作业

- 下载`elasticsearch` `kibana` `logstash`安装包，并修改其中的配置文件

```
#elasticsearch.yml 添加下面几项
node.name: node-1
network.host: 0.0.0.0
http.port: 9200
cluster.initial_master_nodes: ["node-1"]

#jvm.options 修改下面几项
8-13:-XX:+UseConcMarkSweepGC  修改为  8-13:-XX:+UseG1GC

#kibana.yml 添加下面几项
server.port: 5601
server.host: "0.0.0.0"
elasticsearch.hosts: ["http://localhost:9200"]

#logstash-7.6.1/config中添加文件log_syslog
input{
    syslog{
    type => "system-syslog"
    port => "514"
    }
}
output{
    elasticsearch{
         hosts => "http://10.182.79.36:9200"
         user => es
         password => hillstone
         codec => "rubydebug"
         index => "yushun-%{+YYYY-MM-dd}"
    }
}
```

- 压缩安装包，并移动到dockerfile所在目录

```
tar -zcvf elk.tar.gz elk
mv elk.tar.gz  dockerfile所在目录
```

- 进入到dockerfile所在目录，并创建镜像

```
docker build -t elk . -f ./dockerfile

#dockerfile
from centos:7
ENV TZ=Asia/Shanghai
# 开放端口
expose 9200
expose 5601
expose 9300
expose 514
# 安装jdk
```

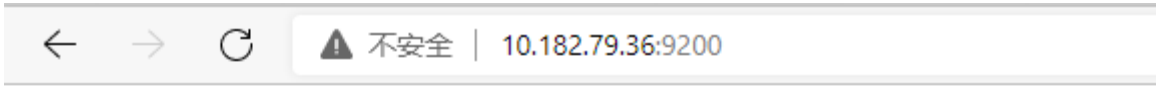
```
run yum update -y  && yum install -y java-1.8.0-openjdk-devel.x86_64
run mkdir /home/elk
run useradd -d /home/elk elk
workdir /home/elk
add elk.tar.gz /home/elk
add run.sh /home/elk
run chmod +x /home/elk/run.sh
run chown -R elk:elk /home/elk
workdir /home/elk/elk
cmd ../run.sh

#run.sh
su elk -c "nohup elasticsearch-7.6.1/bin/elasticsearch &"
su elk -c "nohup kibana-7.6.1-linux-x86_64/bin/kibana &"
nohup logstash-7.6.1/bin/logstash -f logstash-7.6.1/config/log_syslog
```

- 启动容器

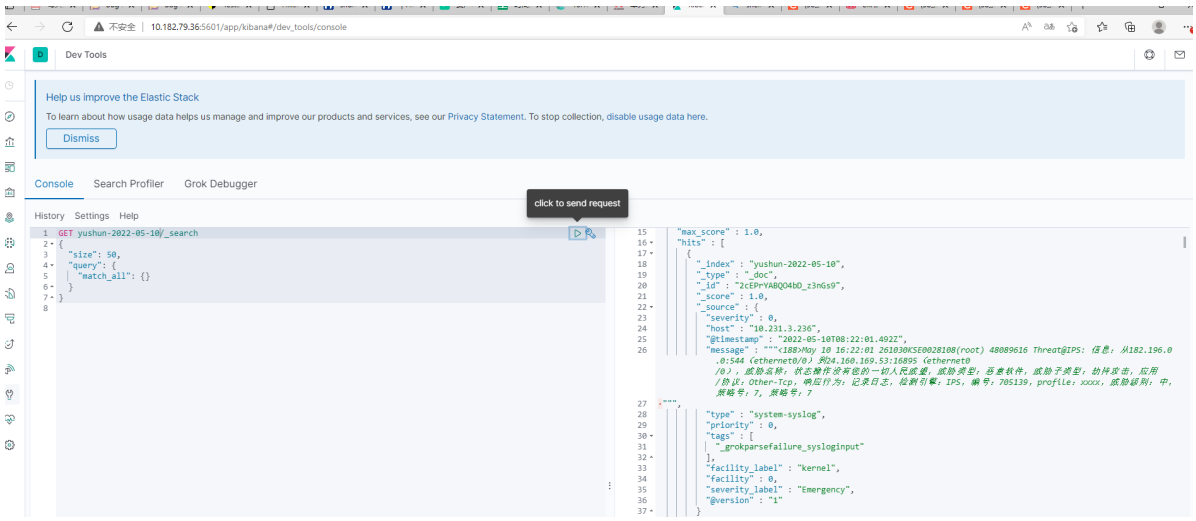
```
docker run --name elk -d -p 9200:9200 -p 5601:5601 -p 515:514/udp  elk
```

es截图




```
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "TsGXocEsR4aRFj6OFWZrww",
  "version" : {
    "number" : "7.6.1",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "aa751e09be0a5072e8570670309b1f12348f023b",
    "build_date" : "2020-02-29T00:15:25.529771Z",
    "build_snapshot" : false,
    "lucene_version" : "8.4.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```


kibana截图



logstash发送到es的截图