Writeup for Deploying ELK Stack on Docker Container

Algorithm:

1.Install Docker:

Ensure Docker is installed on the target machine where you want to deploy ELK Stack.

2.Pull ELK Stack Docker Images:

Use Docker to pull the required ELK Stack images from Docker Hub:

ElasticSearch: docker pull docker.elastic.co/elasticsearch/elasticsearch:7.14.0

Logstash: docker pull docker.elastic.co/logstash/logstash:7.14.0

Kibana: docker pull docker.elastic.co/kibana/kibana:7.14.0

Create a Docker Network:

3.Create a Docker network to enable communication between the containers:

```
docker network create elk_network
```

4.Run ElasticSearch Container:

Start the ElasticSearch container with proper configuration and network settings:

```
docker run -d --name elasticsearch \
 --network elk_network \
 -p 9200:9200 \
 -p 9300:9300 \
 -e "discovery.type=single-node" \
docker.elastic.co/elasticsearch/elasticsearch:7.14.0
```

5.Run Logstash Container:

Create a Logstash configuration file (e.g., logstash.conf) that defines input, filter, and output settings.

Mount the Logstash configuration file to the container: docker

run -d --name logstash \

--network elk_network \

-v /path/to/logstash.conf:/usr/share/logstash/pipeline/logstash.conf \

docker.elastic.co/logstash/logstash:7.14.0

6. Run Kibana Container:

Start the Kibana container, connecting it to the same network: docker

run -d --name kibana \

--network elk_network \ -p

5601:5601 \

docker.elastic.co/kibana/kibana:7.14.0

7.Access Kibana Web Interface:

Once the containers are up and running, access Kibana's web interface in your browser by navigating to http://localhost:5601.

8.Configure Log Sources:

Configure your applications or systems to send logs to the Logstash container using its IP address and the configured input settings.

9.Visualize and Analyze Logs:

In Kibana, set up index patterns to define which Elasticsearch indices to use for log data.

Create visualizations and dashboards to analyze and monitor the logs effectively.

10.Scale and Monitor:

If needed, you can scale the ELK Stack containers by running more instances in a cluster for better performance and redundancy.

Monitor the performance and resource usage of the containers using Docker tools or monitoring solutions.