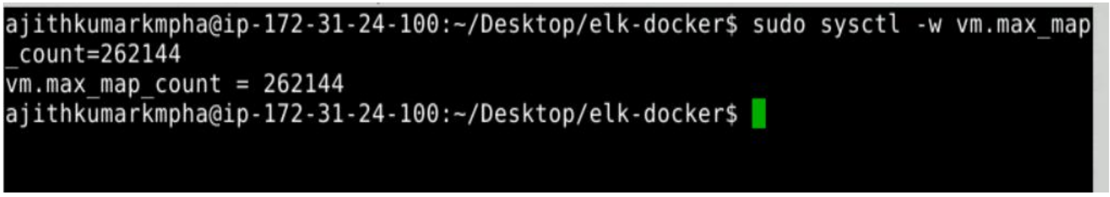
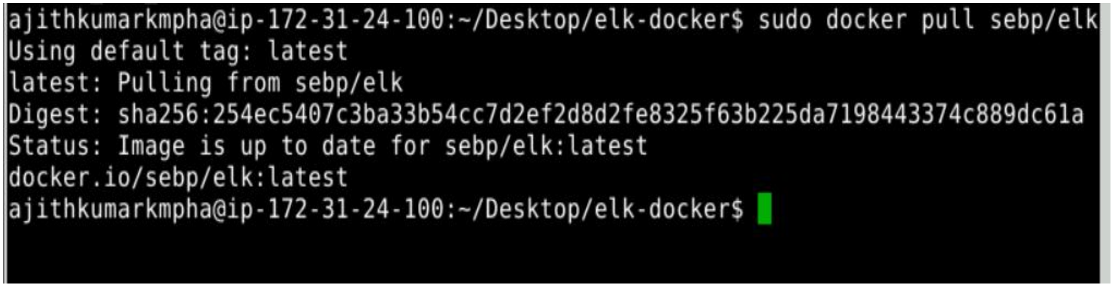
Set mmap count for ELK stack:



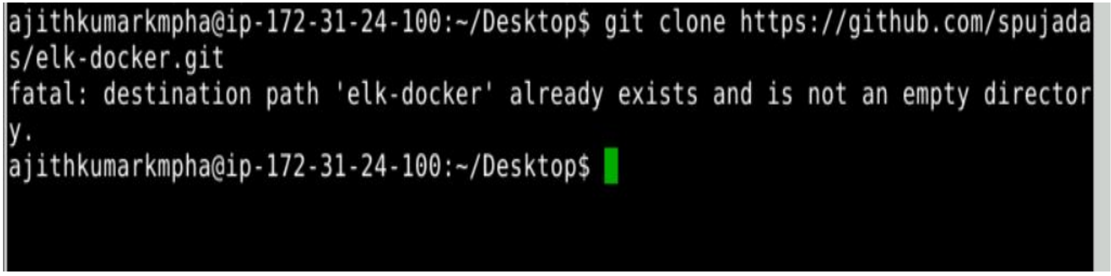
```
ajithkumarkmpha@ip-172-31-24-100:~/Desktop/elk-docker$ sudo sysctl -w vm.max_map
_count=262144
vm.max_map_count = 262144
ajithkumarkmpha@ip-172-31-24-100:~/Desktop/elk-docker$ █
```

pull the ELK image from the Docker registry:



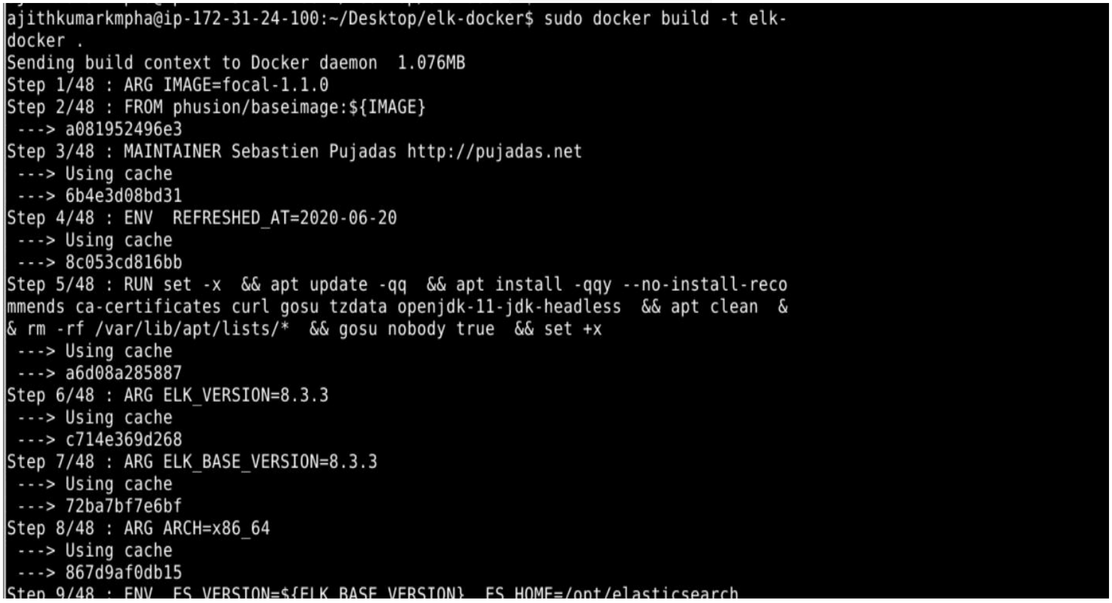
```
ajithkumarkmpha@ip-172-31-24-100:~/Desktop/elk-docker$ sudo docker pull sebp/elk
Using default tag: latest
latest: Pulling from sebp/elk
Digest: sha256:254ec5407c3ba33b54cc7d2ef2d8d2fe8325f63b225da7198443374c889dc61a
Status: Image is up to date for sebp/elk:latest
docker.io/sebp/elk:latest
ajithkumarkmpha@ip-172-31-24-100:~/Desktop/elk-docker$ █
```

build the image from a source file:



```
ajithkumarkmpha@ip-172-31-24-100:~/Desktop$ git clone https://github.com/spujada
s/elk-docker.git
fatal: destination path 'elk-docker' already exists and is not an empty director
y.
ajithkumarkmpha@ip-172-31-24-100:~/Desktop$ █
```

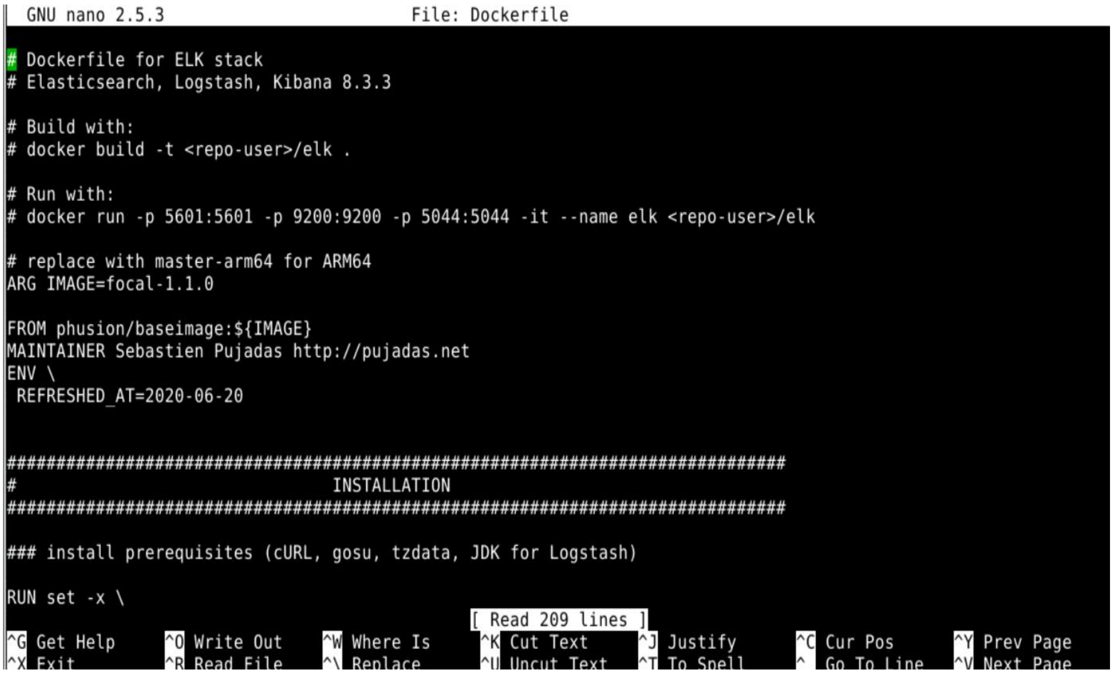
build the Docker image with the docker build:



```
ajithkumarkmpha@ip-172-31-24-100:~/Desktop/elk-docker$ sudo docker build -t elk-
docker .
Sending build context to Docker daemon  1.076MB
Step 1/48 : ARG IMAGE=focal-1.1.0
Step 2/48 : FROM phusion/baseimage:${IMAGE}
 ---> a081952496e3
Step 3/48 : MAINTAINER Sebastien Pujadas http://pujadas.net
 ---> Using cache
 ---> 6b4e3d08bd31
Step 4/48 : ENV  REFRESHED_AT=2020-06-20
 ---> Using cache
 ---> 8c053cd816bb
Step 5/48 : RUN set -x  && apt update -qq  && apt install -qqy --no-install-reco
mmends ca-certificates curl gosu tzdata openjdk-11-jdk-headless  && apt clean  &
& rm -rf /var/lib/apt/lists/*  && gosu nobody true  && set +x
 ---> Using cache
 ---> a6d08a285887
Step 6/48 : ARG ELK_VERSION=8.3.3
 ---> Using cache
 ---> c714e369d268
Step 7/48 : ARG ELK_BASE_VERSION=8.3.3
 ---> Using cache
 ---> 72ba7bf7e6bf
Step 8/48 : ARG ARCH=x86_64
 ---> Using cache
 ---> 867d9af0db15
Step 9/48 : ENV  ES_VERSION=${ELK_BASE_VERSION}  ES_HOME=/opt/elasticsearch
```

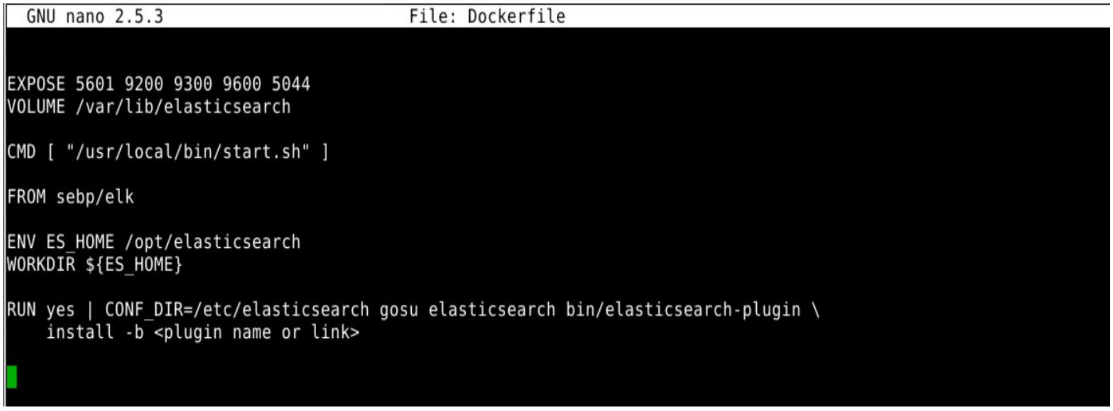
install plugins and build the image to run the installation:

Open Dockerfile:



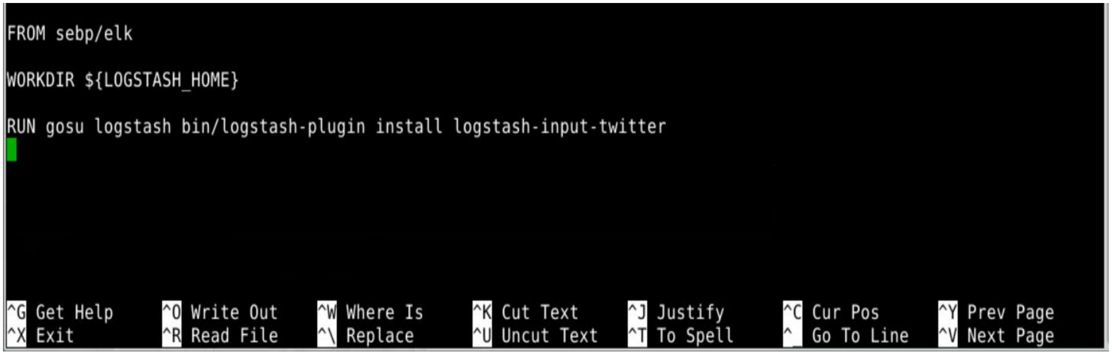
```
  GNU nano 2.5.3                     File: Dockerfile

# Dockerfile for ELK stack
# Elasticsearch, Logstash, Kibana 8.3.3

# Build with:
# docker build -t <repo-user>/elk .

# Run with:
# docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk <repo-user>/elk

# replace with master-arm64 for ARM64
ARG IMAGE=focal-1.1.0

FROM phusion/baseimage:${IMAGE}
MAINTAINER Sebastien Pujadas http://pujadas.net
ENV \
 REFRESHED_AT=2020-06-20


###############################################################################
#                                 INSTALLATION
###############################################################################

### install prerequisites (cURL, gosu, tzdata, JDK for Logstash)

RUN set -x \
                                        [ Read 209 lines ]
```

Install Elasticsearch plugin:



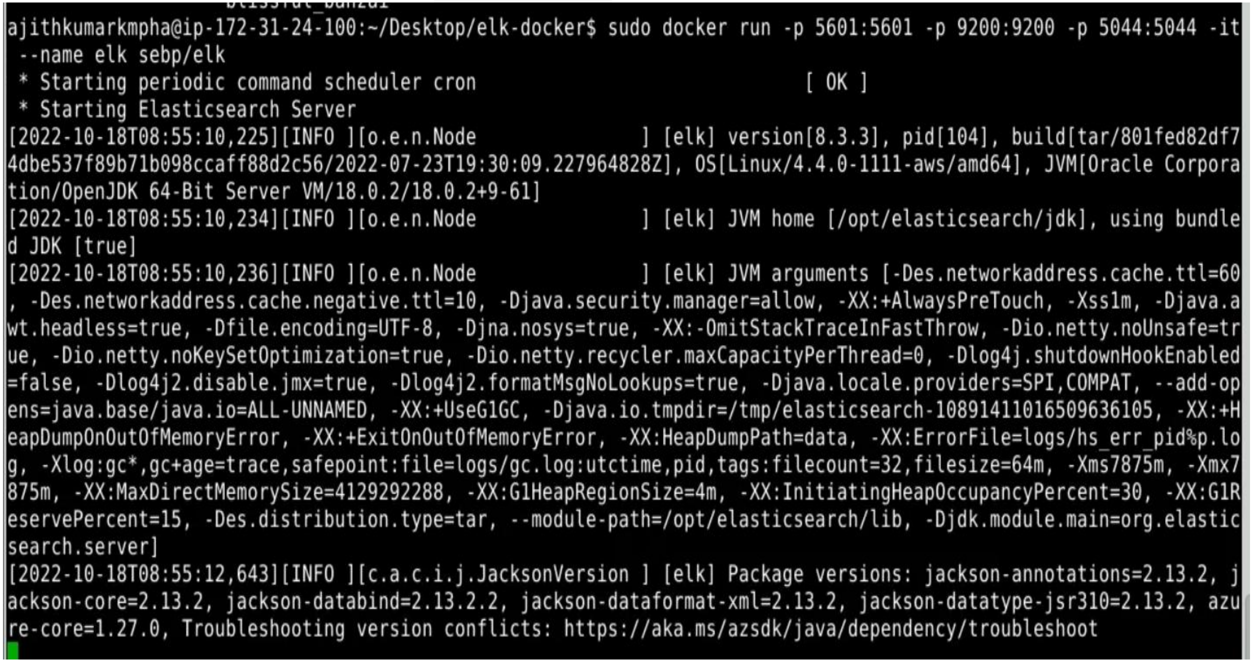
```
  GNU nano 2.5.3                     File: Dockerfile


EXPOSE 5601 9200 9300 9600 5044
VOLUME /var/lib/elasticsearch

CMD [ "/usr/local/bin/start.sh" ]

FROM sebp/elk

ENV ES_HOME /opt/elasticsearch
WORKDIR ${ES_HOME}

RUN yes | CONF_DIR=/etc/elasticsearch gosu elasticsearch bin/elasticsearch-plugin \
    install -b <plugin name or link>
```

Install Logstash plugin:



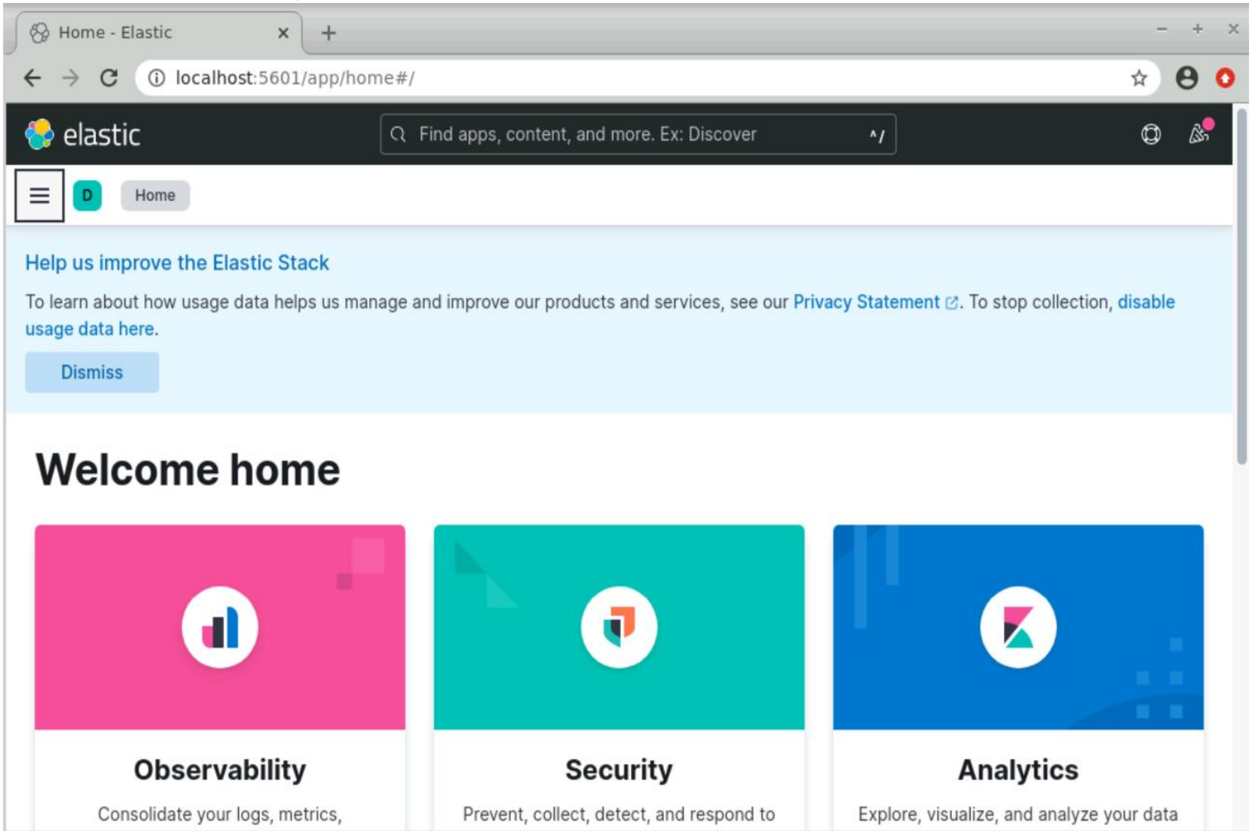
```
FROM sebp/elk

WORKDIR ${LOGSTASH_HOME}

RUN gosu logstash bin/logstash-plugin install logstash-input-twitter
```

Run ELK stack container via docker run:



```
ajithkumarkmpha@ip-172-31-24-100:~/Desktop/elk-docker$ sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it
 --name elk sebp/elk
 * Starting periodic command scheduler cron                                   [ OK ]
 * Starting Elasticsearch Server
[2022-10-18T08:55:10,225][INFO ][o.e.n.Node               ] [elk] version[8.3.3], pid[104], build[tar/801fed82df7
4dbe537f89b71b098ccaff88d2c56/2022-07-23T19:30:09.227964828Z], OS[Linux/4.4.0-1111-aws/amd64], JVM[Oracle Corpora
tion/OpenJDK 64-Bit Server VM/18.0.2/18.0.2+9-61]
[2022-10-18T08:55:10,234][INFO ][o.e.n.Node               ] [elk] JVM home [/opt/elasticsearch/jdk], using bundle
d JDK [true]
[2022-10-18T08:55:10,236][INFO ][o.e.n.Node               ] [elk] JVM arguments [-Des.networkaddress.cache.ttl=60
, -Des.networkaddress.cache.negative.ttl=10, -Djava.security.manager=allow, -XX:+AlwaysPreTouch, -Xss1m, -Djava.a
wt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=tr
ue, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled
=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMsgNoLookups=true, -Djava.locale.providers=SPI,COMPAT, --add-op
ens=java.base/java.io=ALL-UNNAMED, -XX:+UseG1GC, -Djava.io.tmpdir=/tmp/elasticsearch-10891411016509636105, -XX:+H
eapDumpOnOutOfMemoryError, -XX:+ExitOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs_err_pid%p.lo
g, -Xlog:gc*,gc+age=trace,safepoint:file=logs/gc.log:utctime,pid,tags:filecount=32,filesize=64m, -Xms7875m, -Xmx7
875m, -XX:MaxDirectMemorySize=4129292288, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -XX:G1R
eservePercent=15, -Des.distribution.type=tar, --module-path=/opt/elasticsearch/lib, -Djdk.module.main=org.elastic
search.server]
[2022-10-18T08:55:12,643][INFO ][c.a.c.i.j.JacksonVersion ] [elk] Package versions: jackson-annotations=2.13.2, j
ackson-core=2.13.2, jackson-databind=2.13.2.2, jackson-dataformat-xml=2.13.2, jackson-datatype-jsr310=2.13.2, azu
re-core=1.27.0, Troubleshooting version conflicts: https://aka.ms/azsdk/java/dependency/troubleshoot
```

ELK stack is running on localhost:5601:



Home - Elastic
localhost:5601/app/home#/
elastic
Find apps, content, and more. Ex: Discover
D
Home

Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Welcome home

Observability

Consolidate your logs, metrics,

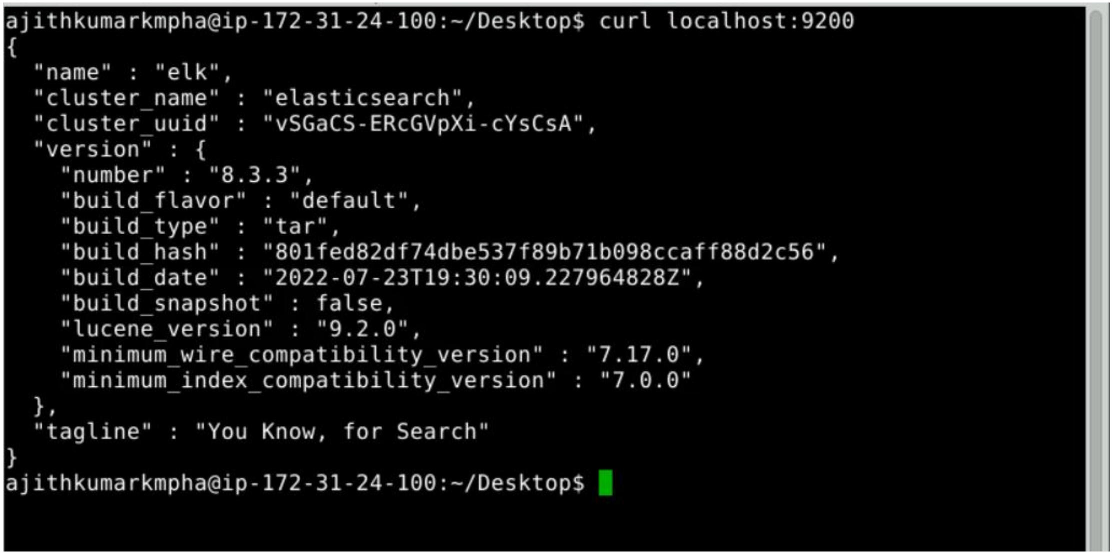
Security

Prevent, collect, detect, and respond to

Analytics

Explore, visualize, and analyze your data

Check that Elasticsearch is running with a curl request:



```
ajithkumarkmpha@ip-172-31-24-100:~/Desktop$ curl localhost:9200
{
  "name" : "elk",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "vSGaCS-ERcGVpXi-cYsCsA",
  "version" : {
    "number" : "8.3.3",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "801fed82df74dbe537f89b71b098ccaff88d2c56",
    "build_date" : "2022-07-23T19:30:09.227964828Z",
    "build_snapshot" : false,
    "lucene_version" : "9.2.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
ajithkumarkmpha@ip-172-31-24-100:~/Desktop$ 
```