

A)

```
#####installation and configuration of elasticsearch#####
```

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

```
sudo apt-get install apt-transport-https
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt-get update && sudo apt-get install elasticsearch
```

```
nano //etc//elasticsearch//elasticsearch.yml
```

```
http.port: 9200
```

```
discovery.type: single-node
```

```
network.host: 0.0.0.0
```

```
xpack.security.enabled: true
```

```
xpack.security.authc.api_key.enabled: true
```

```
#####installation and configuration of kibana#####
```

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

```
sudo apt-get install apt-transport-https
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt-get update && sudo apt-get install kibana
```

```
nano /etc/kibana/kibana.yml
```

```
server.port: 5601
```

```
server.host: "0.0.0.0"
```

```
xpack.encryptedSavedObjects.encryptionKey:
```

```
"asfgshdsfhkjfhfjkfhghgnbndaahdgjahjhjaakjkjadjdhhjgdhfhghdhdhfajhagh|"
```

```
##### configuration of username and password####
```

```
cd //usr//share//elasticsearch
```

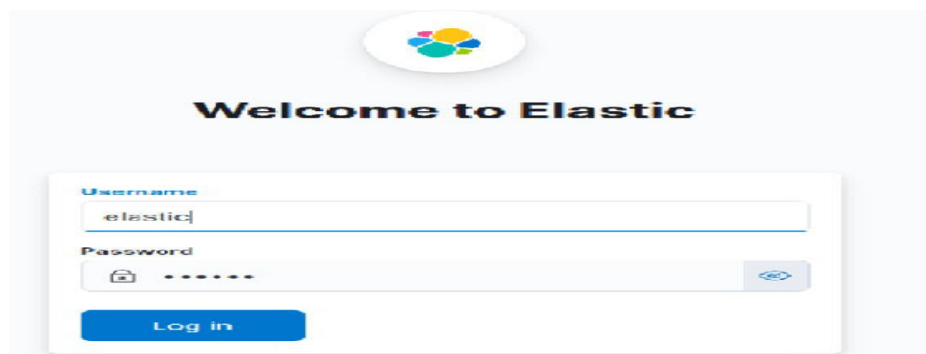
```
./bin/elasticsearch-setup-passwords interactive
```

```
sudo systemctl restart kibana
```

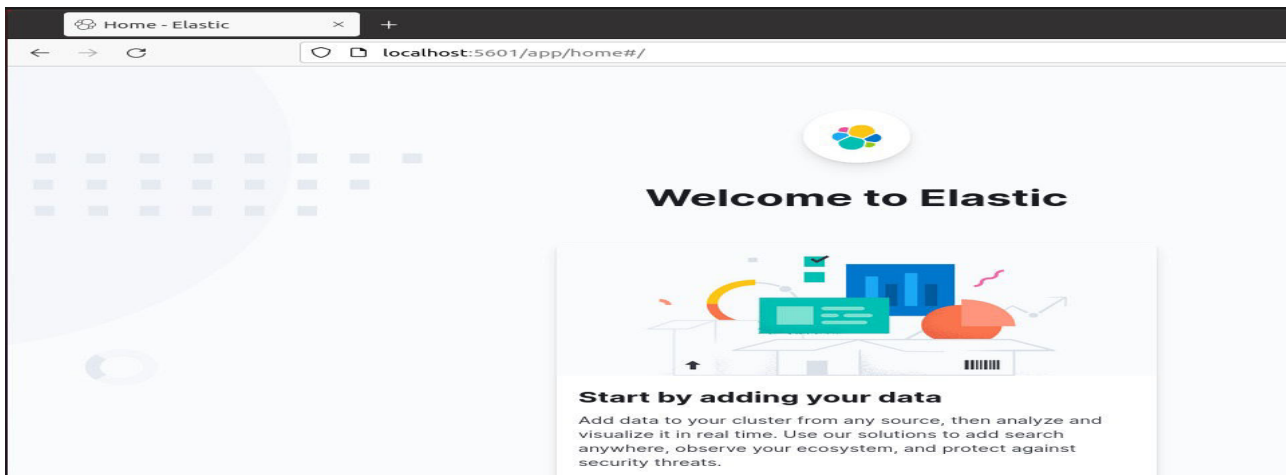
```
sudo systemctl restart elasticsearch
```

```
saroj@ubuntu-serv2: ~  
saroj@ubuntu-serv2:~$ systemctl status kibana  
● kibana.service - Kibana  
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)  
   Active: active (running) since Tue 2021-11-30 10:56:51 PST; 17min ago  
     Docs: https://www.elastic.co  
    Main PID: 961 (node)  
      Tasks: 11 (limit: 2260)  
     Memory: 305.8M  
    CGroup: /system.slice/kibana.service  
            └─961 /usr/share/kibana/bin/../../node/bin/node /usr/share/kibana/bin/kibana  
Nov 30 10:56:51 ubuntu-serv2 systemd[1]: Started Kibana.  
lines 1-11/11 (END)
```

```
saroj@ubuntu-serv2: ~  
saroj@ubuntu-serv2:~$ systemctl status elasticsearch  
● elasticsearch.service - Elasticsearch  
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)  
   Active: active (running) since Tue 2021-11-30 11:03:42 PST; 10min ago  
     Docs: https://www.elastic.co  
    Main PID: 2414 (java)  
      Tasks: 80 (limit: 2260)  
     Memory: 883.6M  
    CGroup: /system.slice/elasticsearch.service  
            └─2414 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net.svc.name=elasticsearch  
              2603 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/elasticsearch-plugin install --silent  
Nov 30 11:03:13 ubuntu-serv2 systemd[1]: Starting Elasticsearch...  
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: A terminally deprecated method java.io.File#mkdirs() called from  
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecurityProperty() is deprecated. Please consider  
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: Please consider switching to the newer SecurityManager.  
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecurityProperty() is deprecated. Please consider  
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecurityProperty() is deprecated. Please consider  
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: A terminally deprecated method java.io.File#mkdirs() called from  
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecurityProperty() is deprecated. Please consider  
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: Please consider switching to the newer SecurityManager.  
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecurityProperty() is deprecated. Please consider  
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecurityProperty() is deprecated. Please consider  
Nov 30 11:03:42 ubuntu-serv2 systemd[1]: Started Elasticsearch.  
lines 1-21/21 (END)
```



```
172.16.59.131:9200  
JSON Raw Data Headers  
Save Copy Collapse All Expand All Filter JSON  
{  
  "name": "ubuntu-serv2",  
  "cluster_name": "elasticsearch",  
  "cluster_uuid": "VbmV3tjnSCi5SzFEm2AP6Q",  
  "version": {  
    "number": "7.15.2",  
    "build_flavor": "default",  
    "build_type": "deb",  
    "build_hash": "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",  
    "build_date": "2021-11-04T14:04:42.515624022Z",  
    "build_snapshot": false,  
    "lucene_version": "8.9.0",  
    "minimum_wire_compatibility_version": "6.8.0",  
    "minimum_index_compatibility_version": "6.0.0-beta1",  
    "tagline": "You Know, for Search"  
  }  
}
```



#####allow ports of kibana and elastic search#####

```
ufw allow 9200/tcp
```

```
ufw allow 5601/tcp
```

```
ufw reload
```

#####installation and configuration of metricbeat of elk server and second server#####

in elk server

```
sudo ufw allow from 172.16.59.130/24 to any port 9200
```

###from second server test the port

```
telnet 192.16.59.131 9200
```

connected

quit

#####for templete#####

```
sudo apt install metricbeat
```

```
sudo nano /etc/metricbeat/metricbeat.yml
```

```
output.elasticsearch:
```

```
  hosts: ["localhost:9200"]
```

```
  username: "elastic"
```

```
  password: "123456"
```

```
systemctl restart metricbeat
```

```
sudo metricbeat setup --index-management -E output.logstash.enabled=false -E  
'output.elasticsearch.hosts=["localhost:9200"]'
```

#####installation of metricbeat in second server#####

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add  
-
```

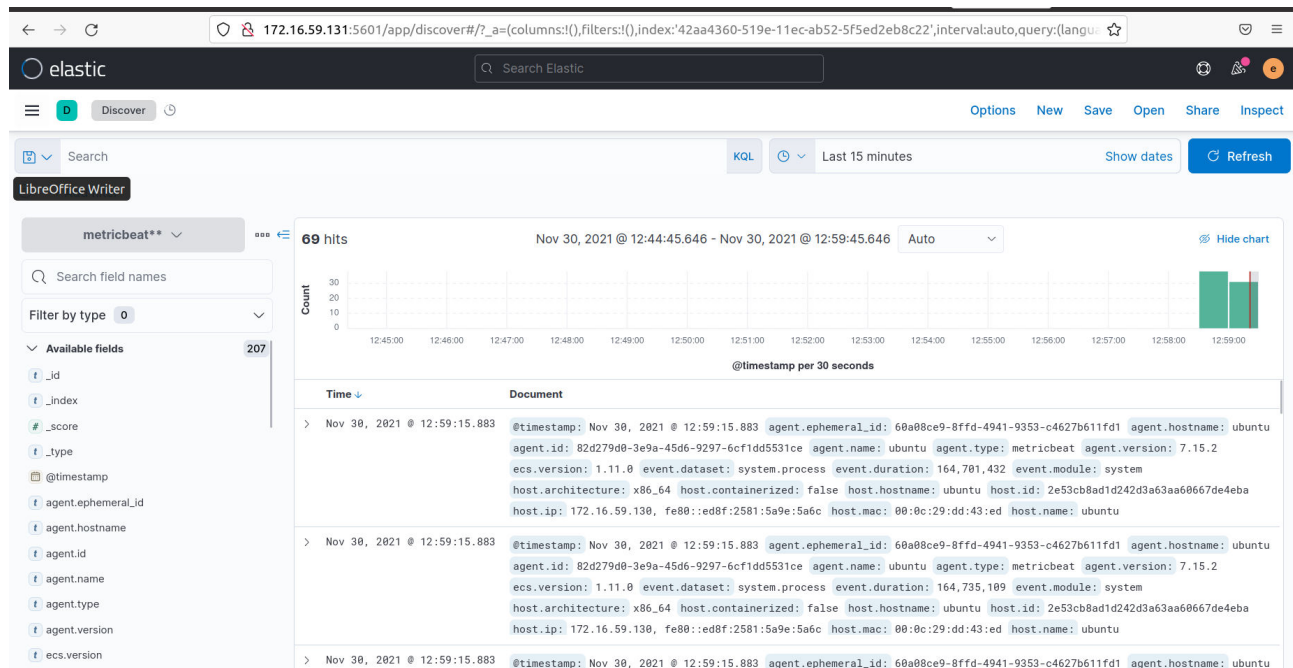
```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee  
-a /etc/apt/sources.list.d/elastic-7.x.list
```

```

sudo apt update
sudo apt install metricbeat
sudo nano /etc/metricbeat/metricbeat.yml
output.elasticsearch:
  hosts: ["172.16.59.131:9200"]
  username: "elastic"
  password: "123456"

```

```
systemctl restart metricbeat
```

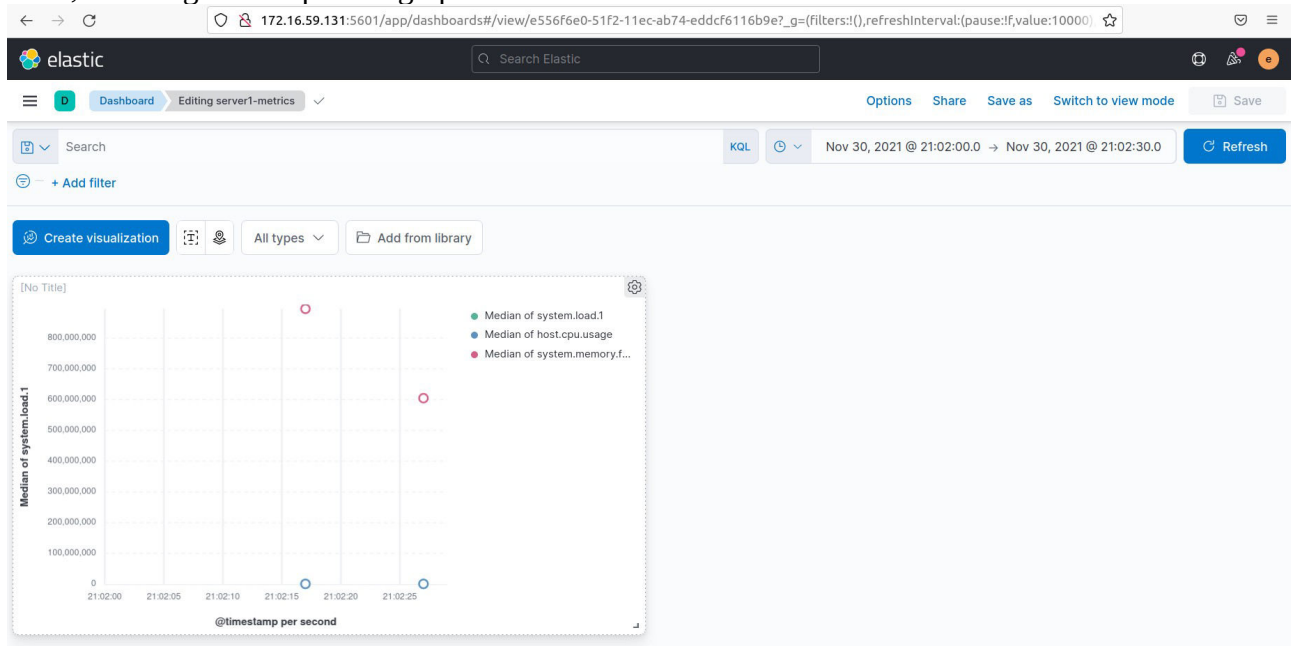


#####

1)

#####created dashboard#####

load ,disk usages and cpu line graph dashboard



2)

#####creating the rule #####

#cpu rule

#Disk Usages

### About

you have very few memory

**Severity** ● High

**Risk score** 73

### Definition

**Index patterns**

**Custom query** system.memory.used.pct > 0.8

**Rule type** Query

**Timeline template** None

### Schedule

**Runs every** 2m

**Additional look-back time** 1m

### Investigate

Timelines

Cases

**Manage**

Endpoints

Trusted applications

Event filters

the cpu usages

**Severity** ● Low

**Risk score** 21

**Index patterns**

**Custom query** host.cpu.usage > 70%

**Rule type** Query

**Timeline template** None

## #System Load

### About

load metrics is high

**Severity** ● High

**Risk score** 73

### Definition

**Index patterns**

**Custom query**

**Rule type** Query

**Timeline template** None

### Schedule

**Runs every** 2m

**Additional look-** 1m

## #list of rules

elastic

Search Elastic

Security Rules

ML job settings Add data

### Rules

Load Elastic prebuilt rules

Upload value lists

Import rules

Create new rule

Security

Overview

Detect

Alerts

Rules

Exceptions

Explore

Hosts

Network

Investigate

Timelines

Cases

Manage

Endpoints

Trusted applications

Event filters

Rules

Rule Monitoring

All rules

Updated 20 seconds ago

Tags 0

Elastic rules (0) Custom rules (3)

Showing 3 rules

Selected 0 rules

Bulk actions

Refresh

Refresh settings

<input type="checkbox"/>	Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
<input type="checkbox"/>	load-metrics	73	High	1 minute ago	succeeded	Nov 30, 2021 @ 22:26:03.853	2	—	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Alert CPU	21	Low	1 minute ago	succeeded	Nov 30, 2021 @ 22:18:41.726	4	—	<input checked="" type="checkbox"/>
<input type="checkbox"/>	memory alert	73	High	21 seconds ago	succeeded	Nov 30, 2021 @ 22:55:46.386	7	—	<input checked="" type="checkbox"/>

Rows per page: 20

< 1 >

2)

#####after activating the rules .....Alert in slack of load and  
cpu#####

> taking free trail for alerting

>creating a channel and webhook url

### Integration Settings

#### Post to Channel

Messages that are sent to the incoming webhook will be posted here.

# alert

or create a new channel

#### Webhook URL

Send your JSON payloads to this URL.  
[Show setup instructions](#)

https://hooks.slack.com/services/T02K9NY18JC/B02P19NDV6X/9gXwvEDJZLb

Copy URL • Regenerate

#### Descriptive Label

Use this label to provide extra context in your list of integrations (optional).

Optional description of this integration

Alert on slack load and cpu

← → ↺

https://app.slack.com/client/T02K9NY18JC/C02P3FR54H2/thread/C02JL4HK926-1634826293.000200

🔍 Search DevOps Internship

DevOps Internship

# alert

+ Add a bookmark

This is the very beginning of the #alert channel

Saroj Shah 10:00 PM

set the channel description: resources alert

Yesterday

Saroj Shah 10:05 PM

added an integration to this channel: cpu alert

✓ 🗨 🧑🏻 🧑🏻 🧑🏻 🗨 🗨 🗨 🗨

cpu alert APP 11:15 PM

Rule load-metrics generated 7 alerts

cpu alert APP 11:28 PM

alert of cpu

Saroj Shah 11:29 PM

added an integration to this channel: incoming-webhook

Today

incoming-webhook APP 10:09 AM

Rule load-metrics generated 12 alerts

Rule load-metrics generated 5 alerts

high disk usages Alert

Rule load-metrics generated 8 alerts

high disk usages Alert

Rule load-metrics generated 10 alerts

New

###Alert of disk usages