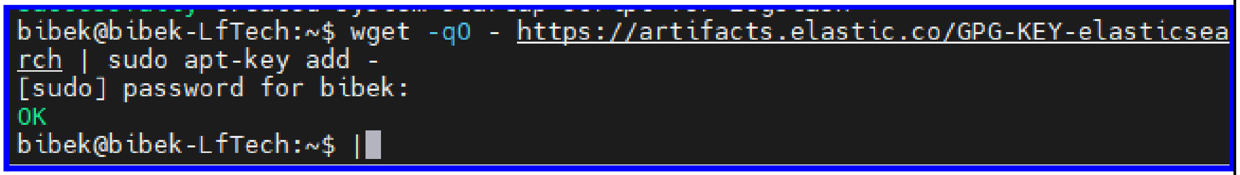
A. Create two linux servers, server1 => install and configure kibana and elasticsearch with basic username and password authentication server2 => install and configure metricbeat.

Installing ElasticSearch

Download and install the public signing key:

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



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

Install the apt-transport-https package

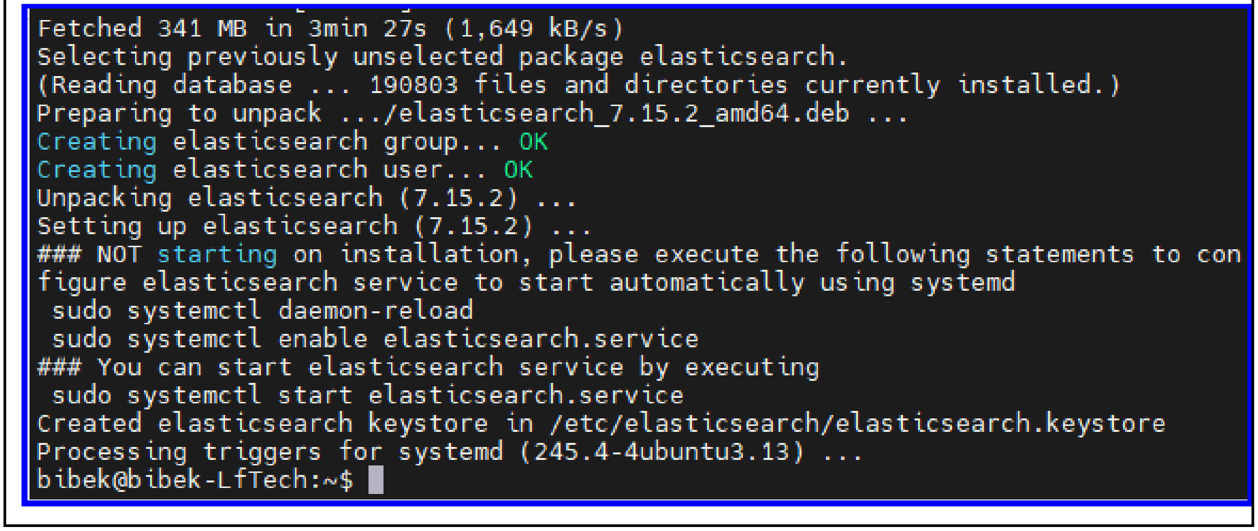
We have already installed this package during installation of logstash

Save the repository definition to /etc/apt/sources.list.d/elastic-7.x.list:

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

You can install the Elasticsearch Debian package with:

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



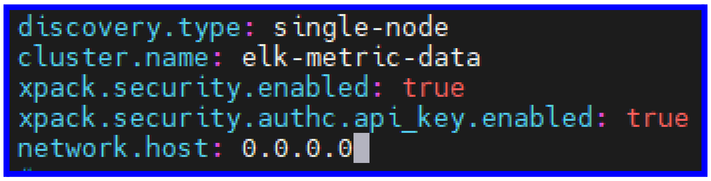
```
Fetched 341 MB in 3min 27s (1,649 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 190803 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.15.2_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.15.2) ...
Setting up elasticsearch (7.15.2) ...
### NOT starting on installation, please execute the following statements to con
figure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
Processing triggers for systemd (245.4-4ubuntu3.13) ...
bibek@bibek-LfTech:~$
```

The hostname of server 1 is set to elasticsearch

sudo hostnamectl set-hostname elasticsearch

Configuring ElasticSearch

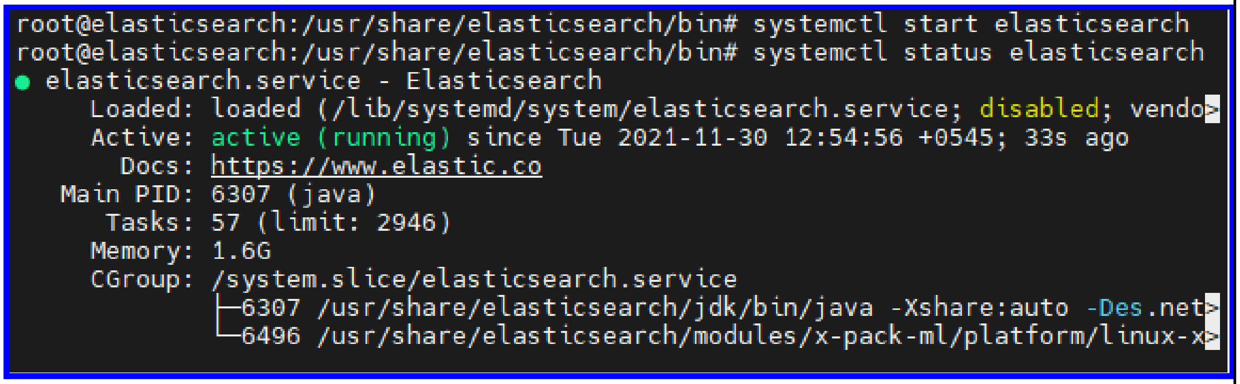
vi /etc/elasticsearch/elasticsearch.yml



```
discovery.type: single-node
cluster.name: elk-metric-data
xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
network.host: 0.0.0.0
```

Starting elasticsearch

systemctl start elasticsearch



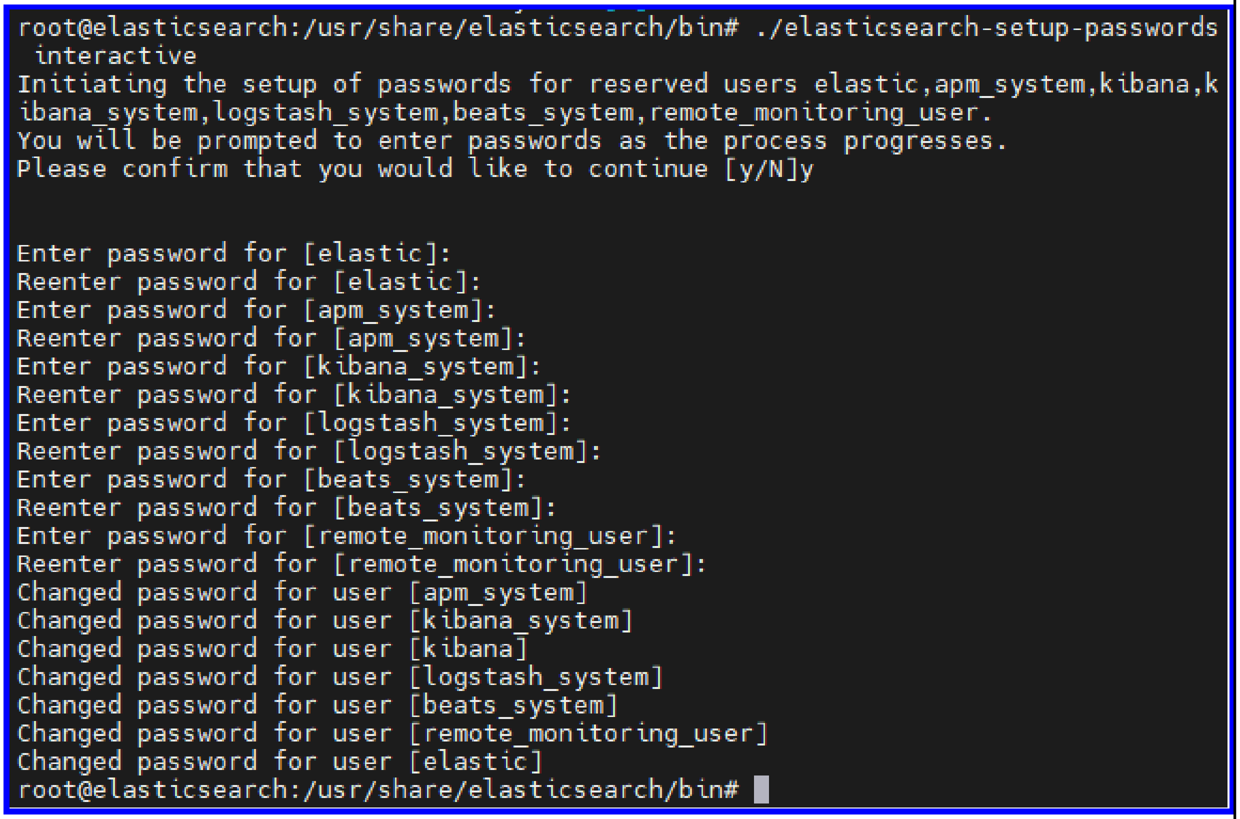
```
root@elasticsearch:/usr/share/elasticsearch/bin# systemctl start elasticsearch
root@elasticsearch:/usr/share/elasticsearch/bin# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; disabled; vendo>
     Active: active (running) since Tue 2021-11-30 12:54:56 +0545; 33s ago
       Docs: https://www.elastic.co
   Main PID: 6307 (java)
      Tasks: 57 (limit: 2946)
     Memory: 1.6G
     CGroup: /system.slice/elasticsearch.service
             ├─6307 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net>
             └─6496 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>
```

Setting up the password

cd /usr/share/elasticsearch/

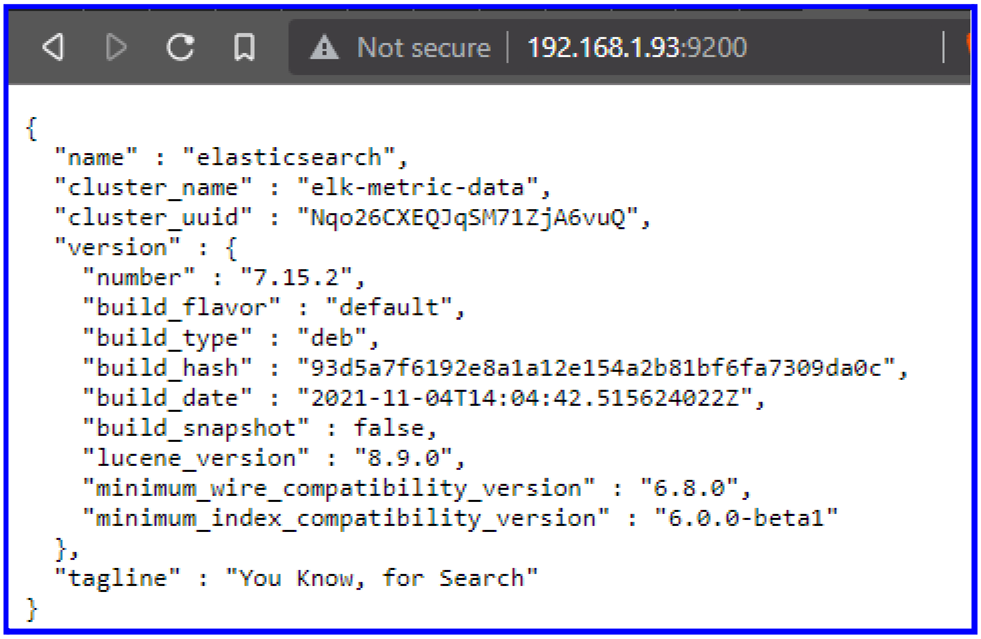
cd bin

./elasticsearch-setup-passwords interactive



```
root@elasticsearch:/usr/share/elasticsearch/bin# ./elasticsearch-setup-passwords
 interactive
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,k
ibana_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]
root@elasticsearch:/usr/share/elasticsearch/bin#
```

Browsing in web



```
{
  "name" : "elasticsearch",
  "cluster_name" : "elk-metric-data",
  "cluster_uuid" : "Nqo26CXEQJqSM71ZjA6vuQ",
  "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"
}
```

Installing Kibana

Download and install the public signing key:

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

Install the apt-transport-https package

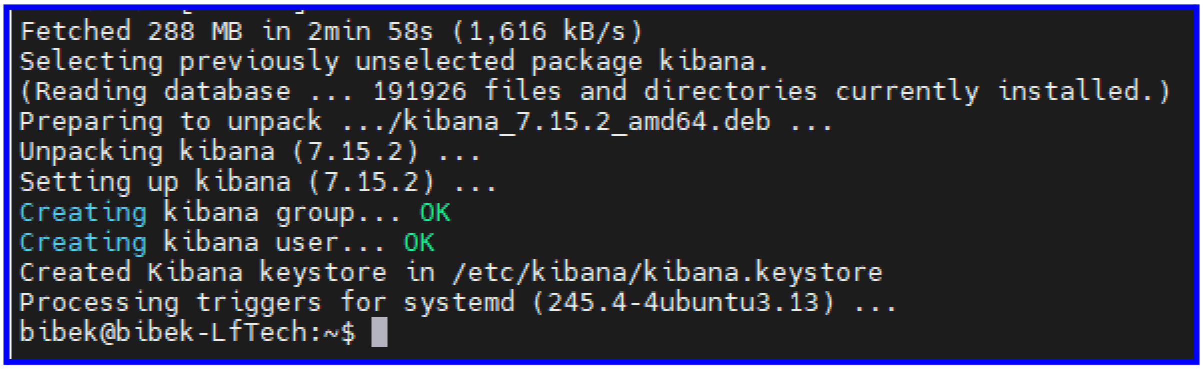
We have already installed this package during installation of logstash

Save the repository definition to /etc/apt/sources.list.d/elastic-7.x.list:

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

You can install the Kibana Debian package with:

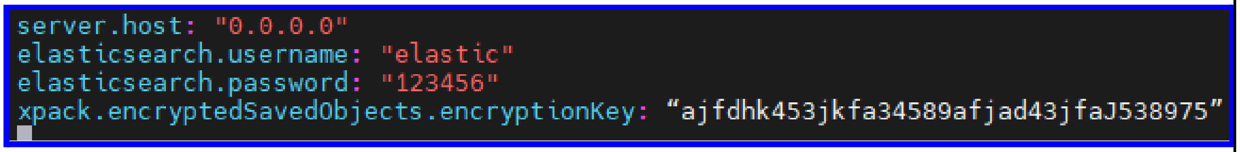
sudo apt-get update && sudo apt-get install kibana



```
Fetched 288 MB in 2min 58s (1,616 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 191926 files and directories currently installed.)
Preparing to unpack .../kibana_7.15.2_amd64.deb ...
Unpacking kibana (7.15.2) ...
Setting up kibana (7.15.2) ...
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
Processing triggers for systemd (245.4-4ubuntu3.13) ...
bibek@bibek-LfTech:~$
```

Configuring Kibana

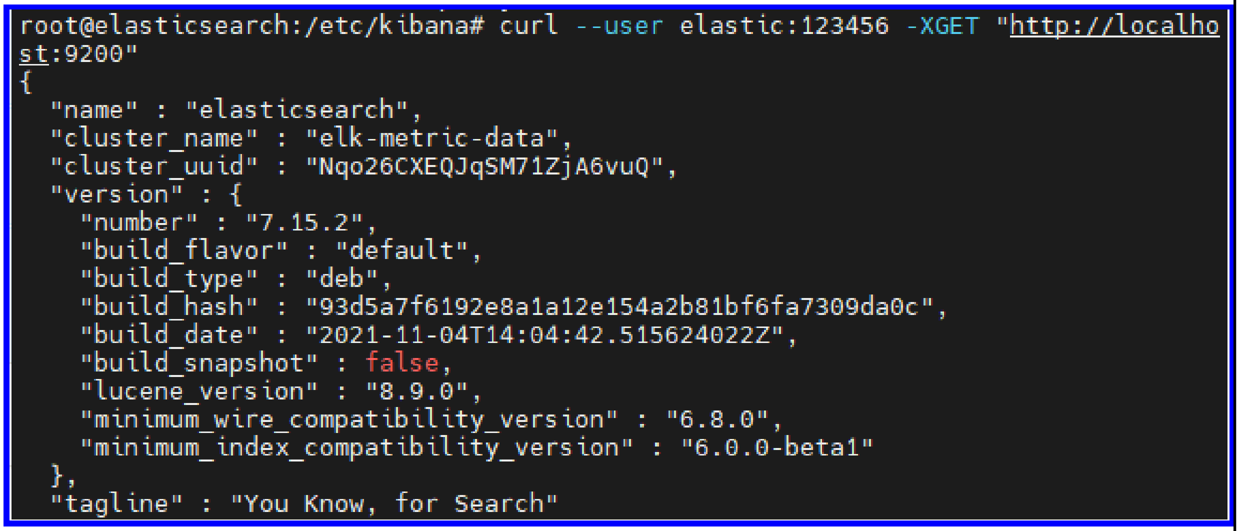
vi /etc/kibana/kibana.yml



```
server.host: "0.0.0.0"
elasticsearch.username: "elastic"
elasticsearch.password: "123456"
xpack.encryptedSavedObjects.encryptionKey: “ajfdhk453jkfa34589afjad43jfaJ538975”
```

elasticsearch.hosts: ["http://localhost:9200"]

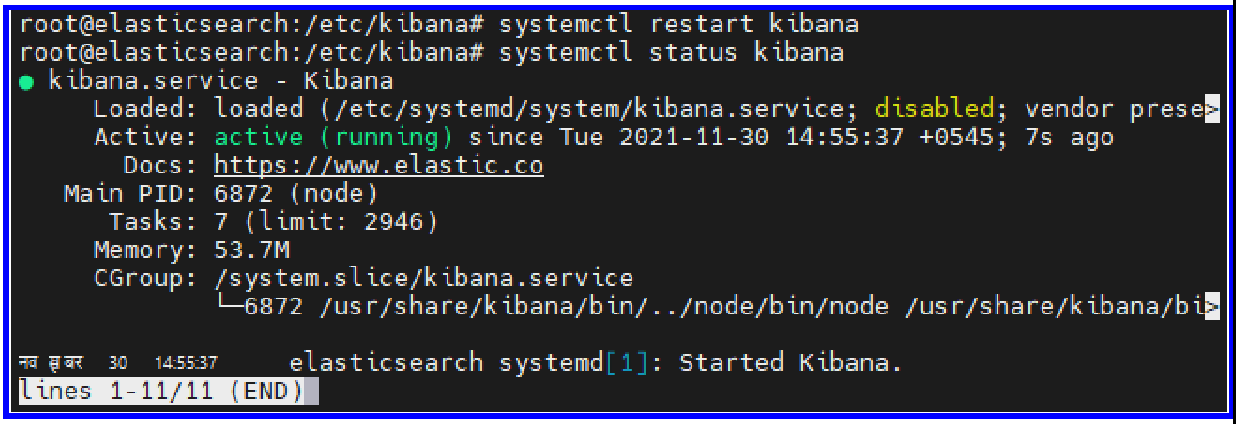
Curl at localhost



```
root@elasticsearch:/etc/kibana# curl --user elastic:123456 -XGET "http://localho
st:9200"
{
  "name" : "elasticsearch",
  "cluster_name" : "elk-metric-data",
  "cluster_uuid" : "Nqo26CXEQJqSM71ZjA6vuQ",
  "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"
```

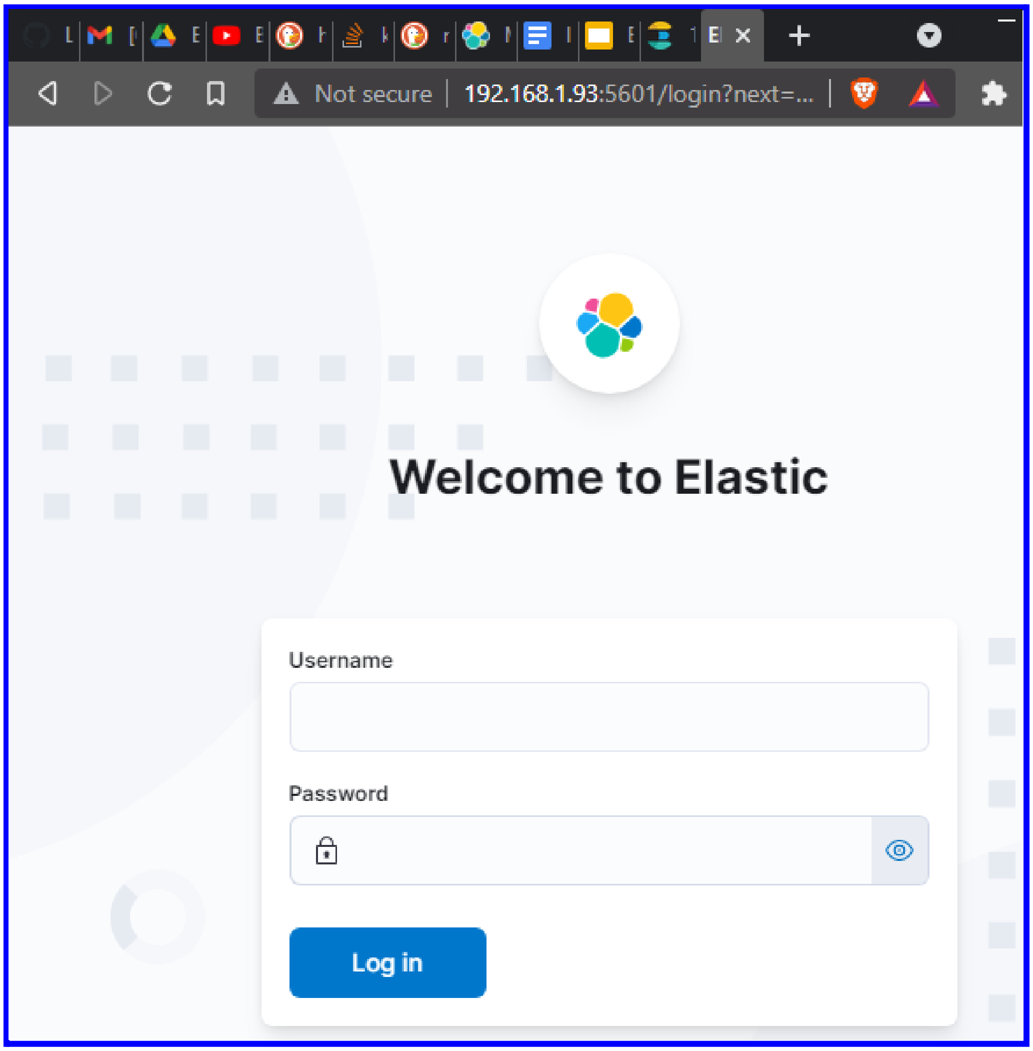
Starting the kibana

systemctl restart kibana



```
root@elasticsearch:/etc/kibana# systemctl restart kibana
root@elasticsearch:/etc/kibana# systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; disabled; vendor prese>
     Active: active (running) since Tue 2021-11-30 14:55:37 +0545; 7s ago
       Docs: https://www.elastic.co
   Main PID: 6872 (node)
      Tasks: 7 (limit: 2946)
     Memory: 53.7M
     CGroup: /system.slice/kibana.service
             └─6872 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bi>

नव हृबर 30 14:55:37 elasticsearch systemd[1]: Started Kibana.
lines 1-11/11 (END)
```

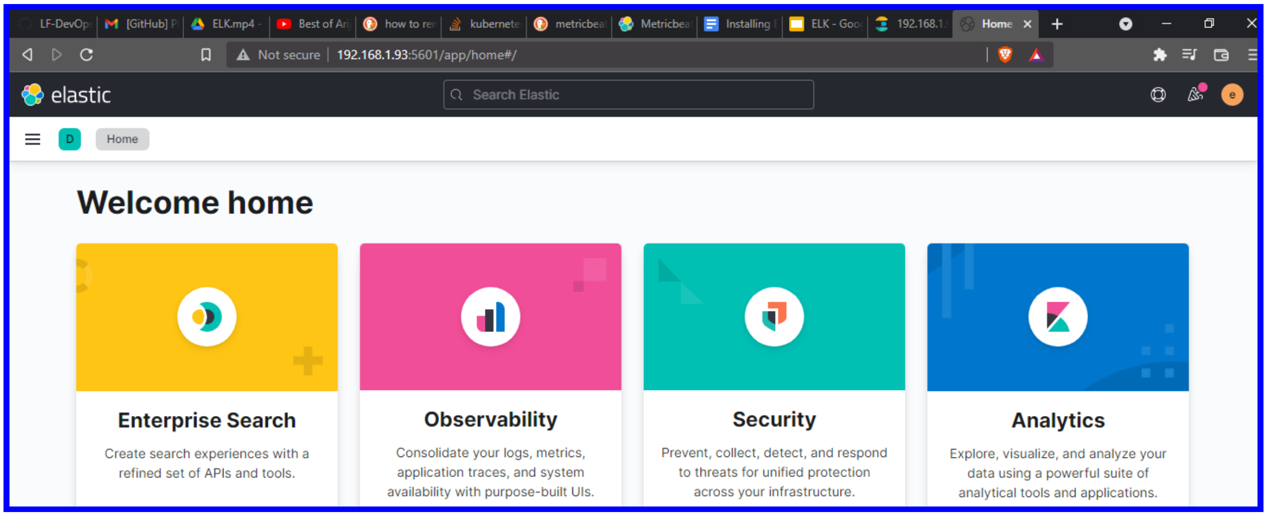
Browsing in the web



Not secure | 192.168.1.93:5601/login?next=...

Welcome to Elastic

After login - > Exploring on my own



Not secure | 192.168.1.93:5601/app/home#/

Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

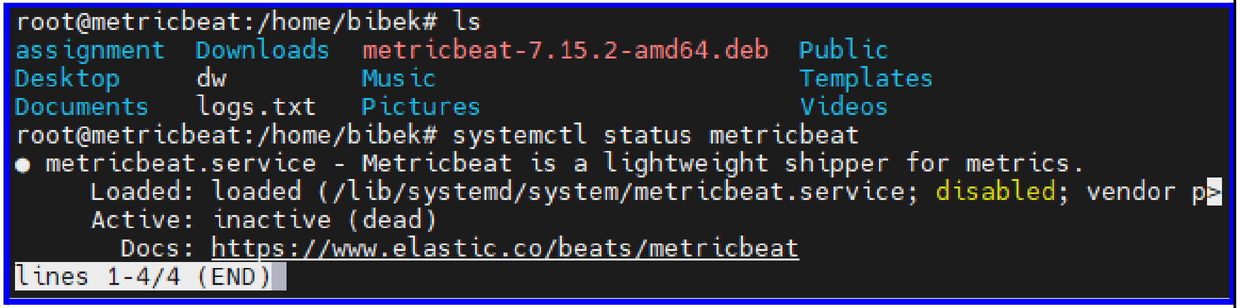
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Installing Metricbeat in Server 2

Server 2 Hostname = metricbeat

curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.15.2-amd64.deb

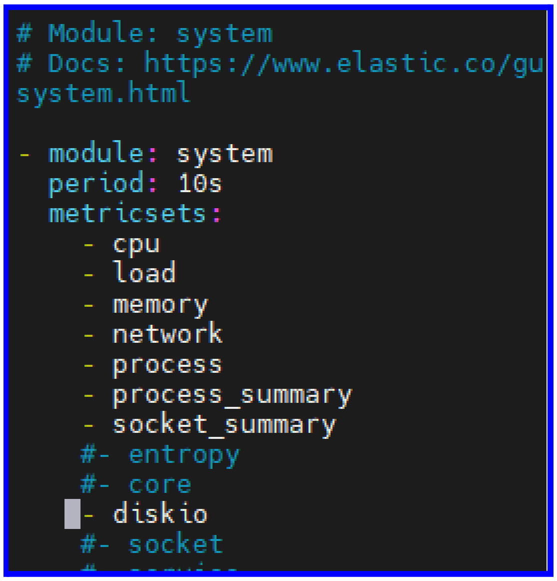
sudo dpkg -i metricbeat-7.15.2-amd64.deb



```
root@metricbeat:/home/bibek# ls
assignment  Downloads  metricbeat-7.15.2-amd64.deb  Public
Desktop     dw         Music                        Templates
Documents   logs.txt   Pictures                     Videos
root@metricbeat:/home/bibek# systemctl status metricbeat
● metricbeat.service - Metricbeat is a lightweight shipper for metrics.
     Loaded: loaded (/lib/systemd/system/metricbeat.service; disabled; vendor p>
     Active: inactive (dead)
       Docs: https://www.elastic.co/beats/metricbeat
lines 1-4/4 (END)
```

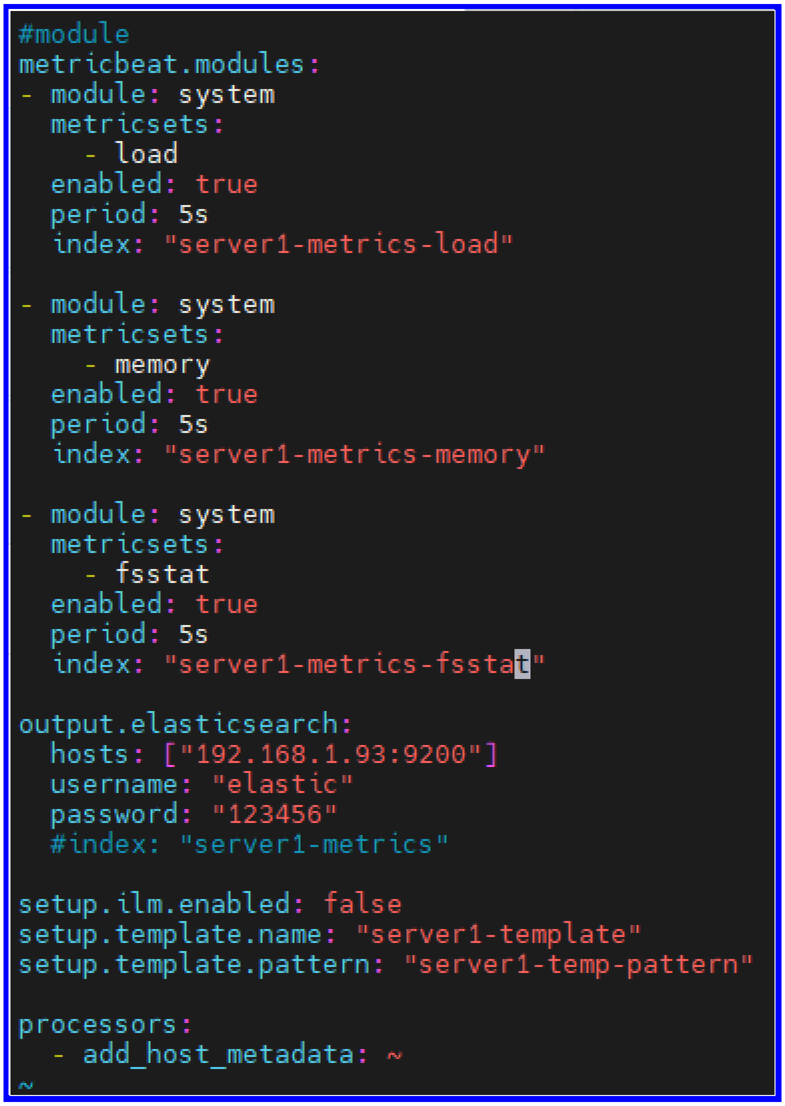
Configuring metricbeat for load, disk usage and memory

vi /etc/metricbeat/modules.d/system.yml



```
# Module: system
# Docs: https://www.elastic.co/gu
system.html

- module: system
  period: 10s
  metricsets:
    - cpu
    - load
    - memory
    - network
    - process
    - process_summary
    - socket_summary
    #- entropy
    #- core
    - diskio
    #- socket
```

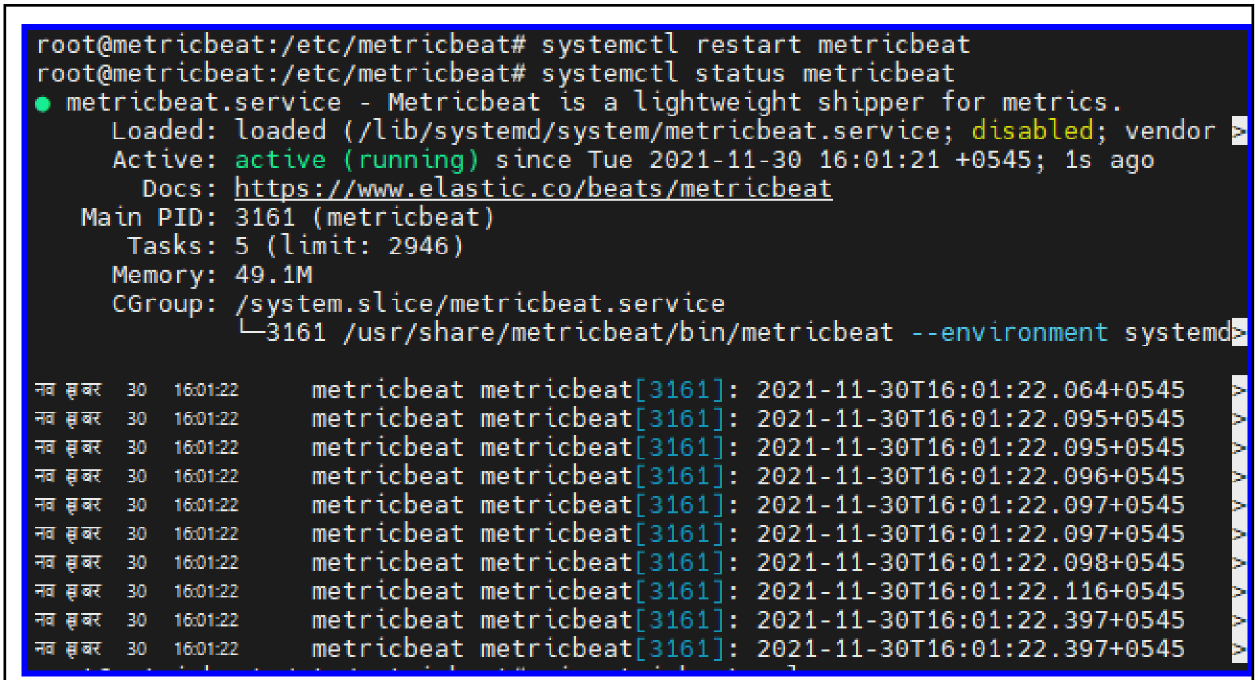
vi /etc/metricbeat/metricbeat.yml



```
#module
metricbeat.modules:
- module: system
  metricsets:
    - load
  enabled: true
  period: 5s
  index: "server1-metrics-load"

- module: system
  metricsets:
    - memory
  enabled: true
  period: 5s
  index: "server1-metrics-memory"

- module: system
  metricsets:
    - fsstat
  enabled: true
  period: 5s
  index: "server1-metrics-fsstat"

output.elasticsearch:
  hosts: ["192.168.1.93:9200"]
  username: "elastic"
  password: "123456"
  #index: "server1-metrics"

setup.ilm.enabled: false
setup.template.name: "server1-template"
setup.template.pattern: "server1-temp-pattern"

processors:
  - add_host_metadata: ~
~
```

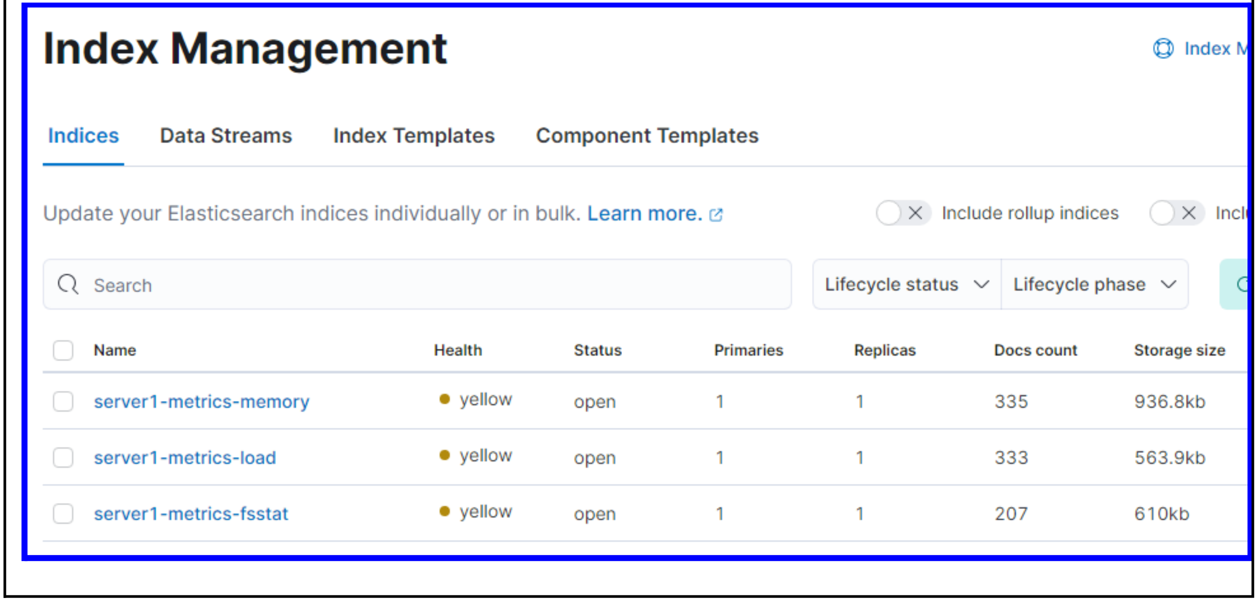
Starting metricbeat

systemctl start metricbeat



```
root@metricbeat:/etc/metricbeat# systemctl restart metricbeat
root@metricbeat:/etc/metricbeat# systemctl status metricbeat
● metricbeat.service - Metricbeat is a lightweight shipper for metrics.
     Loaded: loaded (/lib/systemd/system/metricbeat.service; disabled; vendor >
     Active: active (running) since Tue 2021-11-30 16:01:21 +0545; 1s ago
       Docs: https://www.elastic.co/beats/metricbeat
   Main PID: 3161 (metricbeat)
      Tasks: 5 (limit: 2946)
     Memory: 49.1M
     CGroup: /system.slice/metricbeat.service
             └─3161 /usr/share/metricbeat/bin/metricbeat --environment systemd>

नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.064+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.095+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.095+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.096+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.097+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.097+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.098+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.116+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.397+0545  >
नव ह्बर  30  16:01:22     metricbeat metricbeat[3161]: 2021-11-30T16:01:22.397+0545  >
```

Index management in kibana



Index Management

Update your Elasticsearch indices individually or in bulk. Learn more.

□	Name	Health	Status	Primaries	Replicas	Docs count	Storage size
□	server1-metrics-memory	● yellow	open	1	1	335	936.8kb
□	server1-metrics-load	● yellow	open	1	1	333	563.9kb
□	server1-metrics-fsstat	● yellow	open	1	1	207	610kb

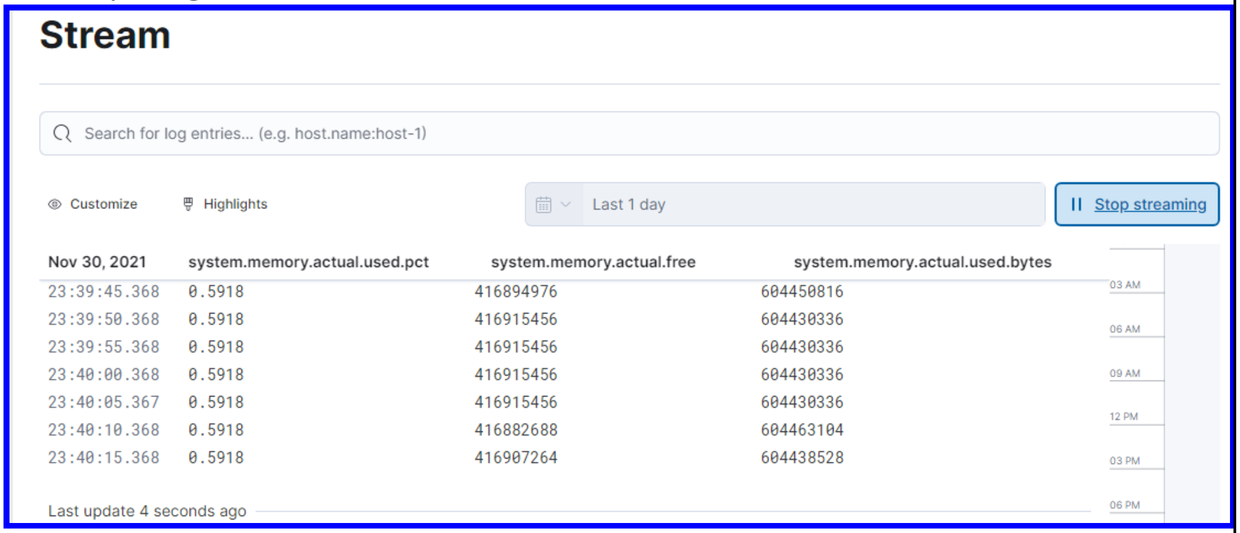
Collect metric from following sources in server1 and send them to elasticsearch. Store them in an index named "server1-metrics". a. Memory usage b. Disk usage c. Load average

To get the metrics,

Logs >> stream >> live Stream

(and configure setting according to the metrics we need)

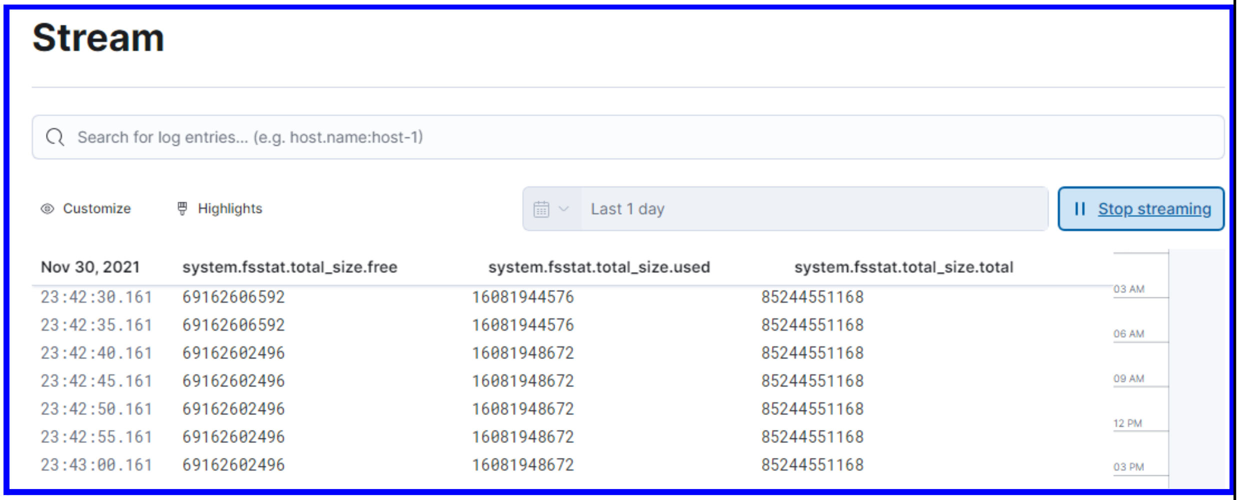
Memory usage



Nov 30, 2021	system.memory.actual.used.pct	system.memory.actual.free	system.memory.actual.used.bytes
23:39:45.368	0.5918	416894976	604450816
23:39:50.368	0.5918	416915456	604430336
23:39:55.368	0.5918	416915456	604430336
23:40:00.368	0.5918	416915456	604430336
23:40:05.367	0.5918	416915456	604430336
23:40:10.368	0.5918	416882688	604463104
23:40:15.368	0.5918	416907264	604438528

The above shown metrics is shown from the live stream.
*We have columns of **actual.used.pct, actual.free & actual.used** for **memory***

Disk Usage



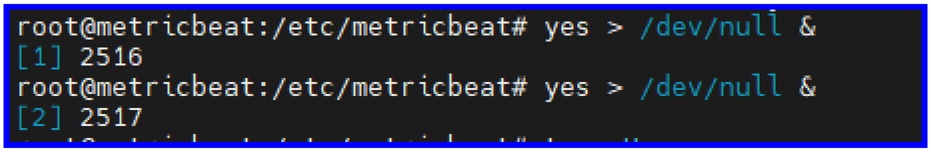
Nov 30, 2021	system.fsstat.total_size.free	system.fsstat.total_size.used	system.fsstat.total_size.total
23:42:30.161	69162606592	16081944576	85244551168
23:42:35.161	69162606592	16081944576	85244551168
23:42:40.161	69162602496	16081948672	85244551168
23:42:45.161	69162602496	16081948672	85244551168
23:42:50.161	69162602496	16081948672	85244551168
23:42:55.161	69162602496	16081948672	85244551168
23:43:00.161	69162602496	16081948672	85244551168

The above shown metrics is shown from the live stream.

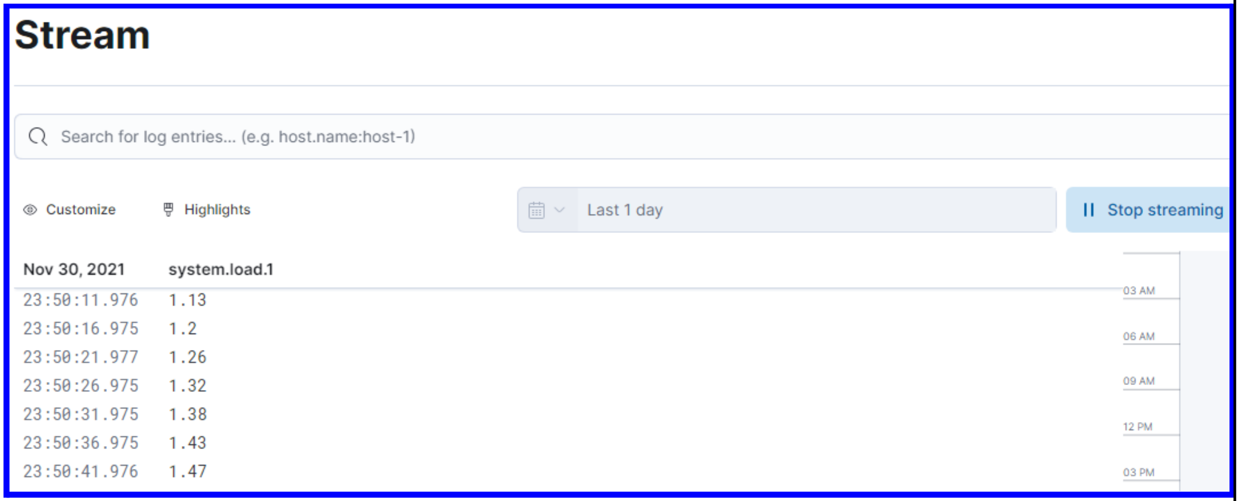
*We have columns of **total.size.free, total.size.used & total.size.total** for **fsstat***

Load

I have run 2 yes command to increase the load of metricbeat server



```
root@metricbeat:/etc/metricbeat# yes > /dev/null &
[1] 2516
root@metricbeat:/etc/metricbeat# yes > /dev/null &
[2] 2517
```



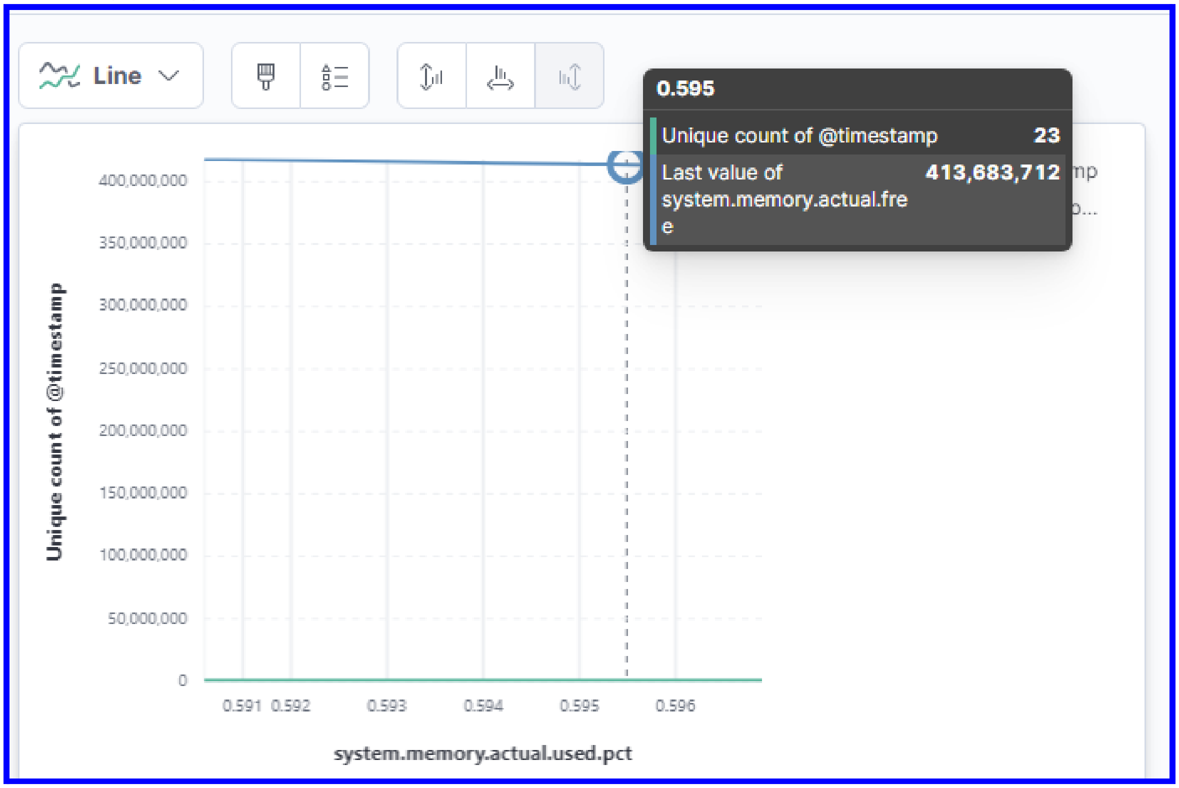
```
Nov 30, 2021    system.load.1
23:50:11.976    1.13
23:50:16.975    1.2
23:50:21.977    1.26
23:50:26.975    1.32
23:50:31.975    1.38
23:50:36.975    1.43
23:50:41.976    1.47
```

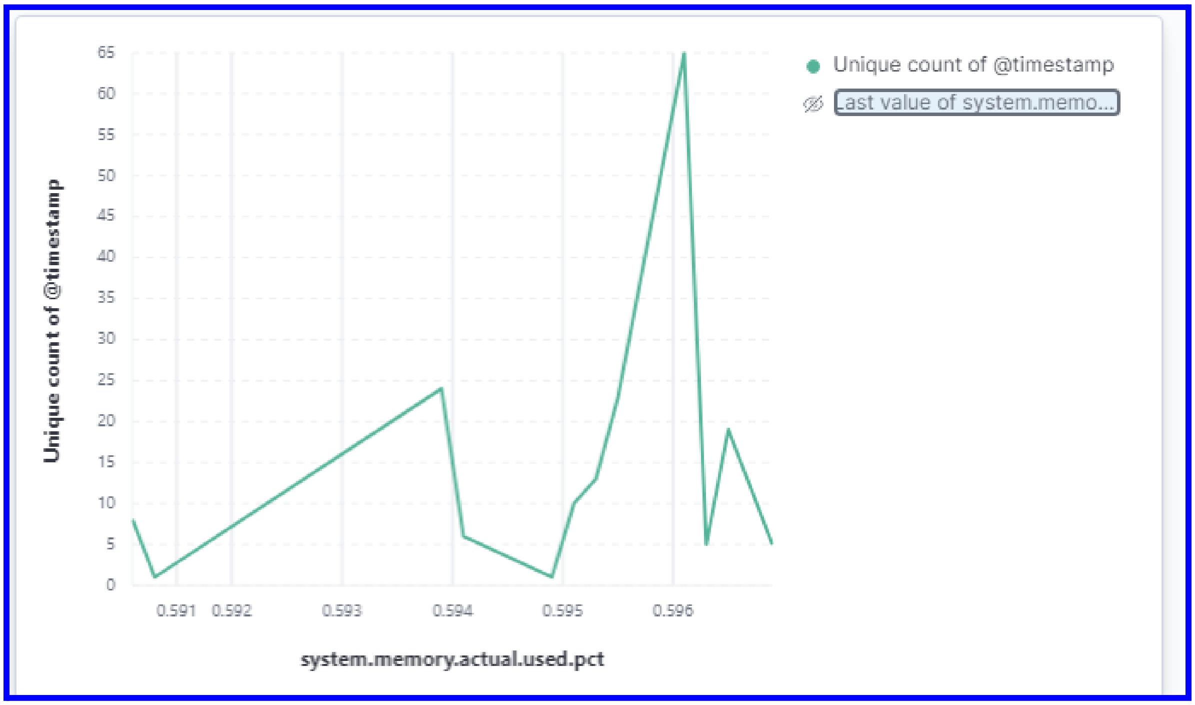
We can see it has recorded the increasing load metric

We have columns of ***system.load.1*** *for* ***load***

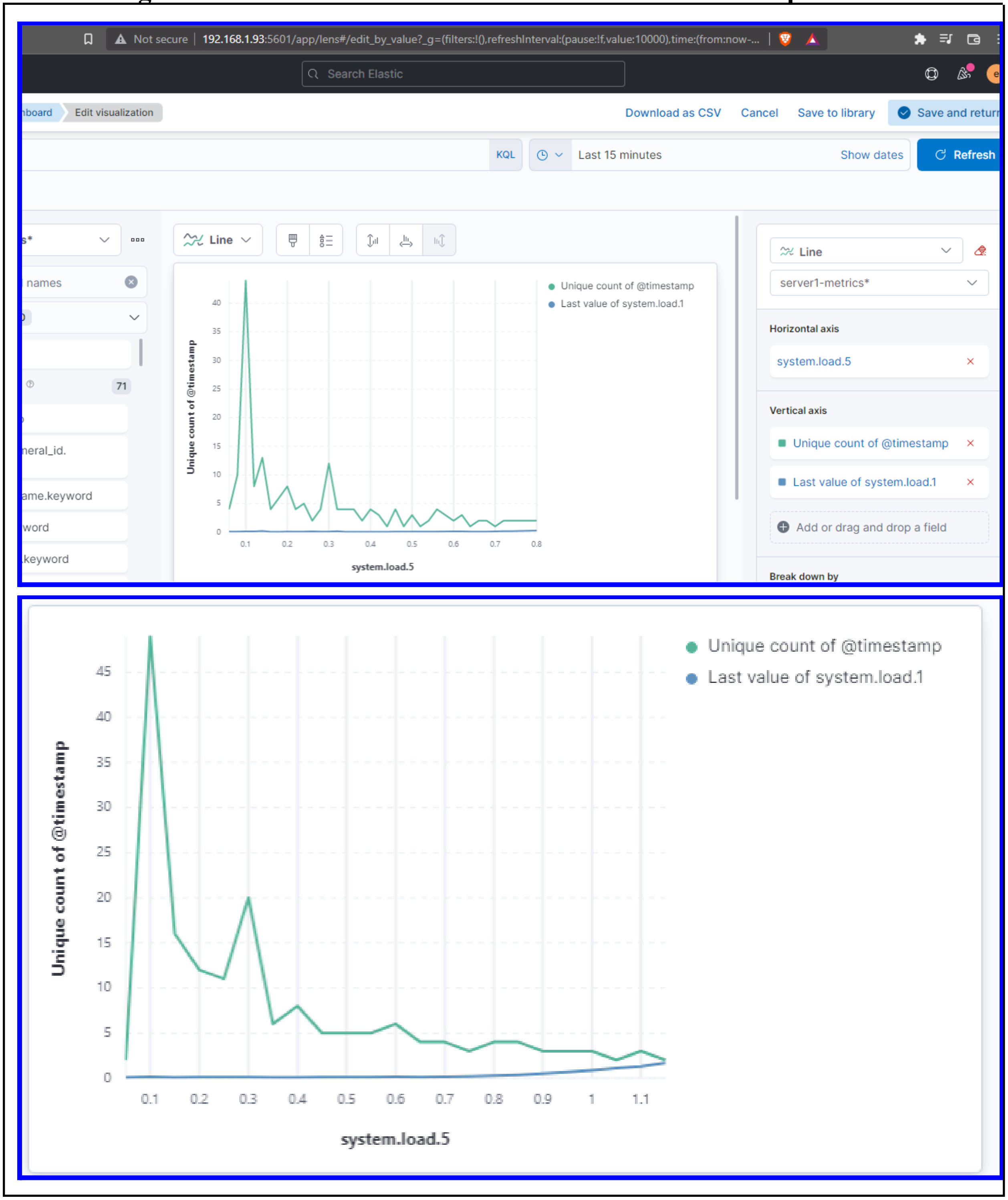
1. **Create a dashboard in kibana and generate visual report(line graph) for Memory usage and load average of server1 with relation to time**

Memory usage vs timestamp


Line
0.595
Unique count of @timestamp 23
Last value of system.memory.actual.free 413,683,712
400,000,000
350,000,000
300,000,000
250,000,000
200,000,000
150,000,000
100,000,000
50,000,000
0
Unique count of @timestamp
0.591
0.592
0.593
0.594
0.595
0.596
system.memory.actual.used.pct


65
60
55
50
45
40
35
30
25
20
15
10
5
0
Unique count of @timestamp
0.591
0.592
0.593
0.594
0.595
0.596
system.memory.actual.used.pct
● Unique count of @timestamp
Last value of system.memo...

Load average in 5 mins and load in 1 minutes value with timestamp



Not secure | 192.168.1.93:5601/app/lens#/edit_by_value?_g=(filters:!(),refreshInterval:(pause:!f,value:10000),time:(from:now-...

Last 15 minutes

Line

server1-metrics*

Horizontal axis

system.load.5

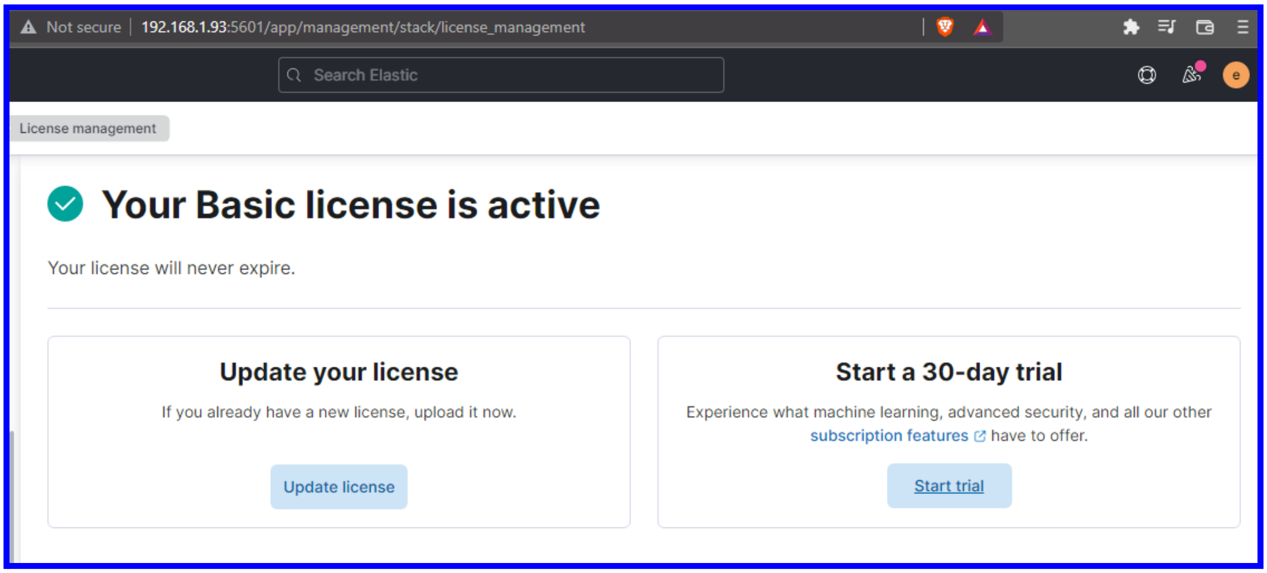
Vertical axis

Unique count of @timestamp

Last value of system.load.1

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

To enable alerts, we should have subscribed version



Not secure | 192.168.1.93:5601/app/management/stack/license_management

Search Elastic

License management

Your Basic license is active

Your license will never expire.

Update your license

If you already have a new license, upload it now.

Update license

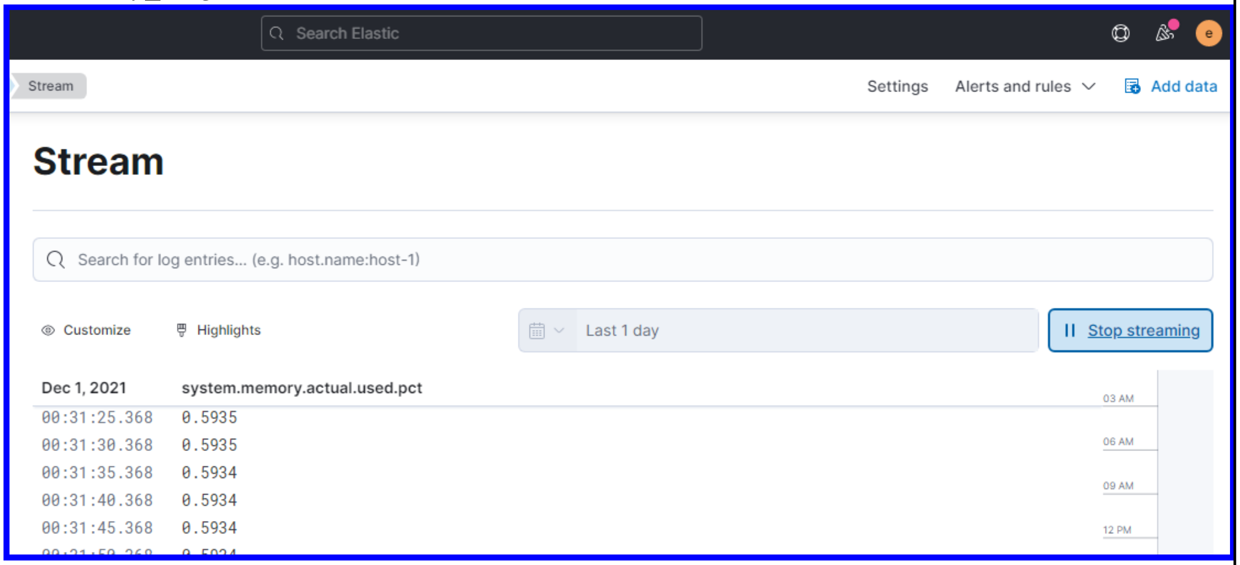
Start a 30-day trial

Experience what machine learning, advanced security, and all our other subscription features have to offer.

Start trial

Enabled 30-day trial

For memory_usage



Search Elastic

Stream

Settings | Alerts and rules | Add data

Stream

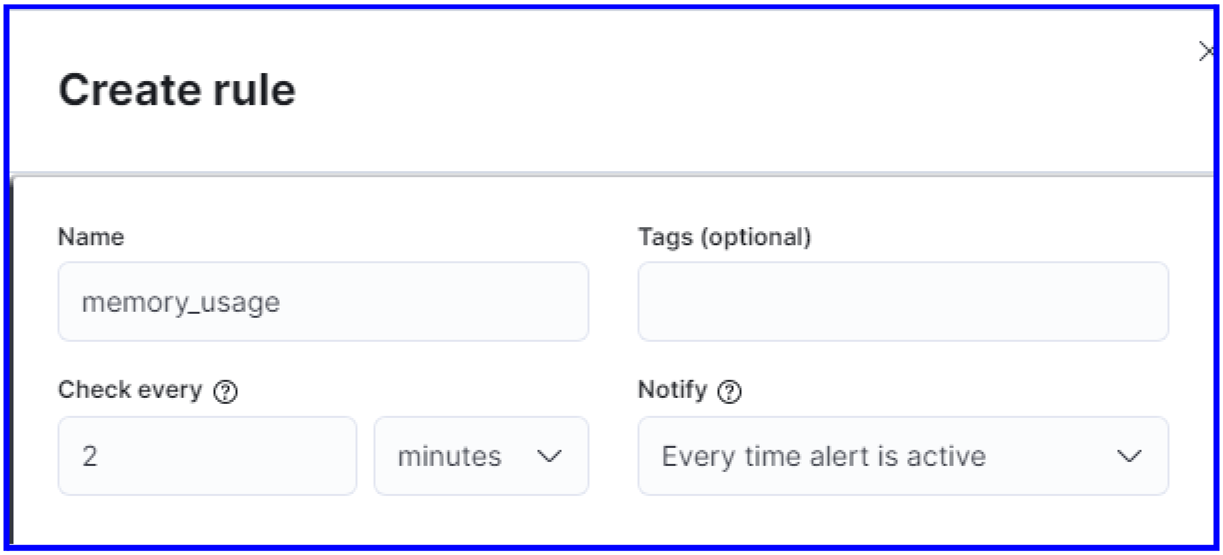
Search for log entries... (e.g. host.name:host-1)

Customize | Highlights | Last 1 day | Stop streaming

```
Dec 1, 2021    system.memory.actual.used.pct
00:31:25.368   0.5935
00:31:30.368   0.5935
00:31:35.368   0.5934
00:31:40.368   0.5934
00:31:45.368   0.5934
```

To generate alert, click on top left corner - (alert and rules)

For memory Usage



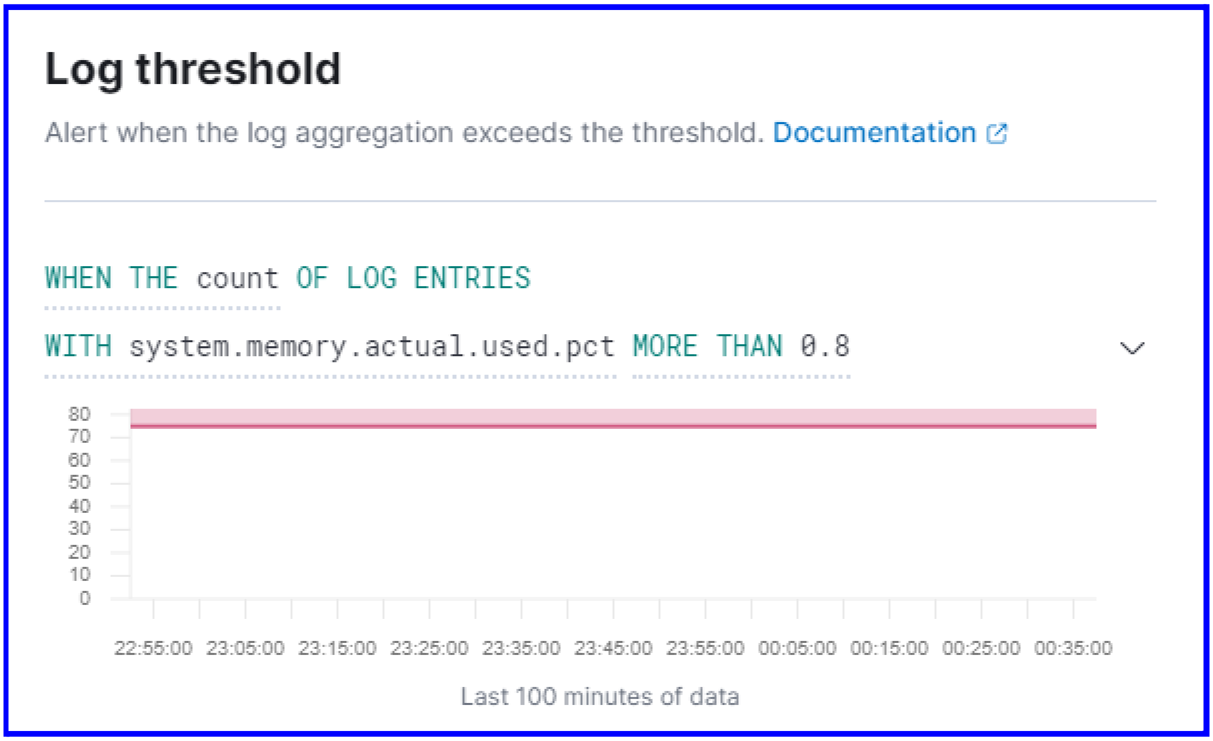
Create rule

Name: memory_usage

Tags (optional):

Check every: 2 minutes

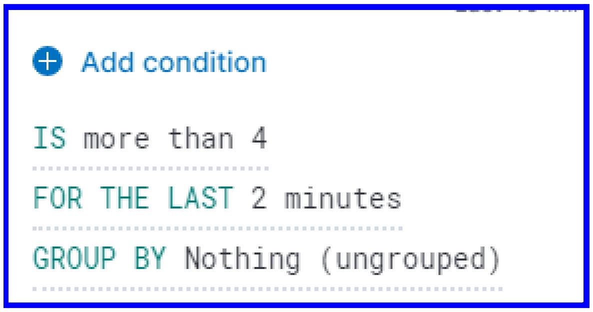
Notify: Every time alert is active



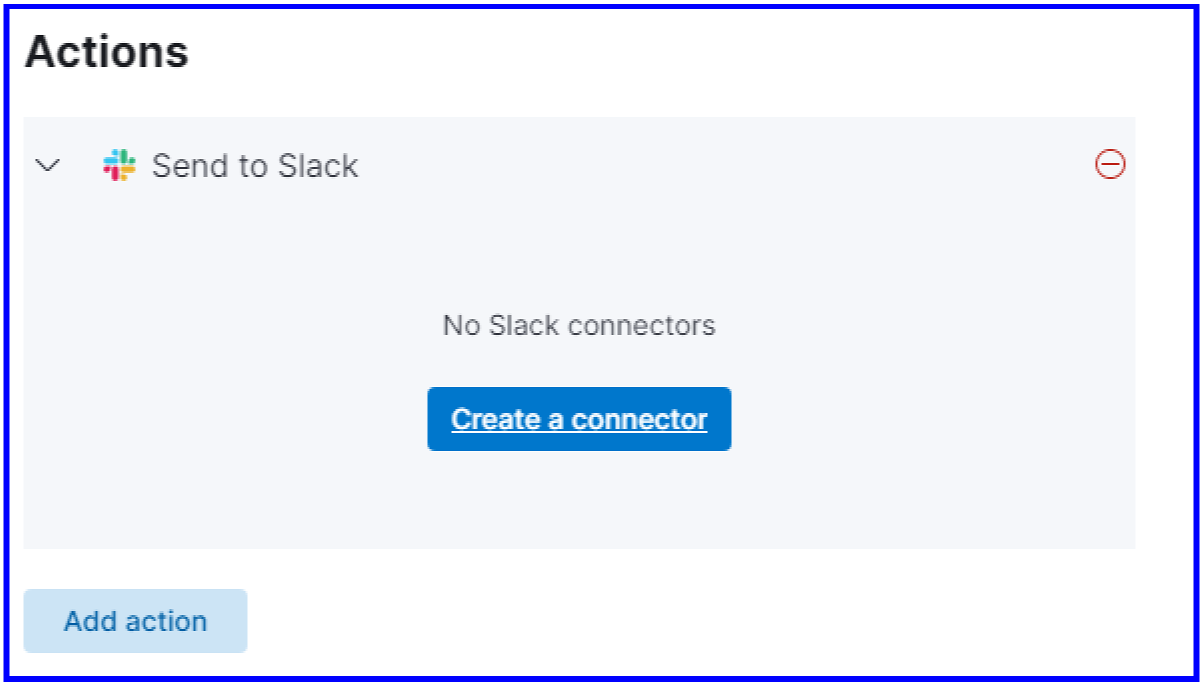
Log threshold

Alert when the log aggregation exceeds the threshold. Documentation

```
WHEN THE count OF LOG ENTRIES
WITH system.memory.actual.used.pct MORE THAN 0.8
```



```
IS more than 4
FOR THE LAST 2 minutes
GROUP BY Nothing (ungrouped)
```

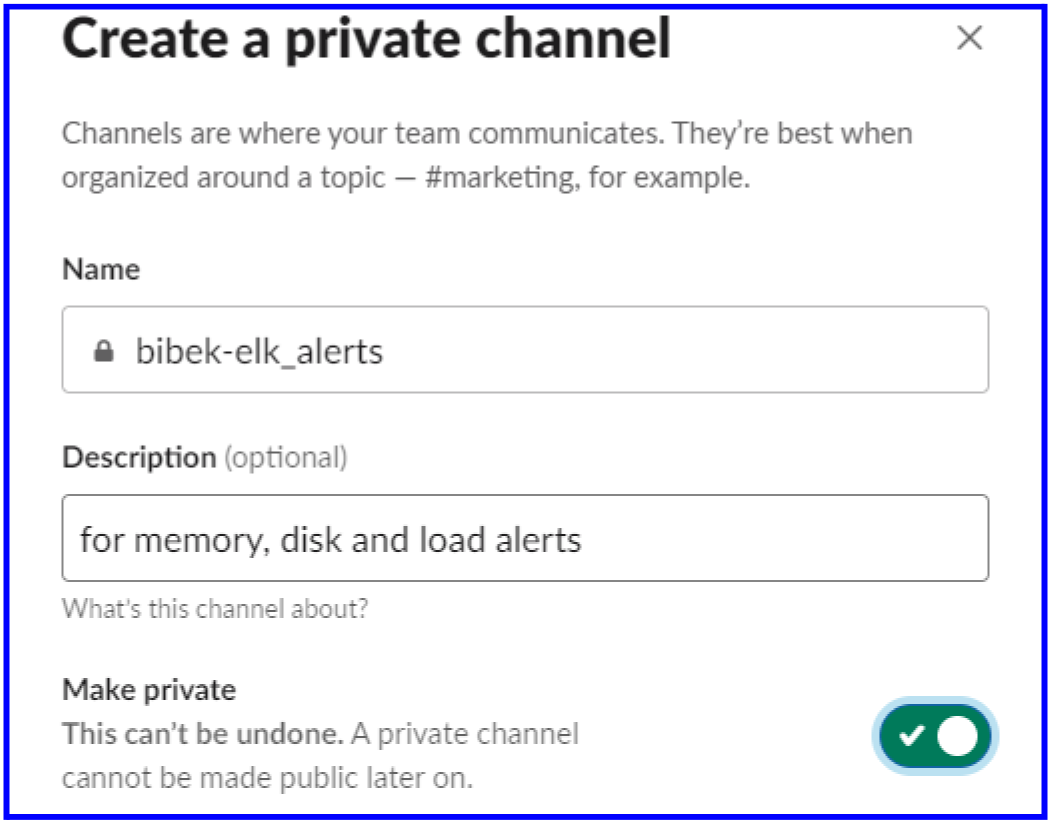


Actions

Send to Slack

No Slack connectors

Creating a slack channel



Create a private channel

Channels are where your team communicates. They're best when organized around a topic — #marketing, for example.

Name: bibek-elk_alerts

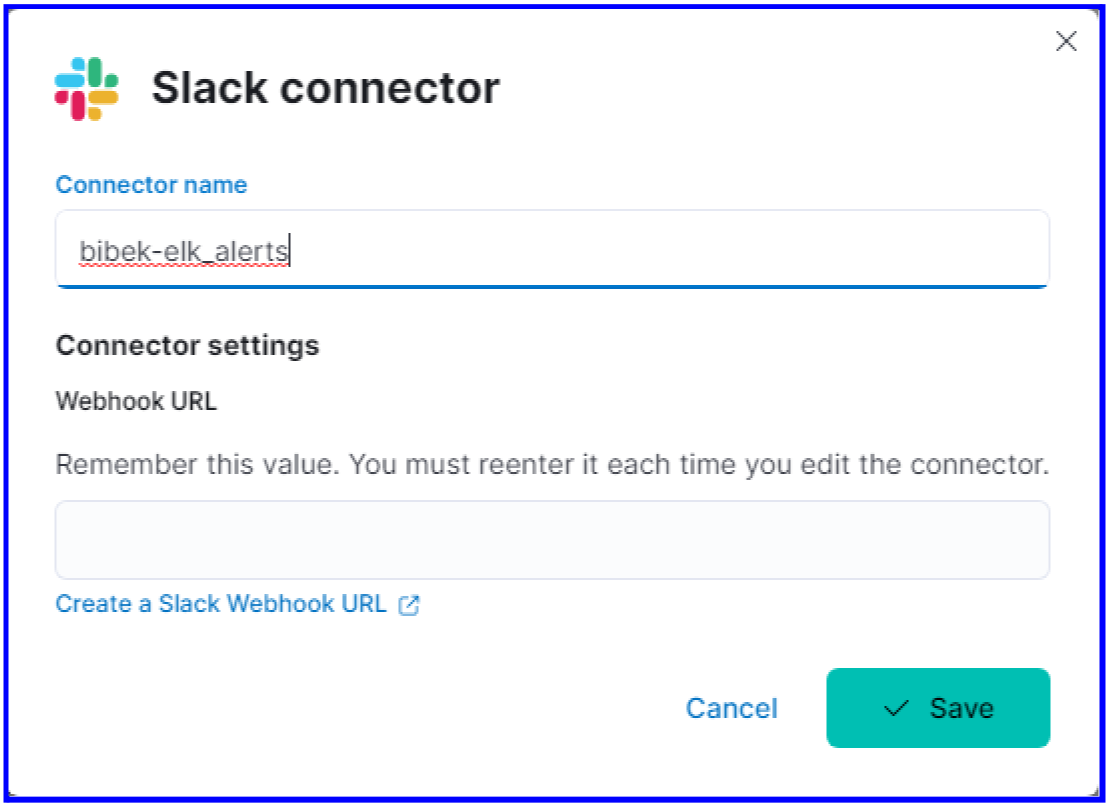
Description (optional): for memory, disk and load alerts

What's this channel about?

Make private ✓

This can't be undone. A private channel cannot be made public later on.

Creating a slack web-hook url



Slack connector

Connector name

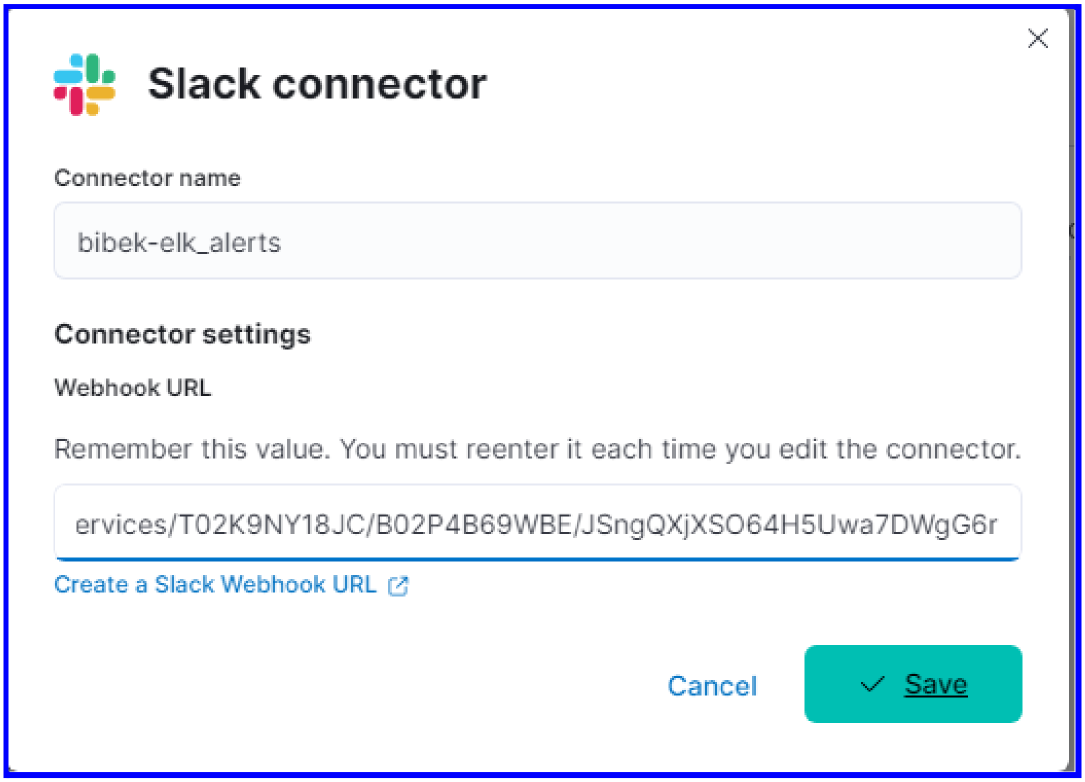
bibek-elk_alerts

Connector settings

Webhook URL

Remember this value. You must reenter it each time you edit the connector.

Create a Slack Webhook URL



Slack connector

Connector name

bibek-elk_alerts

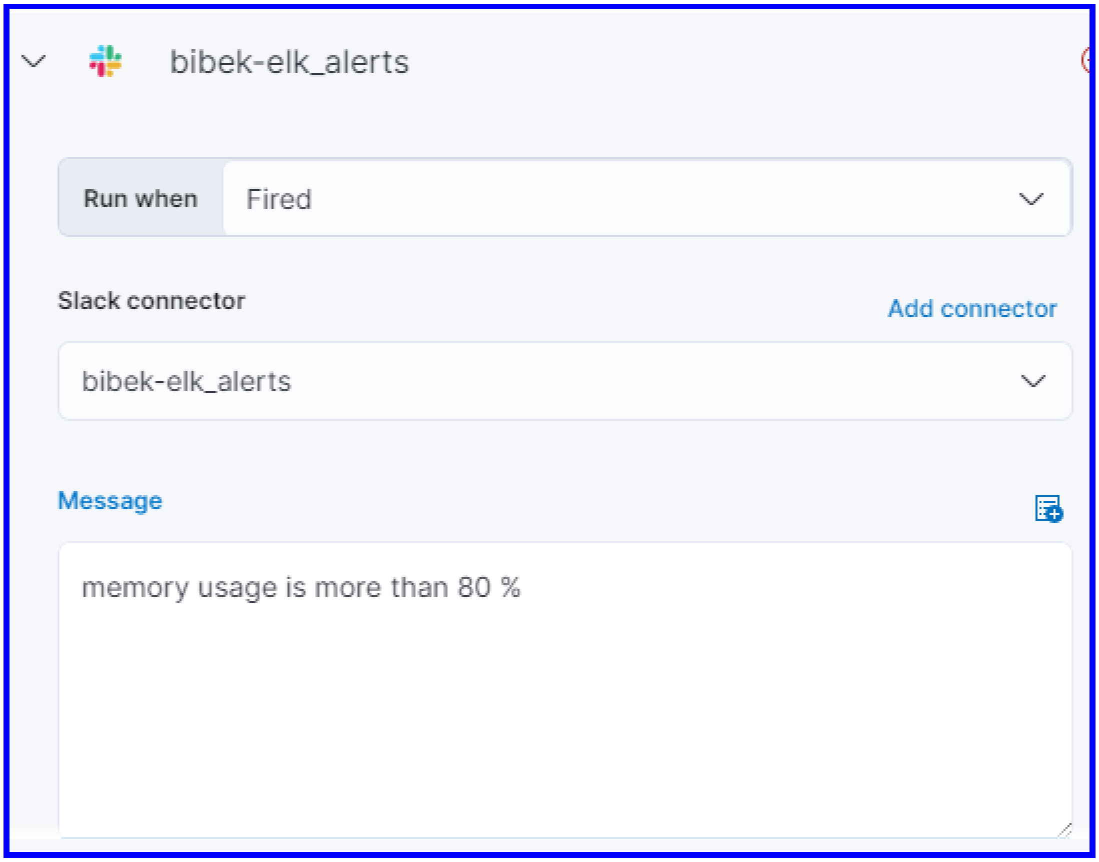
Connector settings

Webhook URL

Remember this value. You must reenter it each time you edit the connector.

ervices/T02K9NY18JC/B02P4B69WBE/JSngQXjXSO64H5Uwa7DWgG6r

Create a Slack Webhook URL



bibek-elk_alerts

Run when: Fired

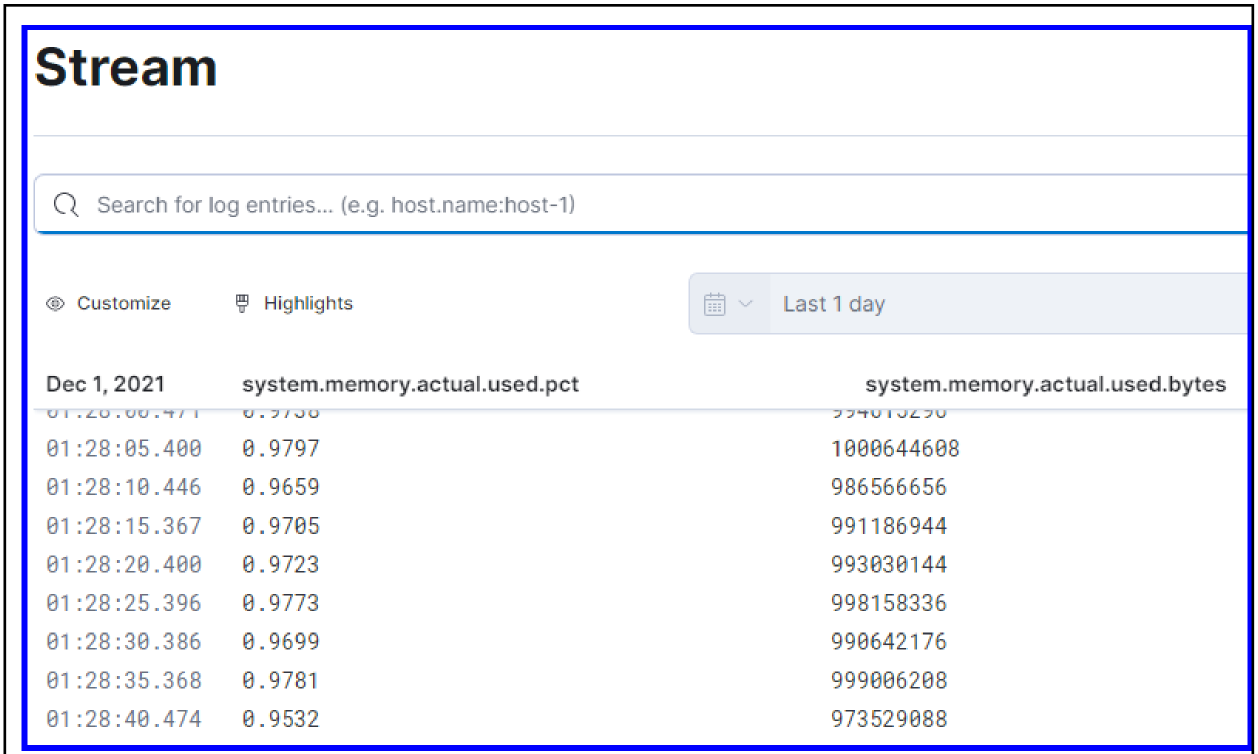
Slack connector: bibek-elk_alerts

Message:

memory usage is more than 80 %

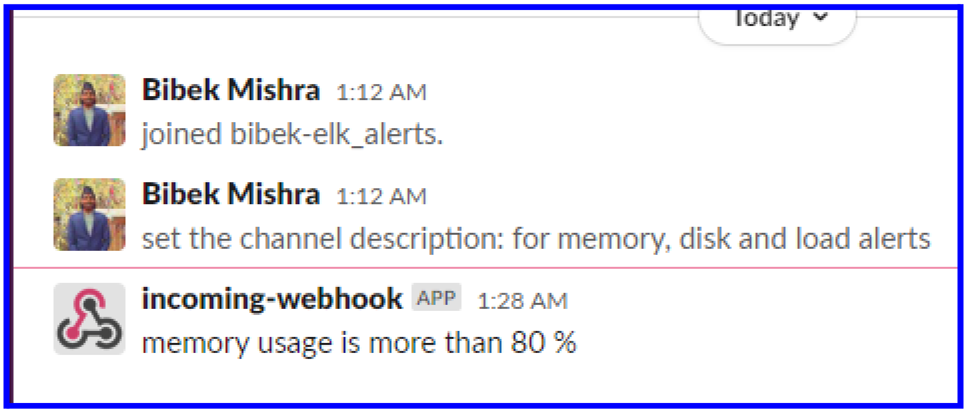
I have used echo {1..100000000} command to increase the ram usage

We can also use tail /dev/zero command



```
Dec 1, 2021    system.memory.actual.used.pct    system.memory.actual.used.bytes
01:28:05.400   0.9797                           1000644608
01:28:10.446   0.9659                           986566656
01:28:15.367   0.9705                           991186944
01:28:20.400   0.9723                           993030144
01:28:25.396   0.9773                           998158336
01:28:30.386   0.9699                           990642176
01:28:35.368   0.9781                           999006208
01:28:40.474   0.9532                           973529088
```

When memory usage reached higher 0.9 i.e 90 %. It alerts with sending a message in slack channel



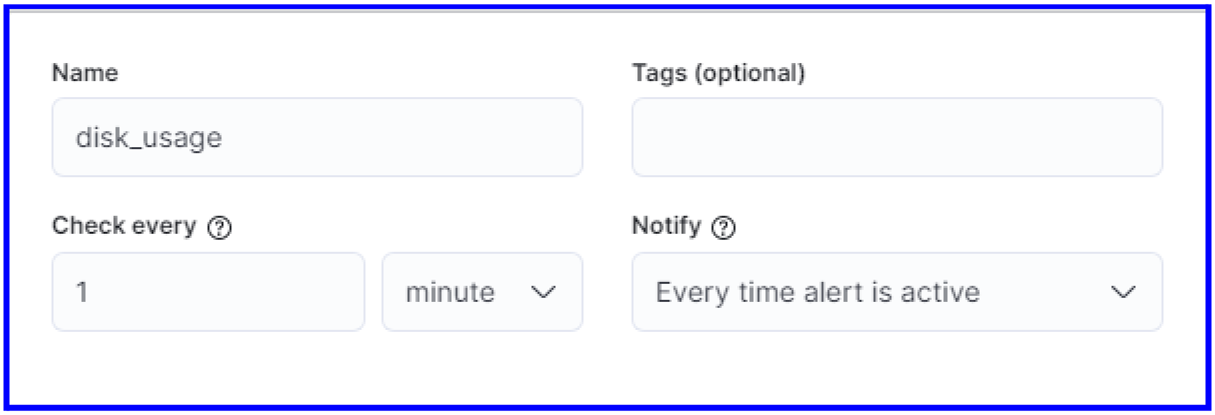
Bibek Mishra 1:12 AM
joined bibek-elk_alerts.

Bibek Mishra 1:12 AM
set the channel description: for memory, disk and load alerts

incoming-webhook APP 1:28 AM
memory usage is more than 80 %

In this way, memory usage alerts can be generated

For Disk Usage

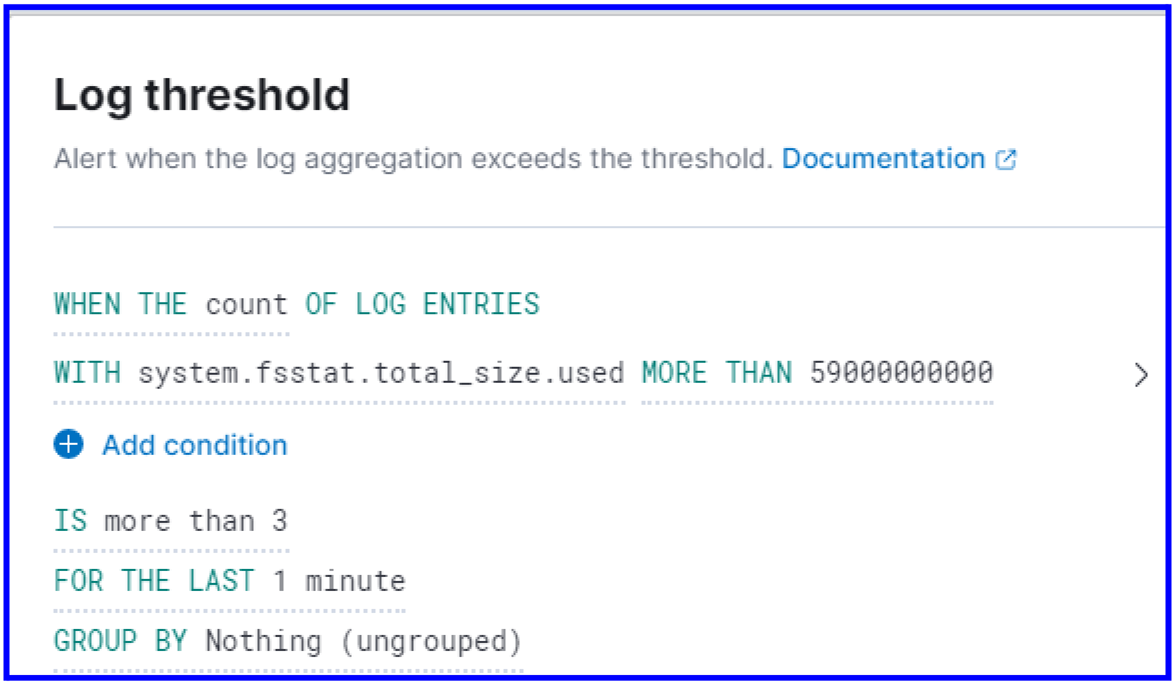


Name: disk_usage

Tags (optional):

Check every: 1 minute

Notify: Every time alert is active

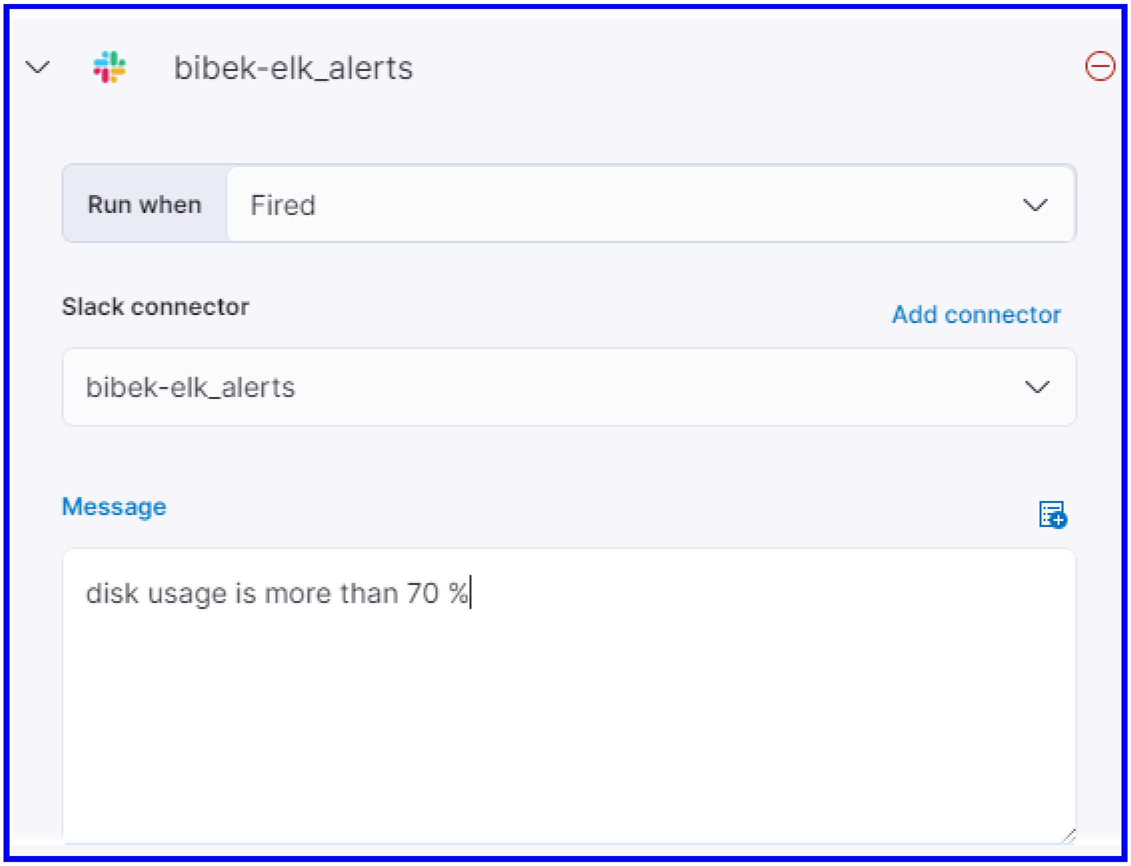


Log threshold

Alert when the log aggregation exceeds the threshold. Documentation

```
WHEN THE count OF LOG ENTRIES
WITH system.fsstat.total_size.used MORE THAN 59000000000
```

```
IS more than 3
FOR THE LAST 1 minute
GROUP BY Nothing (ungrouped)
```



bibek-elk_alerts

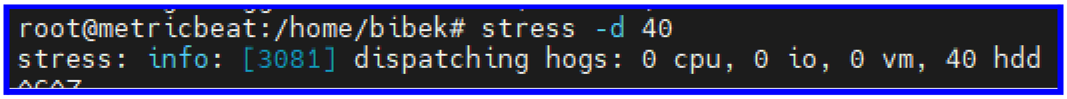
Run when: Fired

Slack connector: bibek-elk_alerts

Message:

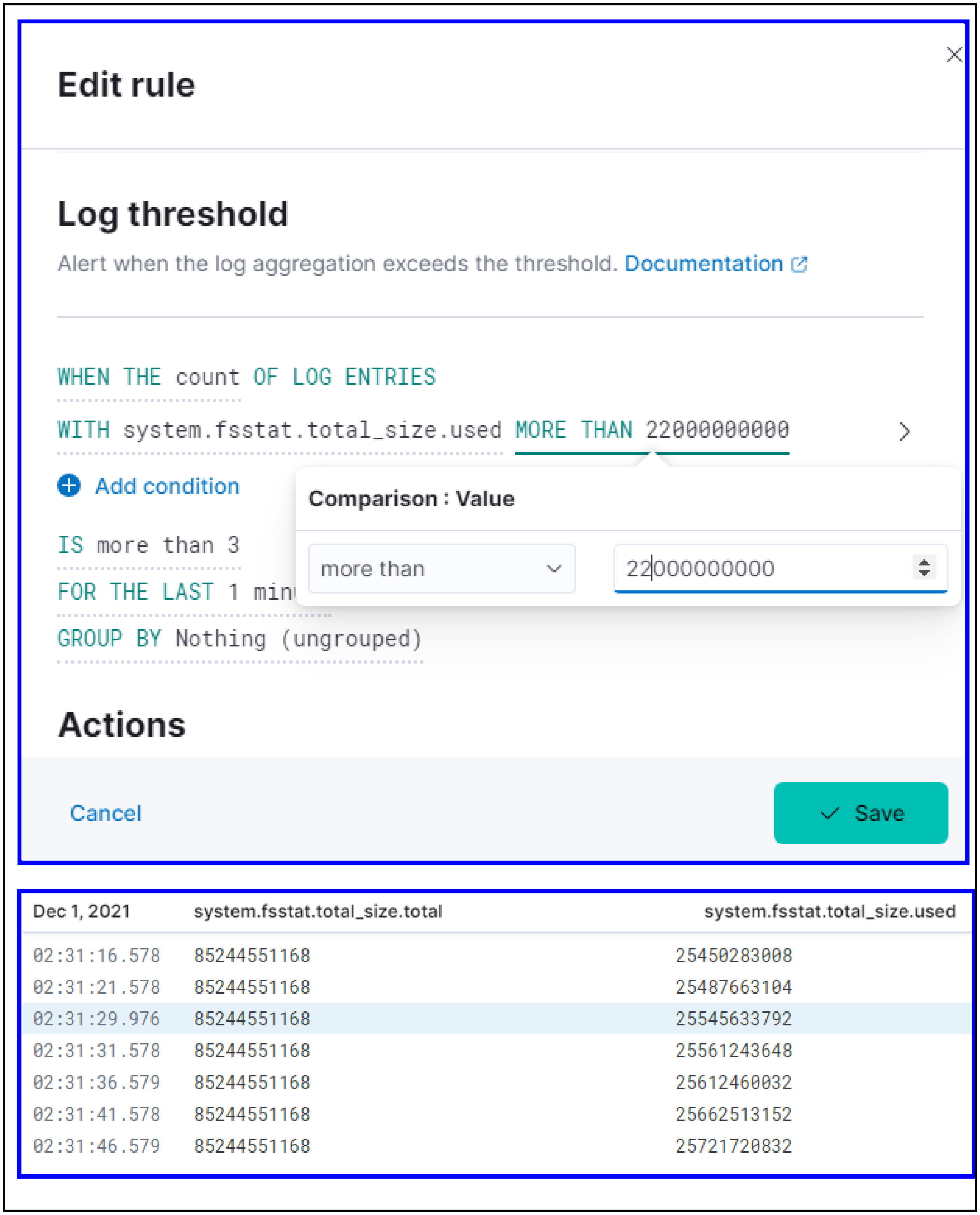
disk usage is more than 70 %

*I installed **stress** package to increase the disk usage*
*And used **stress -d 40 -** To increase disk usage to 70 %*



```
root@metricbeat:/home/bibek# stress -d 40
stress: info: [3081] dispatching hogs: 0 cpu, 0 io, 0 vm, 40 hdd
```

*Since I have used **80 GB HDD** for this VM, 14 GB was already occupied by system files*
***It takes a lot of time to occupy up to 70 %** of the disk through the stress command.*
So I decided to edit the rule and keep up to 22 GB which was already hit by the stress command.



Edit rule

Log threshold

Alert when the log aggregation exceeds the threshold. Documentation

```
WHEN THE count OF LOG ENTRIES
WITH system.fsstat.total_size.used MORE THAN 22000000000
```

Add condition

```
IS more than 3
FOR THE LAST 1 min
GROUP BY Nothing (ungrouped)
```

Comparison : Value

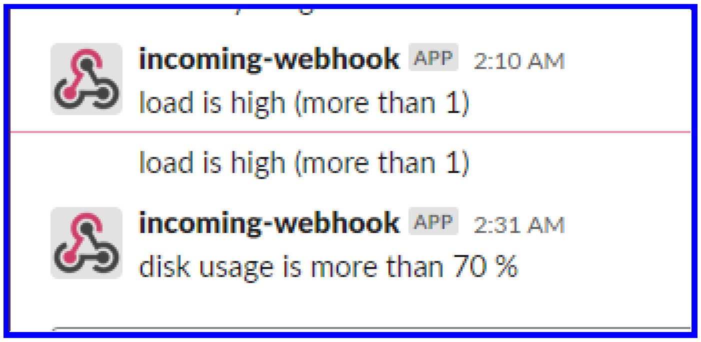
more than ⌄ | 22000000000

Actions

Cancel

✓ Save

Dec 1, 2021	system.fsstat.total_size.total	system.fsstat.total_size.used
02:31:16.578	85244551168	25450283008
02:31:21.578	85244551168	25487663104
02:31:29.976	85244551168	25545633792
02:31:31.578	85244551168	25561243648
02:31:36.579	85244551168	25612460032
02:31:41.578	85244551168	25662513152
02:31:46.579	85244551168	25721720832



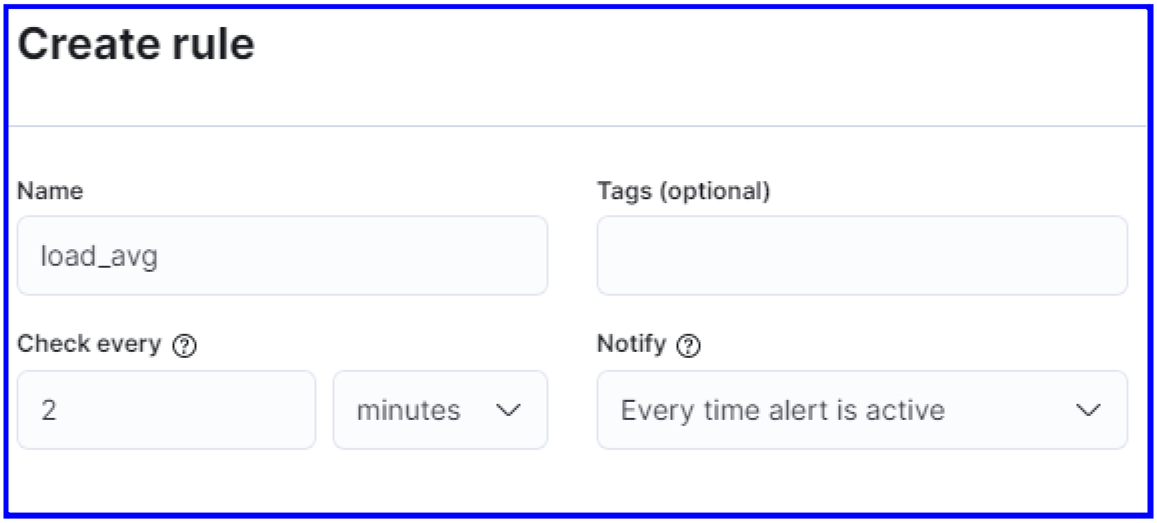
incoming-webhook APP 2:10 AM
load is high (more than 1)

load is high (more than 1)

incoming-webhook APP 2:31 AM
disk usage is more than 70 %

In this way, disk usage alerts can be generated.

For load



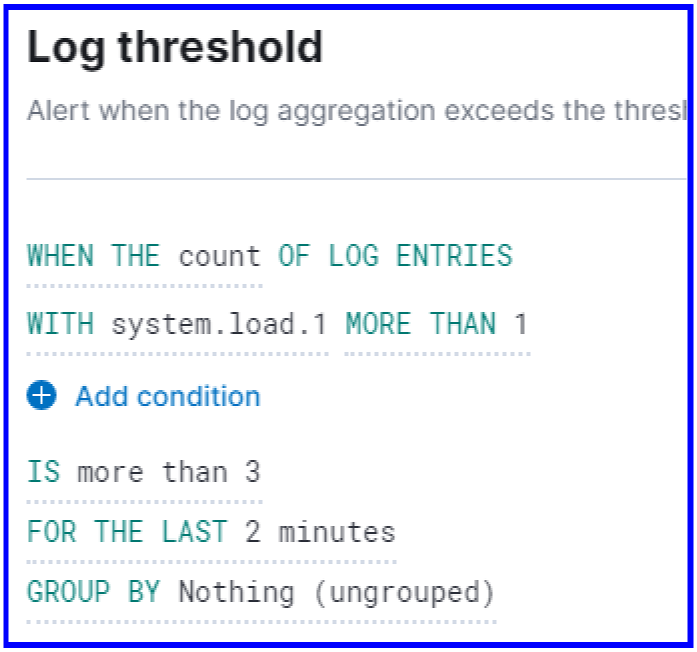
Create rule

Name: load_avg

Tags (optional):

Check every: 2 minutes

Notify: Every time alert is active



Log threshold

Alert when the log aggregation exceeds the thresl

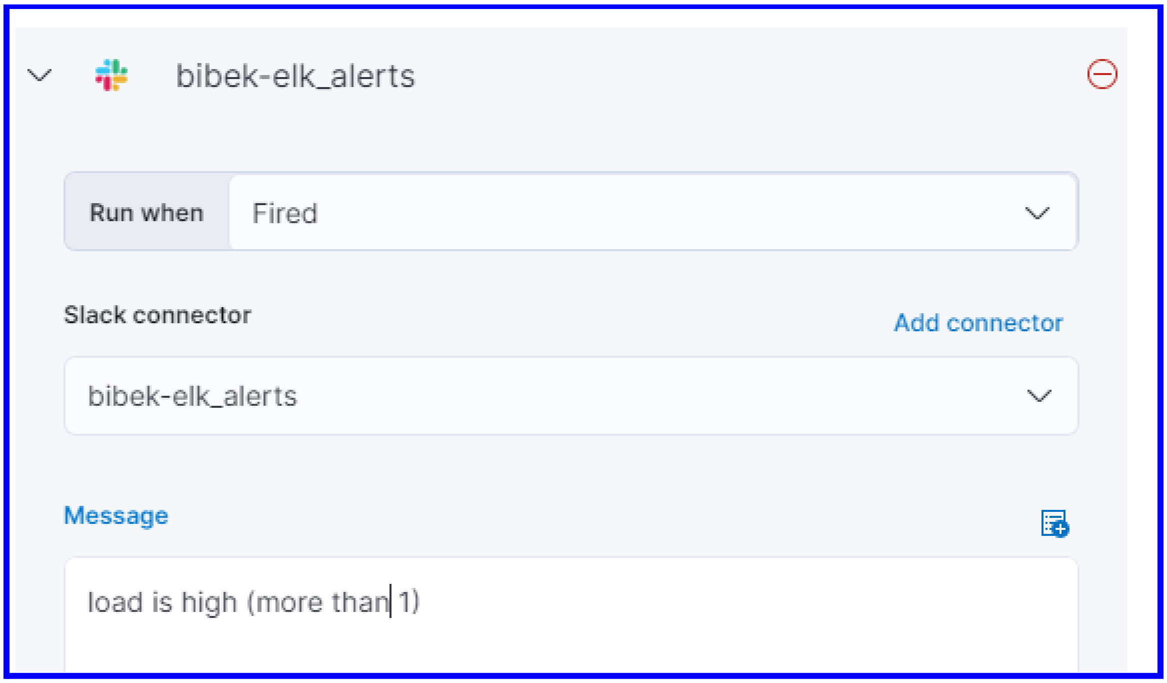
WHEN THE count OF LOG ENTRIES

WITH system.load.1 MORE THAN 1

IS more than 3

FOR THE LAST 2 minutes

GROUP BY Nothing (ungrouped)



bibek-elk_alerts

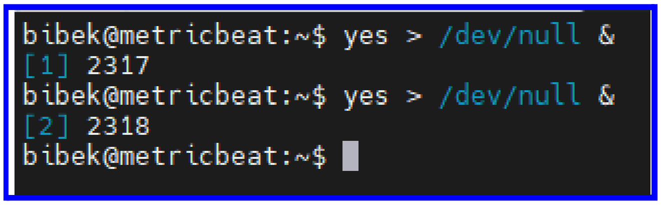
Run when: Fired

Slack connector: bibek-elk_alerts

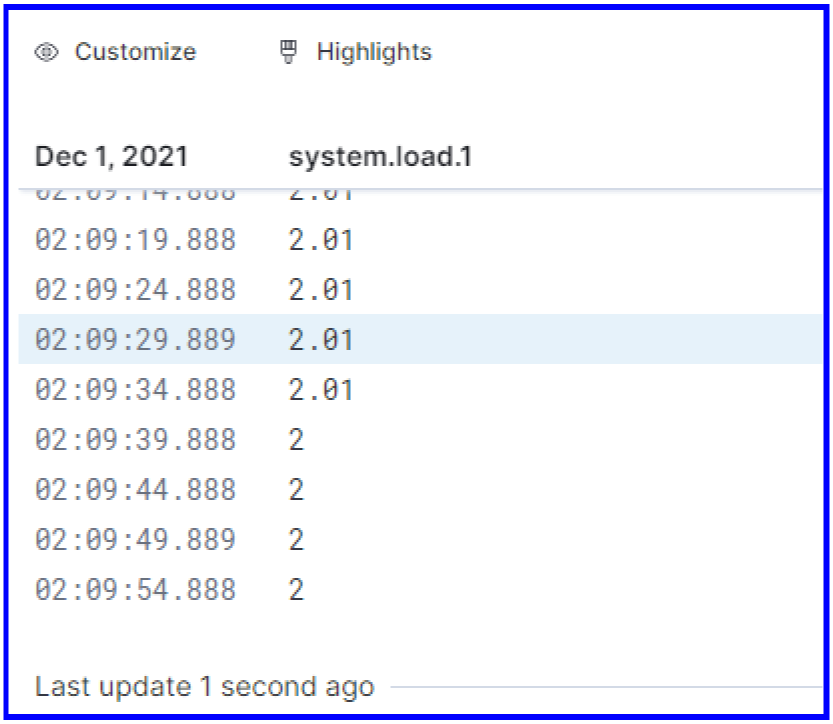
Message

load is high (more than 1)

*I used **yes command** <u>to increase the load of the system</u>*

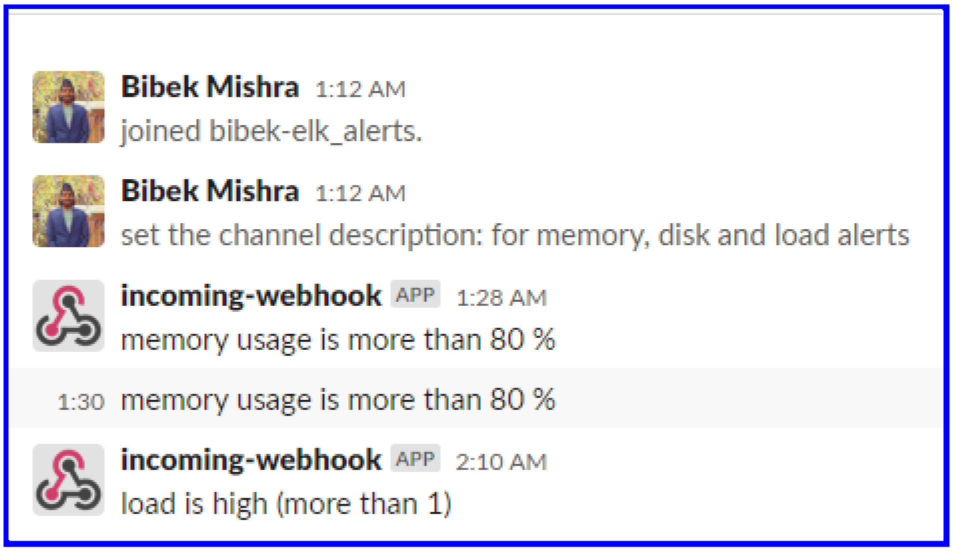


```
bibek@metricbeat:~$ yes > /dev/null &
[1] 2317
bibek@metricbeat:~$ yes > /dev/null &
[2] 2318
bibek@metricbeat:~$ 
```



Dec 1, 2021	system.load.1
02:09:14.888	2.01
02:09:19.888	2.01
02:09:24.888	2.01
02:09:29.889	2.01
02:09:34.888	2.01
02:09:39.888	2
02:09:44.888	2
02:09:49.889	2
02:09:54.888	2

Last update 1 second ago



Bibek Mishra 1:12 AM
joined bibek-elk_alerts.

Bibek Mishra 1:12 AM
set the channel description: for memory, disk and load alerts

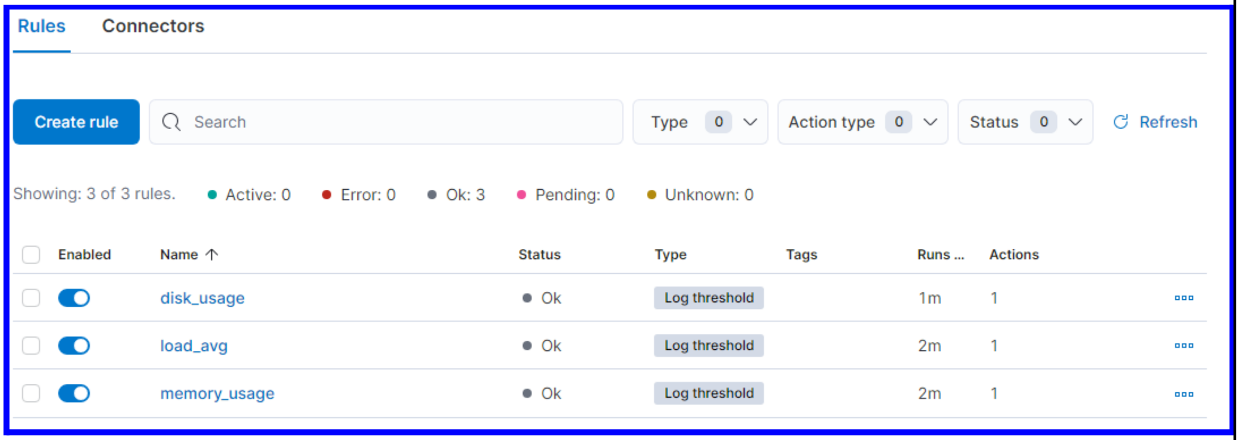
incoming-webhook APP 1:28 AM
memory usage is more than 80 %

1:30 memory usage is more than 80 %

incoming-webhook APP 2:10 AM
load is high (more than 1)

In this way load alerts can be generated.

At last if we see in manage rules, we can have three rules (*Memory, Disk, Load*)



Showing: 3 of 3 rules. ● Active: 0 ● Error: 0 ● Ok: 3 ● Pending: 0 ● Unknown: 0

□	Enabled	Name ↑	Status	Type	Tags	Runs ...	Actions	
□	●	disk_usage	● Ok	Log threshold		1m	1	···
□	●	load_avg	● Ok	Log threshold		2m	1	···
□	●	memory_usage	● Ok	Log threshold		2m	1	···

The rules ***become active*** *when threshold value is reached and sends alerts after successful count for the given time period.*

Thank you !!!