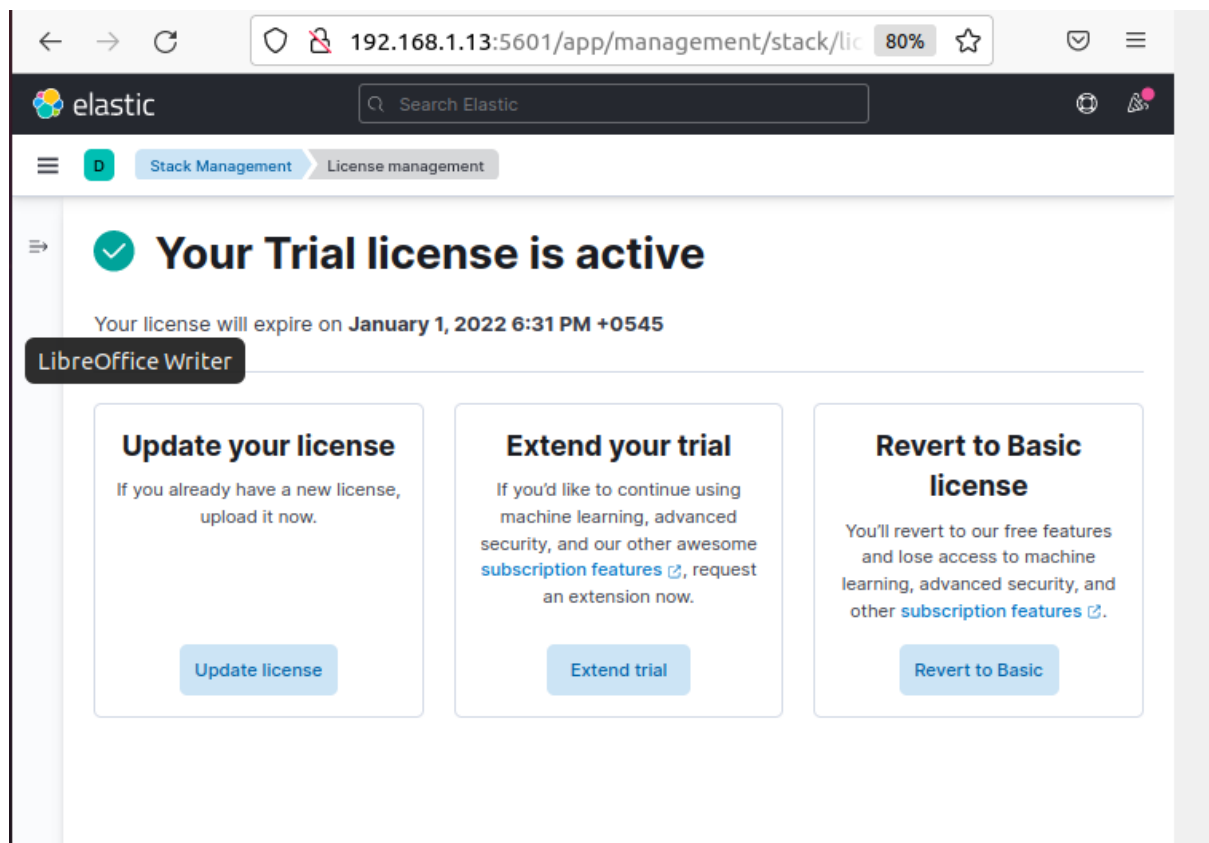


2.

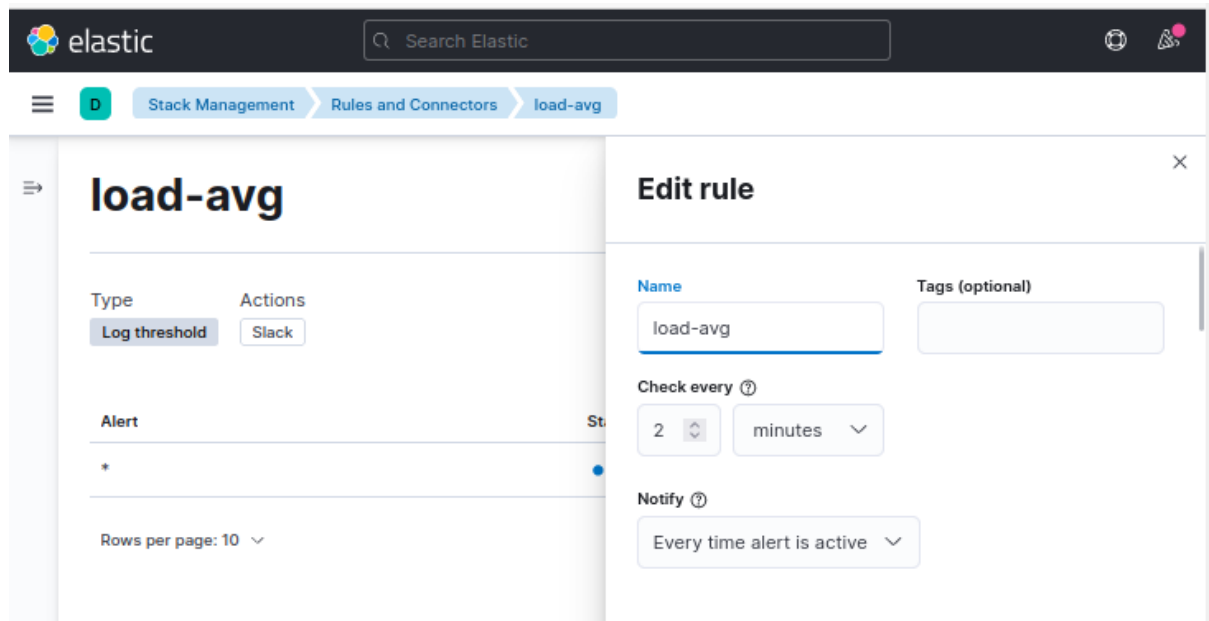
Generate alerts through the kibana system for following thresholds a. when memory usage > 80% for the last 2 minutes send an alert to a slack channel b. When Disk usage > 70% send alerts to a slack channel c. When load average > 1 for the last 2 minutes send an alert to a slack channel.

**Answer:**

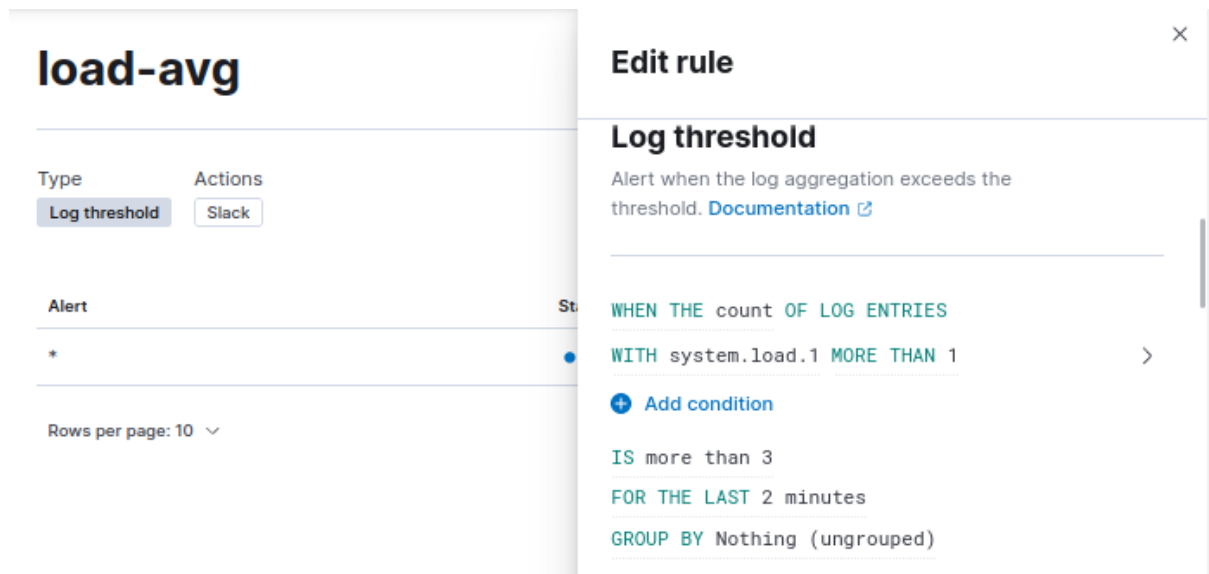
To add alerts, first, we need to activate **Trial license(Free trial for 30 days)** from stack management as follows;



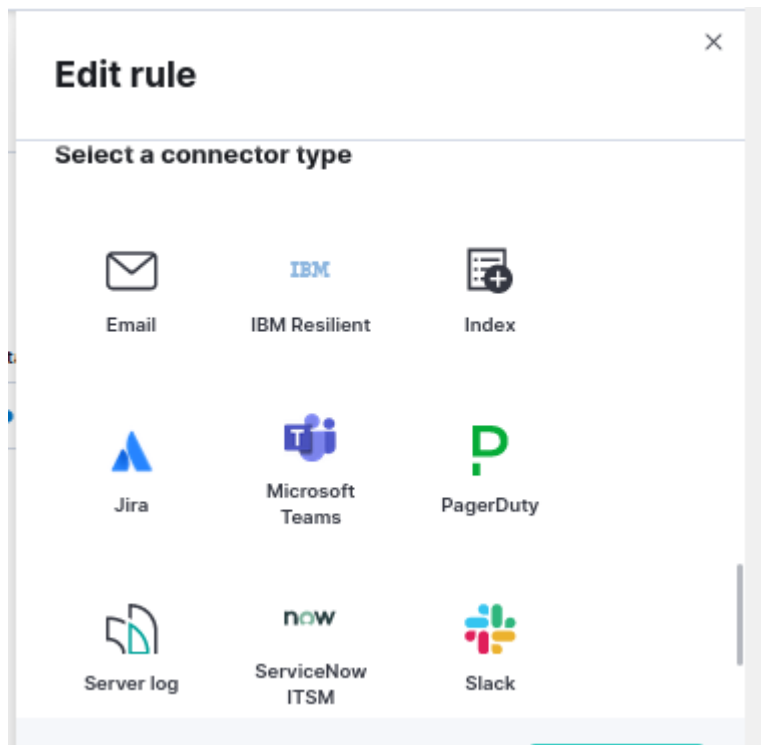
Now, we generate alerts for **load average** by clicking alerts and rules on the top left corner. We set the rules as follows;



Next, we set the log threshold as follows for **load average**;

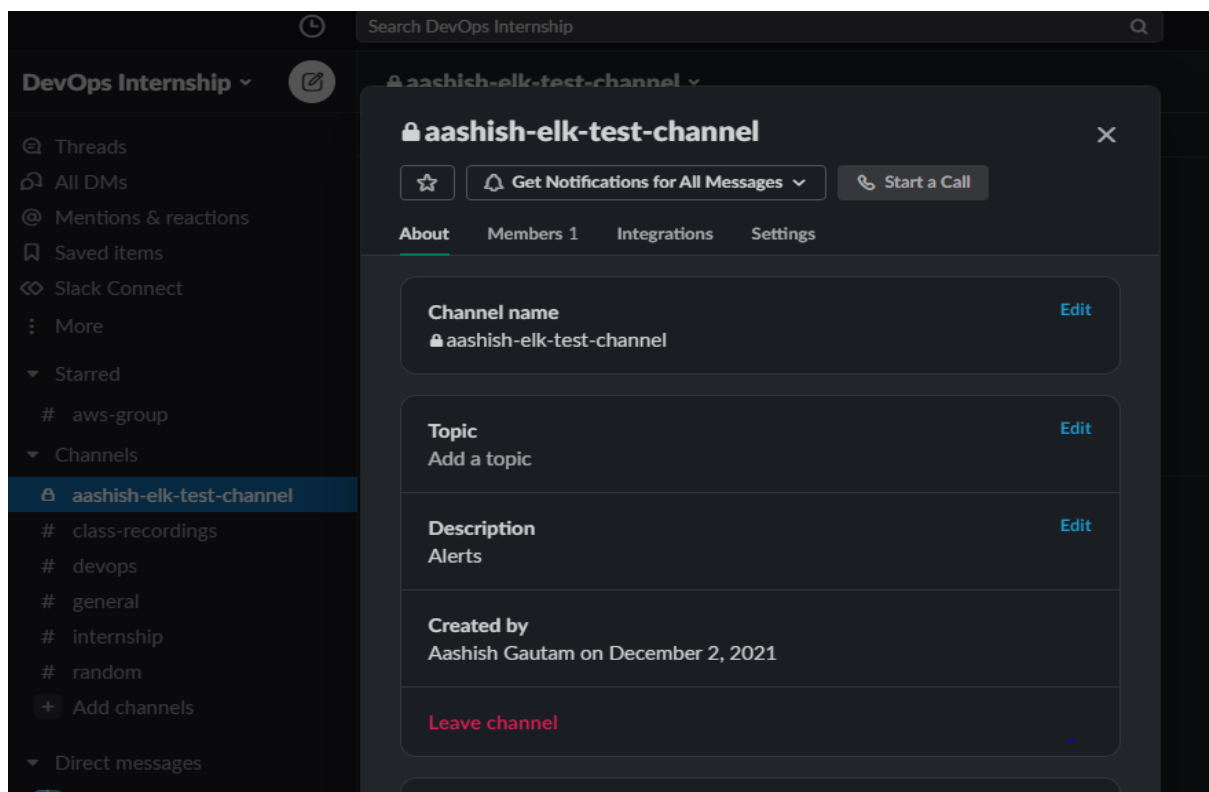


Next, Inorder to add actions, we used slack as a connector.

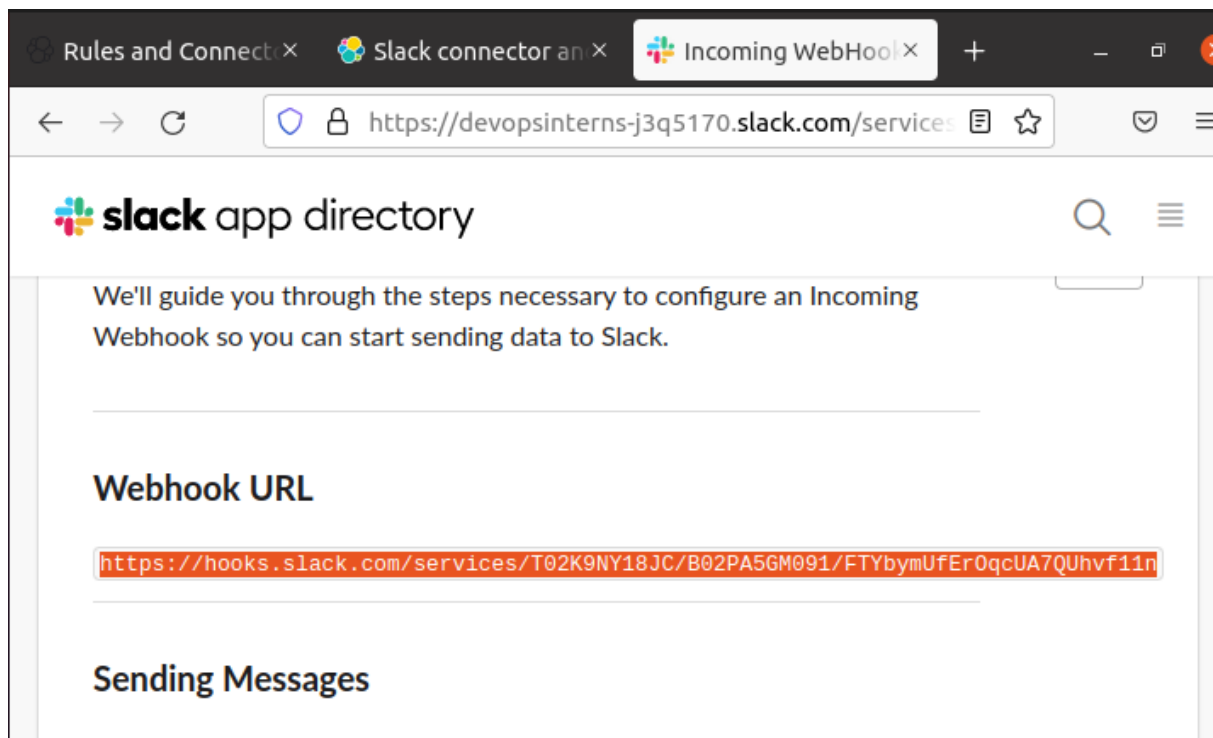


Now, we create a private slack channel for alerts named;

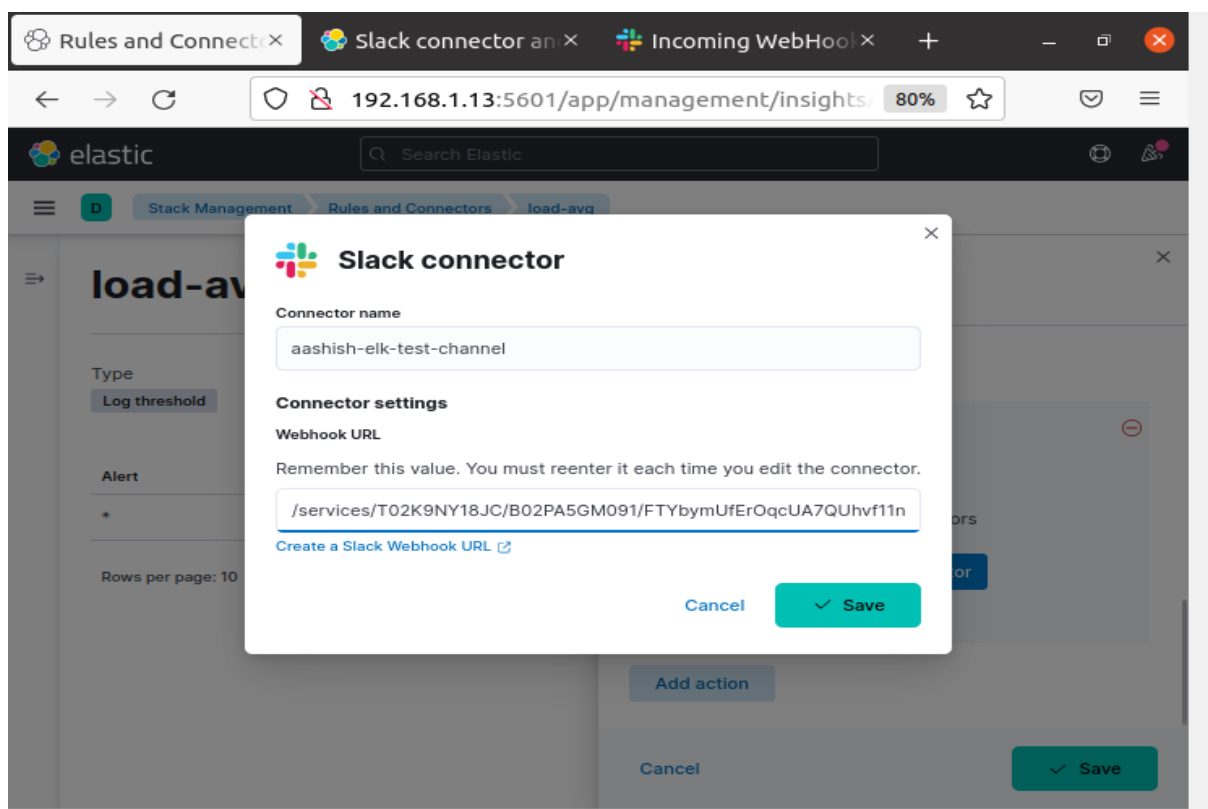
- **aashish-elk-test-channel**



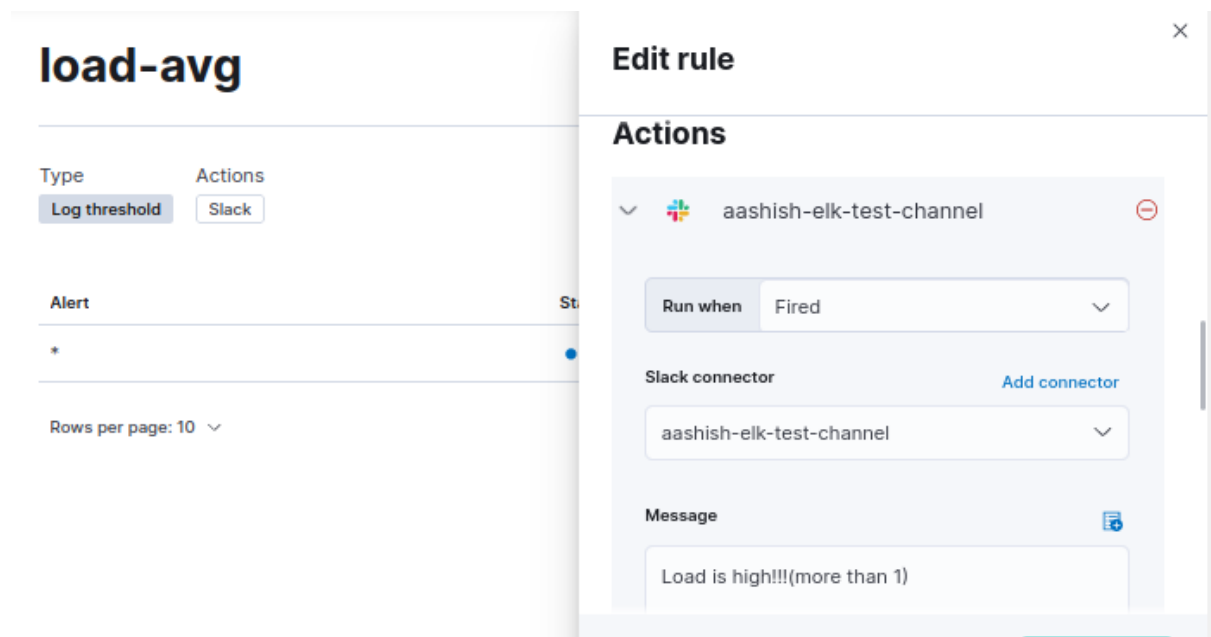
Then we create a slack **web-hook url** as follows;



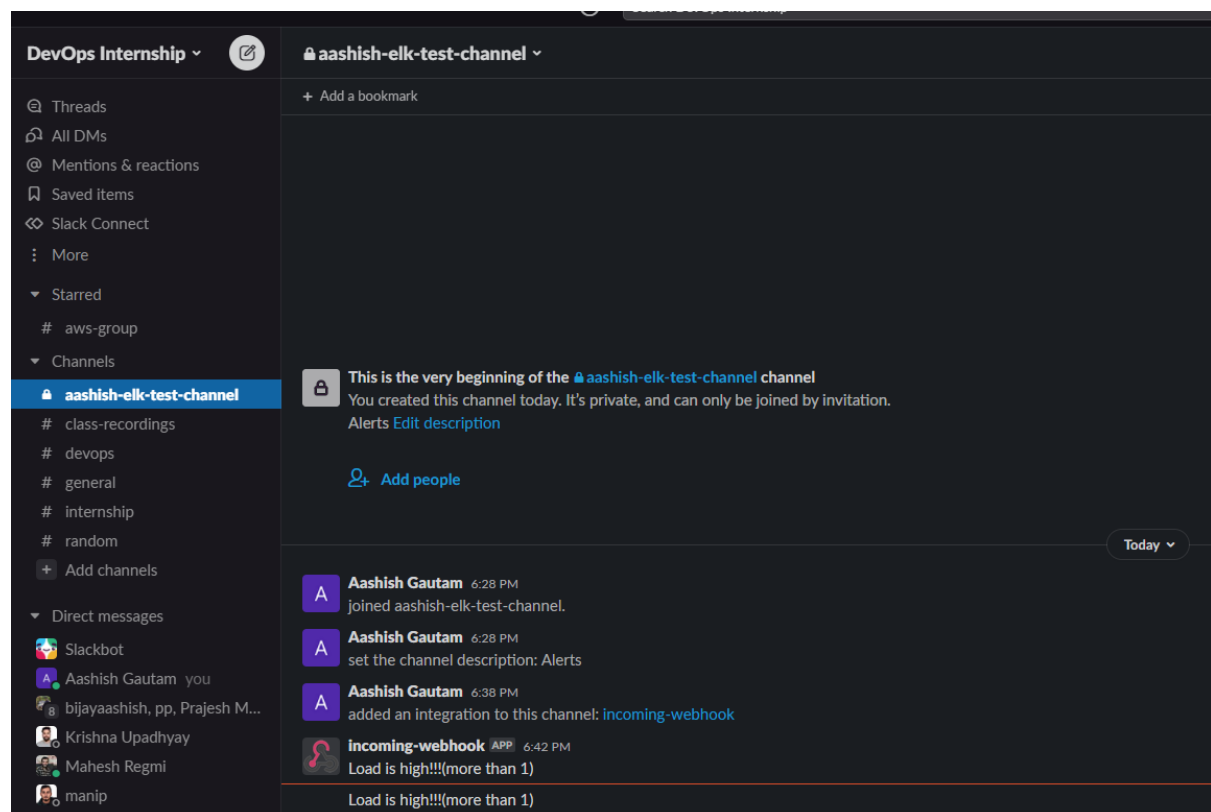
Then added the **webhook url** as follows;



Then, we save it and add actions and messages as follows;



Then, we save the rule for **load average** and wait for the alert on the slack and verify it as follows;



For **memory usage**, we add rules as follows;

**memoryUsage**

Type: Log threshold Actions: Slack

Alert

Rows per page: 10

**Edit rule**

Name: memory-usage Tags (optional):

Check every: 2 minutes

Notify: Every time alert is active

Next, we add **memory usage log threshold** as follows;

**Edit rule**

**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

+ Add condition

IS more than 4

FOR THE LAST 2 minutes

GROUP BY Nothing (ungrouped)



Cancel Save

Then, we add actions for **memory usage** as follows;

✕

Edit rule

Actions

▼  aashish-elk-test-channel 

Run when


Fired ▼

Slack connector

Add connector

aashish-elk-test-channel ▼

Message

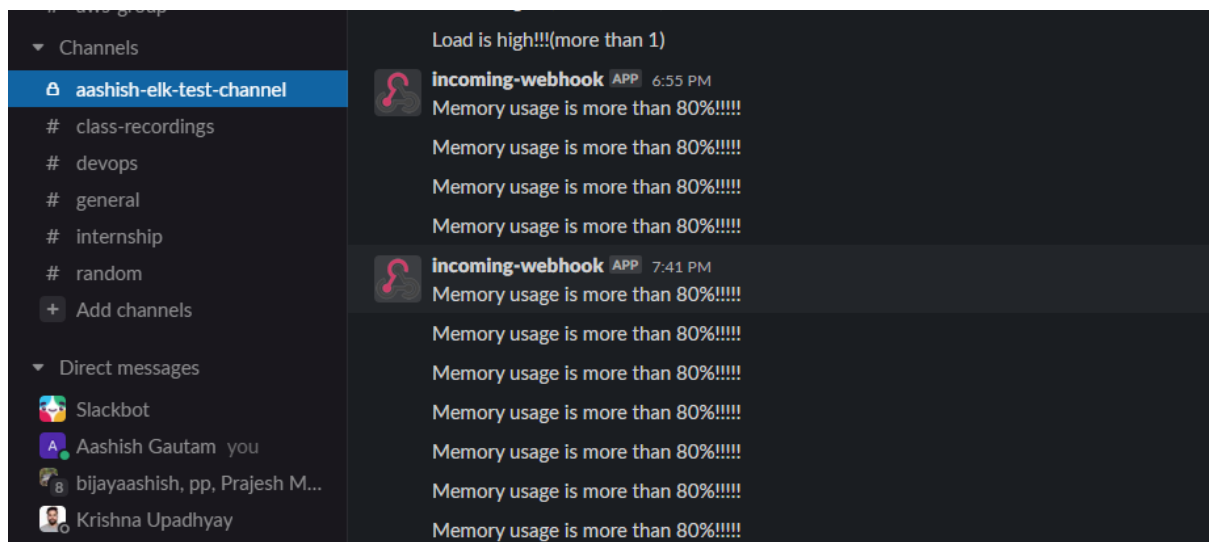


Memory usage is more than 80%!!!!

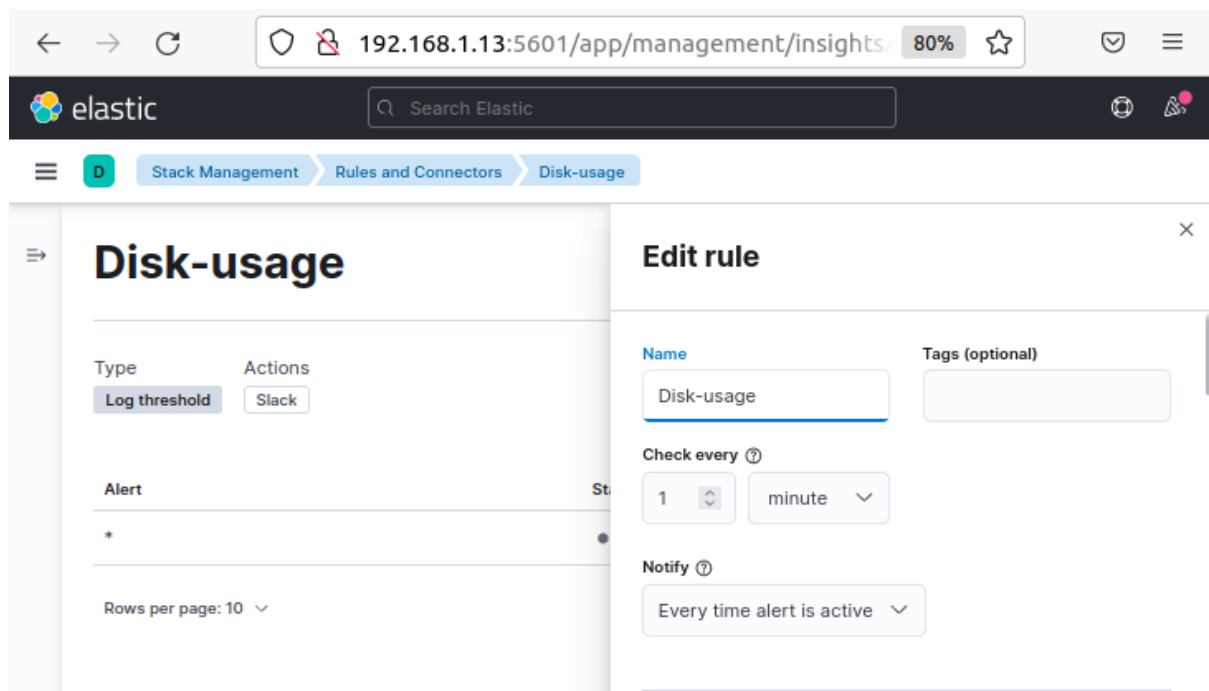
Cancel

✓ Save

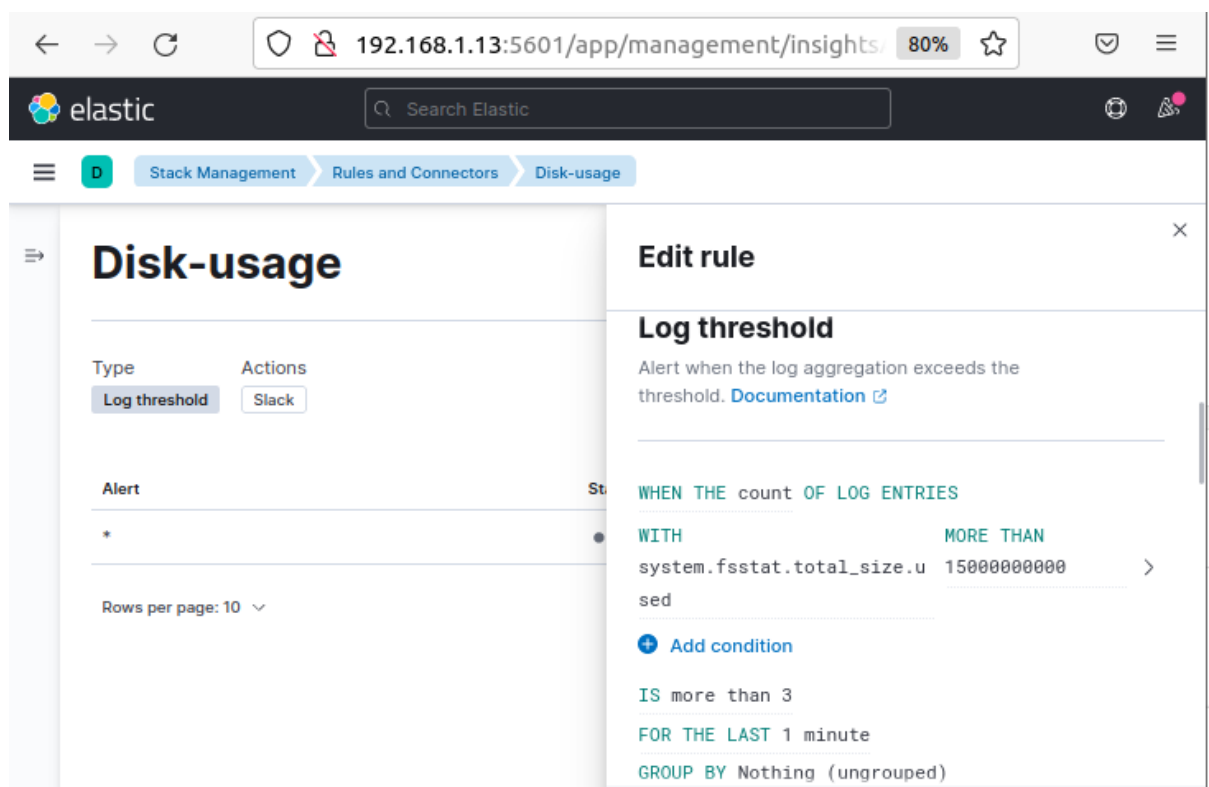
Now, we save the rule for **memory usage** and wait for the alert on the slack as displayed below;



For the **Disk Usage** we create rule as follows;

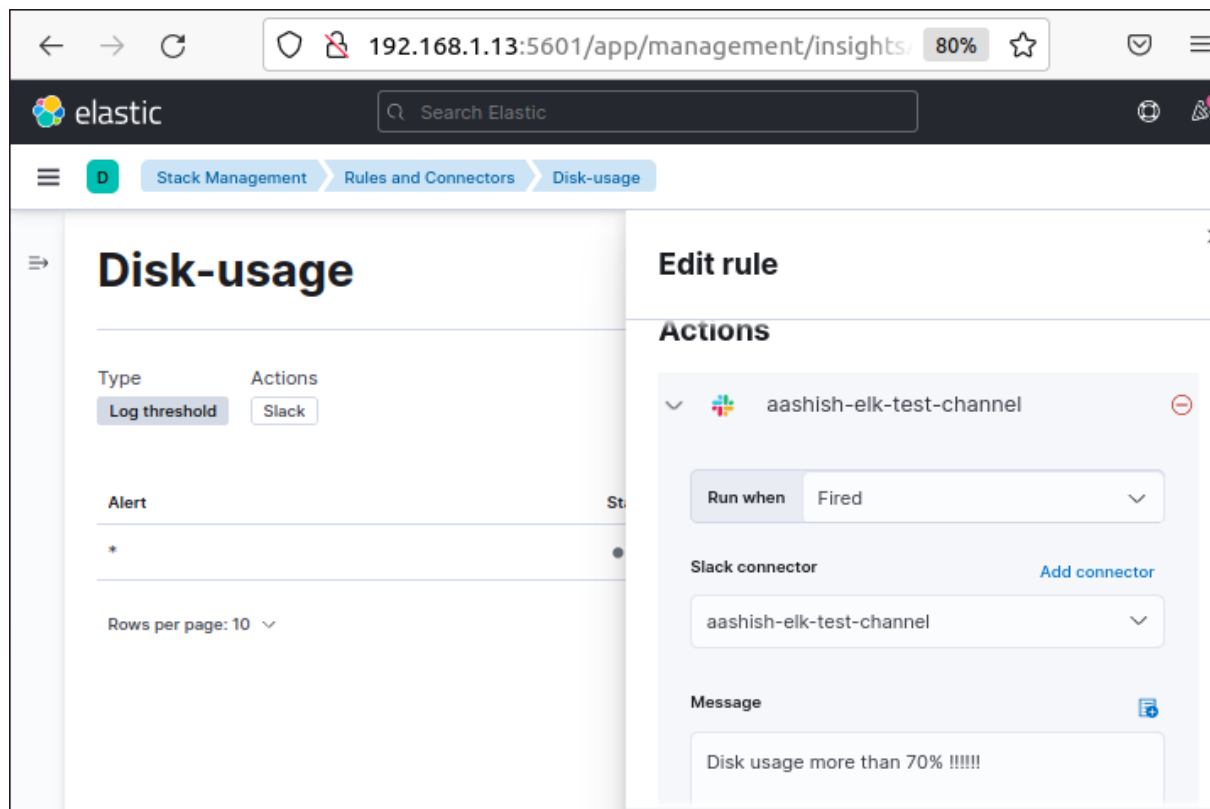


Then, we add disk log threshold as follows;

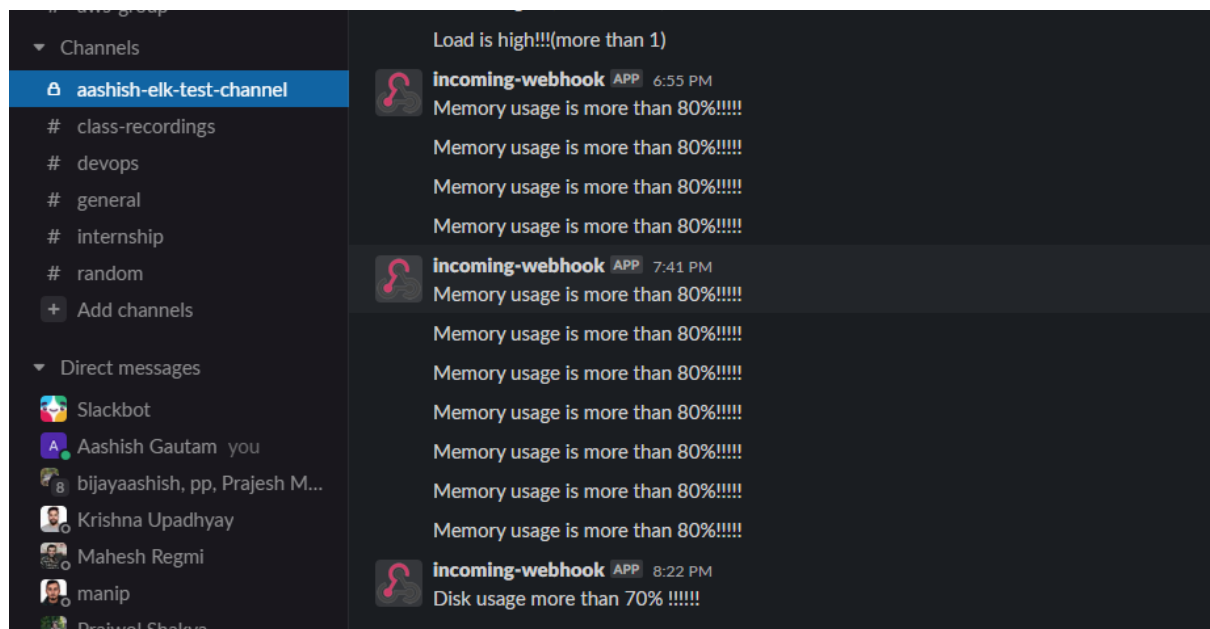




Next, we add actions for **disk usage** as follows;



Lastly, we save the rule and wait for the alerts on the slack channel as follows;



We can see all the rules that we have created as follows;

192.168.1.13:5601/app/management/insights/80%

Search Elastic

D

Stack Management

Rules

Detect conditions using rules, and take actions using connectors.

Rules

Connectors

Create rule

Search

Type0

Action type0

Status0

Refresh

Showing: 3 of 3 rules.

Active: 0

Error: 0

Ok: 3

Pending: 0

Unknown: 0

<input type="checkbox"/>	Enabled	Name ↑	Status	Type	Tags	Run...	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disk-usage	● Ok	Lo...		1m	1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	load-avg	● Ok	Lo...		2m	1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	memory-usage	● Ok	Lo...		2m	1