**Step 1: Update System Packages**

Before installing, update your system packages:

sudo apt update && sudo apt upgrade -y

**Step 2: Install Java (If Not Installed)**

Elasticsearch requires Java. Install OpenJDK:

sudo apt install -y openjdk-17-jdk

Verify the installation:

java -version

**Step 3: Add Elasticsearch Repository**

1. Download and install the GPG key:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

1. Add the Elasticsearch repository:

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

1. Update the package list:

sudo apt update

**Step 4: Install Elasticsearch**

sudo apt install -y elasticsearch=8.17.1

After Insttallation is completed.

**Note: password will be provided post installation copy that password for elastic super user from all the nodes (the server who will become master that password we will use to auth)**

**Step 5: Configure Elasticsearch**

Edit the Elasticsearch configuration file:

Cd /etc/elasticsearch  
sudo vim /etc/elasticsearch/elasticsearch.yml

network.host: 0.0.0.0   
cluster.name: my-cluster

node.name: node-1  
discovery.seed\_hosts: ["172.31.94.58","172.31.91.124","172.31.88.147"]  
cluster.initial\_master\_nodes: ["node-1", "node-2","node-3"]

Save and exit (CTRL+X, then Y, then ENTER).

**Step 9: Open Ports (If Needed)**

If accessing Elasticsearch remotely, allow traffic:  
sudo ufw allow 9200/tcp

**Self Sign Certificate Binding**

To generate self sign certificate, we have to use elastic search utility   
  
**/usr/share/elasticsearch/bin/elasticsearch-certutil**

Run below command to generate ca certificate

/usr/share/elasticsearch/bin/elasticsearch-certutil ca --pem --out /etc/elasticsearch/certs/ca\_elastic.zip  
  
go to   
cd /etc/elasticsearch/certs/  
unzip /etc/elasticsearch/certs/ca\_elastic.zip  
  
Give permission and ownership to this certificate  
chown -R elasticsearch:elasticsearch /etc/elasticsearch  
chmod -R 775 /etc/elasticsearch

**below command to generate certificate for elastic**

/usr/share/elasticsearch/bin/elasticsearch-certutil cert --out /etc/elasticsearch/certs/certificate.zip --name elastic --ca-cert /etc/elasticsearch/certs/ca/ca.crt --ca-key /etc/elasticsearch/certs/ca/ca.key --dns sys.fcc --pem

go to /etc/elasticsearch/certs/  
unzip /etc/elasticsearch/certs/ certificate.zip  
  
chown -R elasticsearch:elasticsearch /etc/elasticsearch  
chmod -R 775 /etc/elasticsearch

Give permission and ownership with elasticsearch user and 775 permission

open vim /etc/elasticsearch/elasticsearch.yml

and configure certificates path below  
  
xpack.security.http.ssl:

enabled: true

key: /etc/elasticsearch/certs/elastic/elastic.key

certificate: /etc/elasticsearch/certs/elastic/elastic.crt

certificate\_authorities: ["/etc/elasticsearch/certs/ca/ca.crt"]  
  
  
xpack.security.transport.ssl:

enabled: true  
 verification\_mode: certificate

key: /etc/elasticsearch/certs/elastic/elastic.key

certificate: /etc/elasticsearch/certs/elastic/elastic.crt

certificate\_authorities: ["/etc/elasticsearch/certs/ca/ca.crt"]

**Restart elastic search Before starting elastic search make sure you are giving correct permission**  
  
chown -R elasticsearch:elasticsearch /etc/default/elasticsearch

chown -R elasticsearch:elasticsearch /var/lib/elasticsearch

chown -R elasticsearch:elasticsearch /var/log/elasticsearch

chown -R elasticsearch:elasticsearch /etc/elasticsearch

chown -R elasticsearch:elasticsearch /etc/sysconfig/elasticsearch

chmod -R 775 /etc/default/elasticsearch

chmod -R 775 /var/lib/elasticsearch

chmod -R 775 /var/log/elasticsearch

chmod -R 775 /etc/elasticsearch

chmod -R 775 /etc/sysconfig/elasticsearch

Try to access elastic search make sure to do host entry

Make sure to add all the certificates to all the nodes similler as node 1

**Step 6: Start and Enable Elasticsearch**

Start the Elasticsearch service:

sudo systemctl start elasticsearch

Enable it to start on boot:

sudo systemctl enable elasticsearch

Check if it’s running:

sudo systemctl status elasticsearch

**Step 7: Test Elasticsearch**

Run the following command:

curl -X GET <https://localhost:9200> -k

You should see a response with Elasticsearch details.

vim /etc/hosts

localhost sys.fcc  
127.0.0.1 sys.fcc

in your pc also do host entry

localhost sys.fcc  
127.0.0.1 sys.fcc

C:\Windows\System32\drivers\etc\hosts