\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Containerized ELK Stack\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ELK stack can be containerized and used on demand without provisioning additional infrastructure. In this project I have completed all the implementation and steps which can help us to containerize Elasticsearch and Kibana on RHEL EC2 instances.

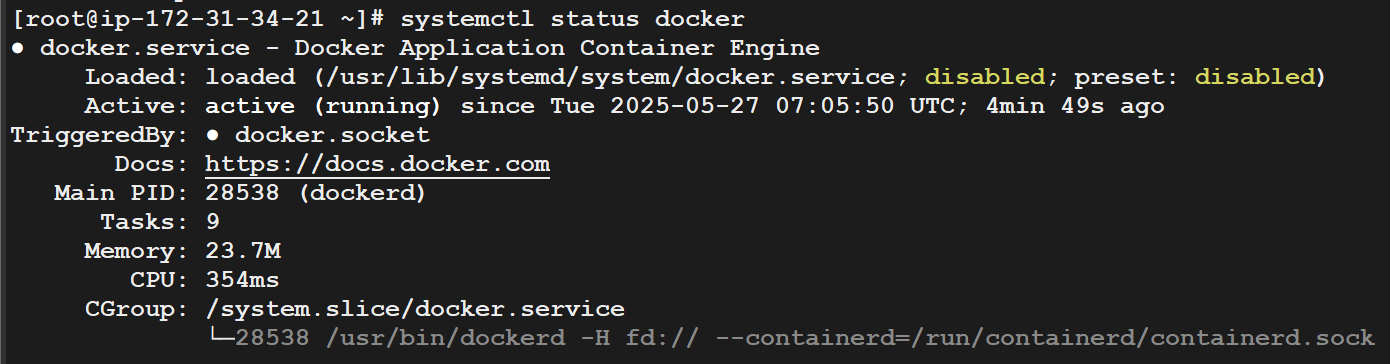
Pre-requisites are,

As a prerequisite, docker should be installed and running, also the host should be updated.

Documentation: https://docs.docker.com/engine/install/rhel/

Use below commands,

yum update -y && curl -fsSL https://get.docker.com -o get-docker.sh && sudo sh get-docker.sh && systemctl start docker && yum install net-tools -y



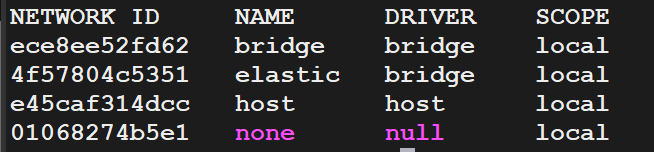
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Elasticsearch\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Elasticsearch is a distributed, open-source search and analytics engine used for a variety of applications, including log analysis, full-text search, security intelligence, and business analytics. It excels at handling large volumes of data with near real-time search capabilities.

Steps to install elasticsearch are as follows,

1. Create a new docker network.

docker network create elastic

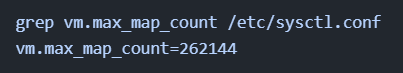


1. Pull elasticsearch container by below command,

docker pull docker.elastic.co/elasticsearch/elasticsearch:9.0.0



1. Before production container creation, run below command and modify the file /etc/sysctl.conf

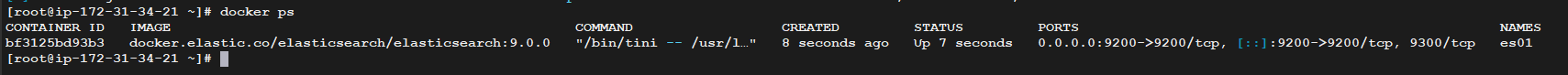


Run below commands as well (if required)



1. Run elastic container in background.

docker run --name es01 --net elastic -p 9200:9200 -m 2GB --restart=always -v elastic\_data:/usr/share/elasticsearch/data/ -it docker.elastic.co/elasticsearch/elasticsearch:9.0.0

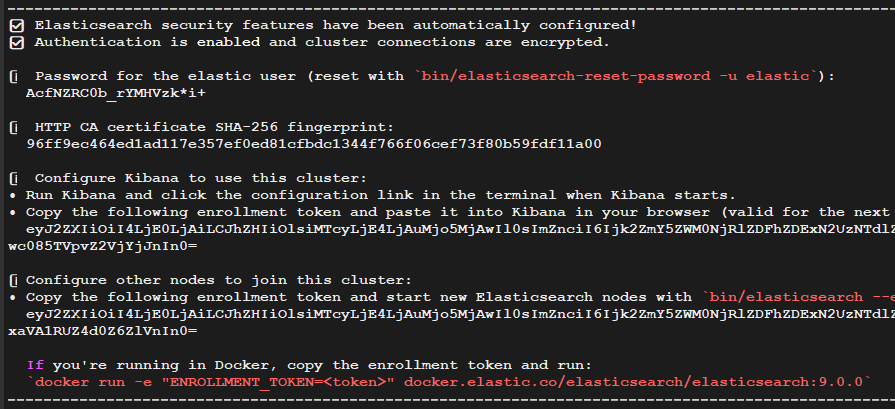


Note 🡪 If that container stops by itself bring it up manually by docker start <containerid> &

Make sure that it is always running.

1. Check the logs and copy paste to your note pad,

docker logs <containerid> (if required)



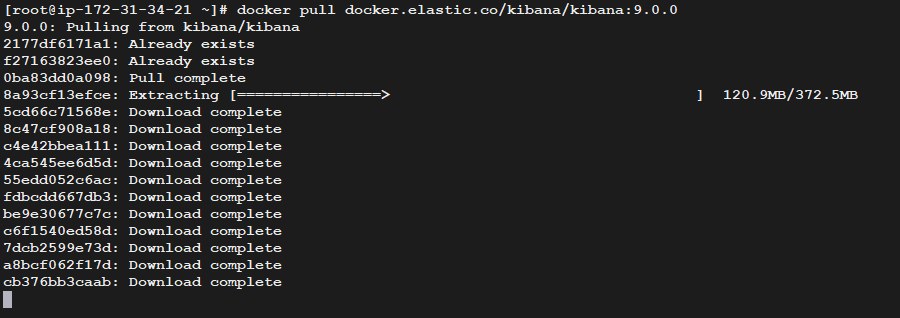
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Kibana\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Kibana is an open-source analytics and visualization platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. You can easily perform advanced data analysis and visualize your data in a variety of charts, tables, and maps.

Steps to install Kibana are as follows,

1. Pull Kibana official image,

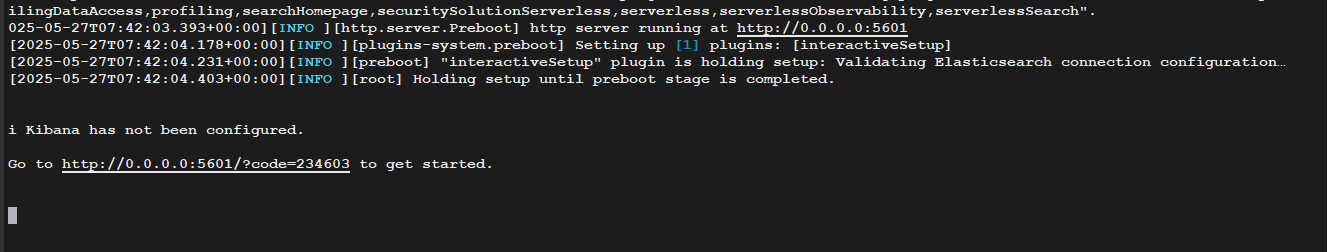
docker pull docker.elastic.co/kibana/kibana:9.0.0



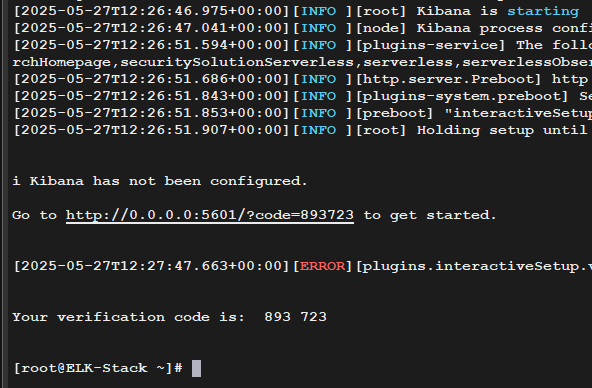
1. Run the image by below command.

docker run --name kib01 --net elastic -p 5601:5601 --restart=always docker.elastic.co/kibana/kibana:9.0.0

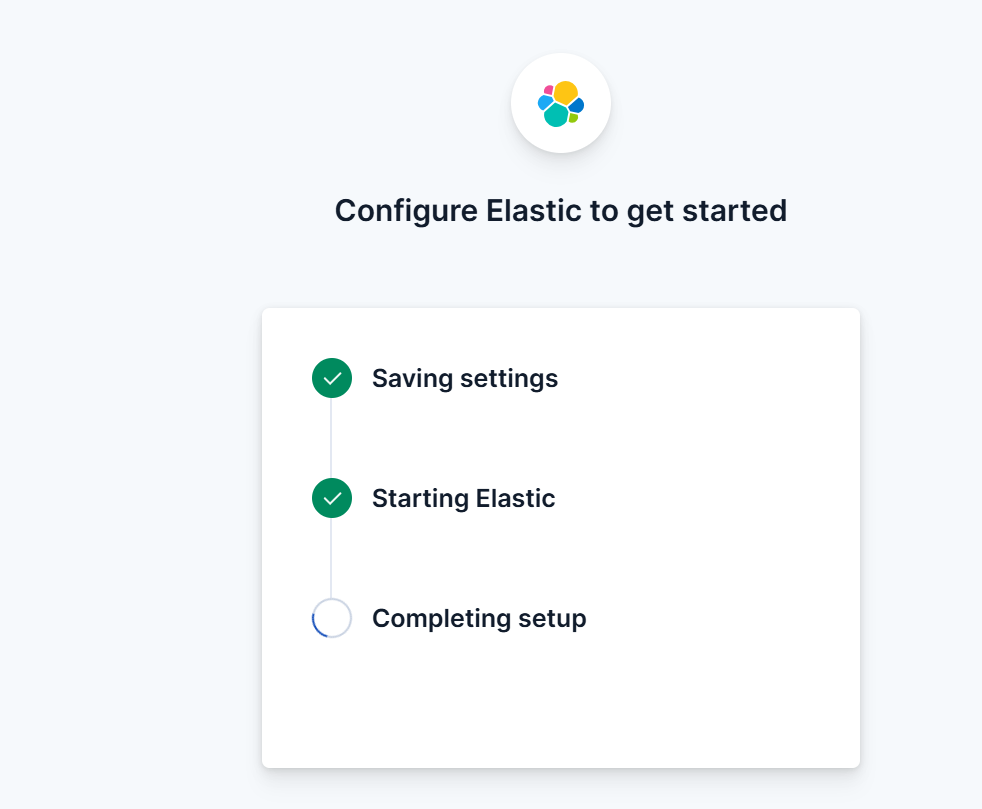
1. Inspect the logs of the kibana container and copy the URL to access kibana in browser window.



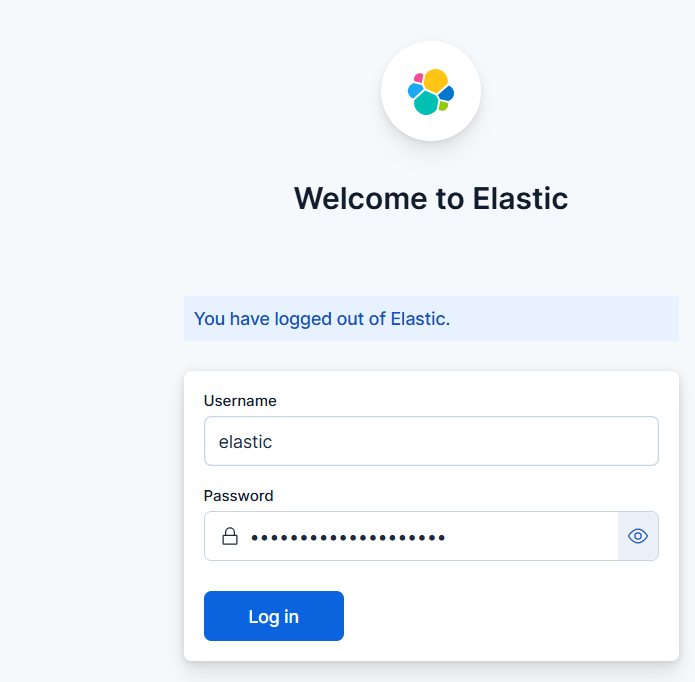
NOTE 🡪 After this step if Ui asks you a 6-digit passcode, then use docker logs commands, it will show up.



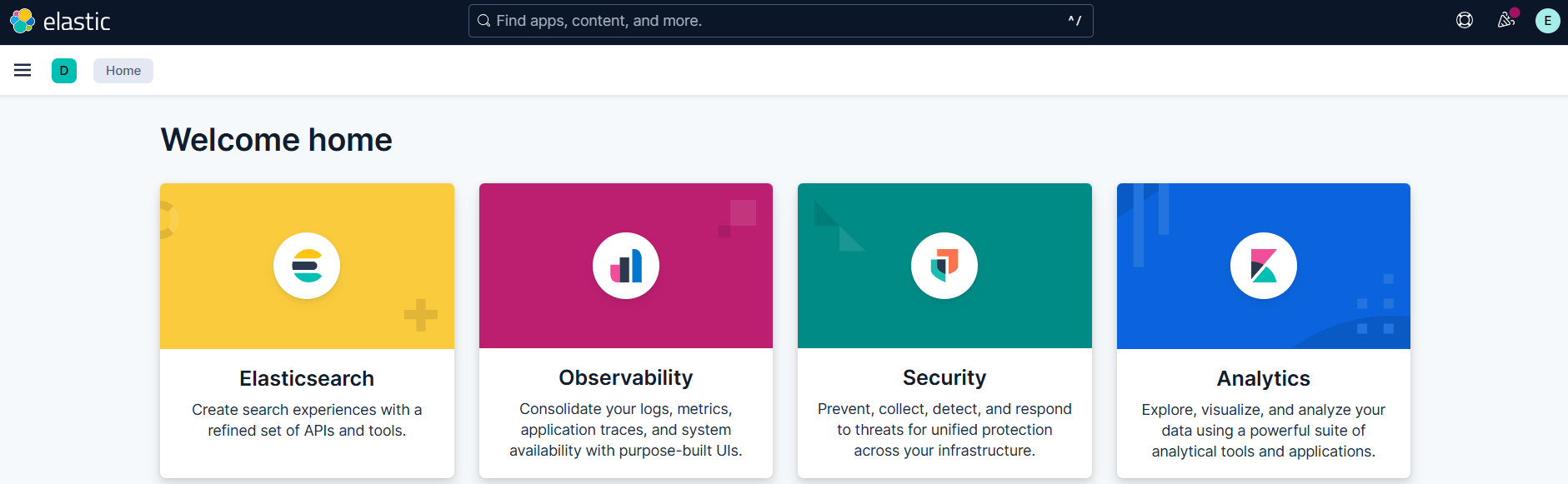
1. After accessing, now enter the token from step 5, point no 3. After entering token, you will see UI like below.



1. Use default password from line one step 5, and login as elastic user.



1. After that you can see login details,



\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Logstash\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Logstash is an open-source data collection engine with real-time pipelining capabilities. Logstash can dynamically unify data from disparate sources and normalize the data into destinations of your choice.

Steps to install logstash are,

1. Create a simple Dcokerfile which uses the base image for logstash.

FROM docker.elastic.co/logstash/logstash:9.0.0

COPY logstash.conf /usr/share/logstash/pipeline/logstash.conf

EXPOSE 5044

1. For configuring logstash, we can use a simple input/output file like below. Currently not setting up any pipeline configuration.

input {

tcp {

port => 5044

codec => json

}

}

output {

elasticsearch {

hosts => ["https:// 15.207.18.14:9200"]

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

ssl\_verification\_mode => "none"

user=> "elastic"

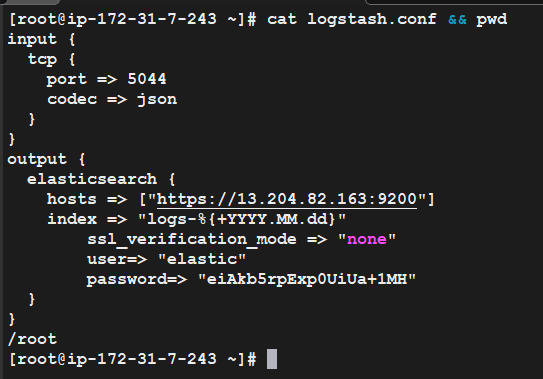
password=> "eiAkb5rpExp0UiUa+1MH"

}

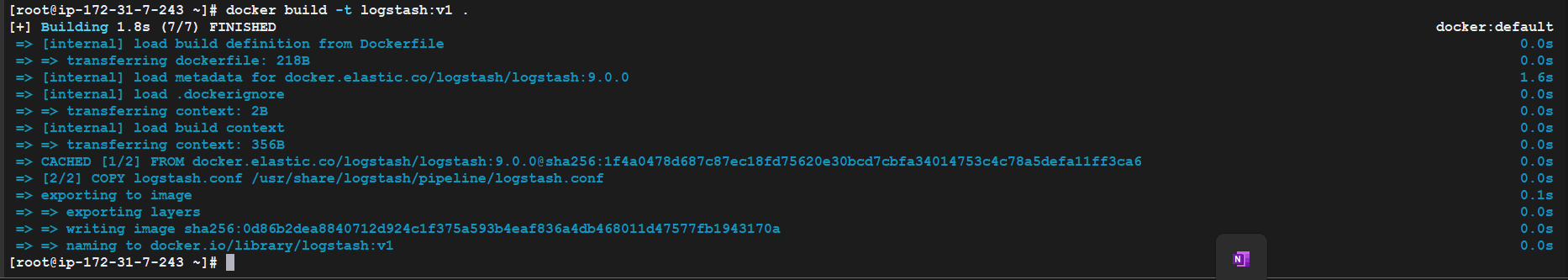
}

So, the above file states that the input to logstash container would be on port 5044 by default & the input data would be in. json format. Output describes the elastic search host user credentials & SSL settings which are turned off for demonstration purposes.

1. Make sure that this logstash.conf file is present in same directory as of Dockerfile.



1. Build the docker image,



1. Run the container by below command. Container logs should reflect like below which should be good.

docker run --name ls01 --net elastic -p 5044:5044 -m 2GB --restart=always -it <image id>

