

SET UP EFK ON EC2

Efk

Efk stands for Elasticsearch Fluentd and kibana. Efk is a popular and the best open-source choice for the kubernetes logs aggregation and analysis. Elasticsearch is a distributed and scalable search engine commonly used to sift through large volumes of log data.

Ec2

- Ec2 stands for Amazon elastic compute cloud
- Amazon ec2 is a web service that provides resizable compute capacity in the cloud
- To run the application security group zones. user data applications installation it's nothing but remote server
- You can scale the computer capacity up and down as per computer requirement changes

First launch 2 ec2 instance

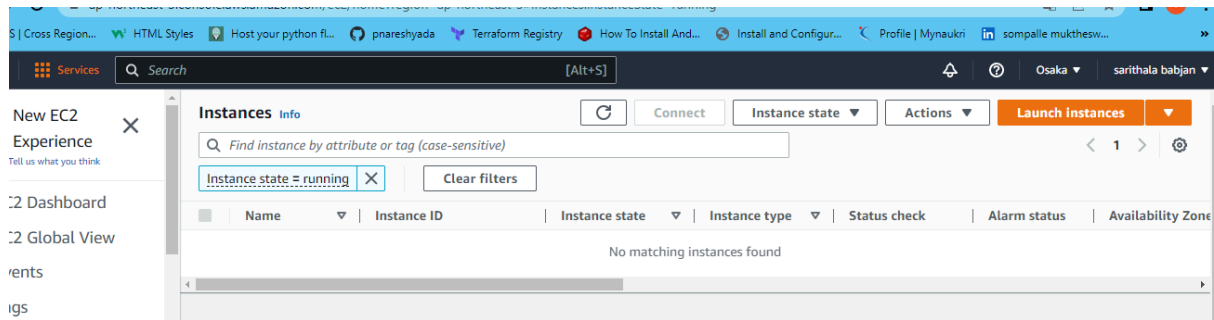
1.Go to the **ec2 dashboard**—>click on instance

The screenshot displays the AWS Management Console's EC2 Dashboard. On the left, a navigation sidebar includes links for 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances' (expanded), 'Instances' (with a 'New' tag), 'Instance Types', and 'Launch'. The main content area, titled 'Resources', shows a summary of EC2 resources in the 'Europe (Ireland) Region'. A table lists the following resources and their counts:

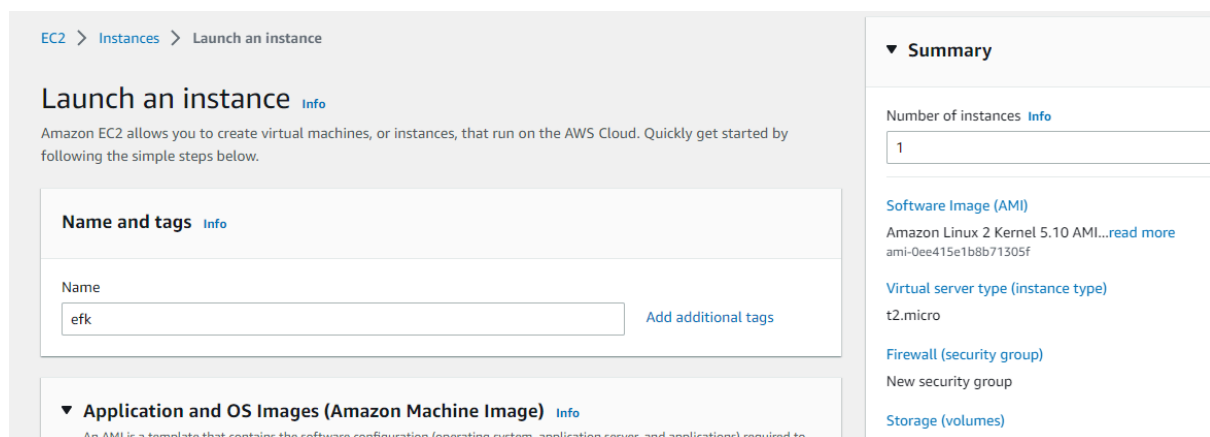
Resource	Count
Instances (running)	4
Elastic IPs	0
Key pairs	1
Placement groups	0
Snapshots	0
Dedicated Hosts	0
Instances	4
Load balancers	0
Security groups	6
Volumes	4

Below the table, a blue notification box states: 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)'. On the right side of the dashboard, the 'Account attributes' section lists 'Supported platforms' (VPC), 'Default VPC' (vpc-01eb5ab29763782), and various settings like 'EBS encryption', 'Zones', 'EC2 Serial Console', 'Default credit specification', and 'Console experiments'. At the bottom right is an 'Explore AWS' button.

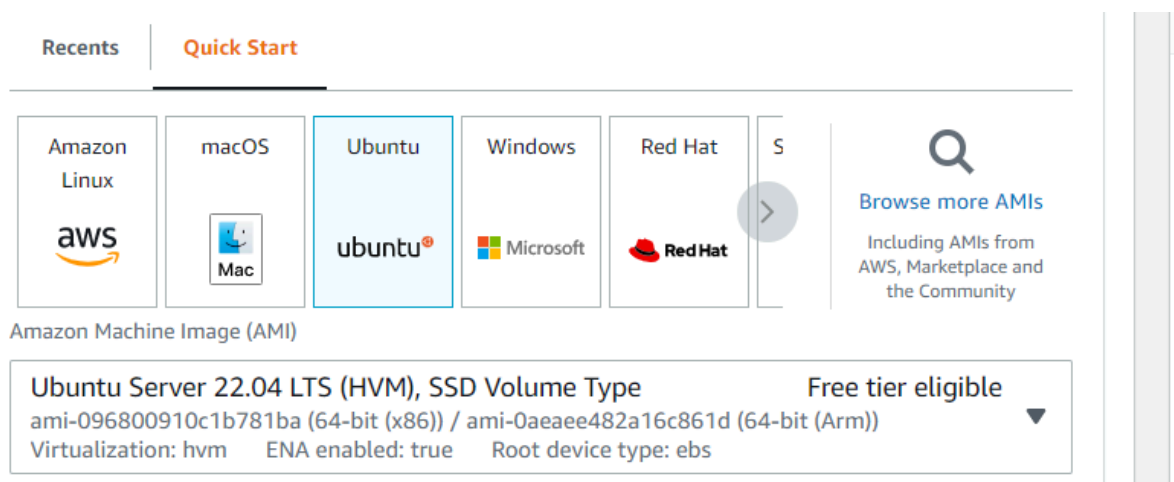
2. Next click on **launch instance**



3. Give proper name of the instance



4. we can select ami depending upon the requirement



5. we can select the **family type**

▼ Instance type [Info](#)

Instance type

t2.xlarge

Family: t2 4 vCPU 16 GiB Memory

On-Demand Linux pricing: 0.2016 USD per Hour

On-Demand Windows pricing: 0.2426 USD per Hour

▼

[Compare](#)

6. we can select key pair, here we can create new **key pair** and select it


▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

efk123

▼

 [Create new key pair](#)

7. Click on security groups—> Depending upon the application we can pass sg rules

instance.

☒ Create security group
 ☐ Select existing security group

Security group name - *required*

efk-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!\$*

Description - *required* [Info](#)

efk

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 45.249.77.103/32) Remove

Type Info	Protocol Info	Port range Info
ssh ▼	TCP	22

Source type Info	Name Info	Description - <i>optional</i> Info
My IP ▼	<input type="text"/> <input type="button" value="Add CIDR, prefix list or security"/>	e.g. SSH for admin desktop

Sg1 rules:(server,logstash)

Ssh—22—my ip

logstash—5044—0.0.0.0/0

Sg2 rules:(elasticsearch,kibana)

Ssh—22—my ip

Elasticsearch—9200—logstash sg

kibana—5601—0.0.0.0/0

8.click on launch instance ec2 will be created

▼ **Configure storage** [Info](#) [Advanced](#)

1x GiB Root volume

(Not encrypted)

[Free tier eligible customers can get up to 30 GB of EBS General Purpose \(SSD\) or Magnetic storage](#)

0 x File systems [Edit](#)

► **Advanced details** [Info](#)

▼ **Summary**

Number of instances [Info](#)

[Software Image \(AMI\)](#)

Amazon Linux 2 Kernel 5.10 AMI...[read more](#)

ami-0ee415e1b8b71305f

[Virtual server type \(instance type\)](#)

t2.micro

[Firewall \(security group\)](#)

New security group

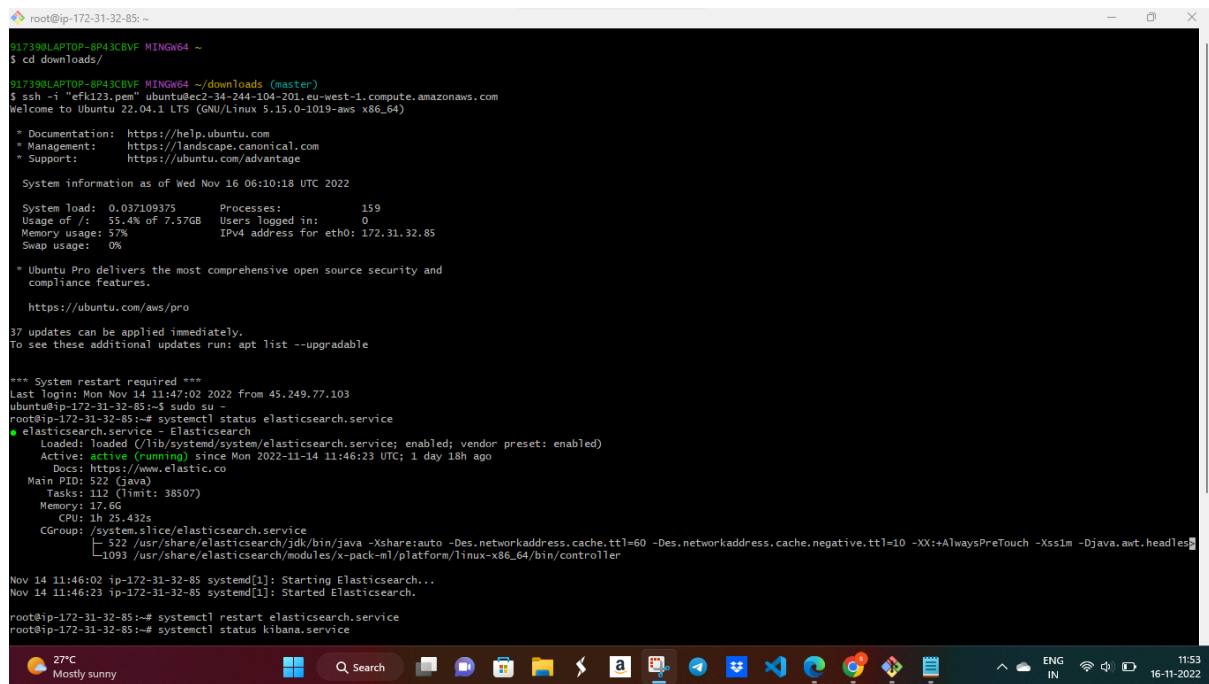
[Storage \(volumes\)](#)

1 volume(s) - 8 GiB

We are Connecting to the server first you copy public ip and go to git bash and give shown below command

ssh -i "pem.file name" ec2-user@publicip

when you are connected to the ec2 instance using ssh, you should see the shown below.



```
root@ip-172-31-32-85: ~
$ cd downloads/
$ ssh -i "efk123.pem" ubuntu@ec2-34-244-104-201.eu-west-1.compute.amazonaws.com
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1019-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Nov 16 06:10:18 UTC 2022

System load: 0.037109375      Processes: 159
Usage of /: 55.4% of 7.57GB   Users logged in: 0
Memory usage: 57%           IPv4 address for eth0: 172.31.32.85
Swap usage: 0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance Features.
   https://ubuntu.com/aws/pro

37 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Mon Nov 14 11:47:02 2022 from 45.249.77.103
ubuntu@ip-172-31-32-85:~$ sudo su -
root@ip-172-31-32-85:~# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-11-14 11:46:23 UTC; 1 day 18h ago
     Docs: https://www.elastic.co
   Main PID: 522 (java)
    Tasks: 112 (limit: 38507)
   Memory: 17.6G
     CPU: 1h 25.432s
   CGroup: /system.slice/elasticsearch.service
           └─ 522 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless
              1093 /usr/share/elasticsearch/modules/x-pack-m1/platform/linux-x86_64/bin/controller

Nov 14 11:46:02 ip-172-31-32-85 systemd[1]: Starting Elasticsearch...
Nov 14 11:46:23 ip-172-31-32-85 systemd[1]: Started Elasticsearch.
root@ip-172-31-32-85:~# systemctl restart elasticsearch.service
root@ip-172-31-32-85:~# systemctl status kibana.service
```

Install elastic search

Import the GPG key,run the below command.

rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

Create a file called **elasticsearch.repo** in the **/etc/yum.repos.d/** directory,Add the ELK repository in that file.

vi /etc/yum.repos.d/elasticsearch.repo

Copy and paste the below content in **elasticsearch.repo** file

```
[elasticsearch]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
```

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=0
auto refresh=1
type=rpm-md

Install **Elasticsearch**

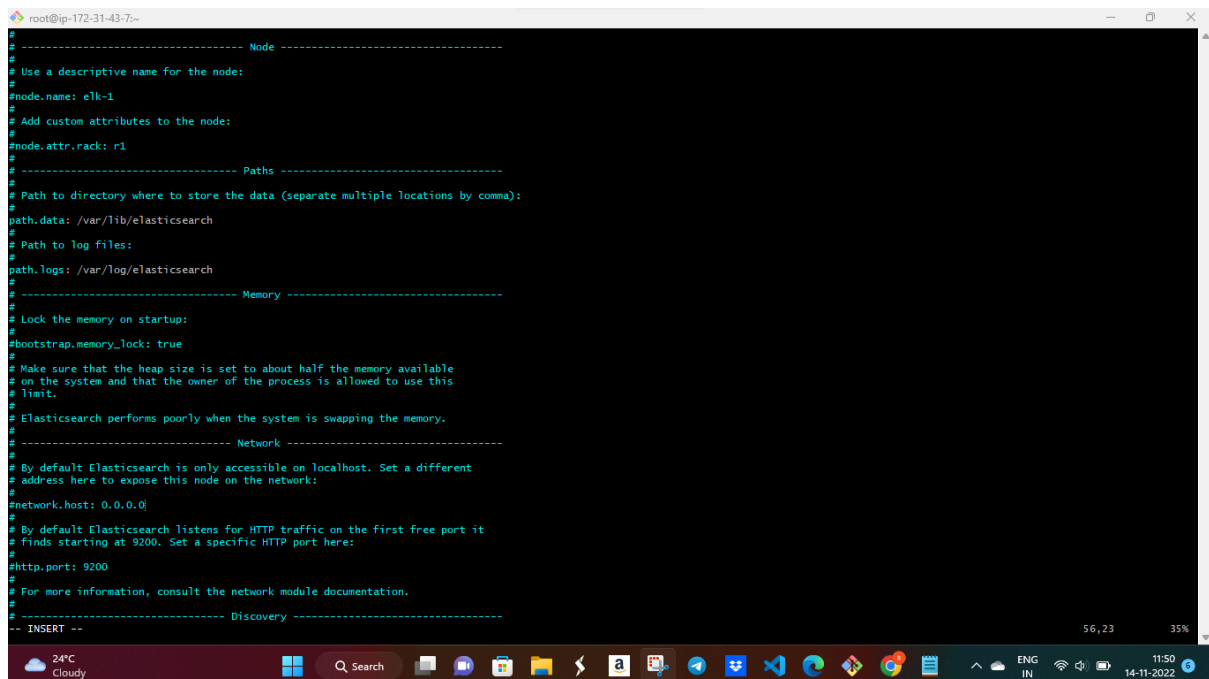
yum install --enablerepo=elasticsearch elasticsearch -y

After the installation, change below configurations in **elasticsearch.yml** file

vi /etc/elasticsearch/elasticsearch.yml

Uncomment and change below ones

cluster.name: elk
node.name: elk-1
network.host: 0.0.0.0



```
root@ip-172-31-43-7:~  
#  
# ----- Node -----  
#  
# Use a descriptive name for the node:  
#node.name: elk-1  
#  
# Add custom attributes to the node:  
#node.attr.rack: r1  
#  
# ----- Paths -----  
#  
# Path to directory where to store the data (separate multiple locations by comma):  
#  
path.data: /var/lib/elasticsearch  
#  
# Path to log files:  
#  
path.logs: /var/log/elasticsearch  
#  
# ----- Memory -----  
#  
# Lock the memory on startup:  
#  
#bootstrap.memory_lock: true  
#  
# Make sure that the heap size is set to about half the memory available  
# on the system and that the owner of the process is allowed to use this  
# limit.  
#  
# Elasticsearch performs poorly when the system is swapping the memory.  
#  
# ----- Network -----  
#  
# By default Elasticsearch is only accessible on localhost. Set a different  
# 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 port it  
# finds starting at 9200. Set a specific HTTP port here:  
#http.port: 9200  
#  
# For more information, consult the network module documentation.  
#  
# ----- Discovery -----  
#  
-- INSERT --
```

Enable **elasticsearch** give below command

/bin/systemctl enable elasticsearch.service
Start **elasticsearch** give below command
systemctl start elasticsearch.service
next verify **elasticsearch** is running or not give below command
systemctl l status elasticsearch.service

```
root@ip-172-31-43-7:~
Transaction Summary
Install 1 Package

Total download size: 300 M
Installed size: 501 M
Downloading packages:
elasticsearch-7.17.7-x86_64.rpm | 300 MB 00:00:03
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Installing : elasticsearch-7.17.7-1.x86_64 1/1
## NOT starting on installation, please execute the following statements to configure 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
Verifying : elasticsearch-7.17.7-1.x86_64 1/1

Installed:
  elasticsearch.x86_64 0:7.17.7-1

Complete!
[root@ip-172-31-43-7 ~]# vi /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-43-7 ~]# /bin/systemctl enable elasticsearch.service
Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasticsearch.service.
[root@ip-172-31-43-7 ~]# systemctl start elasticsearch.service
-bash: systemctl: command not found
[root@ip-172-31-43-7 ~]# systemctl start elasticsearch.service
-bash: systemctl: command not found
[root@ip-172-31-43-7 ~]# systemctl start elasticsearch.service
[root@ip-172-31-43-7 ~]# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-11-14 06:25:27 UTC; 1min 32s ago
     Docs: https://www.elastic.co
   Main PID: 3672 (java)
   CGroup: /system.slice/elasticsearch.service
           └─3672 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless...
           └─3639 /usr/share/elasticsearch/modules/x-pack-m1/platform/linux-x86_64/bin/controller

Nov 14 06:24:52 ip-172-31-43-7.eu-west-1.compute.internal systemd[1]: Starting Elasticsearch...
Nov 14 06:25:27 ip-172-31-43-7.eu-west-1.compute.internal systemd[1]: Started Elasticsearch.
[root@ip-172-31-43-7 ~]#
```

After finally i got the elastic page using elastic search public ip and using port number

```
{
  "name" : "ip-172-31-32-85",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "sWz-Gvh-QJiU_x8-_0xH1g",
  "version" : {
    "number" : "7.17.7",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "78dcaaaa8cee33438b91eca7f5c7f56a70fec9e80",
    "build_date" : "2022-10-17T15:29:54.167373105Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Install kibana

=====

Import the GPG key,run the below command.

```
rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

Create a file called **kibana.repo** in the **/etc/kibana/** directory,Add the ELK repository in that file.

```
vi /etc/yum.repos.d/kibana.repo
```

Copy and paste the below content in **kibana.repo** file

```
[kibana-7.x]
name=Kibana repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
auto refresh=1
type=rpm-md
```

Install kibana give below command

```
yum install kibana -y
```

After the installation,change below configurations in **kibana.yaml** file

```
vi /etc/kibana/kibana.yml
```

Uncomment and change below ones

```
server.port: 5601
server.host: "0.0.0.0"
server.name: "kibana"
```

Here in localhost place you have give **elasticsearch private ip**

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

```
root@ip-172-31-43-7:/etc
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# 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 proxy.
# 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 basePath.
server.publicBaseUrl: "http://172.31.43.7:5601/"

# 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: "kibana"

# 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, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
# kibana.index: ".kibana"

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

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
# elasticsearch.username: "kibana_system"
# elasticsearch.password: "pass"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
-- INSERT --
```

Enable **kibana** give below command

systemctl enable kibana.service

Start **kibana** give below command

Systemctl start kibana.service

next verify **kibana** is running or not give below command

Systemctl status kibana.service

```
root@ip-172-31-43-7:/etc
--> Finished Dependency Resolution
Dependencies Resolved

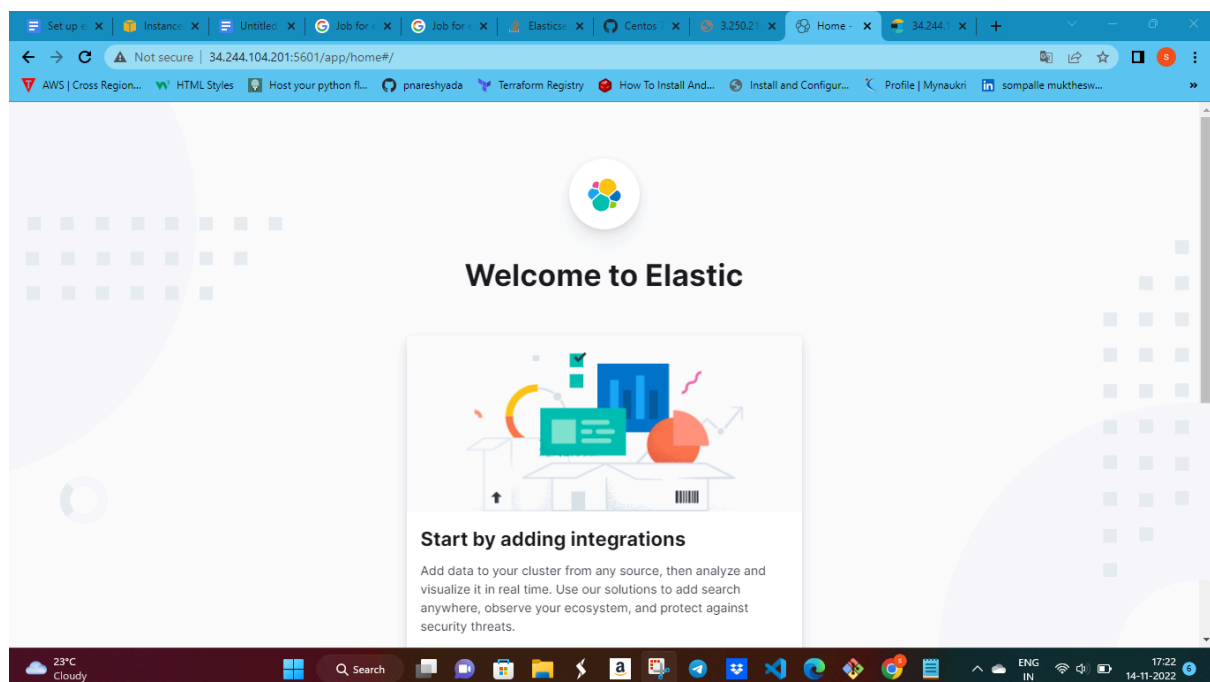
Package Arch Version Repository Size
Installing:
kibana x86_64 7.17.7-1 kibana-7.x 256 M

Transaction Summary
Install 1 Package
Total download size: 256 M
Installed size: 649 M
Downloading packages:
kibana-7.17.7-x86_64.rpm | 256 MB 00:00:30
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : kibana-7.17.7-1.x86_64 1/1
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
Verifying : kibana-7.17.7-1.x86_64 1/1
Installed:
kibana.x86_64 0:7.17.7-1

Complete!
[root@ip-172-31-43-7 /etc]# vi /etc/kibana/kibana.yml
[root@ip-172-31-43-7 /etc]# systemctl enable kibana.service
-bash: systemctl: command not found
[root@ip-172-31-43-7 /etc]# systemctl enable kibana.service
Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service to /etc/systemd/system/kibana.service.
[root@ip-172-31-43-7 /etc]# systemctl start kibana.service
[root@ip-172-31-43-7 /etc]# systemctl status kibana.service
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-11-14 07:15:45 UTC; 10s ago
     Docs: https://www.elastic.co
    Main PID: 643 (node)
    CGroup: /system.slice/kibana.service
            └─643 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bin/./src/cli/dist --logging.dest=/var/log/kibana/kibana.log --pid.file=/run/kibana/kibana.pid --deprecation.s...

Nov 14 07:15:45 ip-172-31-43-7.eu-west-1.compute.internal systemd[1]: Started Kibana.
[root@ip-172-31-43-7 /etc]#
```

Give this one **public ip:5601** in the browser you get below kibana page



Another ec2 machine first install **Tomcat server**

Install **Tomcat** give below commands

Yum update -y

sudo su -

cd /opt

Wget

<https://dlcdn.apache.org/tomcat/tomcat-10/v10.0.27/bin/apache-tomcat-10.0.27.tar.gz>

tar -zxvf apache-tomcat-10.0.27.tar.gz

cd apache-tomcat-10.0.27/bin/

ls -ltra

chmod +x startup.sh

chmod +x shutdown.sh

ls -ltra

echo \$PATH

ln -s /opt/apache-tomcat-10.0.27/bin/startup.sh /usr/local/bin/tomcatup

ln -s /opt/apache-tomcat-10.0.27/bin/shutdown.sh /usr/local/bin/tomcatdown

sudo apt-get update

sudo apt install openjdk-11-jdk

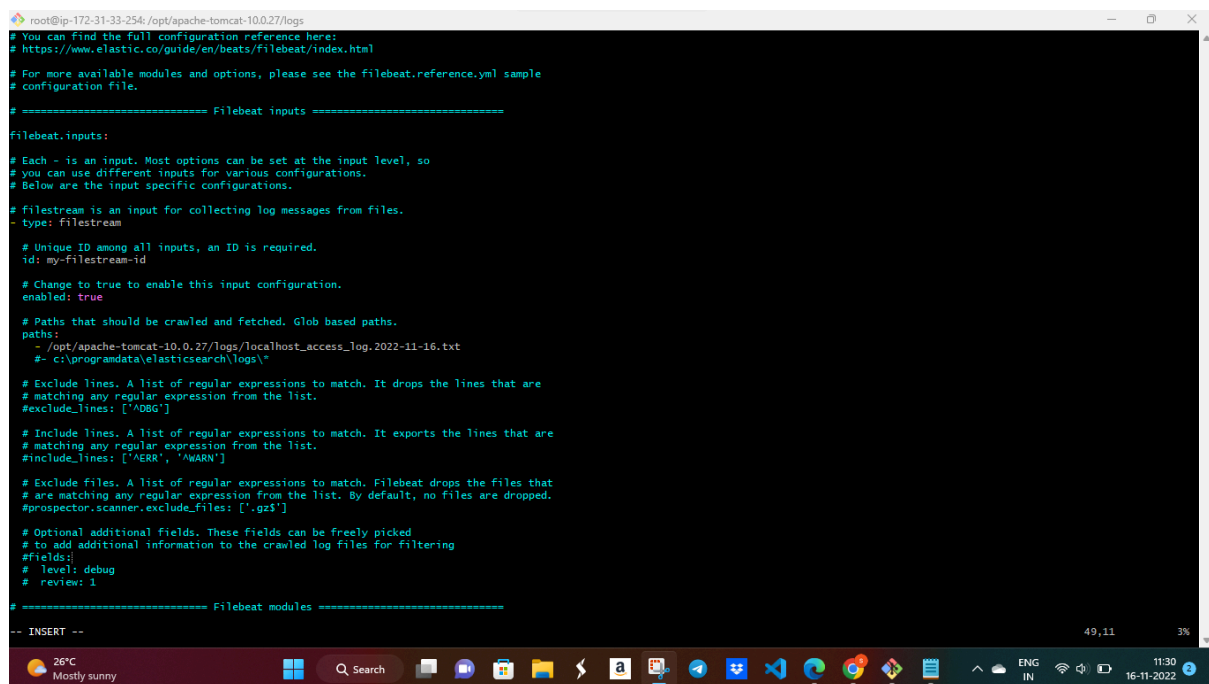
tomcat up

ps -ef | grep tomcat

```
root@ip-172-31-37-178:~
-rw-r--r-- 1 root root 25294 Nov 9 18:43 catalina.sh
-rw-r--r-- 1 root root 1703 Nov 9 18:43 catalina-tasks.xml
-rw-r--r-- 1 root root 2123 Nov 9 18:43 ciphers.bat
-rw-r--r-- 1 root root 1997 Nov 9 18:43 ciphers.sh
-rw-r--r-- 1 root root 25772 Nov 9 18:43 commons-daemon.jar
-rw-r--r-- 1 root root 2040 Nov 9 18:43 configtest.bat
-rw-r--r-- 1 root root 1922 Nov 9 18:43 configtest.sh
-rw-r--r-- 1 root root 9100 Nov 9 18:43 daemon.sh
-rw-r--r-- 1 root root 2091 Nov 9 18:43 digest.bat
-rw-r--r-- 1 root root 1965 Nov 9 18:43 digest.sh
-rw-r--r-- 1 root root 3608 Nov 9 18:43 makebase.bat
-rw-r--r-- 1 root root 3382 Nov 9 18:43 makebase.sh
-rw-r--r-- 1 root root 8951 Nov 9 18:43 service.bat
-rw-r--r-- 1 root root 3460 Nov 9 18:43 setclasspath.bat
-rw-r--r-- 1 root root 3708 Nov 9 18:43 setclasspath.sh
-rw-r--r-- 1 root root 2020 Nov 9 18:43 shutdown.bat
-rw-r--r-- 1 root root 1902 Nov 9 18:43 shutdown.sh
-rw-r--r-- 1 root root 2022 Nov 9 18:43 startup.bat
-rw-r--r-- 1 root root 1904 Nov 9 18:43 startup.sh
-rw-r--r-- 1 root root 2613248 Nov 9 18:43 tcnative-1.dll
-rw-r--r-- 1 root root 144912 Nov 9 18:43 tomcat9.exe
-rw-r--r-- 1 root root 128528 Nov 9 18:43 tomcat9w.exe
-rw-r--r-- 1 root root 49002 Nov 9 18:43 tomcat-juli.jar
-rw-r--r-- 1 root root 4574 Nov 9 18:43 tool-wrapper.bat
-rw-r--r-- 1 root root 5540 Nov 9 18:43 tool-wrapper.sh
-rw-r--r-- 1 root root 2026 Nov 9 18:43 version.bat
-rw-r--r-- 1 root root 1908 Nov 9 18:43 version.sh
[root@ip-172-31-37-178 bin]# chmod 755 *.sh
[root@ip-172-31-37-178 bin]# ./startup.sh
Using CATALINA_BASE: /root/tomcat9
Using CATALINA_HOME: /root/tomcat9
Using CATALINA_TMPDIR: /root/tomcat9/temp
Using JRE_HOME: /usr
Using CLASSPATH: /root/tomcat9/bin/bootstrap.jar:/root/tomcat9/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
[root@ip-172-31-37-178 bin]# ps -ef | grep tomcat9
root      7624      2  0 06:19 pts/0    00:00:03 /usr/bin/java -Djava.util.logging.config.file=/root/tomcat9/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogMa
nager -Djdk.tls.ephemeralDHkeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.SecurityListener.Umask=0027 -Dignore.endorsed.dirs= -classp
ath /root/tomcat9/bin/bootstrap.jar:/root/tomcat9/bin/tomcat-juli.jar -Dcatalina.base=/root/tomcat9 -Dcatalina.home=/root/tomcat9 -Djava.io.tmpdir=/root/tomcat9/temp org.apache.catalina.startu
p.Bootstrap start
root      8287      2  0 06:20 pts/0    00:00:00 grep --color=auto tomcat9
[root@ip-172-31-37-178 bin]# ^C
[root@ip-172-31-37-178 bin]# ^C
[root@ip-172-31-37-178 bin]# cd ..
[root@ip-172-31-37-178 tomcat9]# cd ..
[root@ip-172-31-37-178 ~]# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
sudo: apt-key: command not found
[root@ip-172-31-37-178 ~]# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add |
```

Install filebeat

```
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 filebeat  
sudo vi /etc/filebeat/filebeat.yml  
#outputs hosts: ["34.244.104.201:9200"]
```



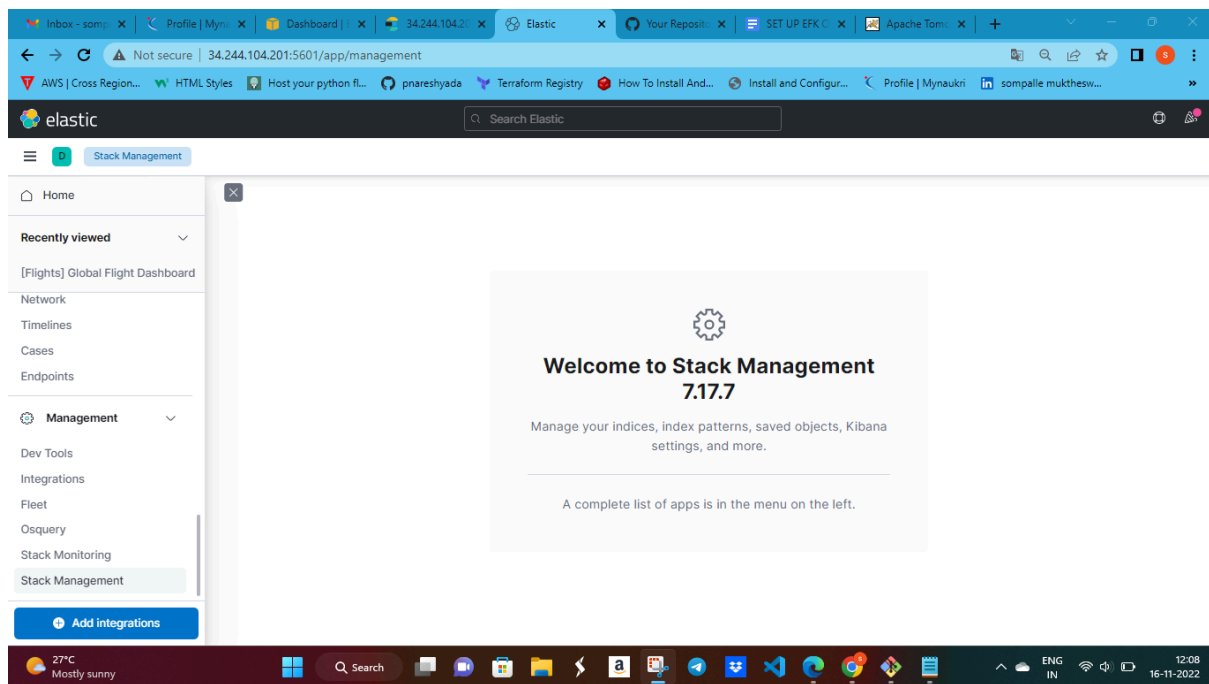
```
root@ip-172-31-33-254: /opt/apache-tomcat-10.0.27/logs  
# You can find the full configuration reference here:  
# https://www.elastic.co/guide/en/beats/filebeat/index.html  
# For more available modules and options, please see the filebeat.reference.yml sample  
# configuration file.  
#  
# ===== Filebeat inputs =====  
filebeat.inputs:  
# Each - is an input. Most options can be set at the input level, so  
# you can use different inputs for various configurations.  
# Below are the input specific configurations.  
# filestream is an input for collecting log messages from files.  
- type: filestream  
  # Unique ID among all inputs, an ID is required.  
  id: my-filestream-id  
  # Change to true to enable this input configuration.  
  enabled: true  
  # Paths that should be crawled and fetched. Glob based paths.  
  paths:  
    - /opt/apache-tomcat-10.0.27/logs/localhost_access_log.2022-11-16.txt  
    - c:\programdata\elasticsearch\logs*  
  # Exclude lines. A list of regular expressions to match. It drops the lines that are  
  # matching any regular expression from the list.  
  #exclude_lines: ['^DBG']  
  # Include lines. A list of regular expressions to match. It exports the lines that are  
  # matching any regular expression from the list.  
  #include_lines: ['^ERR', '^WARN']  
  # Exclude files. A list of regular expressions to match. Filebeat drops the files that  
  # are matching any regular expression from the list. By default, no files are dropped.  
  #prospector.scanner.exclude_files: ['*.gz']  
  # Optional additional fields. These fields can be freely picked  
  # to add additional information to the crawled log files for filtering  
  #fields:  
  # level: debug  
  # review: 1  
# ===== Filebeat modules =====  
-- INSERT --
```

After that run the below command

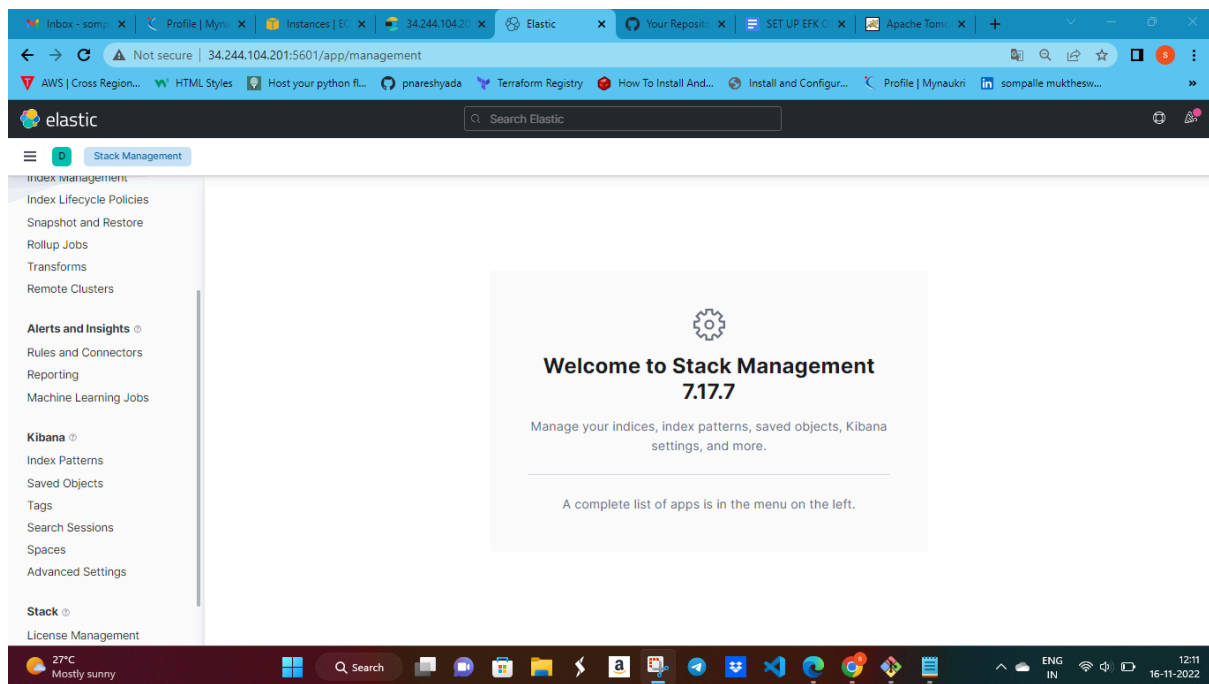
```
/opt/apache-tomcat-10.0.27/logs/localhost_access_log.2022-11-16.txt
```

```
Systemctl status filebeat.service
```

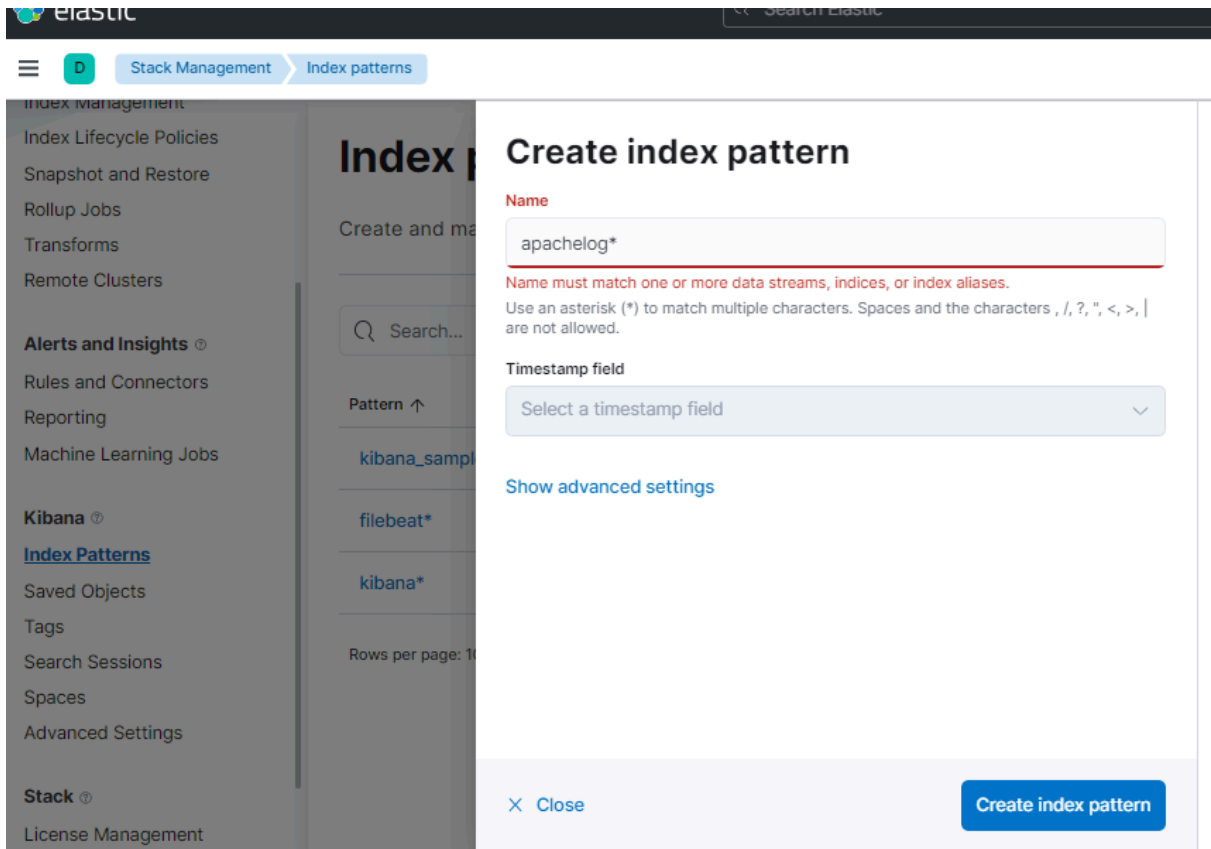
After that we login to **kibana ui**
Click stack manager



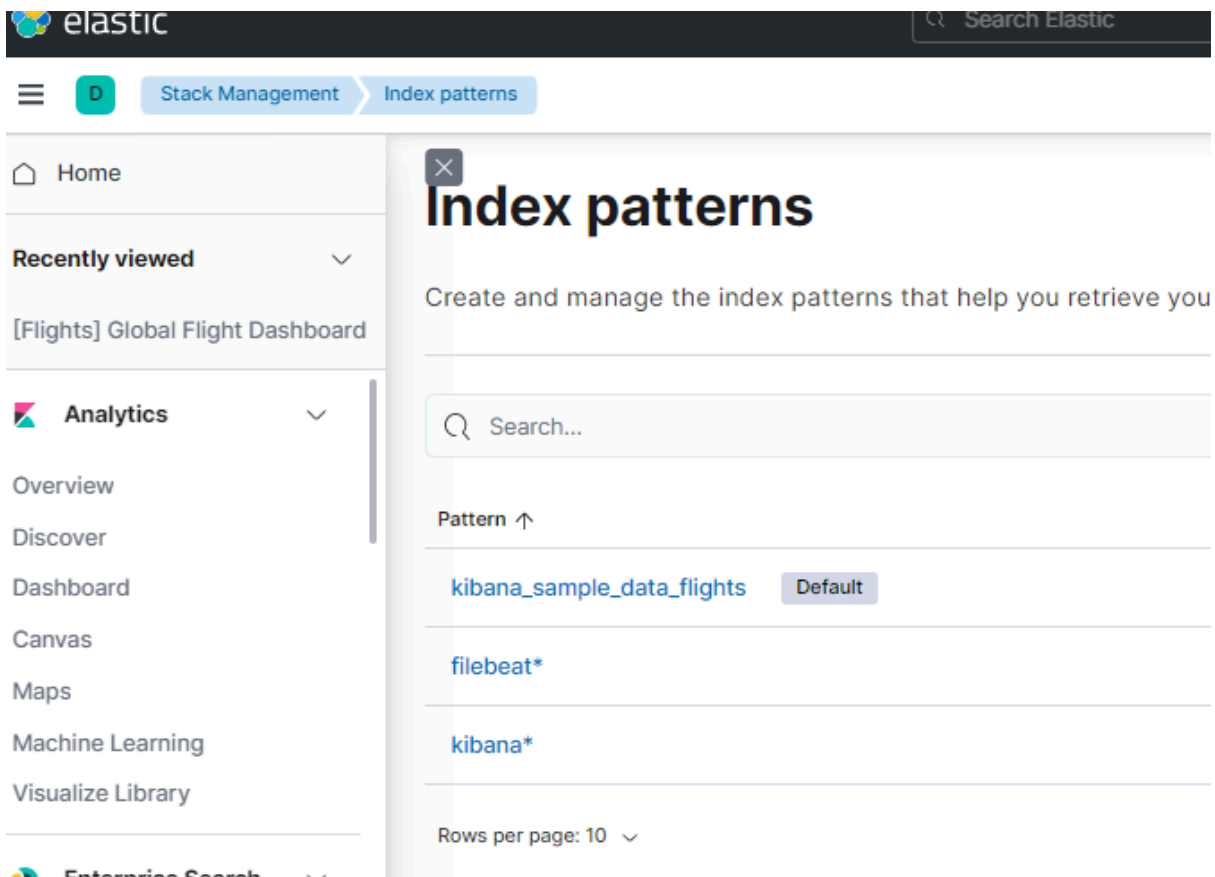
Next click index patterns



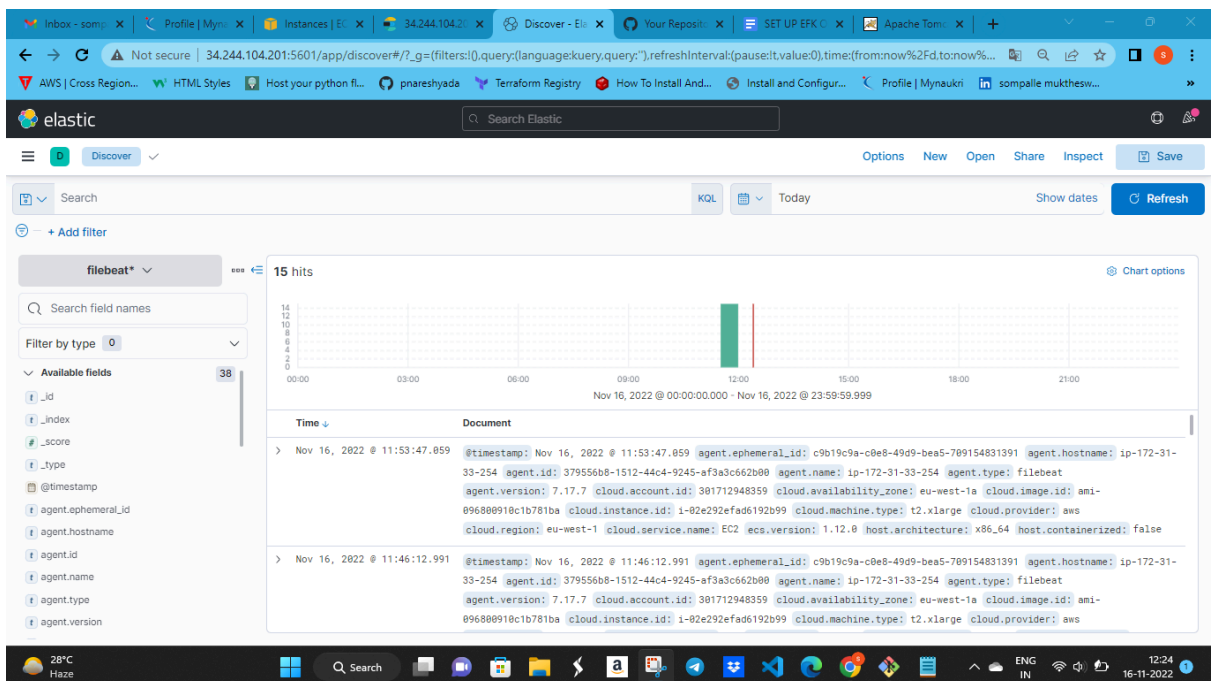
Create new index pattern



Go to home page and click discovery



In the discovery section see the logs



You not get the logs restart it (kibana,filebeat,elasticsearch)
After that you get logs

