日志系统集成

1. 前期准备（下载）

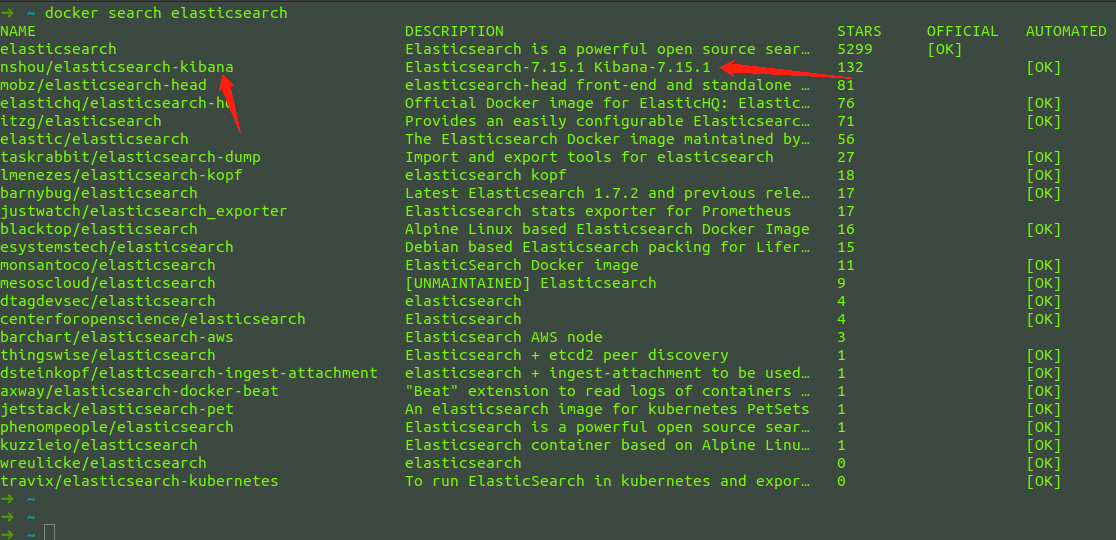
elasticsearch 存储日志的数据库（es）

kibana 管理es的web

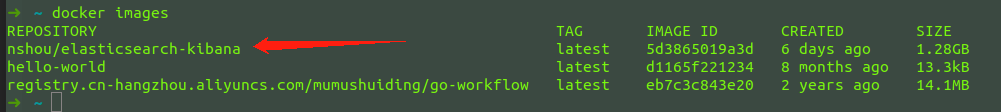
logstash 过滤日志信息以及将信息写入es中

filebeat 实时读取日志发送到logstash(filebeat跟着服务走)

1. 工具安装
2. es和kibana安装，通过docker安装



下载镜像docker pull nshou/elasticsearch-kibana

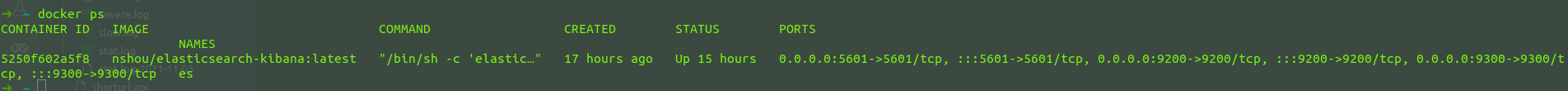


创建及启动容器：

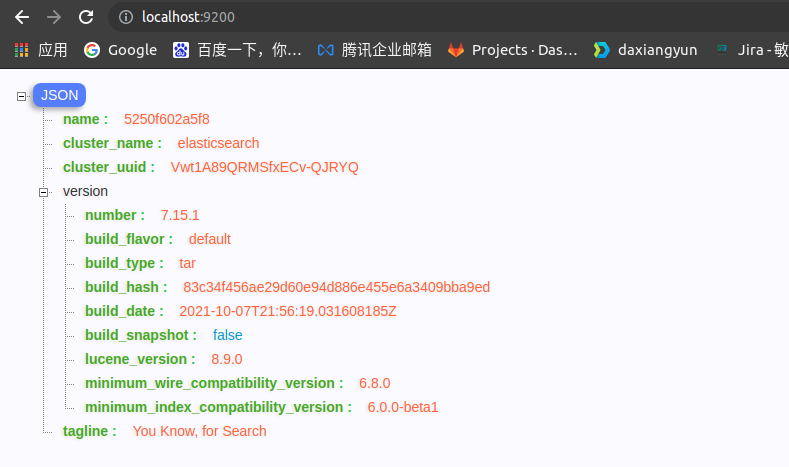
docker run --name es -d -e ES\_JAVA\_OPTS="-Xms512m -Xmx512m"

-e "discovery.type=single-node" -p 9200:9200 -p 9300:9300

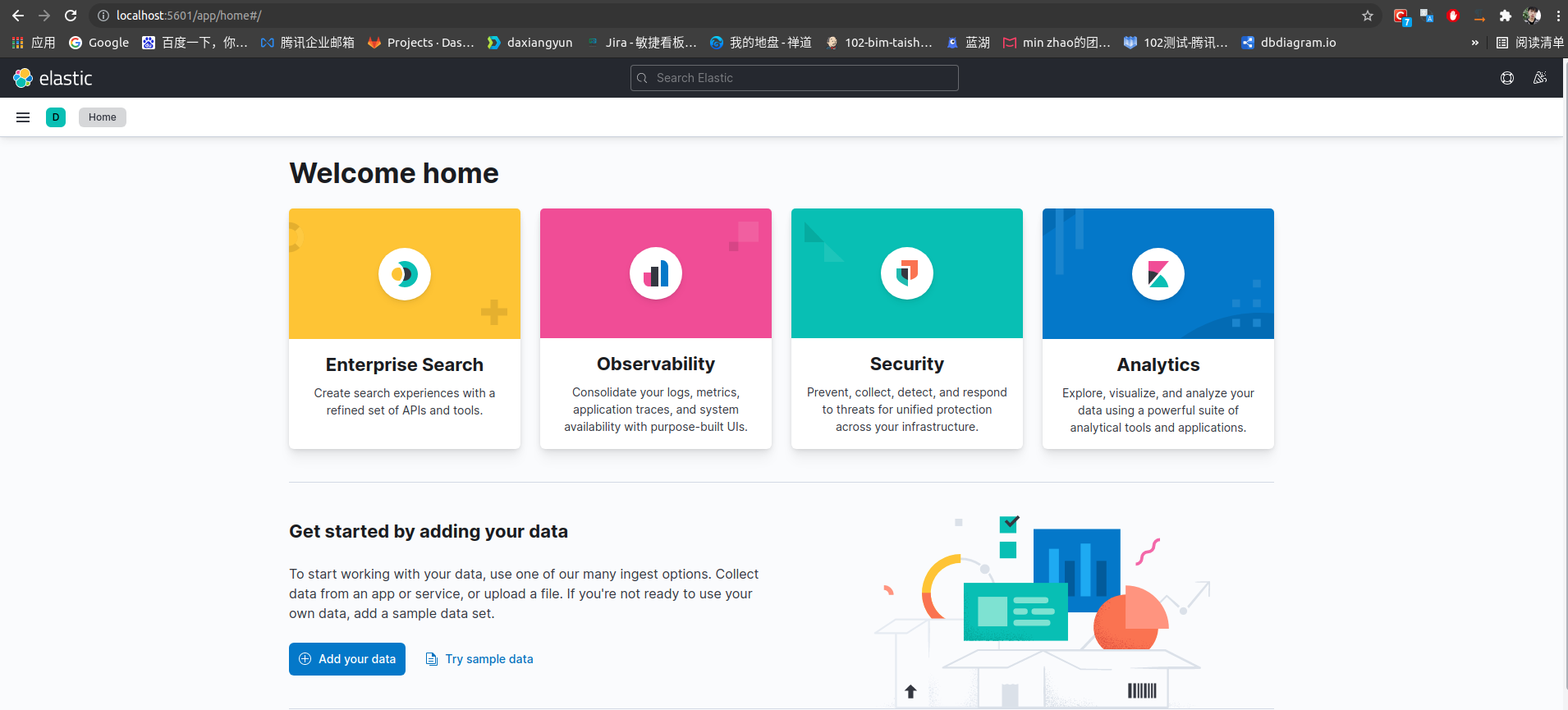
-p 5601:5601 nshou/elasticsearch-kibana:latest



访问es: <http://ip:9200>



访问kibana：<http://ip:5601>

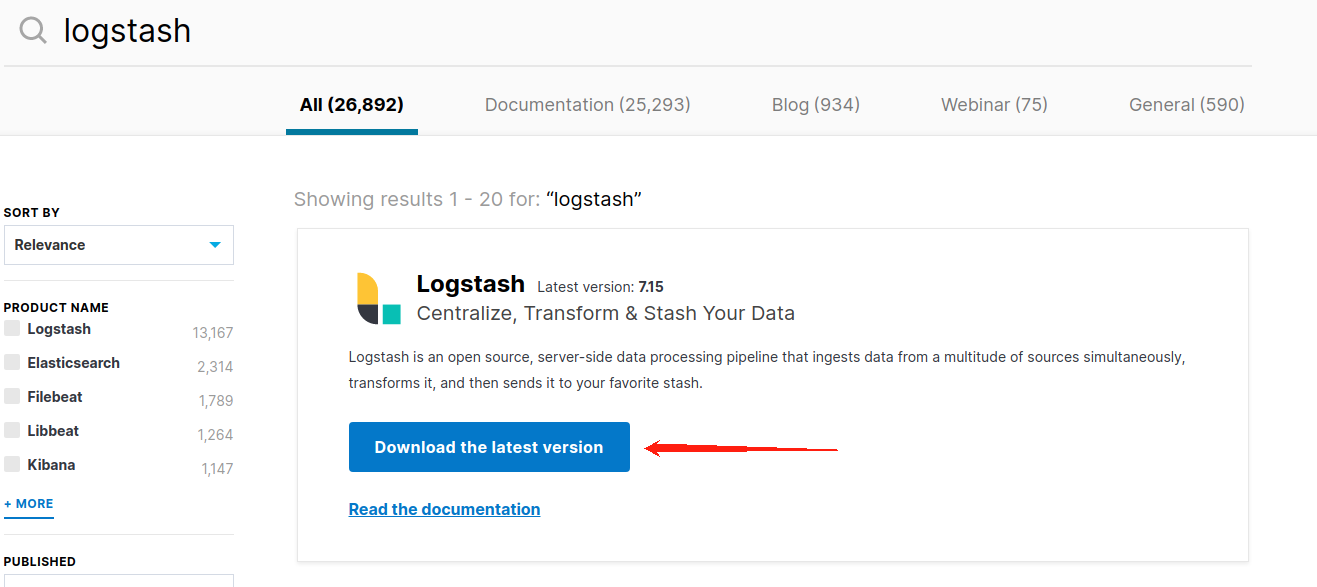


到此es和kibana安装成功

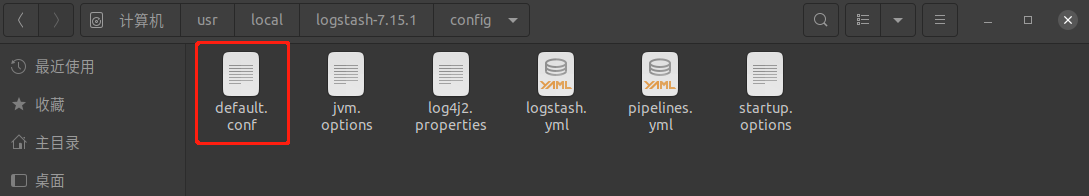
1. logstash安装

去es官网下载tar.gz文件：

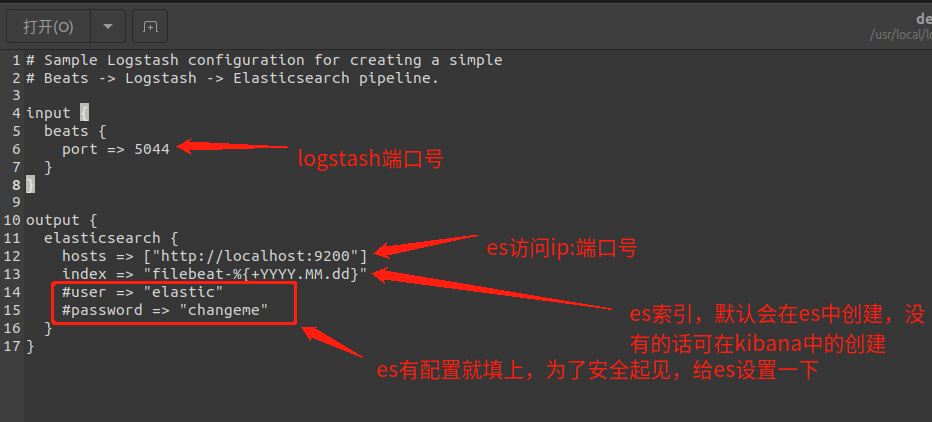
<https://www.elastic.co/search?q=logstash&size=n_20_n>



文件下载好后，解压放到/usr/local下面，然后修改配置文件：

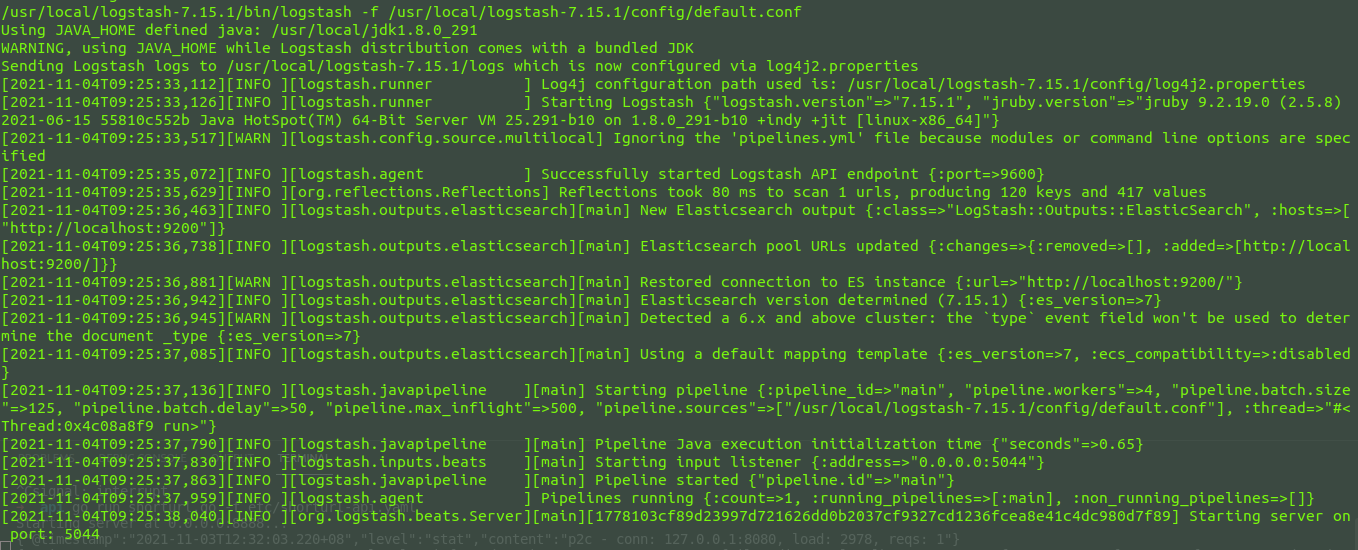


提示：配置文件原名“logstash-sample.conf”，我自己改成了default.conf



配置文件修改好之后可以通过命令：

path/bin/logstash -f path/default.conf进行启动



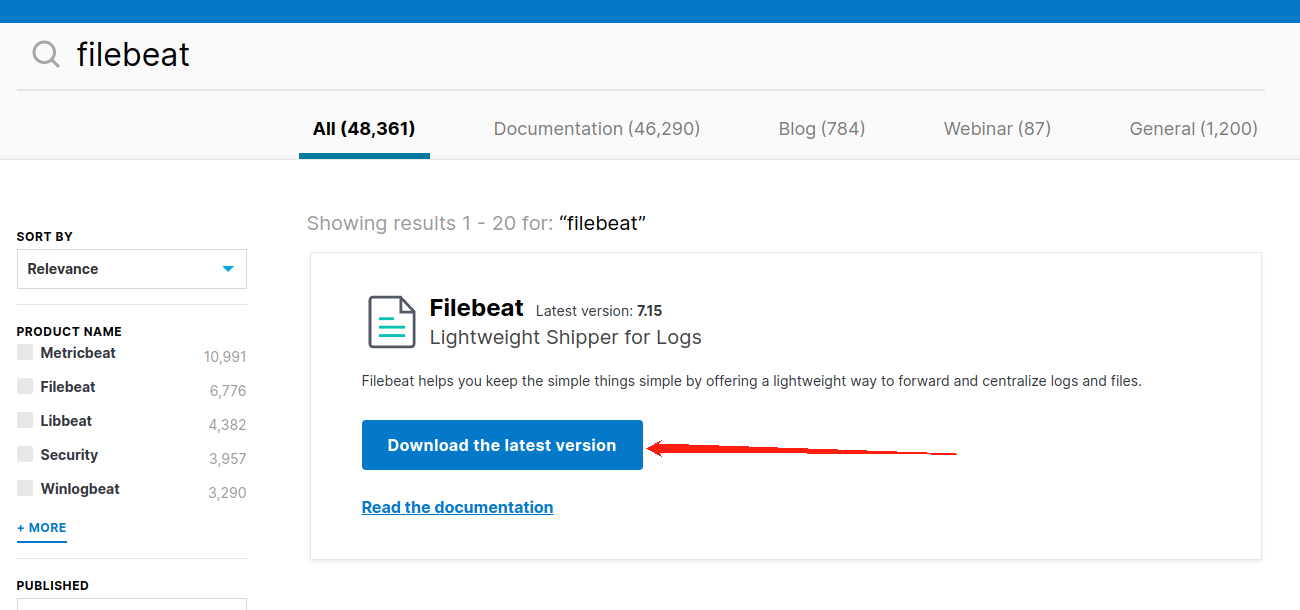
到此logstash安装成功。提示：logstash前面也有提到，可以过滤日志信息，

需要修改grok-patterns和default.conf文件，如有需要再沟通

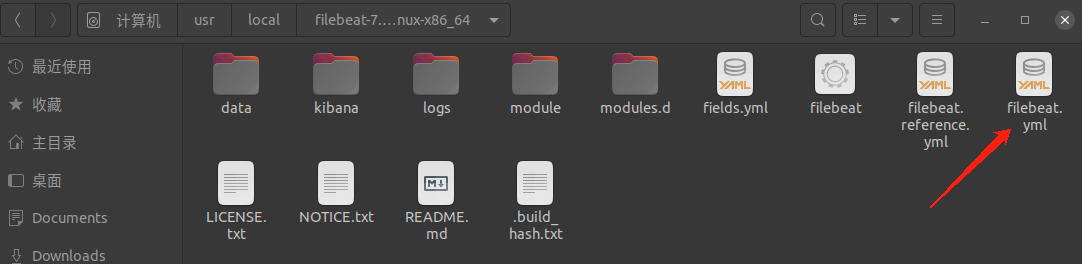
1. filebeat安装

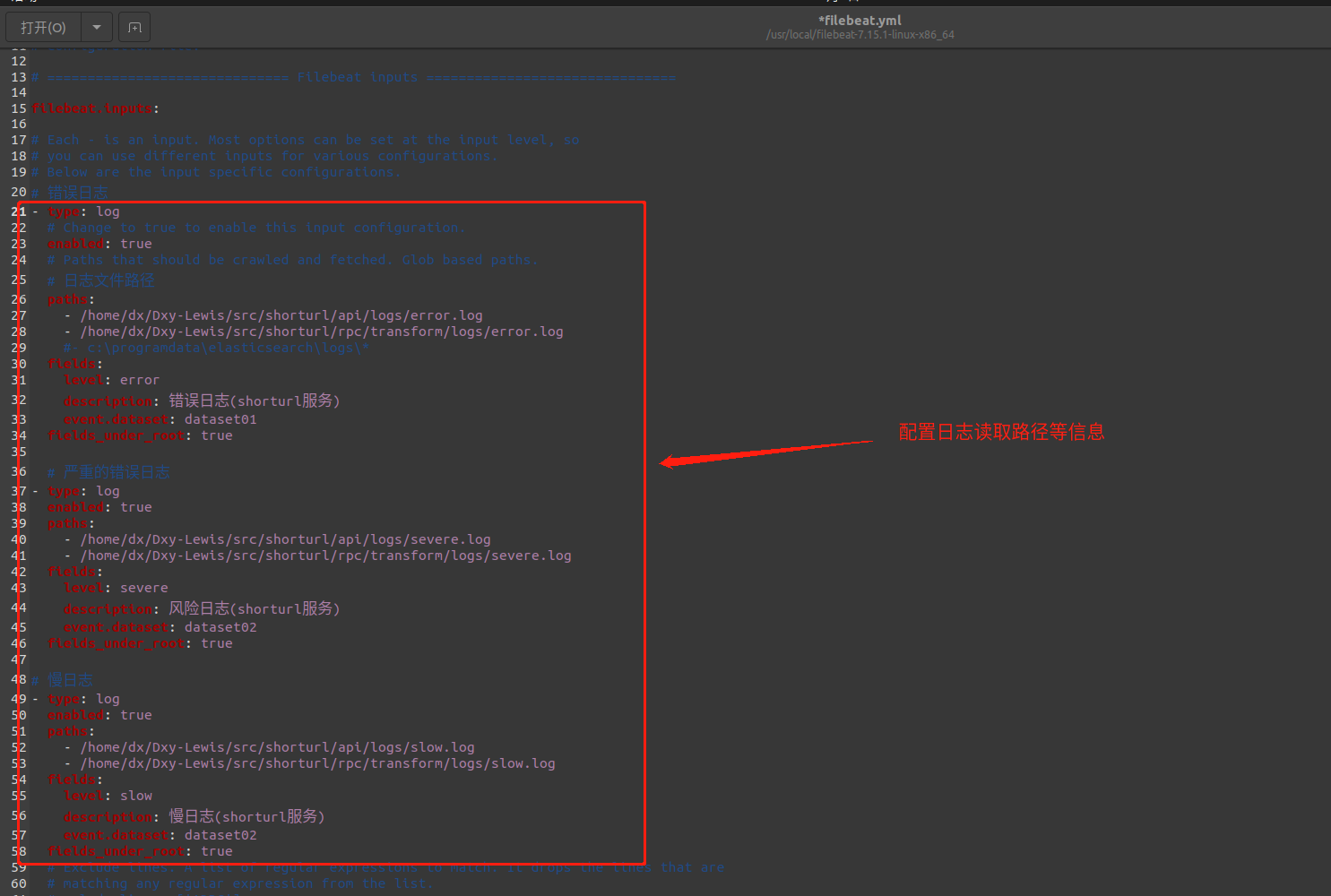
去es官网下载tar.gz文件：

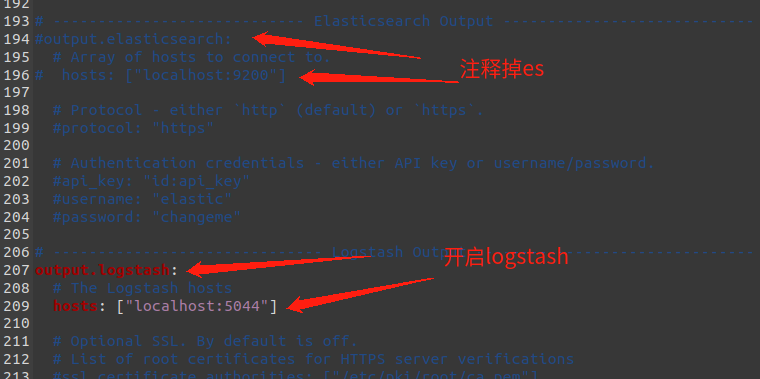
<https://www.elastic.co/search?q=filebeat&size=n_20_n>



文件下载好后，解压放到/usr/local下面，然后修改配置文件：

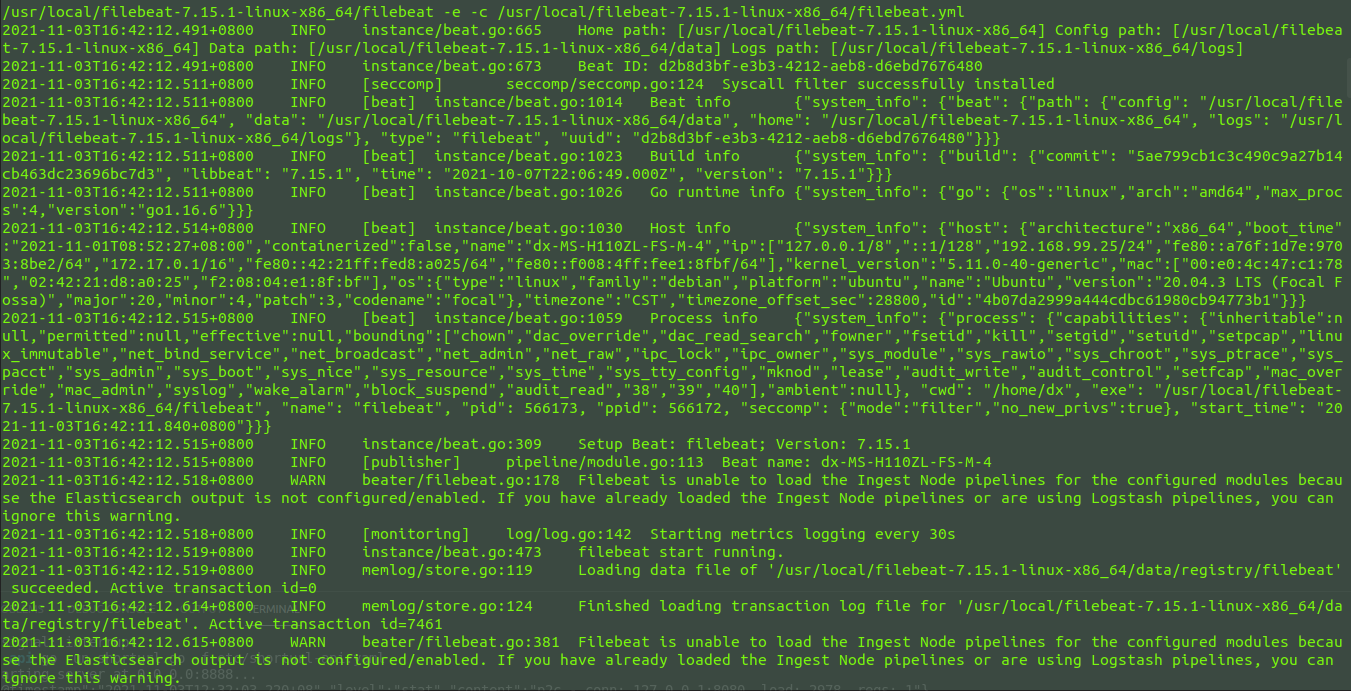






配置文件修改好之后，用以下命令启动：

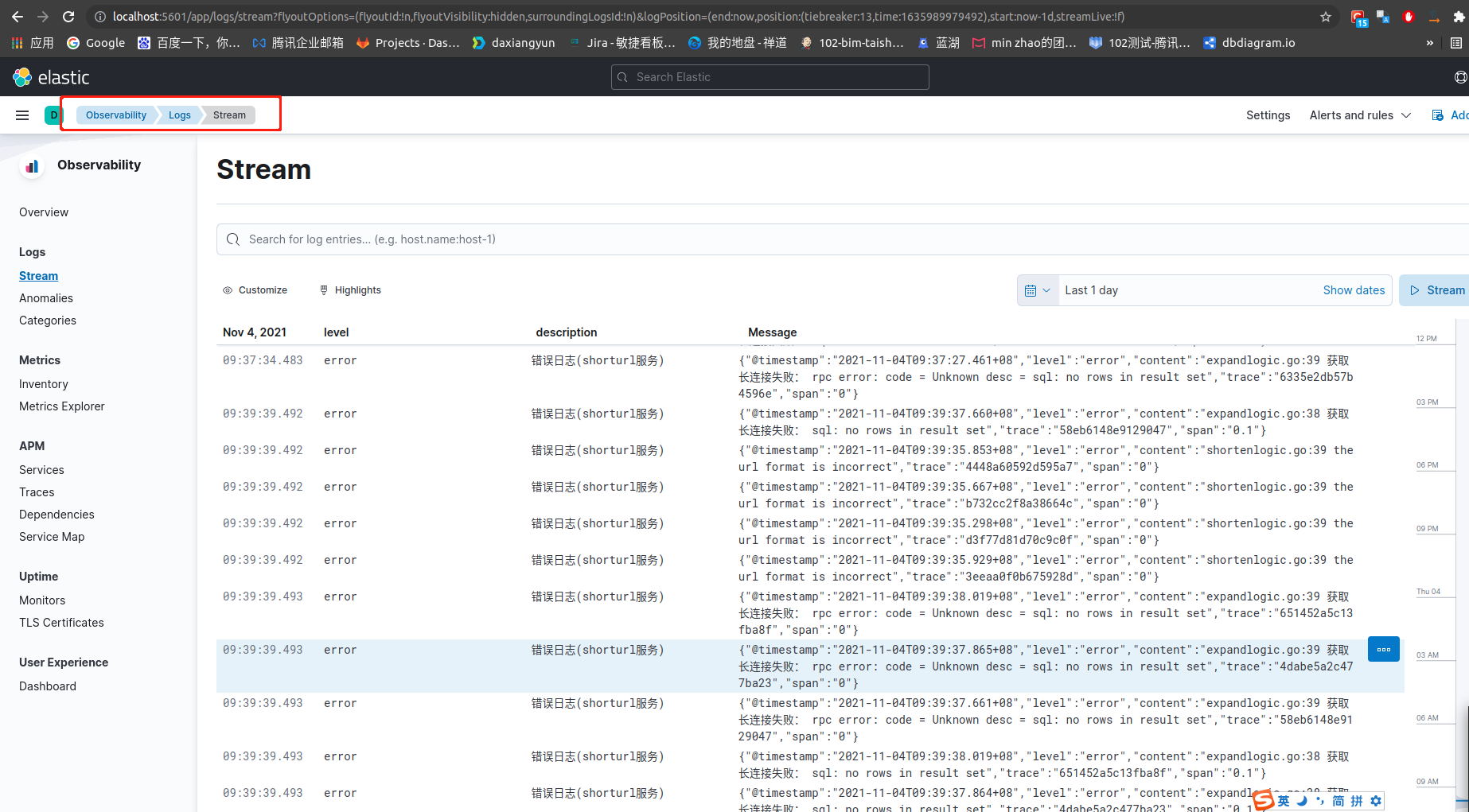
path/filebeat -e -c path/filebeat.yml



到此filebeat安装成功

1. 界面展示

1、直接在日志界面查看



1. 在Discover中查看，需要配置索引模板才可在这里显示

