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

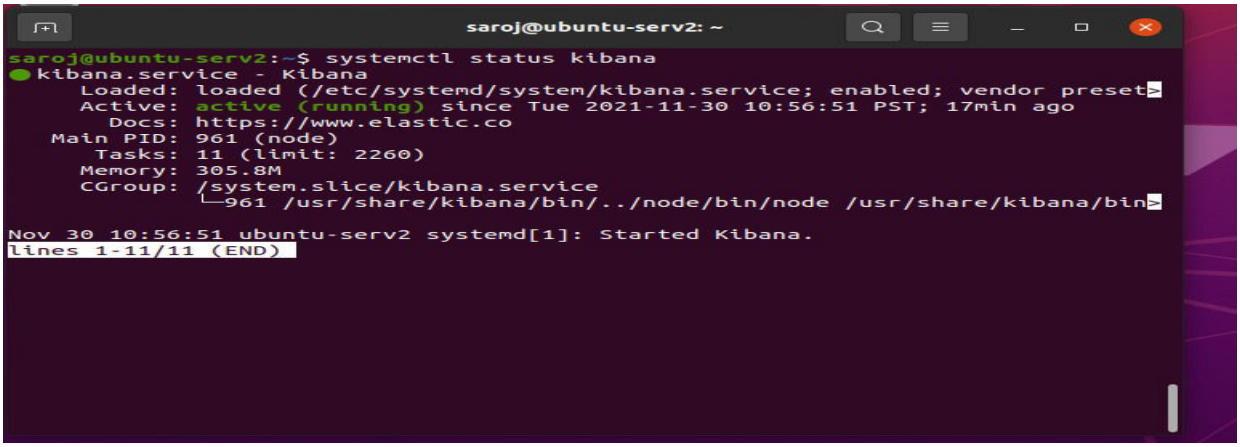
sudo apt-get update && sudo apt-get install kibana

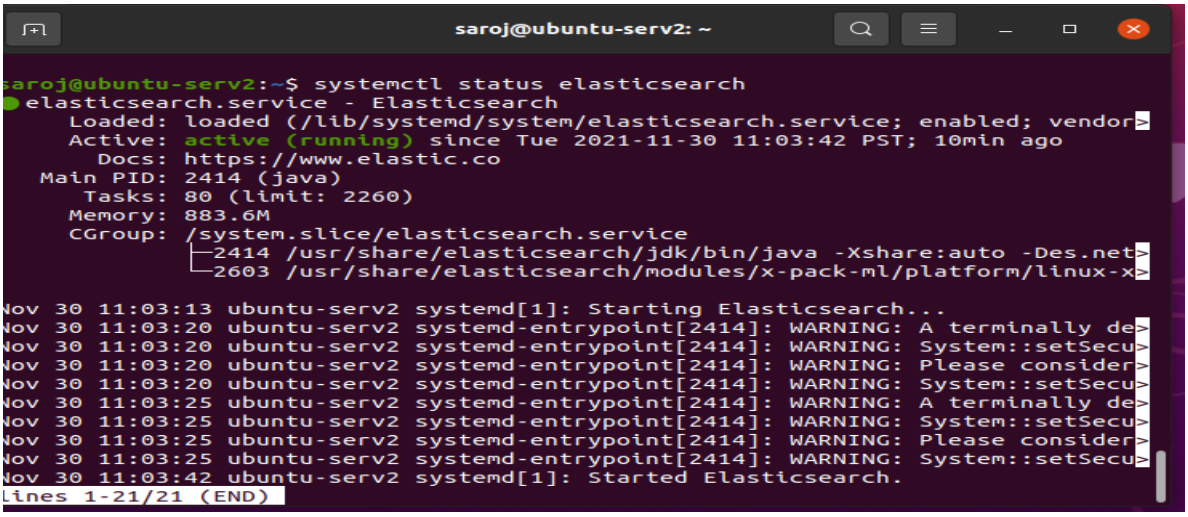
nano /etc/kibana/kibana.yml
server.port: 5601
server.host: "0.0.0.0"
xpack.encryptedSavedObjects.encryptionKey:
"asfgshdsfhkjhfjkhfkghgnbndaahdgjahjhjaakjkjadjdhhjgdhfghdhdfjajhagh|”

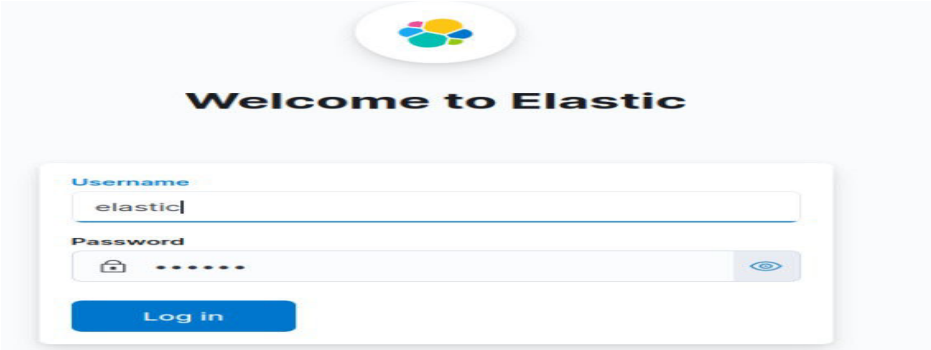
######## configuration of username and password####

cd *//usr//share//elasticsearch*
./bin/elasticsearch-setup-passwords interactive

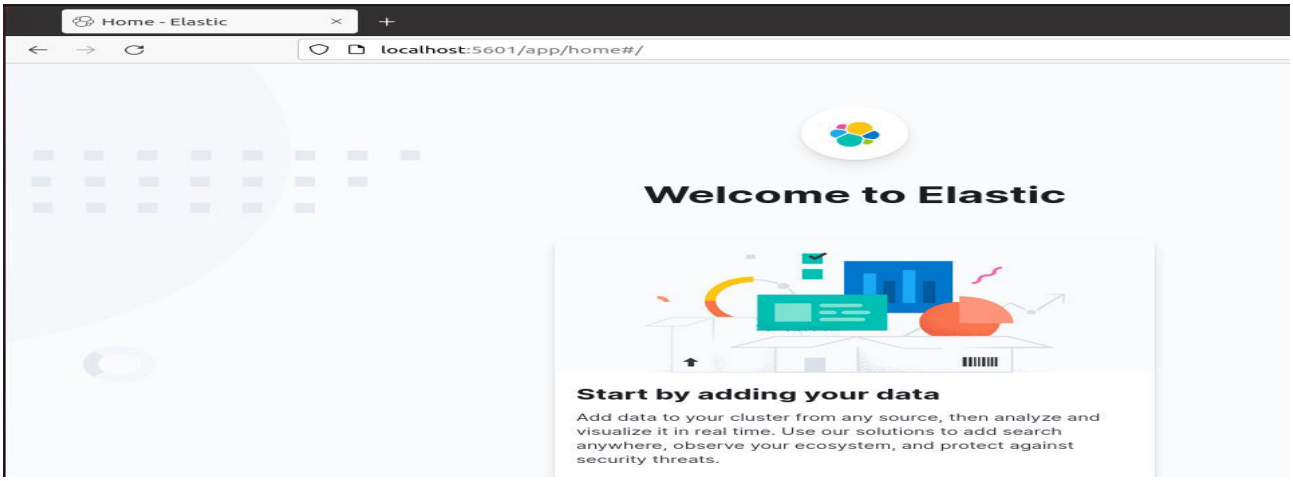
sudo systemctl restart kibana
sudo systemctl restart elasticsearch


saroj@ubuntu-serv2: ~
saroj@ubuntu-serv2:~$ systemctl status kibana
kibana.service - Kibana
Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset
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
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
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
└─2603 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x
Nov 30 11:03:13 ubuntu-serv2 systemd[1]: Starting Elasticsearch...
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: A terminally de
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecu
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: Please consider
Nov 30 11:03:20 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecu
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: A terminally de
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecu
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: Please consider
Nov 30 11:03:25 ubuntu-serv2 systemd-entrypoint[2414]: WARNING: System::setSecu
Nov 30 11:03:42 ubuntu-serv2 systemd[1]: Started Elasticsearch.
lines 1-21/21 (END)


Welcome to Elastic
Username
elastic
Password
Log in


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"

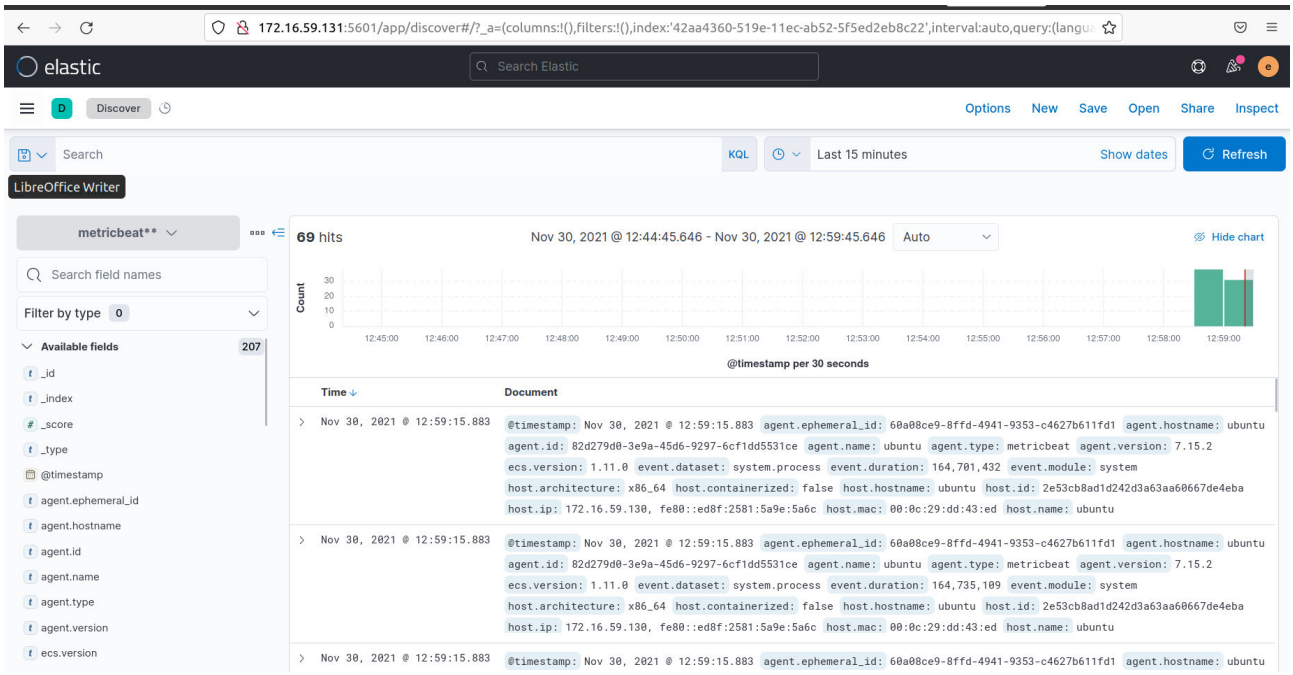


##########allow ports of kibana and elastic search##############
ufw allow 9200/tcp
ufw allow 5601/tcp
ufw reload

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

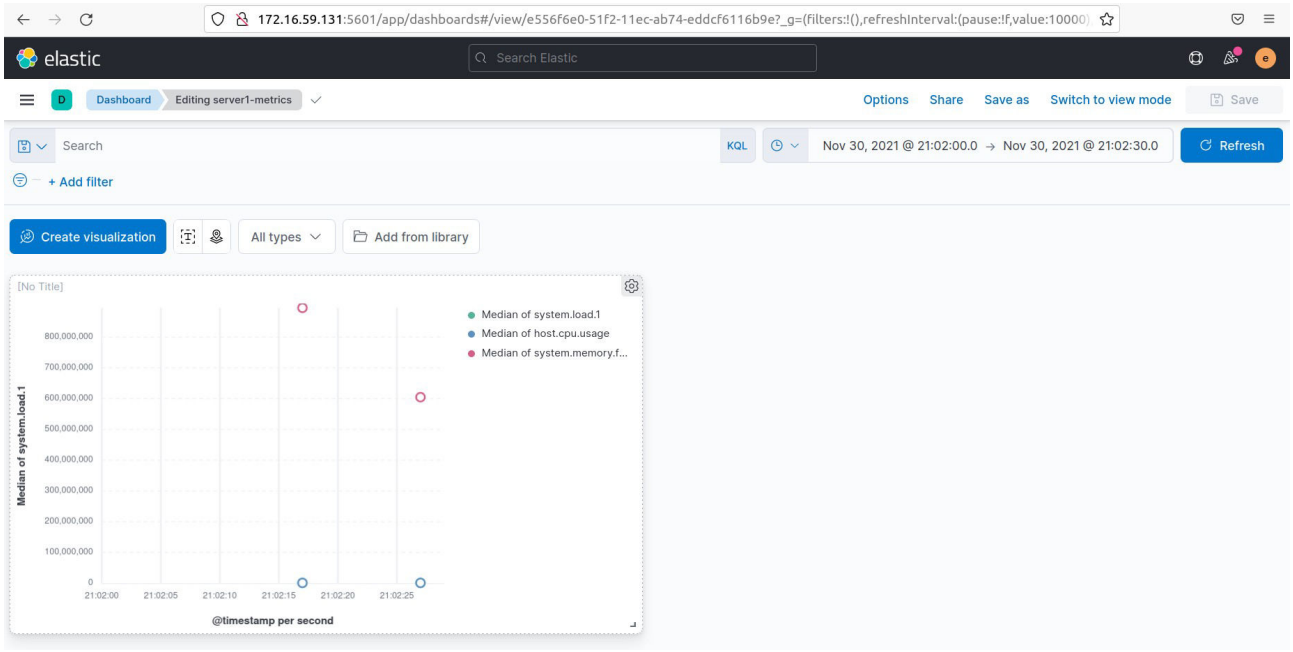
```
sudo ufw allow from 172.16.59.130/24 to any port 9200
###from second server test the port
telnet 192.16.59.131 9200
connected
quit
#################for templete######
sudo apt install metricbeat
sudo nano /etc/metricbeat/metricbeat.yml
output.elasticsearch:
  hosts: ["localhost:9200"]
  username: "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
```



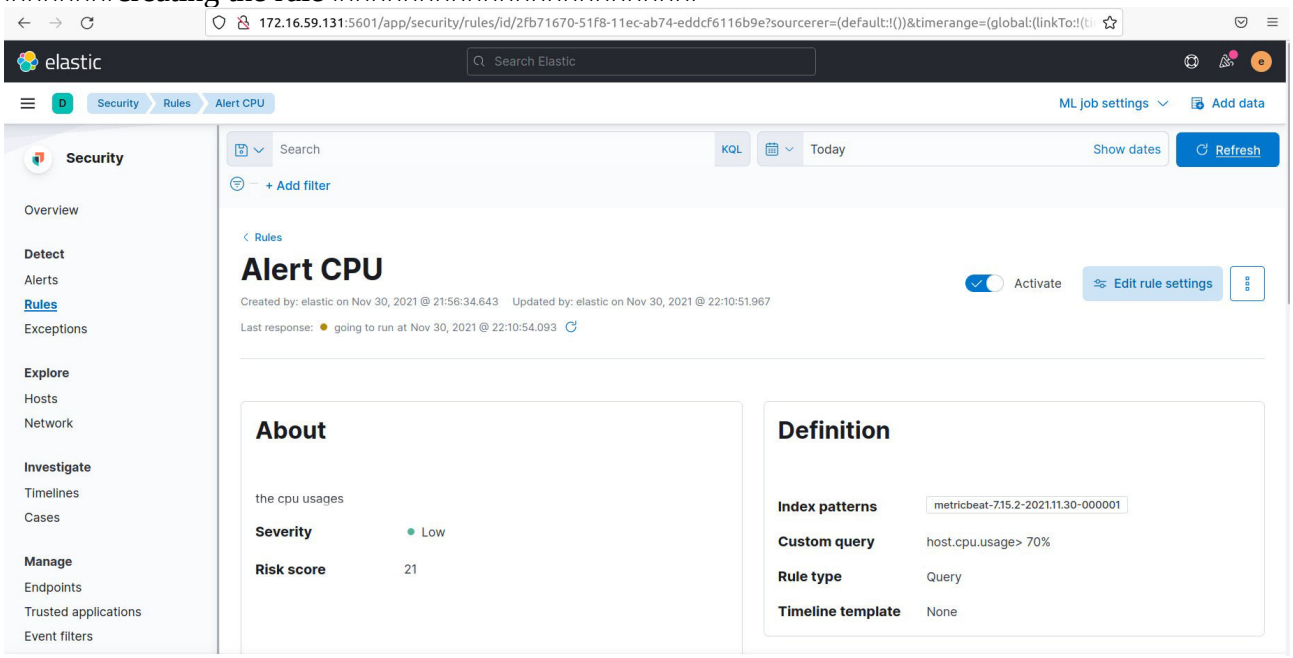
########

1)
##########created dashboard##########



2)

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



About

load metrics is high

Severity High

Risk score 73

Definition

Index patterns metricbeat-7.15.2-2021.11.30-000001

Custom query system.load.1 > 1

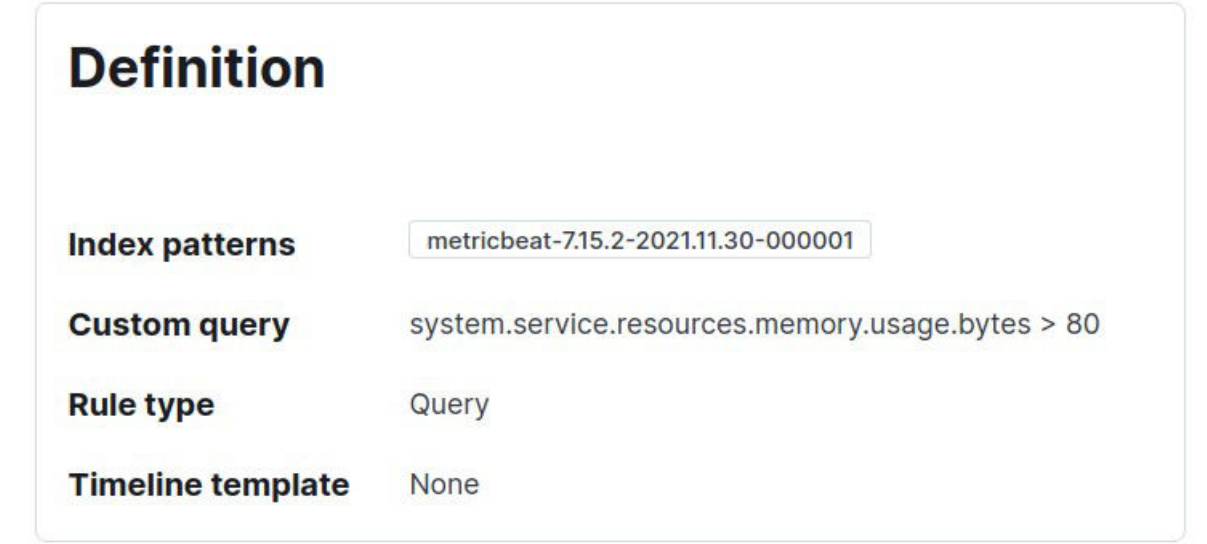
Rule type Query

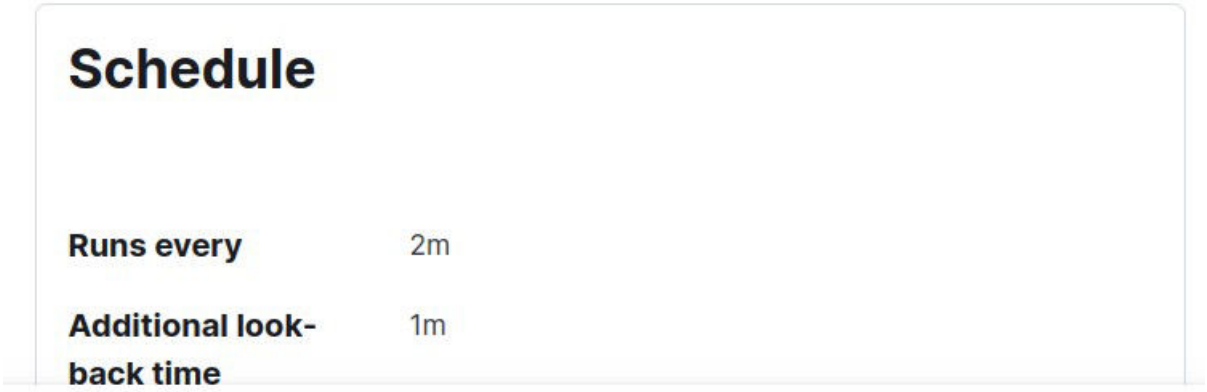
Timeline template None

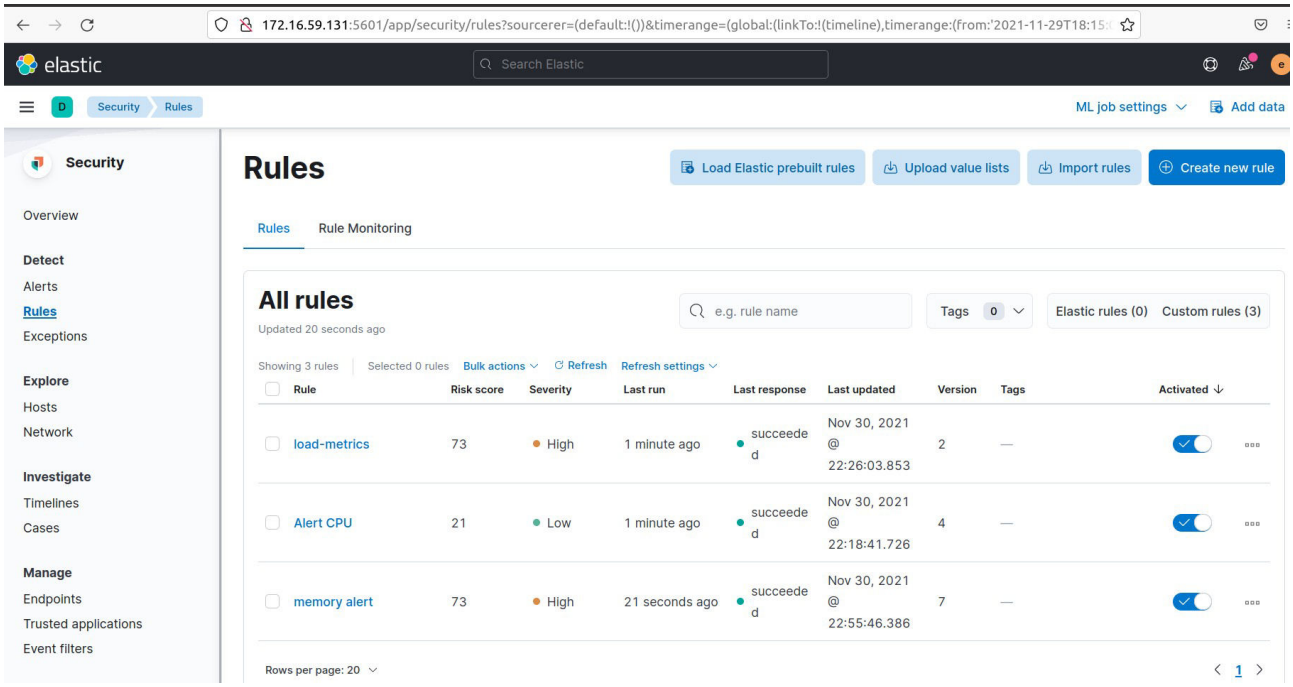
Schedule

Runs every 2m

Additional look- 1m





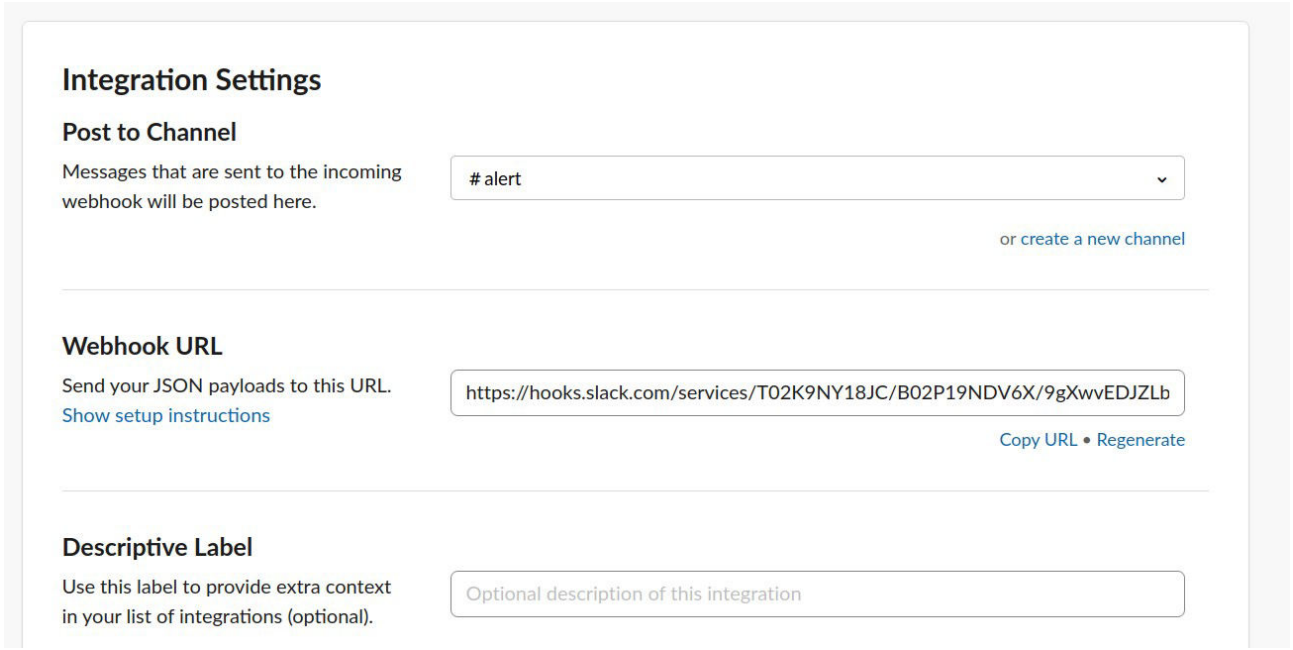


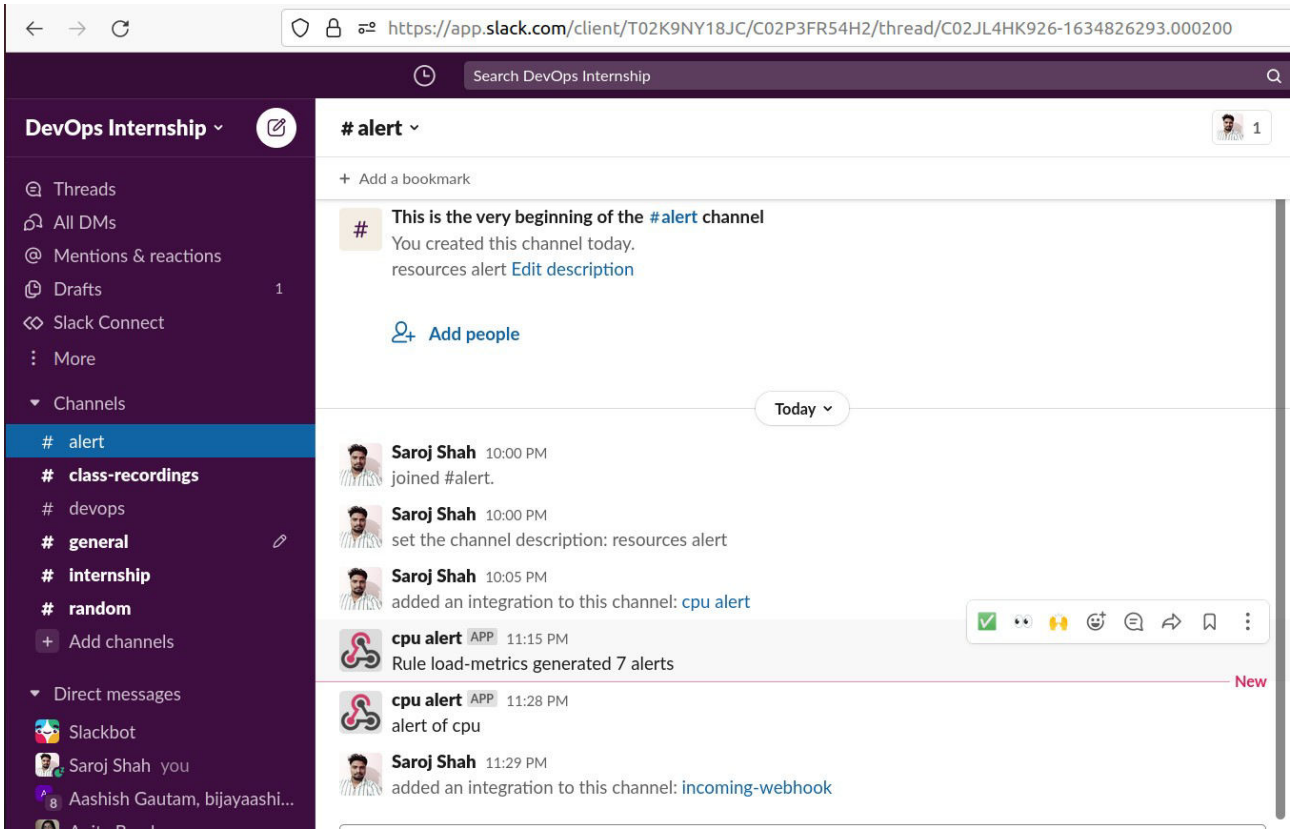
2)

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

> taking free trail for alerting

>creating a channel and webhook url




https://app.slack.com/client/T02K9NY18JC/C02P3FR54H2/thread/C02JL4HK926-1634826293.000200
Search DevOps Internship
DevOps Internship
alert
1
Threads
All DMs
Mentions & reactions
Drafts 1
Slack Connect
More
Channels
alert
class-recordings
devops
general
internship
random
Add channels
Direct messages
Slackbot
Saroj Shah you
Aashish Gautam, bijayaashi...
Add a bookmark
This is the very beginning of the #alert channel
You created this channel today.
resources alert Edit description
Add people
Today
Saroj Shah 10:00 PM
joined #alert.
Saroj Shah 10:00 PM
set the channel description: resources alert
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
New
cpu alert APP 11:28 PM
alert of cpu
Saroj Shah 11:29 PM
added an integration to this channel: incoming-webhook