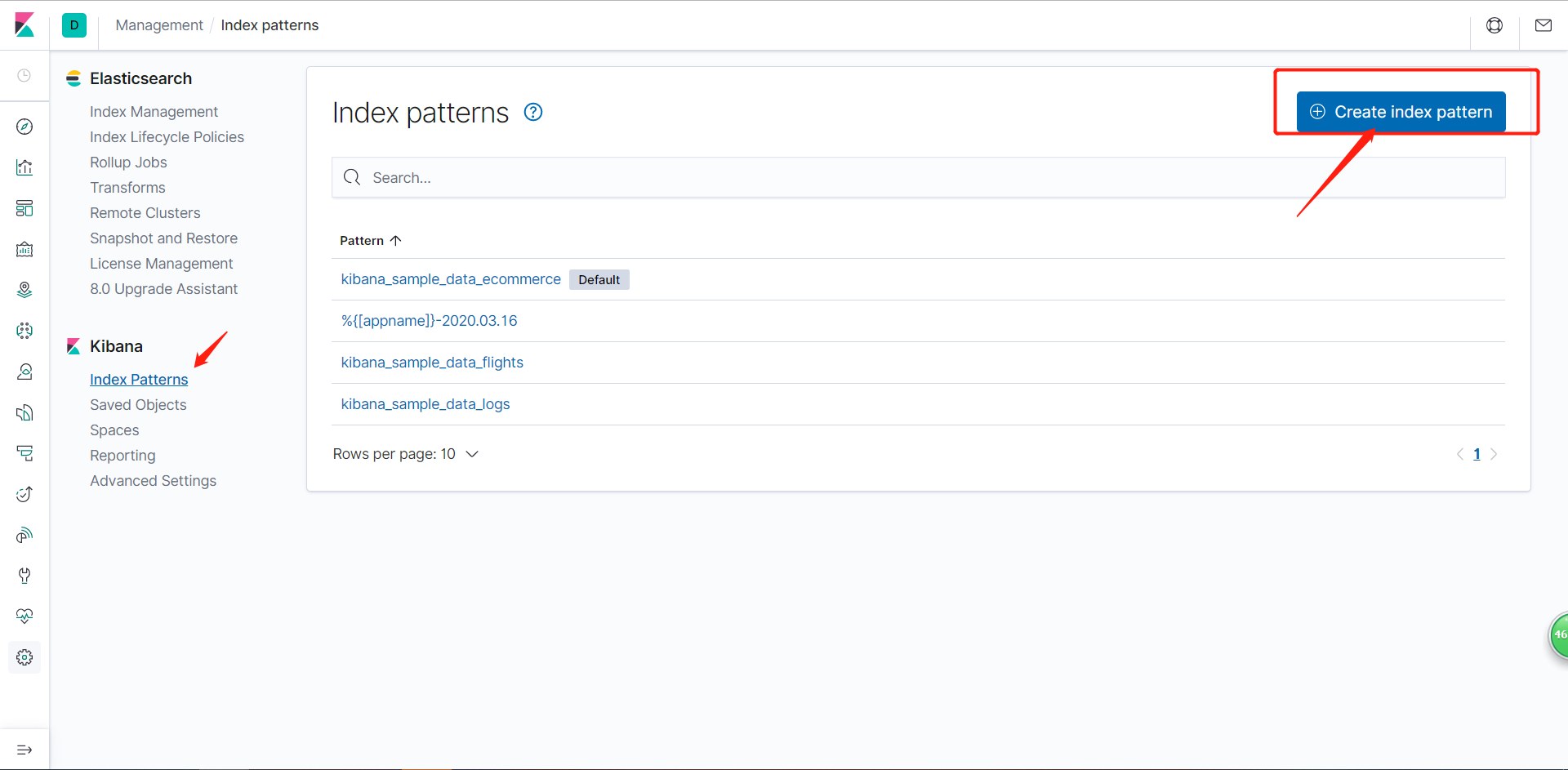
### kibana日志过滤配置和展示

#### 查看配置是否成功

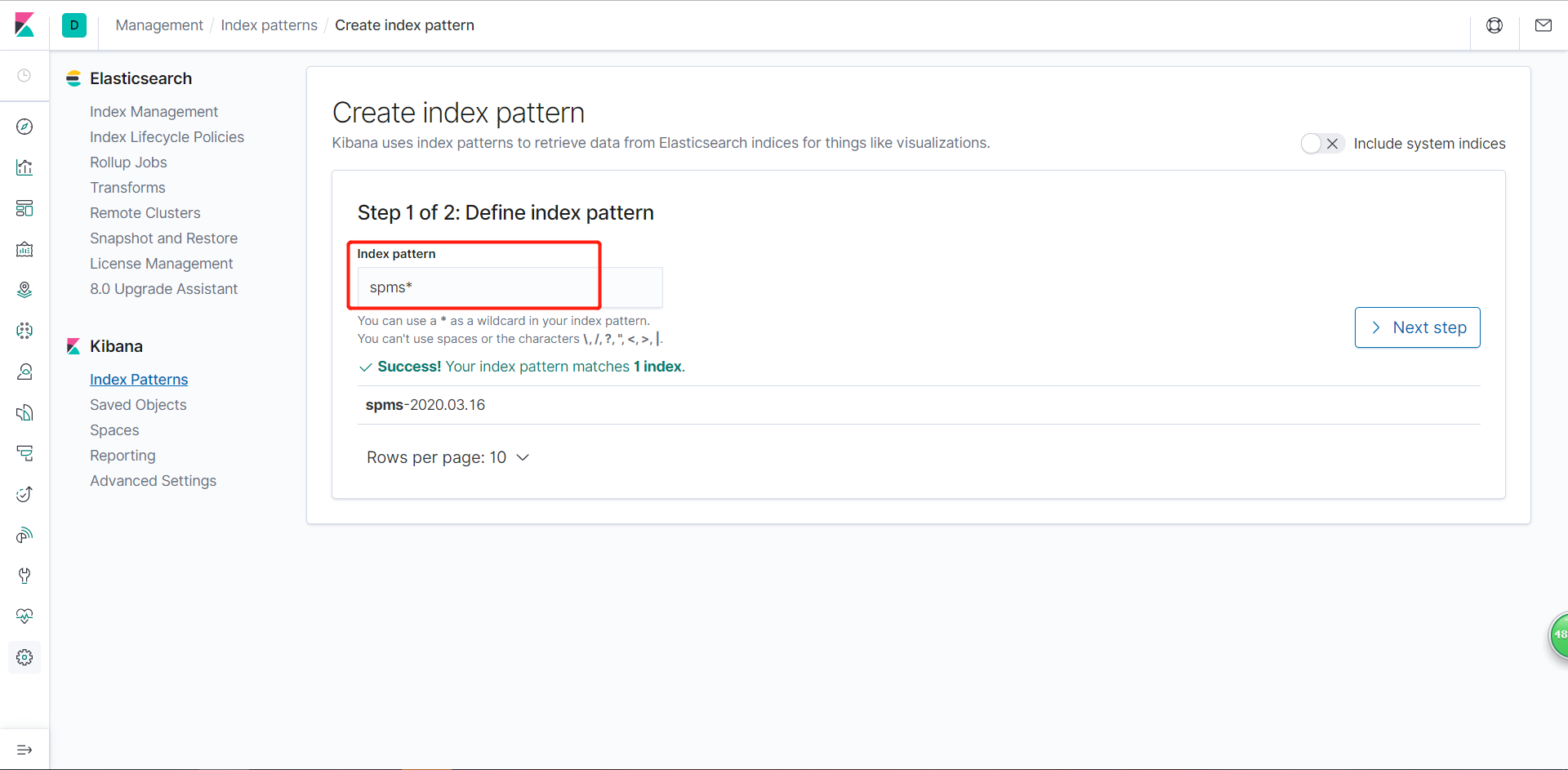




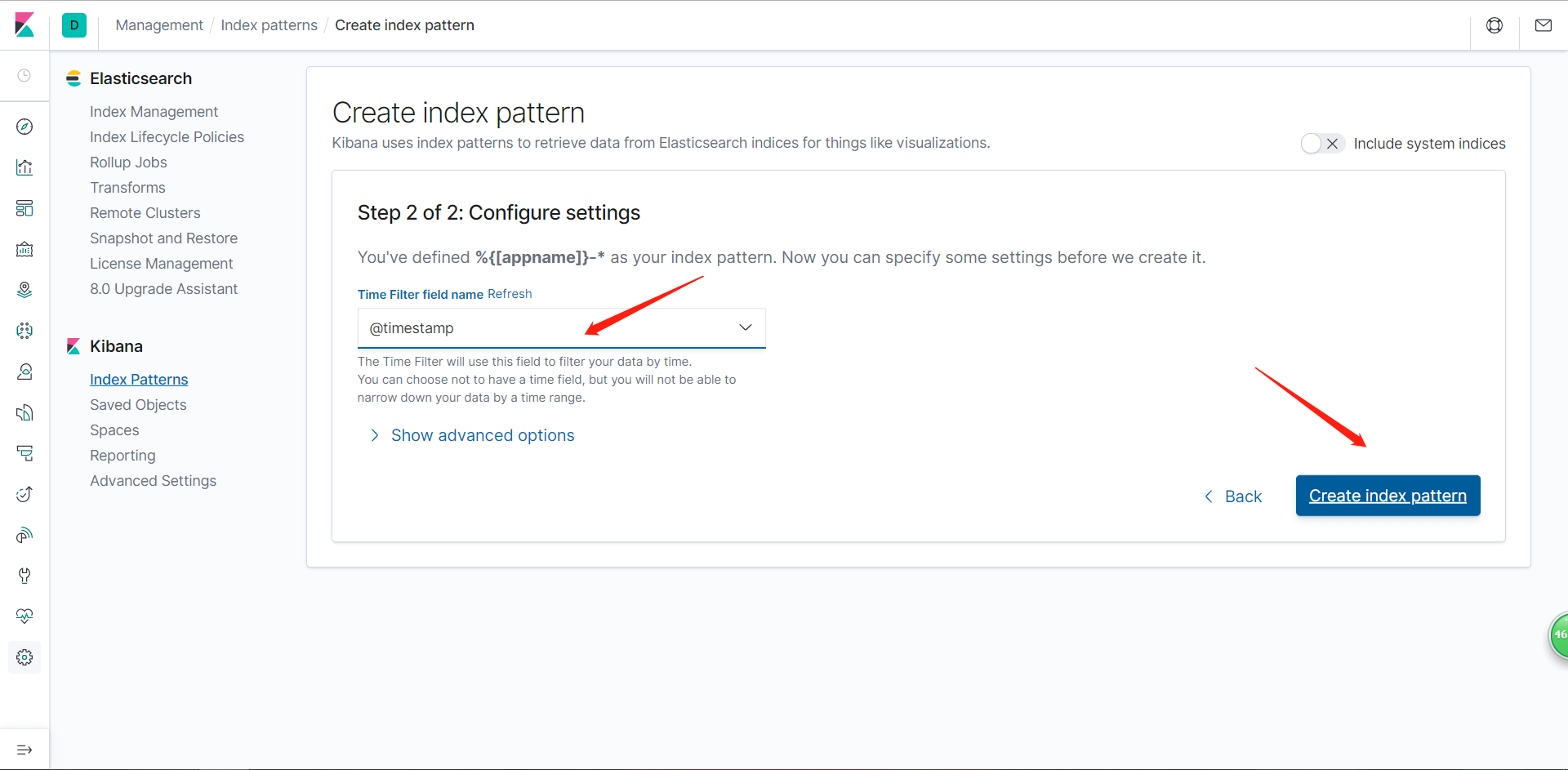
#### 启动springboot服务， 在kibana配置日志拦截器

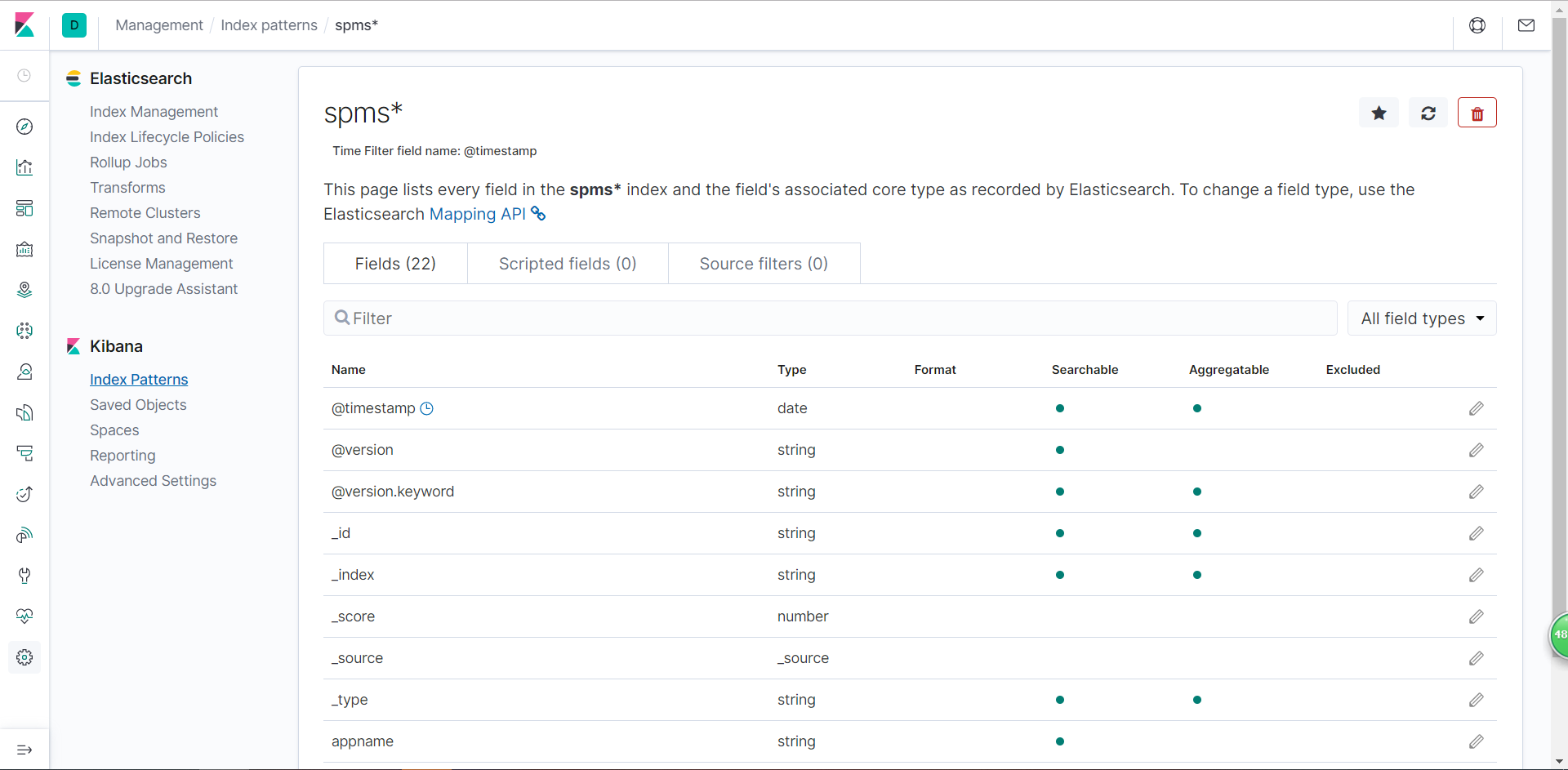


#### 输入我们logstash日志配置的名称



#### 继续下一步，选择带时间戳过滤器





#### 点击左侧Discover菜单，已经发现数据已经展现

