



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:

```
root@ubuntu01:/home/Mr.Rohit# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
 Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
 Active: active (running) since Fri 2025-12-19 05:59:53 UTC; 16min ago
 Docs: https://www.elastic.co
Main PID: 104154 (java)
 Tasks: 88 (limit: 9879)
 Memory: 3.4G (peak: 4.3G swap: 1.1G swap peak: 1.1G)
 CPU: 1min 14.058s
 CGroup: /system.slice/elasticsearch.service
 ├─104154 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch -Dcli.libs=lib/...
 ├─104256 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true
 └─104369 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

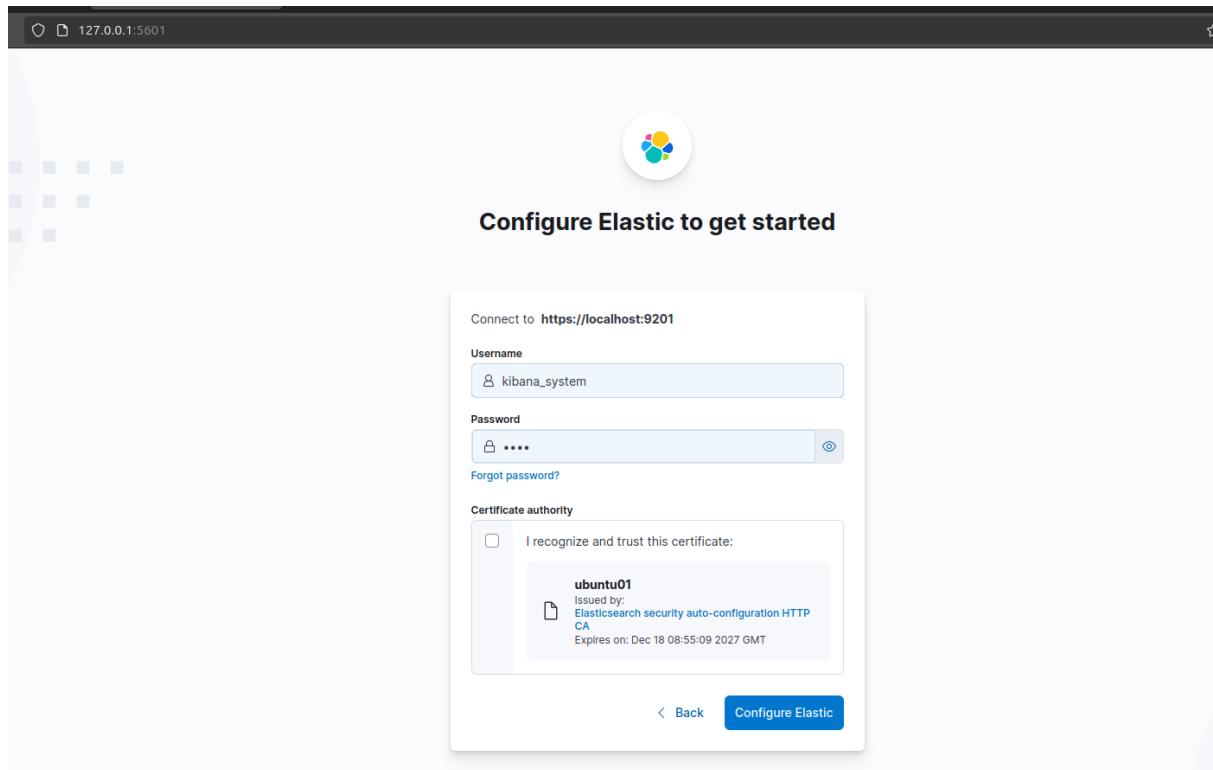
Dec 19 05:59:03 ubuntu01 systemd[1]: Starting elasticsearch.service...
Dec 19 05:59:53 ubuntu01 systemd[1]: Started elasticsearch service - Elasticsearch.
```

Kibana

```
root@ubuntu01:/home/Mr.Rohit# systemctl status kibana
● kibana.service - Kibana
 Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
 Active: active (running) since Fri 2025-12-19 06:01:13 UTC; 15min ago
 Docs: https://www.elastic.co
Main PID: 106576 (node)
 Tasks: 11 (limit: 9879)
 Memory: 351.8M (peak: 527.5M)
 CPU: 22.541s
 CGroup: /system.slice/kibana.service
 └─106576 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Dec 19 06:01:19 ubuntu01 kibana[106576]: Native global console methods have been overridden in production environment.
Dec 19 06:01:24 ubuntu01 kibana[106576]: [2025-12-19T06:01:23.999+00:00][INFO][root] Kibana is starting
Dec 19 06:01:24 ubuntu01 kibana[106576]: [2025-12-19T06:01:24.104+00:00][INFO][node] Kibana process configured with roles: [background_tasks, ui]
Dec 19 06:01:51 ubuntu01 kibana[106576]: [2025-12-19T06:01:51.408+00:00][INFO][plugins-service] The following plugins are disabled: ["cloudChat,cloudExperiments,cloudFullStory,dataUser"]
Dec 19 06:01:51 ubuntu01 kibana[106576]: [2025-12-19T06:01:51.478+00:00][INFO][http-server.Preboot] http server running at http://localhost:5601
Dec 19 06:01:51 ubuntu01 kibana[106576]: [2025-12-19T06:01:51.646+00:00][INFO][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
Dec 19 06:01:51 ubuntu01 kibana[106576]: [2025-12-19T06:01:51.701+00:00][INFO][preboot] "interactiveSetup" plugin is holding setup: Validating Elasticsearch connection configuration...
Dec 19 06:01:51 ubuntu01 kibana[106576]: [2025-12-19T06:01:51.721+00:00][INFO][root] Holding setup until preboot stage is completed.
Dec 19 06:01:59 ubuntu01 kibana[106576]: l Kibana has not been configured.
Dec 19 06:01:59 ubuntu01 kibana[106576]: Go to http://localhost:5601/?code=478156 to get started.
```

Access FLB



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/_source/soc_logs"
{"statusCode":400,"error":"Bad Request","message":"Request must contain a kbn-xsrf header."}root@rootroot@ubrootrootrrroorooot@ubroot@ubrootroorroroot@root@ubuntrorrrrrr
root@ubuntu01:/home/Mr.Rohit/Desktop#
```

### Log Correlation:

Check for the status event.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#
```