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