Assignment

Note 1: I am using **AWS Free tier Account** and Created **ansible IAM** user and assigning EC2 full access permission with console and programmatic access so that he could communicate with AWS environment using Access Key and Secret Key.

Note 2: I am using **Terraform** in my localhost with OS (CentOS 7.6).

Note 3: 1) Terraform should be installed and initialized in the system.
2) This three files should be present into present working directory.

So I have written three files mentioned below which will execute using below mentioned command.

1) ec2-launch.tf
2) variables.tf
3) els.sh

 # terraform apply

It will execute these three files and setup all the things (It takes time to complete).

Ending Output:

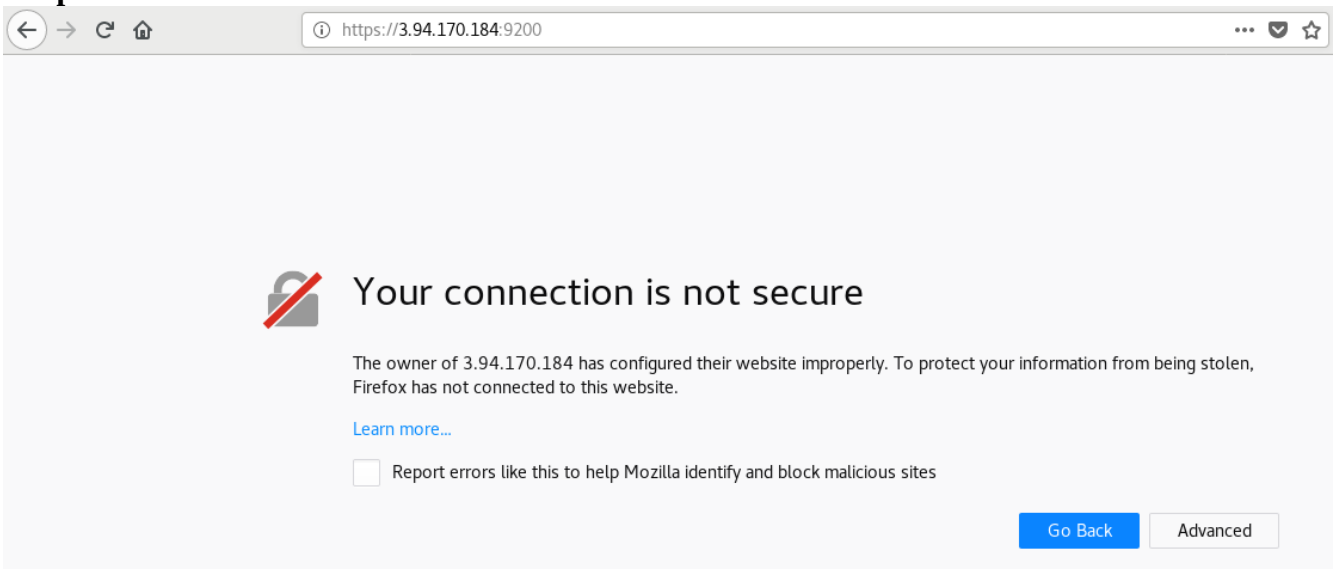
```
aws_instance.elasticsearch_instance: Creation complete after 4m23s [id=i-0d5d7f51c9132204e]

Apply complete! Resources: 5 added, 0 changed, 0 destroyed.

Outputs:

public_ip = 3.94.170.184
```

Step 1: Open the browser and type below **url** with **Public IP** and **Elasticsearch Port**.

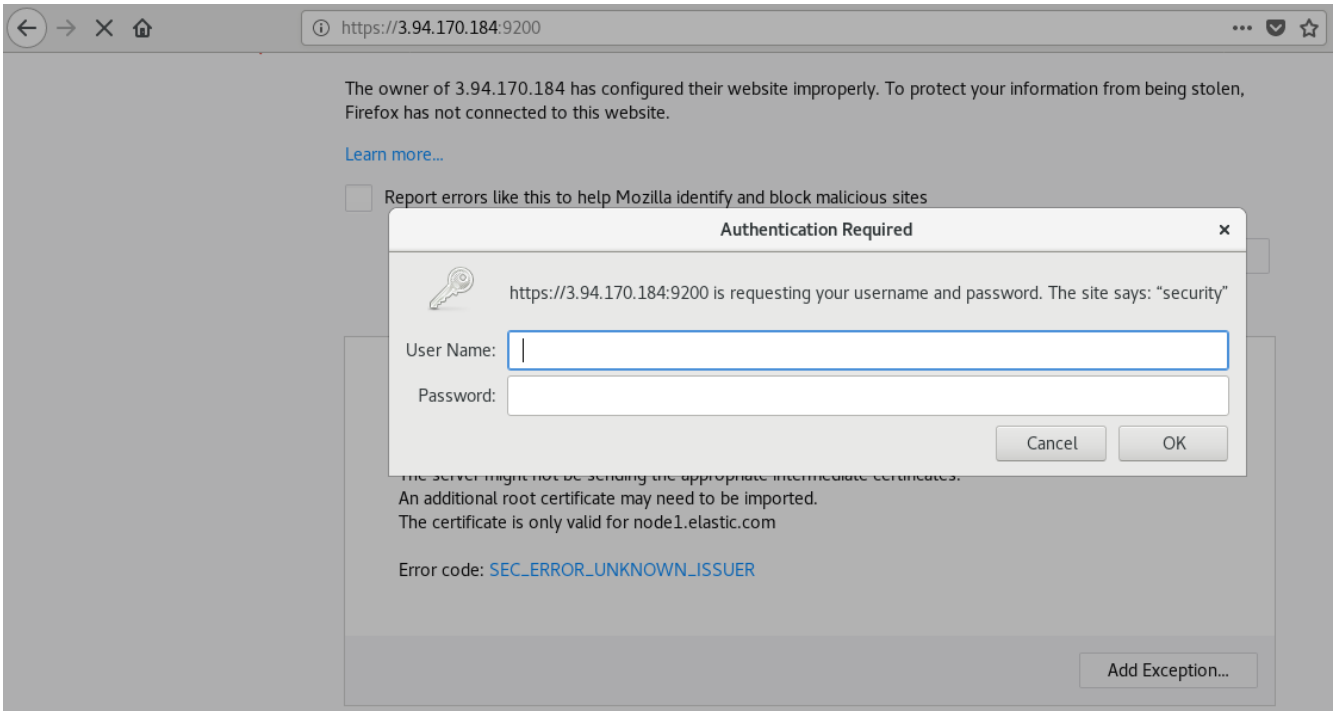
Elasticsearch Port : 9200
URL : https://<Public IP of instance>:Port

Example: https://3.94.170.184:9200

Output:



Click on **Advanced > Add Exceptions > Confirm Security Exception, (It will ask for username and password).**



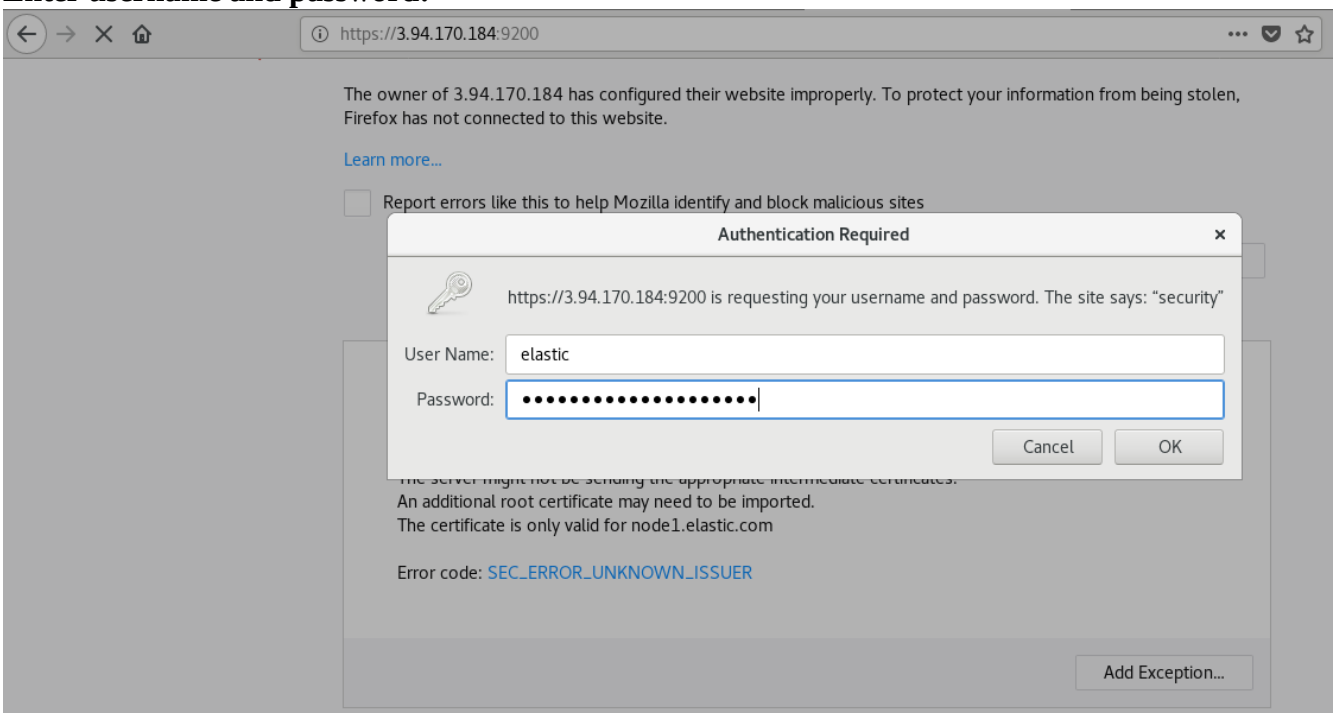
Now login into the instance and copy the password of elastic user from file (/tmp/password.txt).

```
[root@ansible-master final-assignment]# ssh -i ssh-key-private.pem ec2-user@3.94.170.184
The authenticity of host '3.94.170.184 (3.94.170.184)' can't be established.
ECDSA key fingerprint is SHA256:5N4QgqU4YVV1IvLGtqs/GrVKKjtENNPJV+iE8KWRZnI.
ECDSA key fingerprint is MD5:ab:f6:da:c0:cf:63:a0:1e:c2:3b:04:eb:de:8c:8d:d8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '3.94.170.184' (ECDSA) to the list of known hosts.
This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Fri May 29 16:07:35 2020 from 49.35.91.1
[ec2-user@node1 ~]$ sudo -i
[root@node1 ~]#
```

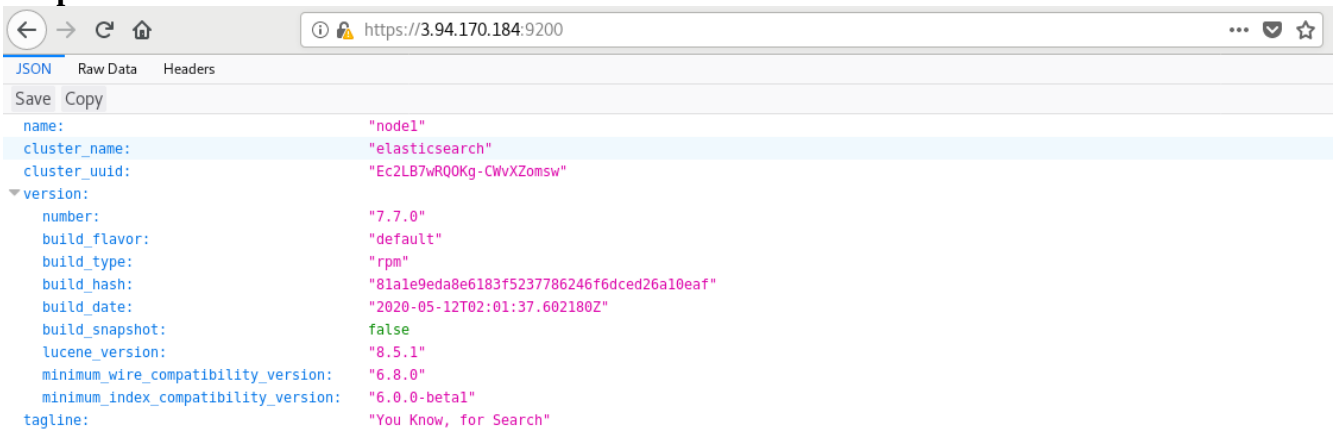
Copy password from file:

```
[root@node1 ~]# cat  /tmp/password.txt
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,logstash_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.


Changed password for user apm_system
PASSWORD apm_system = hAjyjJKFlVGTtGUoACrU

Changed password for user kibana
PASSWORD kibana = dvCDYBNmRPxK6sVTzMdw

Changed password for user logstash_system
PASSWORD logstash_system = ZjnFE8Ht0Bmc16xZNkYX

Changed password for user beats_system
PASSWORD beats_system = YAWmUQJlG9yn67fsEiG2

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = BZlnTXjI6zL6aVkmhRl4

Changed password for user elastic
PASSWORD elastic = 1vFN07bwTLpXwRimHME8

[root@node1 ~]#
```

Enter username and password:



Output:



Now Perform Same thing with command line:

Run the below mentioned command to check communication is secured or not.

curl 'https://node1.elastic.com:9200/_cat/nodes?v'

Output:

```
[root@node1 ~]# curl 'https://node1.elastic.com:9200/_cat/nodes?v'
curl: (60) SSL certificate problem: unable to get local issuer certificate
More details here: https://curl.haxx.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

Now try with SSL/TLS Certificates, It will ask for credentials.
curl --cacert /home/ec2-user/tmp/cert_blog/certs/ca/ca.crt
'https://node1.elastic.com:9200/_cat/nodes?v'

Output:

```
[root@node1 ~]# curl --cacert /home/ec2-user/tmp/cert_blog/certs/ca/ca.crt 'https://node1.elastic.com:9200/_cat/nodes?v'
{"error":{"root_cause":[{"type":"security_exception","reason":"missing authentication credentials for REST request [/_cat/nodes?v]","header":{"WWW-Aut
henticate":["Bearer realm=\"security\"","ApiKey","Basic realm=\"security\" charset=\"UTF-8\""]}}],"type":"security_exception","reason":"missing authen
tication credentials for REST request [/_cat/nodes?v]","header":{"WWW-Authenticate":["Bearer realm=\"security\"","ApiKey","Basic realm=\"security\" ch
arset=\"UTF-8\""]}},"status":401}[root@node1 ~]#
```

Finally execute below command with credentials. It will prompt you to enter the password for elastic user. (Copy from file /tmp/password.txt).

curl --cacert /home/ec2-user/tmp/cert_blog/certs/ca/ca.crt -u elastic
'https://node1.elastic.com:9200/_cat/nodes?v'

Output:

```
[root@node1 ~]# curl --cacert /home/ec2-user/tmp/cert_blog/certs/ca/ca.crt -u elastic  'https://node1.elastic.com:9200/_cat/nodes?v'
Enter host password for user 'elastic':
ip           heap.percent ram.percent cpu load_1m load_5m load_15m node.role master name
172.31.91.51           46          92   5    0.00    0.34     0.38 dilmrt    *      node1
[root@node1 ~]#
```

Try With Wrong Credentials, It will give you error: authentication failed!!!

```
[root@node1 ~]# curl --cacert /home/ec2-user/tmp/cert_blog/certs/ca/ca.crt -u elastic  'https://node1.elastic.com:9200/_cat/nodes?v'
Enter host password for user 'elastic':
{"error":{"root_cause":[{"type":"security_exception","reason":"failed to authenticate user [elastic]","header":{"WWW-Authenticate":["Bearer realm=\"se
curity\"","ApiKey","Basic realm=\"security\" charset=\"UTF-8\""]}}],"type":"security_exception","reason":"failed to authenticate user [elastic]","head
er":{"WWW-Authenticate":["Bearer realm=\"security\"","ApiKey","Basic realm=\"security\" charset=\"UTF-8\""]}},"status":401}[root@node1 ~]#
[root@node1 ~]#
```