**Phase-5**

**Deploying ELK Stack on Docker Container**

DESCRIPTION

**Project objective:**

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

**Code Snippets**

**docker-compose.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:9200 |
|  |

|  |
| --- |
| depends\_on: |
|  |

|  |
| --- |
| - Elasticsearch |
|  |

|  |
| --- |
| networks: |
|  |

|  |
| --- |
| - elk |
|  |

|  |
| --- |
| volumes: |
|  |

|  |
| --- |
| elastic\_data: {} |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| networks: |
|  |

elk:

**logstash.conf**

input {

file {

path => “/root/temp/inlog.log”

}

}

Output {

elasticsearch {

hosts => [<http://elasticsearch:9200>]

}

}

**inlog.log**

This is a test file

This is the log file that is fetched from logstash conf file

**Commands Used: -**

**mkdir**

To create the new directory

**ls**

To list the files in the repository

**vi**

Vi editor to enter the contents as text to execute the file

**docker-compose up**

Aggregates the output of each container