Generating SSL Certificate to Elastic Search using Ubuntu:

Pre-requirement:

To authorize the Elasticsearch:

- Cd /usr/share/elasticsearch
- bin/elasticsearch -setup-passwords interactive (for manual passwords creation.

  Or

- Bin/elasticsearch -setup-passwords auto

Step1:

Install Openssl

sudo su

apt-get install openssl

Step2:

- pre-requirement:
- cd /etc/elasticsearch
- mkdir certs

Step3:

- To generate a Private Key and Certificate enter the below command:

One line code:

- [sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/elasticsearch/certs/elasticsearch.key -out /etc/elasticsearch/certs/elasticsearch.crt]

Step4:

Set the Correct Permissions:

- sudo chown -R elasticsearch:elasticsearch /etc/elasticsearch/certs
- sudo chmod 0400 /etc/elasticsearch/certs/elasticsearch.key
- sudo chmod 0444 /etc/elasticsearch/certs/elasticsearch.crt

Step5:

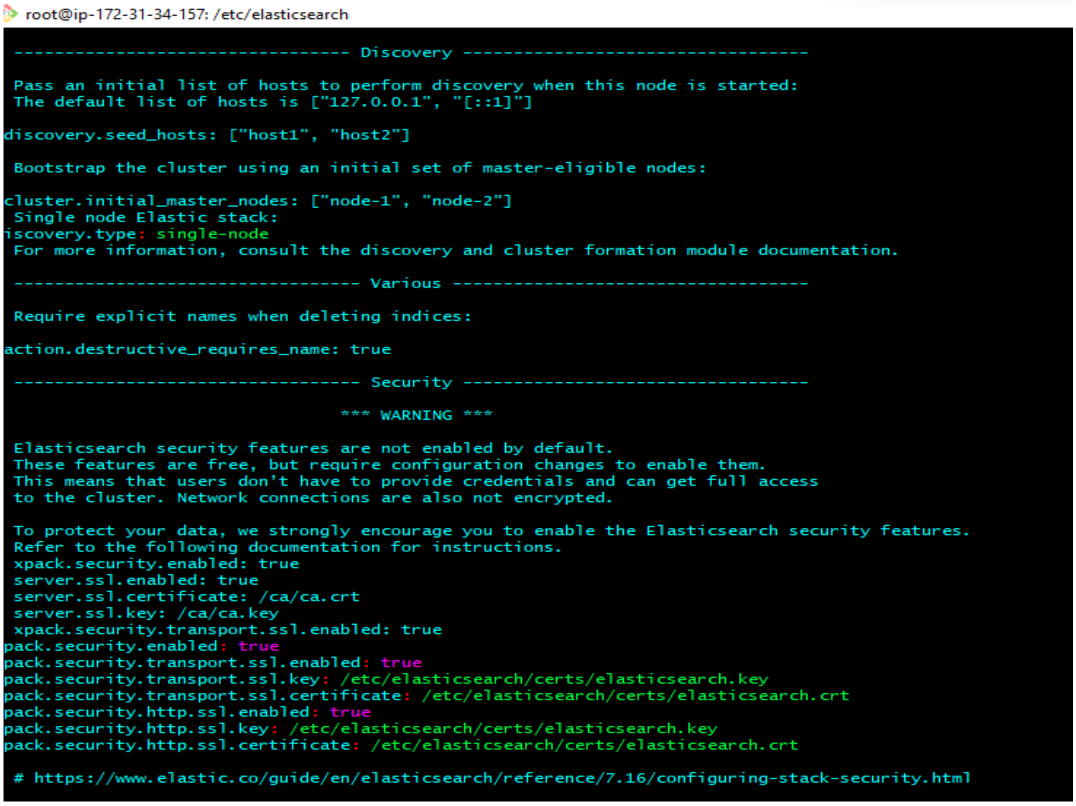
Configure Elasticsearch to Use the Certificate:

Go to:

- cd /etc/elasticsearch
- vim elasticsearch.yml

Paste below:

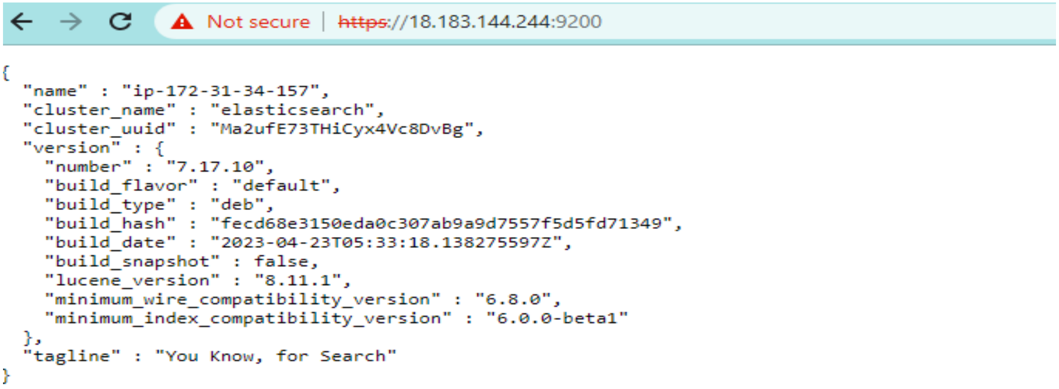
```
xpack.security.enabled: true
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
xpack.security.transport.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
    xpack.security.http.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
```



```
 ---------------------------------- Discovery ----------------------------------

 Pass an initial list of hosts to perform discovery when this node is started:
 The default list of hosts is ["127.0.0.1", "[::1]"]

discovery.seed_hosts: ["host1", "host2"]

 Bootstrap the cluster using an initial set of master-eligible nodes:

cluster.initial_master_nodes: ["node-1", "node-2"]
 Single node Elastic stack:
iscovery.type: single-node
 For more information, consult the discovery and cluster formation module documentation.

 ---------------------------------- Various -----------------------------------

 Require explicit names when deleting indices:

action.destructive_requires_name: true

 ---------------------------------- Security ----------------------------------

                                 *** WARNING ***

 Elasticsearch security features are not enabled by default.
 These features are free, but require configuration changes to enable them.
 This means that users don't have to provide credentials and can get full access
 to the cluster. Network connections are also not encrypted.

 To protect your data, we strongly encourage you to enable the Elasticsearch security features.
 Refer to the following documentation for instructions.
 xpack.security.enabled: true
 server.ssl.enabled: true
 server.ssl.certificate: /ca/ca.crt
 server.ssl.key: /ca/ca.key
 xpack.security.transport.ssl.enabled: true
pack.security.enabled: true
pack.security.transport.ssl.enabled: true
pack.security.transport.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
pack.security.transport.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
pack.security.http.ssl.enabled: true
pack.security.http.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
pack.security.http.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt

 # https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html
```

Step6:

```
sudo systemctl restart elasticsearch

sudo systemctl status elasticsearch
```



```
{
  "name" : "ip-172-31-34-157",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "Ma2ufE73THiCyx4Vc8DvBg",
  "version" : {
    "number" : "7.17.10",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "fecd68e3150eda0c307ab9a9d7557f5d5fd71349",
    "build_date" : "2023-04-23T05:33:18.138275597Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```