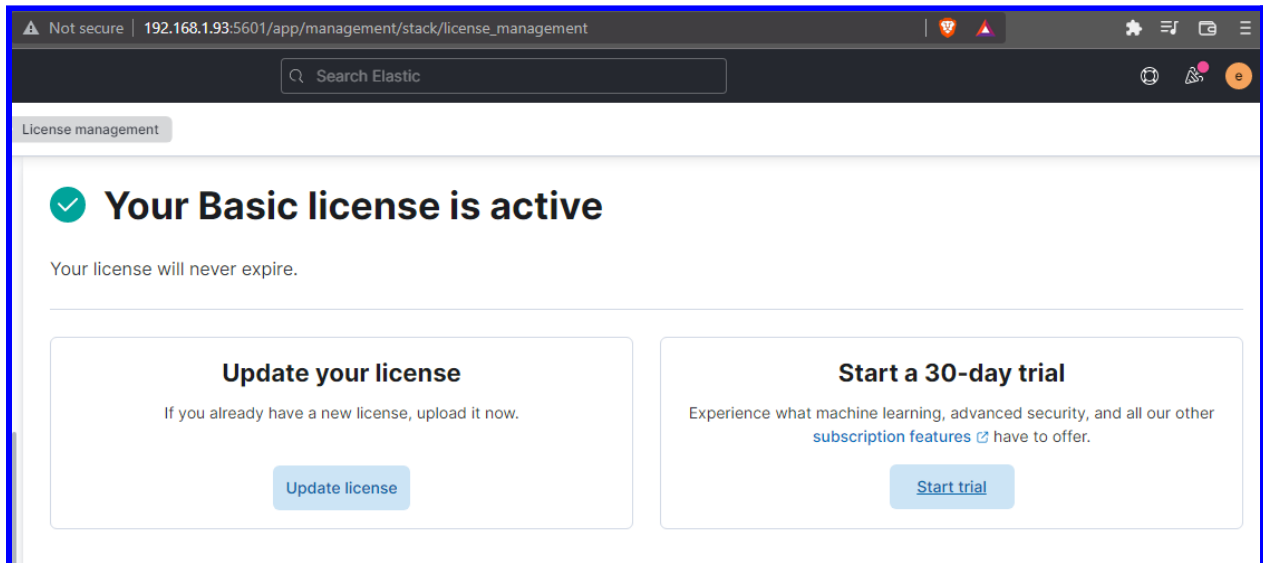
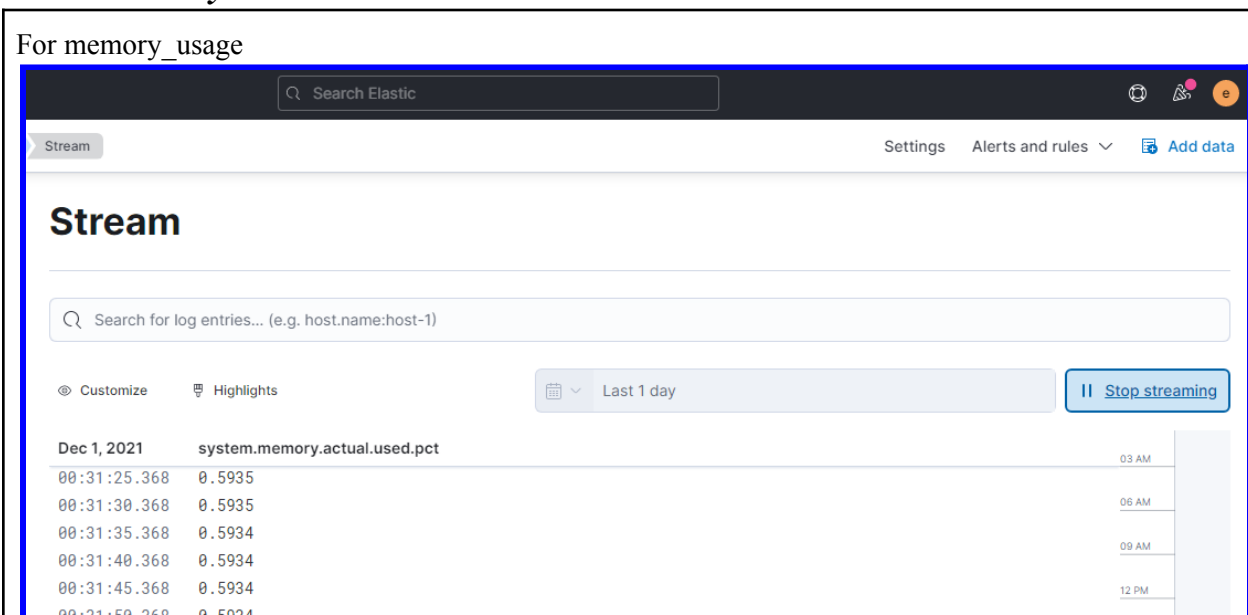


2. Generate alerts through the kibana system for following thresholds a. when memory usage > 80% for the last 2 minutes send an alert to a slack channel b. When Disk usage > 70% send alerts to a slack channel c. When load average > 1 for last 2 minutes send alert to a slack channel

To enable alerts, we should have subscribed version



Enabled 30-day trial



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



Last 100 minutes of data

+ Add condition

IS more than 4

FOR THE LAST 2 minutes

GROUP BY Nothing (ungrouped)

Actions

✓  Send to Slack 

No Slack connectors

[Create a connector](#)

[Add action](#)

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


Connector settings

Webhook URL

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

[Create a Slack Webhook URL](#) 

Cancel ✓ Save


 **Slack connector** ×

Connector name

Connector settings


Webhook URL

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

[Create a Slack Webhook URL](#) 

Cancel ✓ Save

▼

 bibek-elk_alerts

Run when

Fired

▼


Slack connector

Add 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

Stream

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

Customize

Highlights





Last 1 day


Dec 1, 2021	system.memory.actual.used.pct	system.memory.actual.used.bytes
01:28:00.471	0.9758	994013290
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

today ▾

 **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

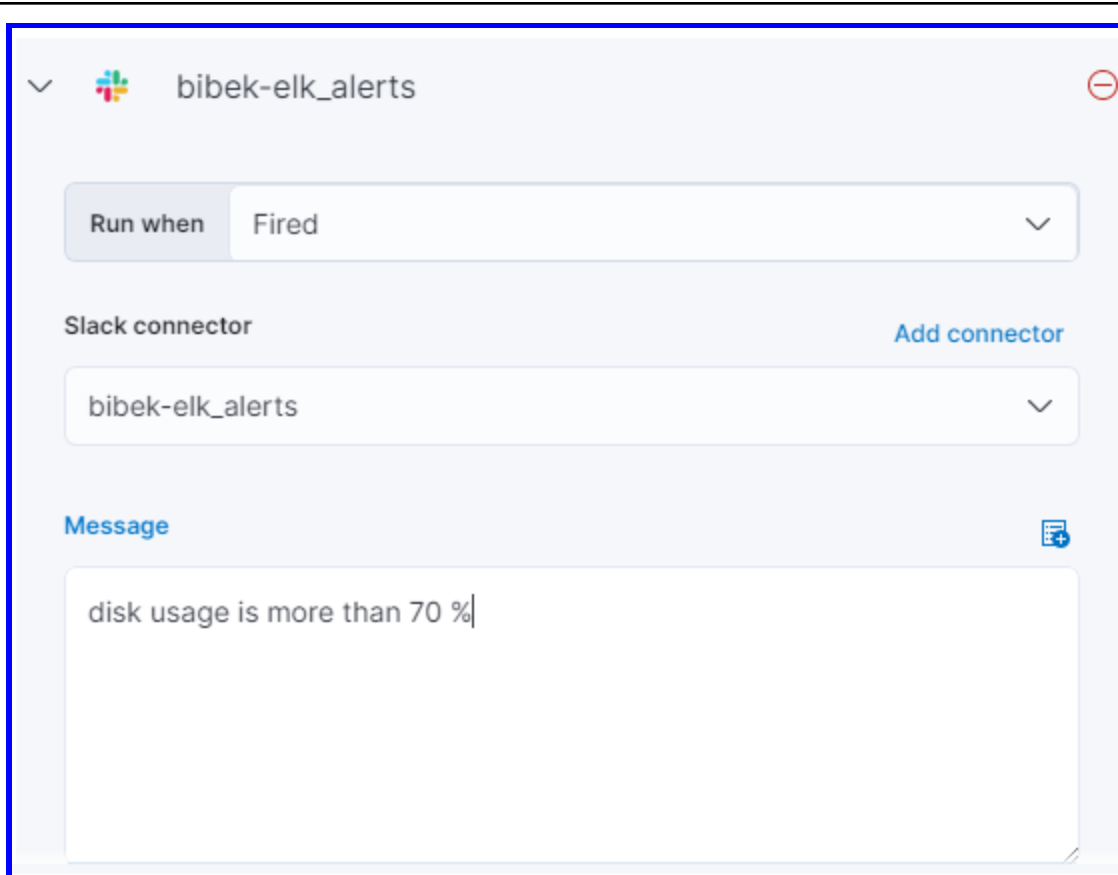
WITH system.fsstat.total_size.used MORE THAN 59000000000 >

 Add condition

IS more than 3

FOR THE LAST 1 minute

GROUP BY Nothing (ungrouped)



▼ bibek-elk_alerts

Run when: Fired

Slack connector: bibek-elk_alerts [Add connector](#)

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
ACAZ
```

*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 threshold

WHEN THE count OF LOG ENTRIES




WITH system.load.1 MORE THAN 1

[+ Add condition](#)


IS more than 3

FOR THE LAST 2 minutes

GROUP BY Nothing (ungrouped)


  bibek-elk_alerts 


Run when

Fired 

Slack connector

[Add connector](#)

bibek-elk_alerts 

Message 

load is high (more than 1)

*I used **yes command** to increase the load of the system*

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

 Customize

 Highlights

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*)

Rules		Connectors					
Create rule		<input type="text" value="Search"/>		Type 0 ▾	Action type 0 ▾	Status 0 ▾	Refresh
Showing: 3 of 3 rules.		● Active: 0 ● Error: 0 ● Ok: 3 ● Pending: 0 ● Unknown: 0					
<input type="checkbox"/>	Enabled	Name ↑	Status	Type	Tags	Runs ...	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	disk_usage	● Ok	Log threshold		1m	1 ...
<input type="checkbox"/>	<input checked="" type="checkbox"/>	load_avg	● Ok	Log threshold		2m	1 ...
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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 !!!