Elk setup:

Specifications:-

Os:Ubuntu

Type:t2.medium

Commands:-

**Update System**

sudo apt-get update

**Install wget if it is not on the system**

sudo apt-get install wget -y

**Manual ElK Stack Installation steps**

**1. Download and install public signing key**

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

**2. Install apt-transport-https package**

sudo apt-get install apt-transport-https -y

**3. Save directory definitions**

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

**4. Update and Install elasticsearch**

sudo apt-get update && sudo apt-get install elasticsearch && sudo apt-get install logstash && sudo apt-get install kibana

**5. configure elasticsearch**

sudo su

nano /etc/elasticsearch/elasticsearch.yml

change cluster name

cluster.name: demo-elk

give the cluster a descriptive name

node.name: elk-1

change network binding

network.host: 0.0.0.0

setup discovery.type as single node

discovery.type: single-node

**6. Start Elasticsearch service**

sudo systemctl start elasticsearch

**7. validate Elasticsearch cluster health**

curl -XGET http://localhost:9200/\_cluster/health?pretty

**8. configure kibana**

nano /etc/kibana/kibana.yml

uncomment server.port

server.port: 5601

server base url however this needs to be corrected everytime you start and stop the server

server.publicBaseUrl: "http://192.168.1.3:5601/"

change server.host

server.host: "0.0.0.0"

change server.name

server.name: "demo-kibana"

uncomment elasticsearch.host

elasticsearch.hosts: ["http://localhost:9200"]

**9. start Kibana service**

systemctl start kibana

**10. enable elasticsearch and kibana**

systemctl enable elasticsearch

systemctl enable kibana

images:





