A. Create two linux servers, server1 => install and configure kibana and elasticsearch with basic username and password authentication server2 => install and configure metricbeat.

First of all, the elasticsearch was setup as follows:

```
samana@samana:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch |
 sudo apt-key add -
[sudo] password for samana:
OK
```

```
samana@samana:~$ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,680 B of archives.
After this operation, 162 kB of additional disk space will be used.
Get:1 http://np.archive.ubuntu.com/ubuntu focal-updates/universe amd64 apt-trans
port-https all 2.0.6 [4,680 B]
Fetched 4,680 B in 1s (9,253 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 190955 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.0.6_all.deb ...
Unpacking apt-transport-https (2.0.6) ...
Setting up apt-transport-https (2.0.6) ...
```

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

```
samana@samana:~$ sudo apt-get update && sudo apt-get install elasticsearch
Hit:1 http://np.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:3 http://np.archive.ubuntu.com/ubuntu focal-updates InRelease
Get:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.6 kB]
Hit:5 http://np.archive.ubuntu.com/ubuntu focal-backports InRelease
Get:6 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [
84.6 kB]
Get:7 https://artifacts.elastic.co/packages/7.x/apt stable/main i386 Packages [6
4.9 kB]
Hit:8 http://download.virtualbox.org/virtualbox/debian hirsute InRelease
Fetched 163 kB in 2s (95.1 kB/s)
Reading package lists... Done
N: Skipping acquire of configured file 'non-free/binary-i386/Packages' as reposi
tory 'http://download.virtualbox.org/virtualbox/debian hirsute InRelease' doesn'
t support architecture 'i386'
```

Now in order to configure elasticsearch properly, we edit the elasticsearch.yml file

```
samana@samana:/etc/elasticsearch$ ls
elasticsearch.keystore  jvm.options.d      roles.yml
elasticsearch.yml       log4j2.properties  users
jvm.options             role_mapping.yml   users_roles
samana@samana:/etc/elasticsearch$ sudo nano elasticsearch.yml
```

We set the discovery type to single-node

```
  GNU nano 4.8                  elasticsearch.yml                  Modified
discovery.type: single-node
# ======================== Elasticsearch Configuration ==================>
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
#       Before you set out to tweak and tune the configuration, make sure>
#       understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template l>
# the most important settings you may want to configure for a production >
#
# Please consult the documentation for further information on configurati>
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster ------------------------------>
#
# Use a descriptive name for your cluster:
#
cluster.name: elk-learn
#
# ------------------------------------ Node ------------------------------->
#
# Use a descriptive name for the node:
#
```

We set the network host to 0.0.0.0 to make it available from all other systems

```
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free por>
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------->
#
# Pass an initial list of hosts to perform discovery when this node is st>
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
```

We set the x-pack security headers to allow username and password based authentication.

```
  GNU nano 4.8                    elasticsearch.yml                    Modified
# By default Elasticsearch is only accessible on localhost. Set a differe>
# address here to expose this node on the network:
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free por>
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------->
#
# Pass an initial list of hosts to perform discovery when this node is st>
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation modul>
#
# ---------------------------------- Various ------------------------------>
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
```

Now we set up the passwords for all users as follows

```
samana@samana:/usr/share/elasticsearch$ sudo ./bin/elasticsearch-setup-pas
swords interactive
Initiating the setup of passwords for reserved users elastic,apm_system,ki
bana,kibana_system,logstash_system,beats_system,remote_monitoring_user.
You will be prompted to enter passwords as the process progresses.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana_system]:
Reenter password for [kibana_system]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
```

Now we enable and start the elasticsearch service

```
samana@samana:~$ sudo systemctl daemon-reload
samana@samana:~$ sudo systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.servic
e → /lib/systemd/system/elasticsearch.service.
samana@samana:~$ sudo systemctl start elasticsearch.service
samana@samana:~$
```

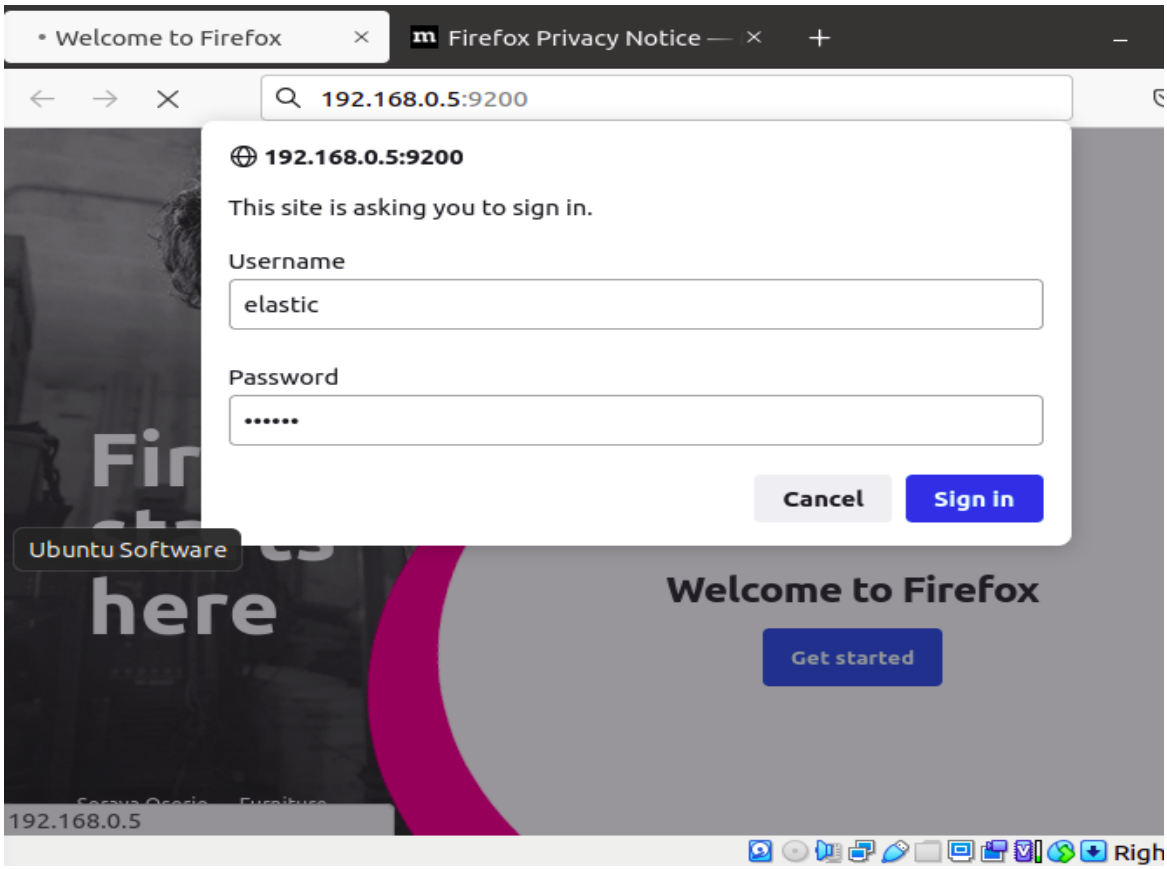
We check the status to verify it is running

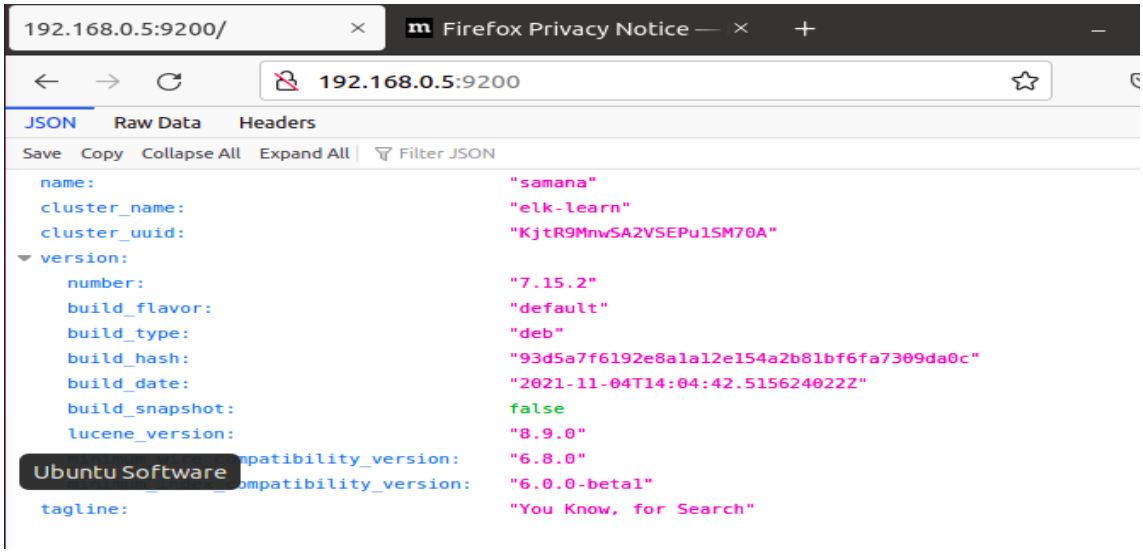
```
samana@samana:~$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Thu 2021-12-02 17:34:36 +0545; 23s ago
       Docs: https://www.elastic.co
   Main PID: 11276 (java)
      Tasks: 82 (limit: 14131)
     Memory: 5.8G
     CGroup: /system.slice/elasticsearch.service
             ├─11276 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.ne>
             └─11468 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux->

दिसम्बर 02 17:34:02 samana systemd[1]: Starting Elasticsearch...
दिसम्बर 02 17:34:10 samana systemd-entrypoint[11276]: WARNING: A terminally depr>
दिसम्बर 02 17:34:10 samana systemd-entrypoint[11276]: WARNING: System::setSecuri>
दिसम्बर 02 17:34:10 samana systemd-entrypoint[11276]: WARNING: Please consider r>
दिसम्बर 02 17:34:10 samana systemd-entrypoint[11276]: WARNING: System::setSecuri>
दिसम्बर 02 17:34:13 samana systemd-entrypoint[11276]: WARNING: A terminally depr>
दिसम्बर 02 17:34:13 samana systemd-entrypoint[11276]: WARNING: System::setSecuri>
दिसम्बर 02 17:34:13 samana systemd-entrypoint[11276]: WARNING: Please consider r>
दिसम्बर 02 17:34:13 samana systemd-entrypoint[11276]: WARNING: System::setSecuri>
दिसम्बर 02 17:34:36 samana systemd[1]: Started Elasticsearch.
lines 1-21/21 (END)
```

The server where elasticsearch is configured has ip 192.168.0.5

```
samana@samana:~$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 10:7d:1a:3d:19:d2  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4889  bytes 476156 (476.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4889  bytes 476156 (476.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.5  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::aef4:89f3:7040:1b79  prefixlen 64  scopeid 0x20<link>
        ether a8:6b:ad:1d:9a:09  txqueuelen 1000  (Ethernet)
        RX packets 1104298  bytes 1590594392 (1.5 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 344108  bytes 34328257 (34.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

samana@samana:~$ R
```

We access the elasticsearch from our another server (server2)





Now we install kibana which provides interactive GUI for elasticsearch.

```
samana@samana:~$ sudo apt-get install kibana
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 288 MB of archives.
After this operation, 786 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd
64 7.15.2 [288 MB]
12% [1 kibana 43.2 MB/288 MB 15%]                                4,848 kB/s 50s
```

We edit the kibana configuration file and set the server host to anywhere.

```
  GNU nano 4.8                    kibana.yml                    Modified
# Kibana is served by a back end server. This setting specifies the port >
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresse>
# The default is 'localhost', which usually means remote machines will no>
# To allow connections from remote users, set this parameter to a non-loo>
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running beh>
# Use the `server.rewriteBasePath` setting to tell Kibana if it should re>
# from requests it receives, and to prevent a deprecation warning at star>
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse pr>
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false
```

We write our previously setup password in our config file (which should normally be replaced by api keys or encrypted values for security reasons)

```
  GNU nano 4.8                    kibana.yml                    Modified
# `server.basePath` or require that they are rewritten by your reverse pr>
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same baseP>
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
#elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualiz>
# dashboards. Kibana creates a new index if the index doesn't already exi>
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these set>
# the username and password that the Kibana server uses to perform mainte>
# index at startup. Your Kibana users still need to authenticate with Ela>
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "123456"
```

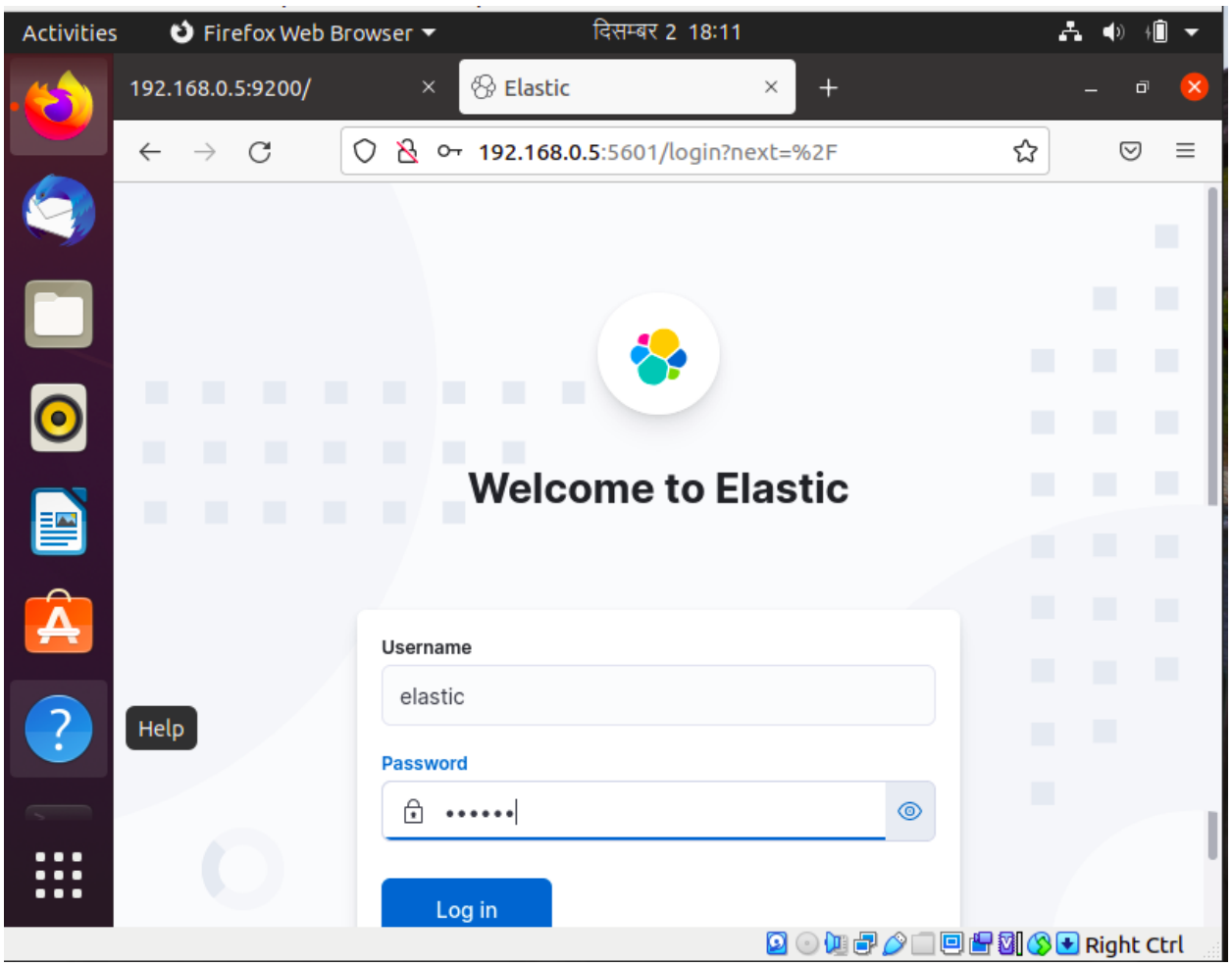
We also setup a encryption key of at least 32 characters

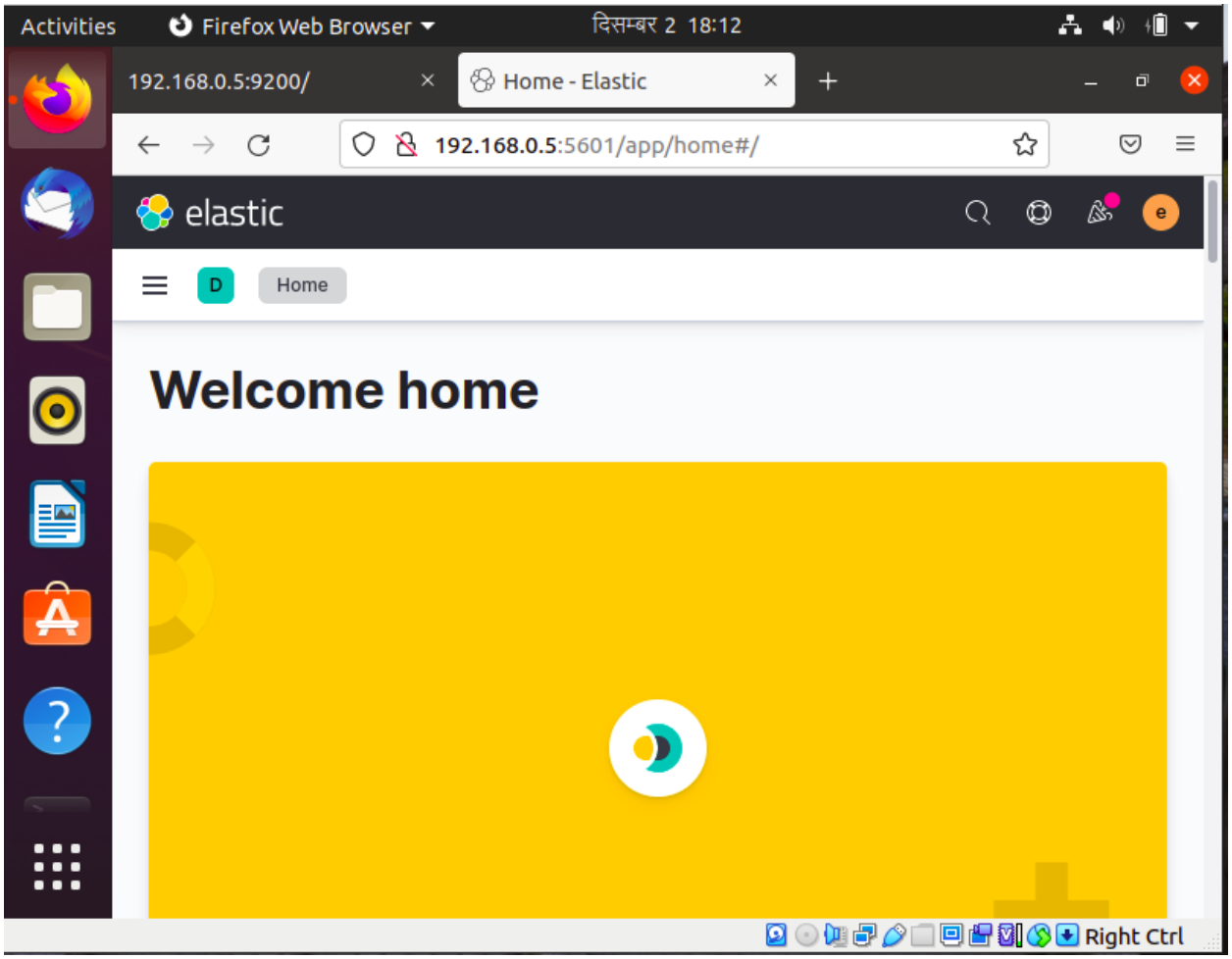
```
  GNU nano 4.8                                                    kibana.yml
#logging.dest: stdout

# Set the value of this setting to true to suppress all logging output.
#logging.silent: false

# Set the value of this setting to true to suppress all logging output other than error messages.
#logging.quiet: false

# Set the value of this setting to true to log all events, including system usage information
# and all requests.
#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance
# metrics. Minimum is 100ms. Defaults to 5000.
#ops.interval: 5000

# Specifies locale to be used for all localizable strings, dates and number formats.
# Supported languages are the following: English - en , by default , Chinese - zh-CN .
#i18n.locale: "en"
xpack.encryptedSavedObjects.encryptionKey: “kdjsadjsjhdsybhcshdgdjfjdhjkdiedleasdjsjdcharactedddfrfdssdvalue"
```

Now we enable and start the kibana service after editing our config file

```
samana@samana:~$ sudo systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /lib/s
ystemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service
 → /etc/systemd/system/kibana.service.
samana@samana:~$ sudo systemctl start kibana.service
samana@samana:~$
```

We can now access our kibana dashboard from our another server




Activities
Firefox Web Browser
दिसम्बर 2 18:12
192.168.0.5:9200/
Home - Elastic
192.168.0.5:5601/app/home#/
elastic
D
Home
Welcome home
Right Ctrl

installing metricbeats in server 2:

```
samana@samana-VM:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsear
ch | sudo apt-key add -
[sudo] password for samana:
OK
samana@samana-VM:~$ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 100 not upgraded.
Need to get 1,708 B of archives.
After this operation, 161 kB of additional disk space will be used.
Get:1 http://security.ubuntu.com/ubuntu focal-security/universe amd64 apt-trans
port-https all 2.0.2ubuntu0.2 [1,708 B]
Fetched 1,708 B in 0s (3,531 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 145618 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.0.2ubuntu0.2_all.deb ...
Unpacking apt-transport-https (2.0.2ubuntu0.2) ...
Setting up apt-transport-https (2.0.2ubuntu0.2) ...
samana@samana-VM:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt sta
ble main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
samana@samana-VM:~$
```

```
samana@samana-VM:~$ sudo apt-get update && sudo apt-get install metricbeat
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.6 kB]
Get:2 https://artifacts.elastic.co/packages/7.x/apt stable/main i386 Packages [
64.9 kB]
Get:3 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages
[84.6 kB]
Err:4 http://security.ubuntu.com/ubuntu focal-security InRelease
  Connection failed [IP: 91.189.88.152 80]
Hit:5 http://np.archive.ubuntu.com/ubuntu focal InRelease
Get:6 http://np.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:7 http://np.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:8 http://np.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,
386 kB]
Ign:9 http://np.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages
Get:10 http://np.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [2
81 kB]
Get:11 http://np.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Meta
data [278 kB]
Get:12 http://np.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 48x48 Icon
s [60.8 kB]
Get:13 http://np.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 64x64 Icon
s [98.3 kB]
```

We edit the yml file for metricbeat as follows

```
  GNU nano 4.8                    metricbeat.yml                    Modif
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` an
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

# ================================== Outputs ===============================

# Configure what output to use when sending the data collected by the beat

# ----------------------------- Elasticsearch Output ----------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.0.5:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "123456"
```

We enable and start the metricbeat service.

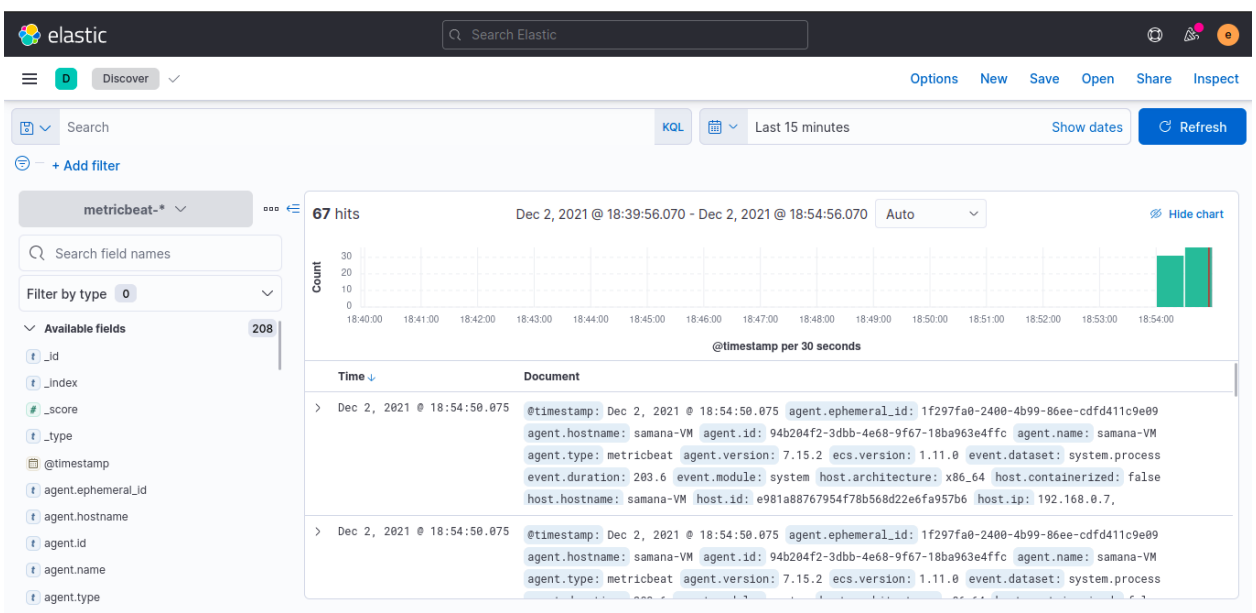
```
samana@samana-VM:~$ sudo systemctl enable metricbeat
[sudo] password for samana:
Synchronizing state of metricbeat.service with SysV service script with /lib/sy
stemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable metricbeat
Created symlink /etc/systemd/system/multi-user.target.wants/metricbeat.service
→ /lib/systemd/system/metricbeat.service.
samana@samana-VM:~$ sudo systemctl start metricbeat
samana@samana-VM:~$
```

We setup a metricbeat index which sends the metrics to the kibana dashboard.

```
samana@samana-VM:/etc/metricbeat$ sudo metricbeat setup --template -E 'output.e
lasticsearch.hosts=["192.168.0.5:9200"]'
Flag --template has been deprecated, please use --index-management instead
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enablin
g.

Index setup finished.
samana@samana-VM:/etc/metricbeat$
```

```
samana@samana-VM:/etc/metricbeat$ sudo metricbeat setup -e -E output.elasticsea
rch.hosts=['192.168.0.5:9200'] -E setup.kibana.host=192.168.0.5:5601
2021-12-02T18:49:01.111+0545    INFO    instance/beat.go:665    Home path: [/us
r/share/metricbeat] Config path: [/etc/metricbeat] Data path: [/var/lib/metricb
eat] Logs path: [/var/log/metricbeat]
2021-12-02T18:49:01.112+0545    INFO    instance/beat.go:673    Beat ID: 94b204
f2-3dbb-4e68-9f67-18ba963e4ffc
2021-12-02T18:49:01.113+0545    INFO    [beat]  instance/beat.go:1014   Beat in
fo      {"system_info": {"beat": {"path": {"config": "/etc/metricbeat", "data":
 "/var/lib/metricbeat", "home": "/usr/share/metricbeat", "logs": "/var/log/metr
icbeat"}, "type": "metricbeat", "uuid": "94b204f2-3dbb-4e68-9f67-18ba963e4ffc"}
}}
2021-12-02T18:49:01.113+0545    INFO    [beat]  instance/beat.go:1023   Build i
nfo     {"system_info": {"build": {"commit": "fd322dad6ceafec40c84df4d2a0694ea3
57d16cc", "libbeat": "7.15.2", "time": "2021-11-04T14:35:34.000Z", "version": "
7.15.2"}}}
2021-12-02T18:49:01.114+0545    INFO    [beat]  instance/beat.go:1026   Go runt
ime info        {"system_info": {"go": {"os":"linux","arch":"amd64","max_procs"
:1,"version":"go1.16.6"}}}
2021-12-02T18:49:01.114+0545    INFO    [beat]  instance/beat.go:1030   Host in
fo      {"system_info": {"host": {"architecture":"x86_64","boot_time":"2021-12-
02T17:56:01+05:45","containerized":false,"name":"samana-VM","ip":["127.0.0.1/8"
,"::1/128","192.168.0.7/24","fe80::d273:a838:40f6:44b3/64"],"kernel_version":"5
```

We can see the following result from metricbeat in kibana dashboard.

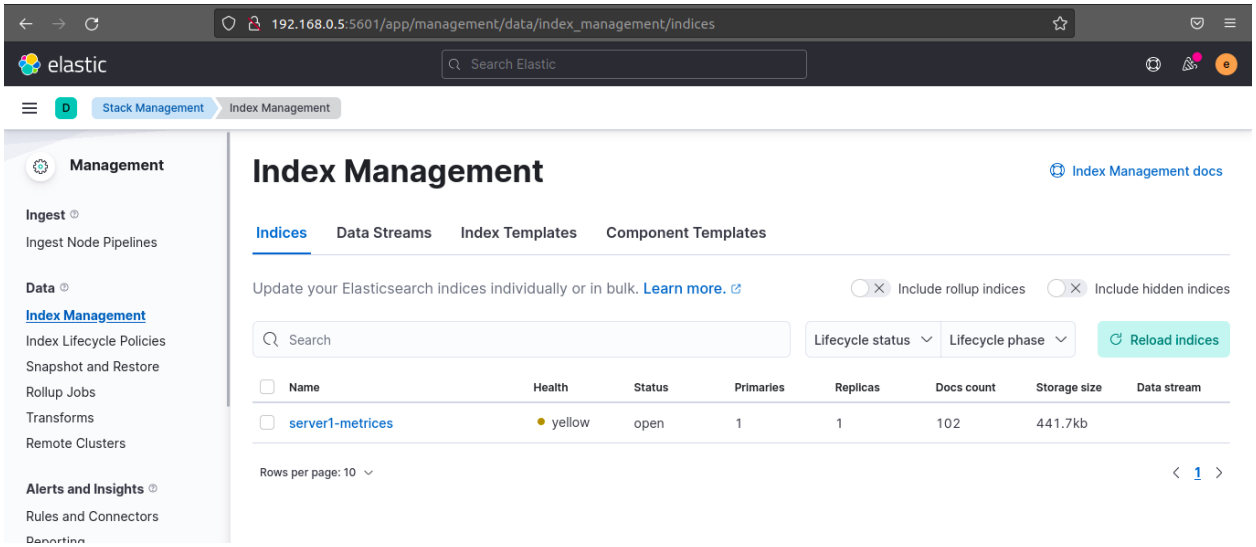


B.Collect metric from following sources in server1 and send them to elasticsearch. Store them in an index named "server1-metrics". a. Memory usage b. Disk usage c. Load average

To collect metrics we edit the config file as follows (with load,memory and disk metrics sets)

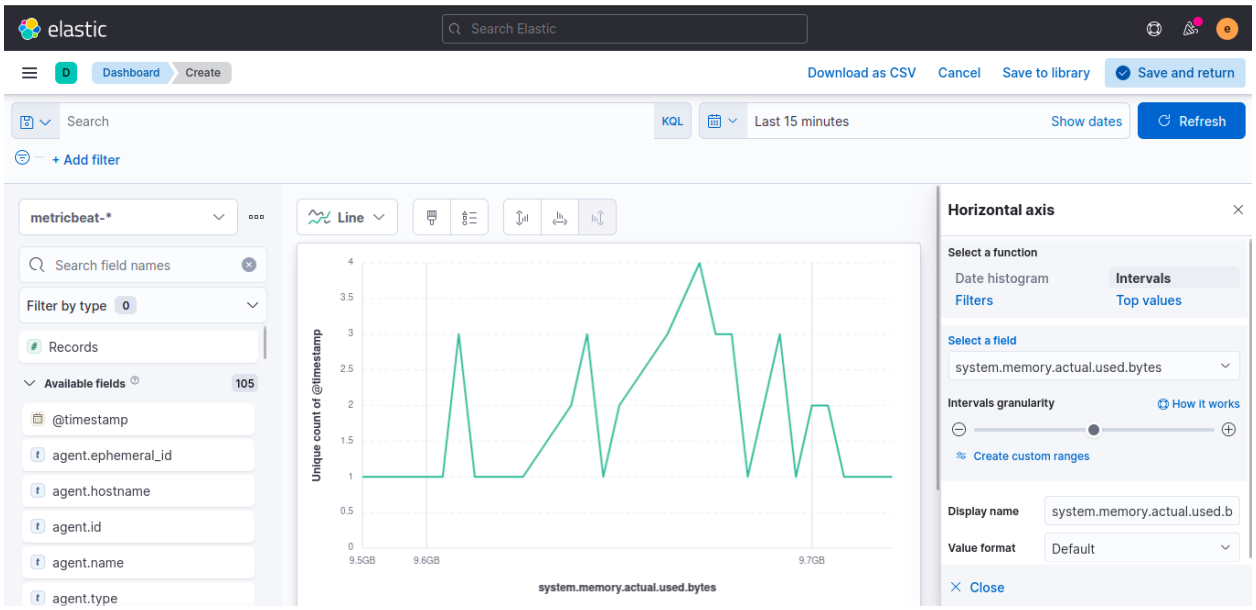
```
  GNU nano 4.8                    metricbeat.yml                    Modified
    # Set to true to enable instrumentation of metricbeat.
    #enabled: false

    # Environment in which metricbeat is running on (eg: staging, product>
    #environment: ""

    # APM Server hosts to report instrumentation results to.
    #hosts:
    #  - http://localhost:8200

    # API Key for the APM Server(s).
    # If api_key is set then secret_token will be ignored.
    #api_key:

    # Secret token for the APM Server(s).
    #secret_token:


# ================================= Migration ==========================>

# This allows to enable 6.7 migration aliases
#migration.6_to_7.enabled: true

metricbeat.modules:
- module: system
  metricsets:
    - load
    - memory
    - diskio
  enabled: true
  period: 5s
  index: "server1-metrices"
```

We can see that the collected metrics have been stored in an index names server1-metrices.

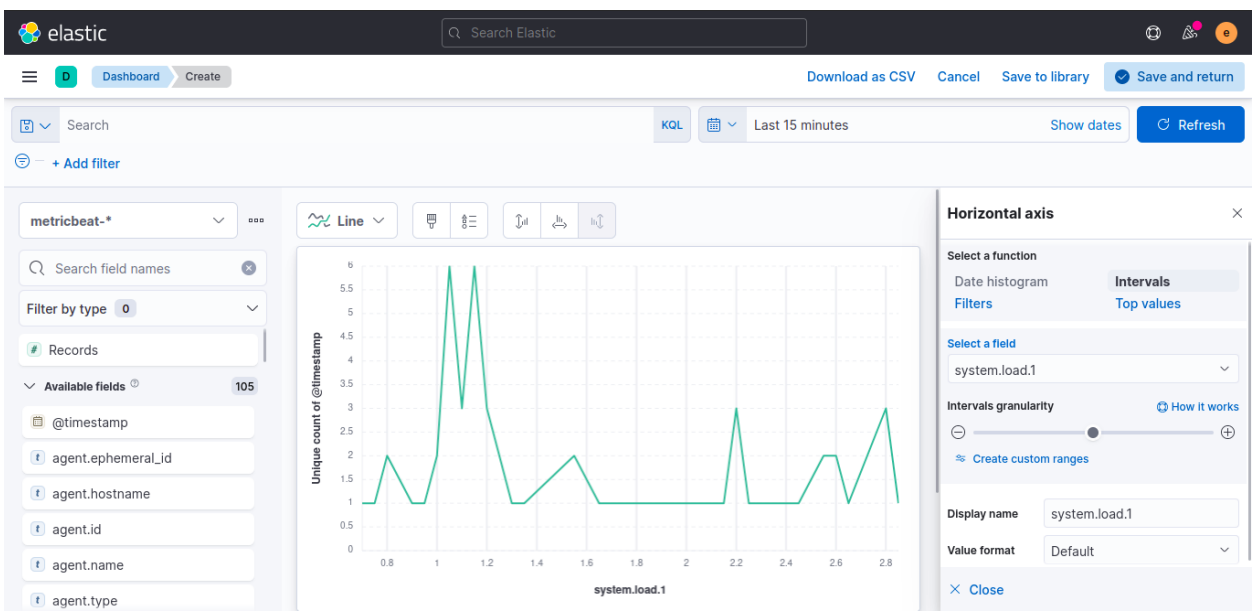


1. **Create a dashboard in kibana and generate visual report(line graph) for Memory usage and load average of server1 with relation to time**

Line graph of memory usage with respect to time:

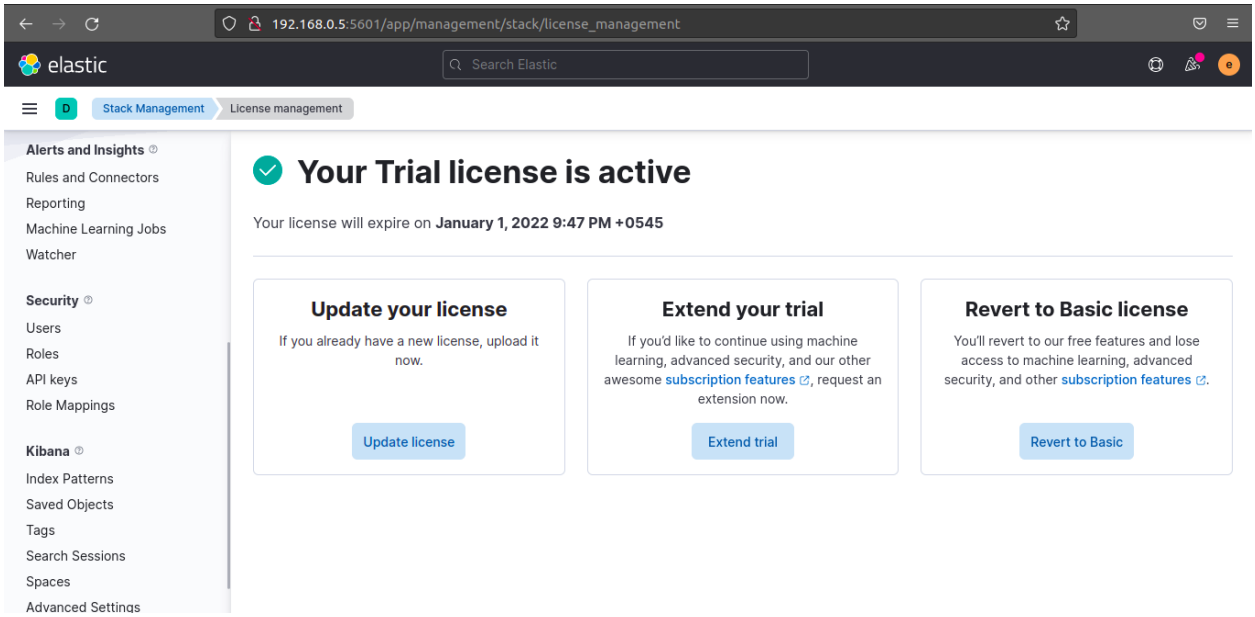


Line graph of load average in relation to time



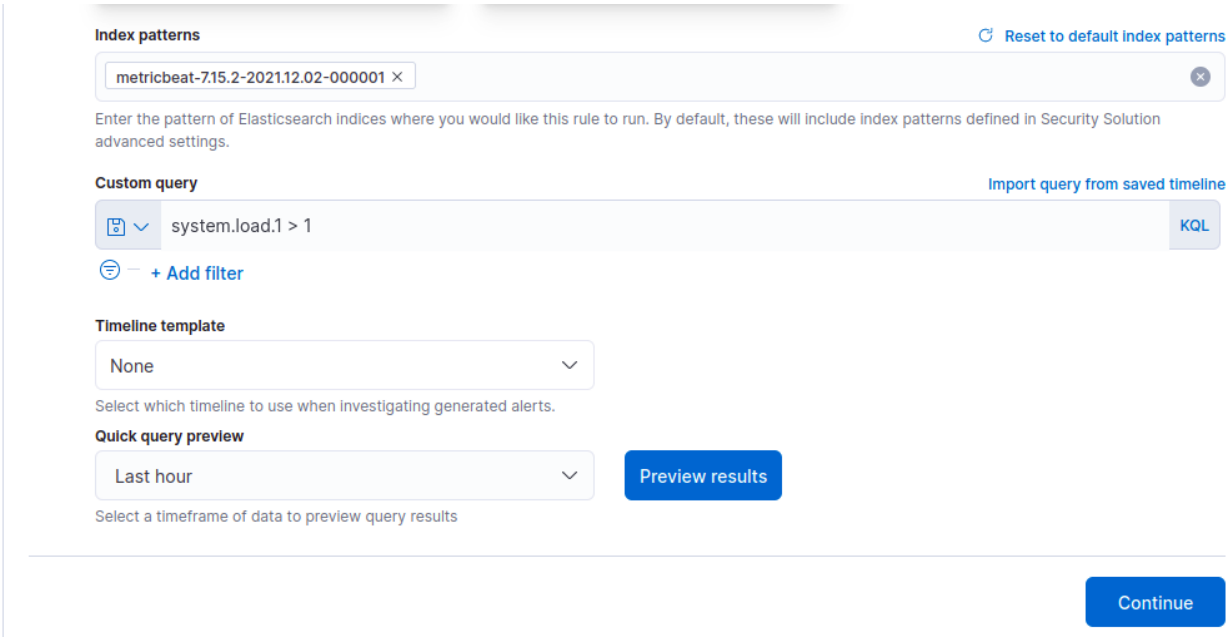
2. **Generate alerts through kibana system for following thresholds a. when memory usage > 80% for last 2 minutes send alert to a slack channel b. When Disk usage > 70% send alert to a slack channel c. When load average > 1 for last 2 minutes send alert to a slack channel**

For creating alerts we start a trial license 30 day free plan.

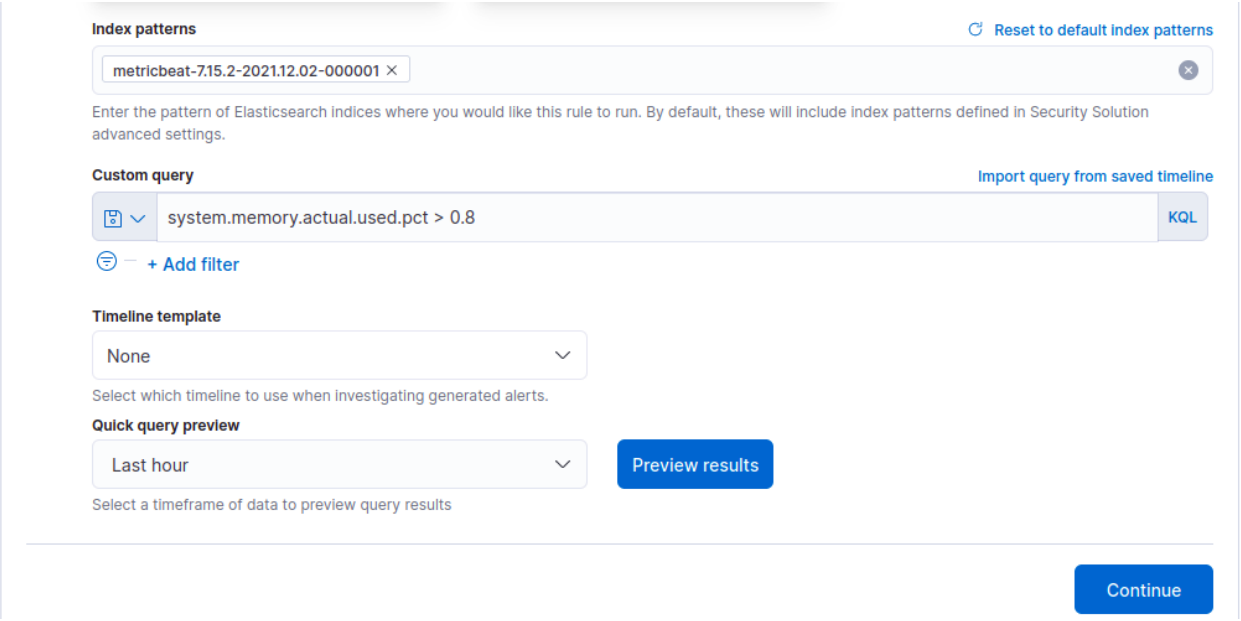


We create rules as follows:

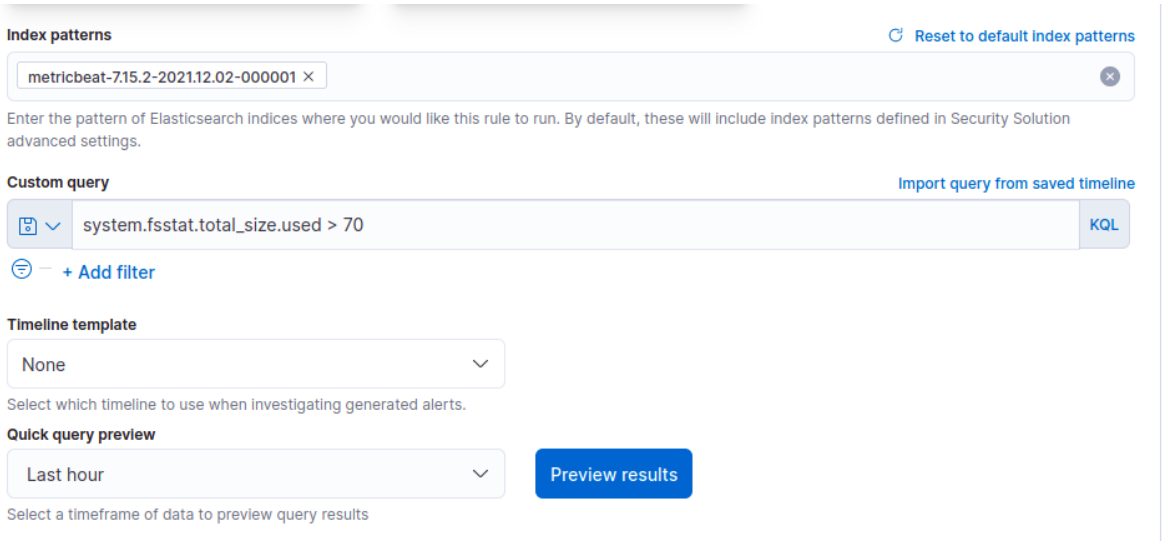
a) **For system load**



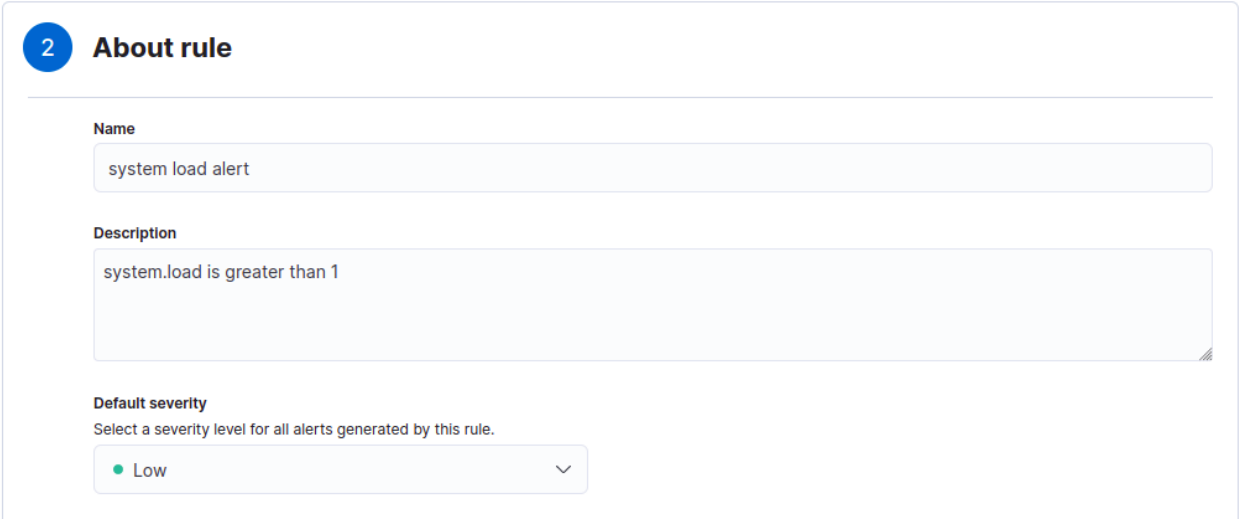
b) For system memory

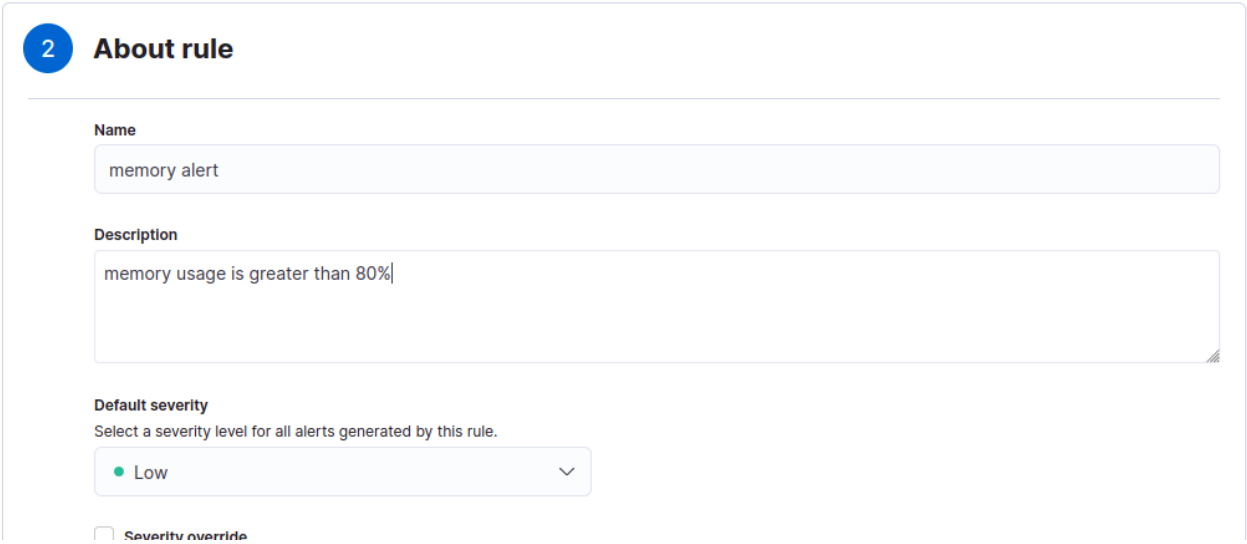


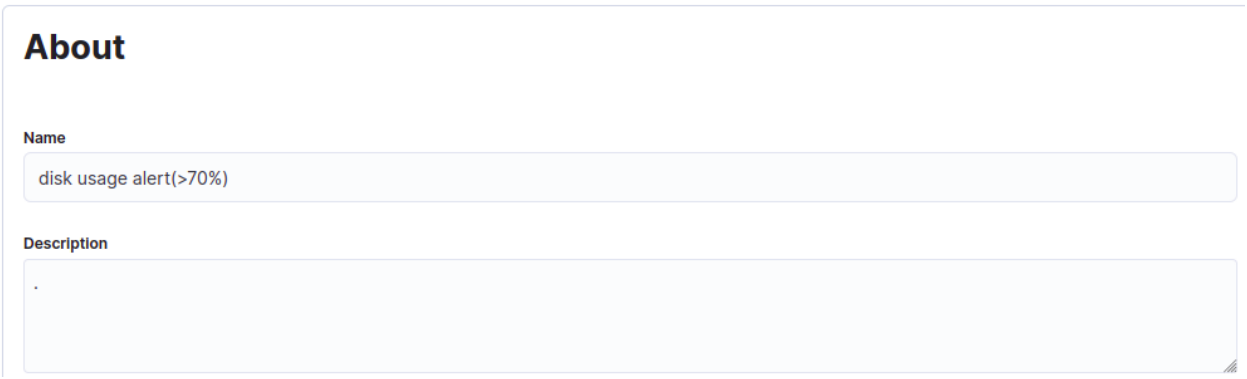
c) For disk usage:



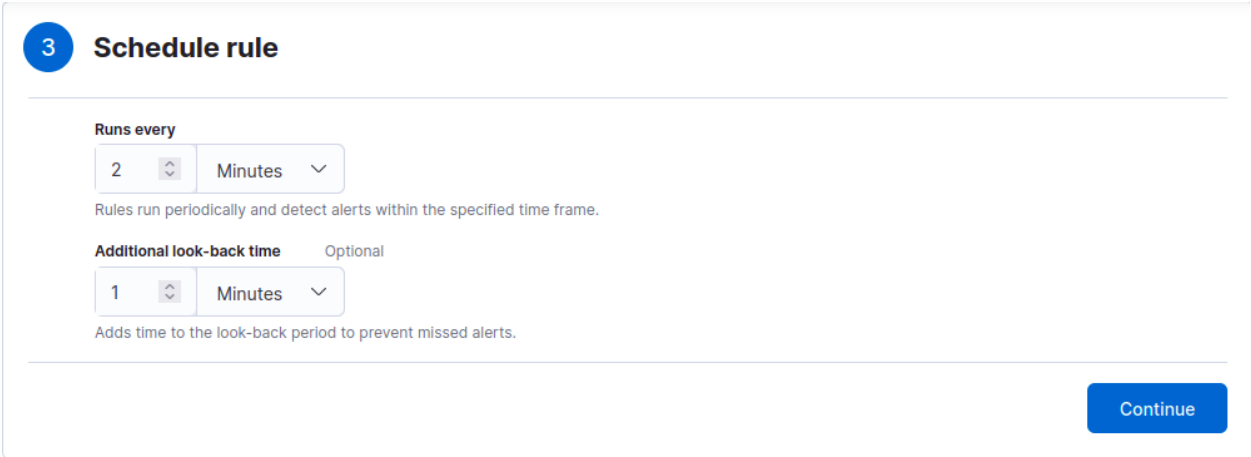
We name the rules as follows:



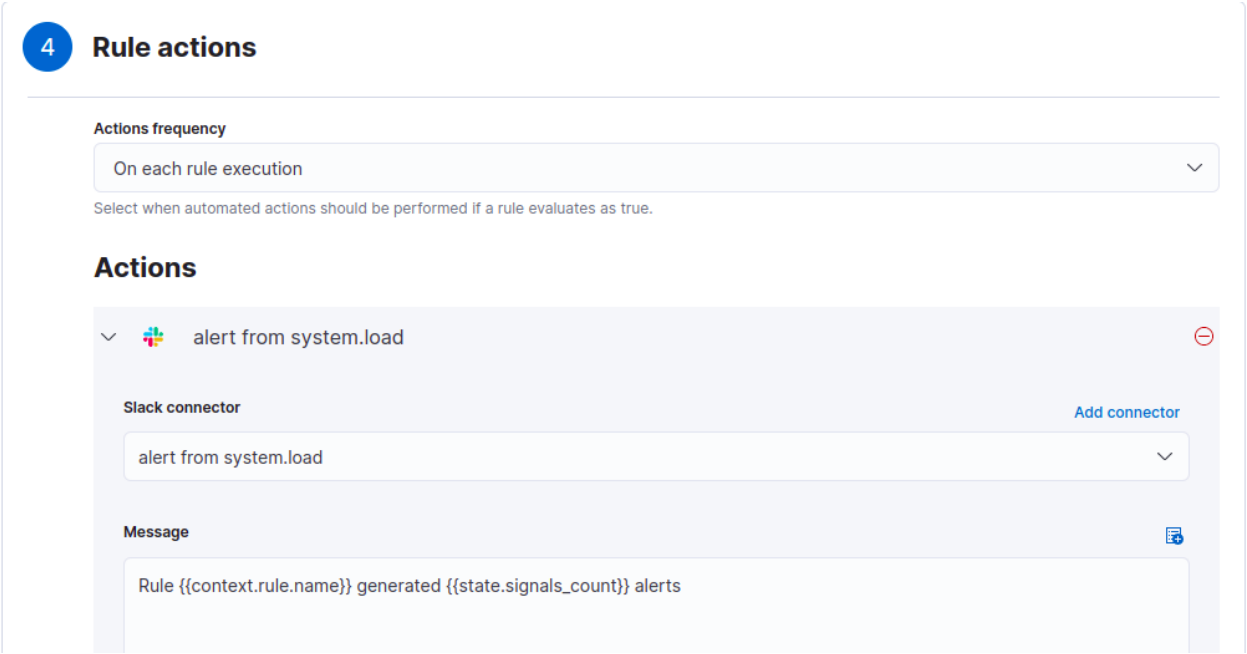




We then schedule the rule(for all 3 cases) to run every 2 minutes:



On the rule execution, we set the rule action to generate alert messages to slack channel using webhook integration.



The created rules can be seen below:

Showing 3 rules | Selected 0 rules | Bulk actions | Refresh | Refresh settings

Rule	Risk score	Severity	Last run	Last respo...	Last updated	Version	Tags	Activated
system load alert	77	Low	2 minutes ago	succeeded	Dec 3, 2021 @ 00:07:30.179	1	—	
memory alert	58	Low	51 seconds ago	succeeded	Dec 3, 2021 @ 00:21:02.598	1	—	
disk usage alert	21	Low	23 seconds ago	succeeded	Dec 3, 2021 @ 00:25:33.886	1	—	

In order to trigger creating alerts, we perform the following action

```
samana@samana:~$ echo {1..1000000000}
```

Finally, we can see that in my slack channel all three kind of alerts are generated