Phase-5

Deploying ELK Stack on Docker Container

Description:

You have to deploy ELK stack on a Docker container to implement continuous monitoring.

Code Snippets

```
Version: '3.6'
Services:
```

Elastic Search

```
image: Elasticsearch:7.16.2
container_name: Elasticsearch
restart: always
volumes:
  - Elastic_data:/usr/share/Elasticsearch/data/
Environment:
  ES_JAVA_OPTS: '-Xmx256m -Xms256m'
  discover.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:9200
depends_on:
    - ElasticSearch
networks:
    - ELK
volumes:
  Elastic-data:{}
networks:
    ELK:
```

logstash.conf

```
input{
  file{
    path => "/root/temp/in log.log"
  }
```

```
}
output {
    ElasticSearch {
        hosts => [http://ElasticSearch:9200]
    }
}
```

in log.log

```
This is a test file
This is the log file that is fetched
        from logstash conf file.
```