Deploying ELK Stack on Docker Container

Source Code :

logstash.conf :-

```
Input {
        File {
                Path  => “/root/temp/inlog.log”
        }
}
Output {
        Elasticsearch {
                Hosts => [“ http://elasticsearch:9200 ”]
        }
}
```

docker-componse.yml :-

```
version: '3.6'
services:
  Elasticsearch:
```

```
 image: elasticsearch:7.16.2
container_name: elasticsearch
restart: always

 volumes:
- elastic_data:/usr/share/elasticsearch/data/
  environment:
   ES_JAVA_OPTS: "-Xmx256m -Xms256m"
   discovery.type: single-node
 ports:
- '9200:9200'  - '9300:9300'  networks:
- elk


Logstash:
 image: logstash:7.16.2
container_name: logstash
restart: always  volumes:
- ./logstash/:/logstash_dir  command: logstash -f
  /logstash_dir/logstash.conf  depends_on:
- Elasticsearch  ports:
- '9600:9600'  environment:

   LS_JAVA_OPTS: "-Xmx256m -Xms256m"
 networks:
```

```
    - elk


  Kibana:
    image: kibana:7.16.2
    container_name: kibana
    restart: always  ports:
    - '5601:5601'  environment:
    - ELASTICSEARCH_URL=http://elasticsearch:9
      200  depends_on:
    - Elasticsearch  networks:
    - elk
 volumes:
  elastic_data: {}


 networks:
   elk:
```

inlog.log :-

```
This is a test file
this is a second
line
```

firewall :- sudo firewall-cmd --add-port=9200/tcp

--permanent sudo firewall-cmd --add-port=5601/tcp

--permanent sudo firewall-cmd --add-port=9600/tcp

--permanent sudo firewall-cmd --add-port=9300/tcp

--permanent sudo firewall-cmd --reload