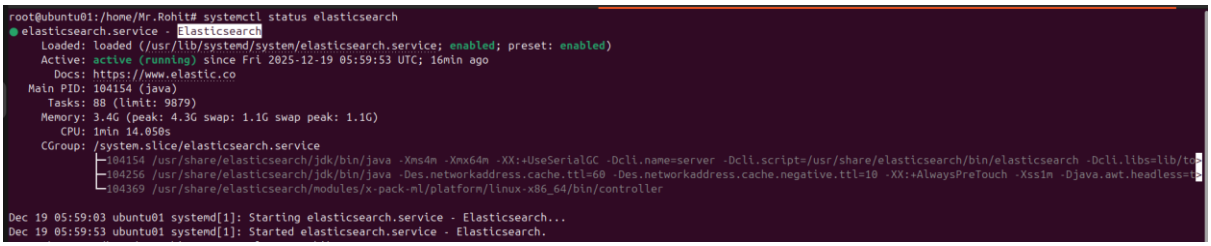
Environmental setup for Alert Management

- On Ubuntu VM
  - sudo apt update
  - sudo apt install -y apt-transport-https ca-certificates curl gnupg
  - curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
  - echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
  - sudo apt update
  - sudo apt install elasticsearch kibana filebeat -y

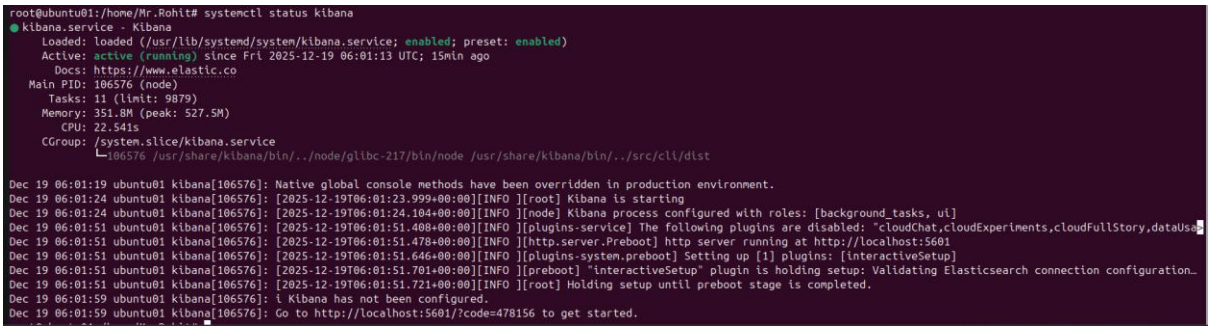
Install all the requirement

- Enable the elasticsearch, Kibana
  - sudo systemctl enable elasticsearch kibana filebeat
  - sudo systemctl start elasticsearch
    - Screenshots:

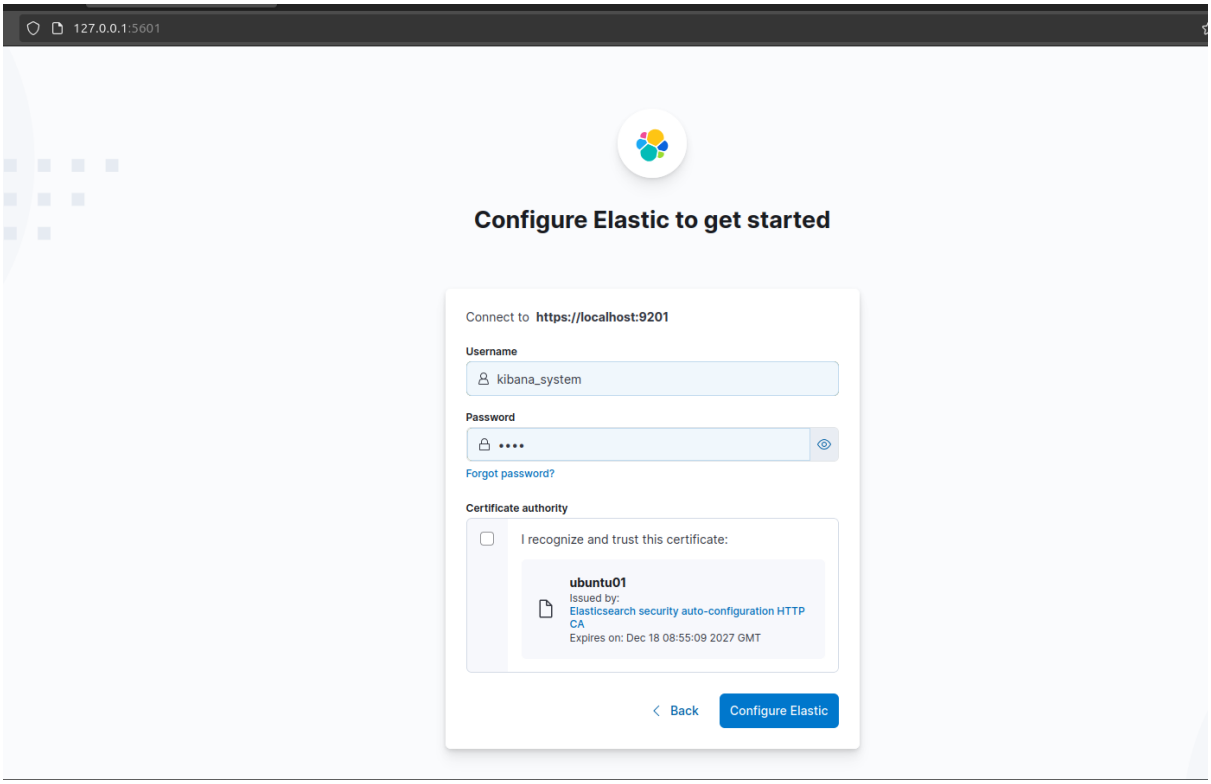
      Elasticsearch:



      Kibana:



      Access ELB:



I was unable to Download the sample date.
So I created the 3 log data:

```
root@ubuntu01:/home/Mr.Rohit/Desktop# curl -X PUT "localhost:5601/soc_logs"
{"statusCode":400,"error":"Bad Request","message":"Request must contain a kbn-xsrf header."}root@rootroot@uburootrootrrroroorootroot@ubroot@ubrootroororroroot@root@ubuntroorrrrrr
root@ubuntu01:/home/Mr.Rohit/Desktop#
```

Log Correlation:
Check for the status event.code: "4625"

```
root@ubuntu01:/home/Mr.Rohit/Desktop# cat soc_logs.json | grep "4625"
{"@timestamp":"2025-08-18T12:00:00Z","event":{"code":"4625","action":"logon-failed"},"source":{"ip":"192.168.1.100"},"destination":{"ip":"10.0.0.5"},"user":{"name":"admin"}}
{"@timestamp":"2025-08-18T12:00:10Z","event":{"code":"4625","action":"logon-failed"},"source":{"ip":"192.168.1.100"},"destination":{"ip":"10.0.0.5"},"user":{"name":"admin"}}
root@ubuntu01:/home/Mr.Rohit/Desktop#
```