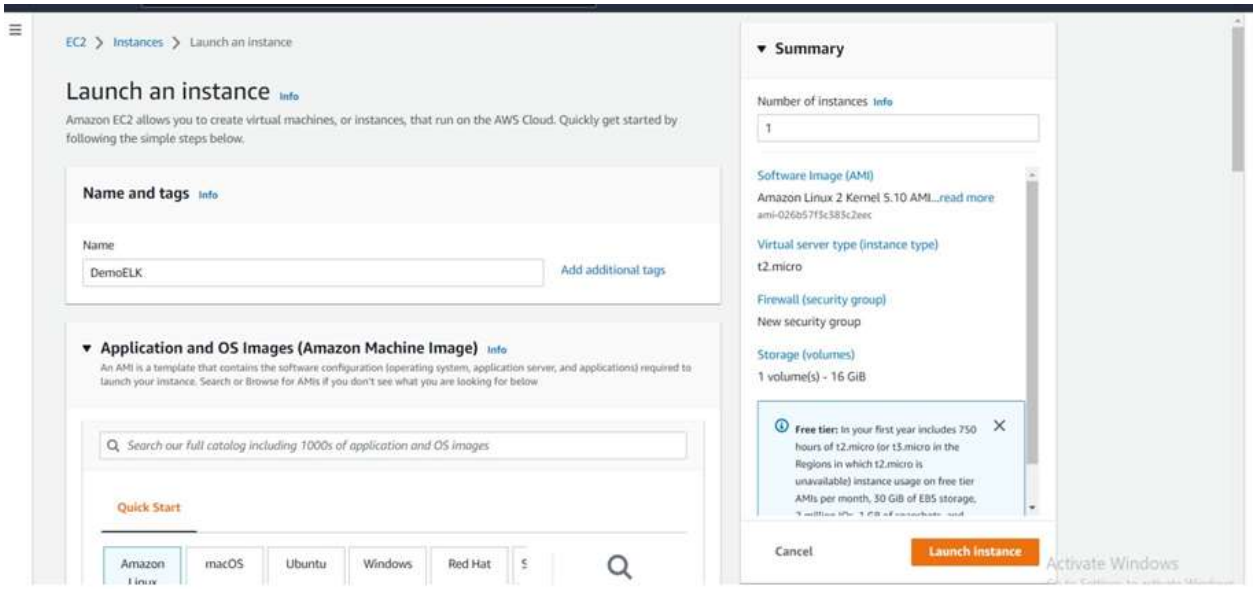
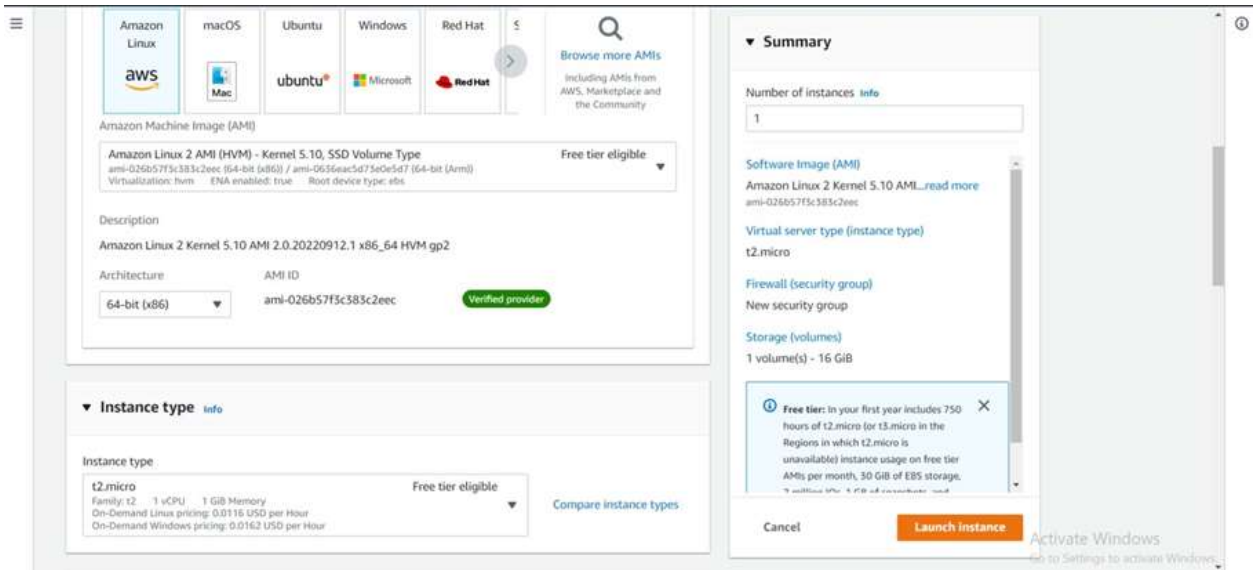
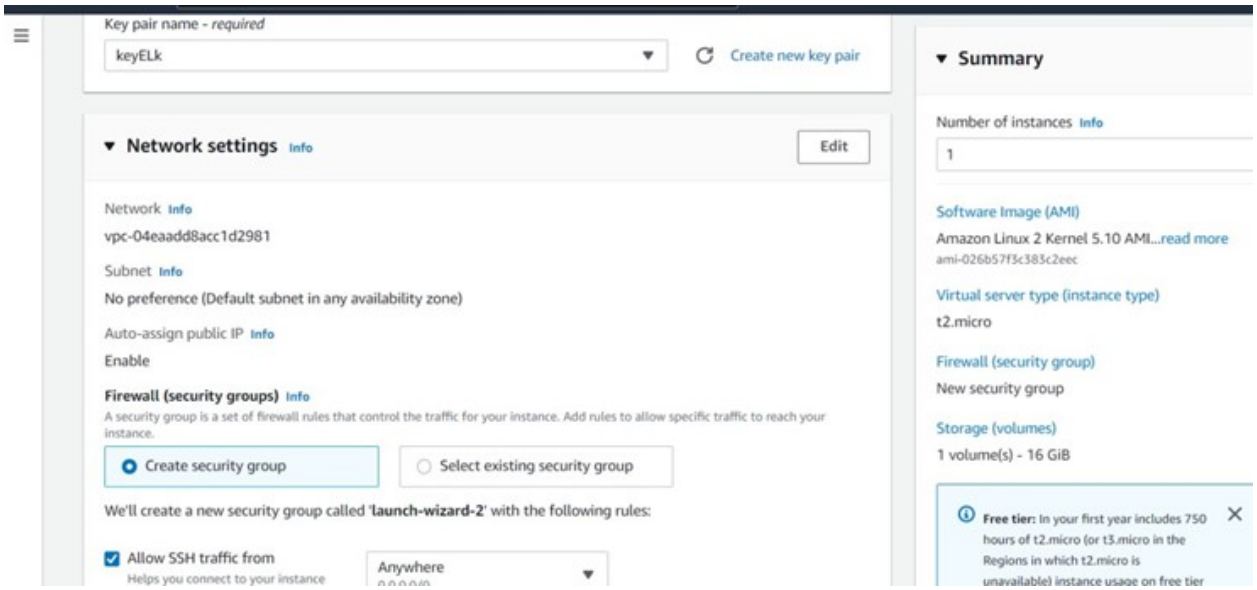
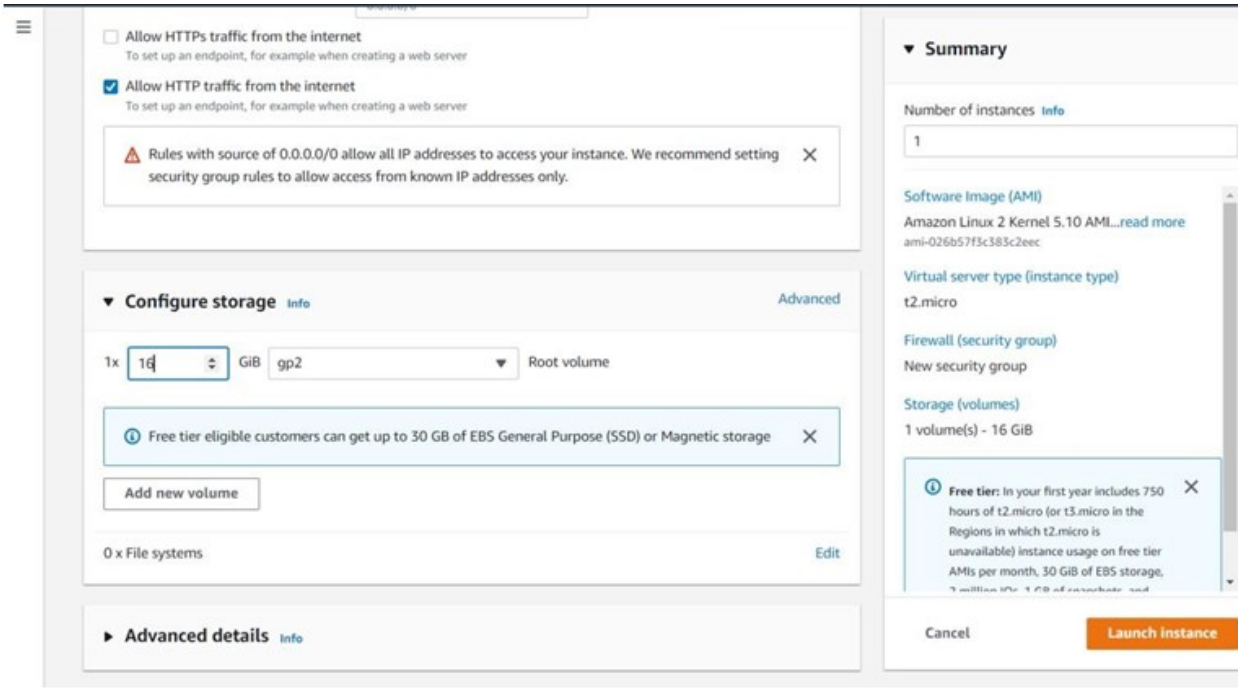
Deploying ELK Stack on Docker Container

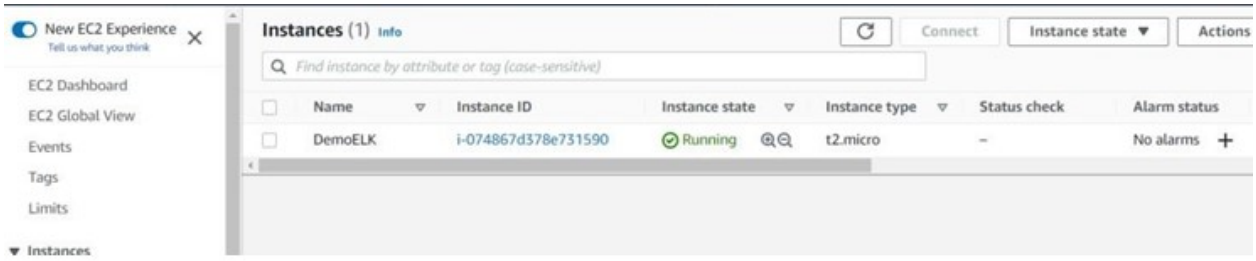
First we need to create an EC2- instance.

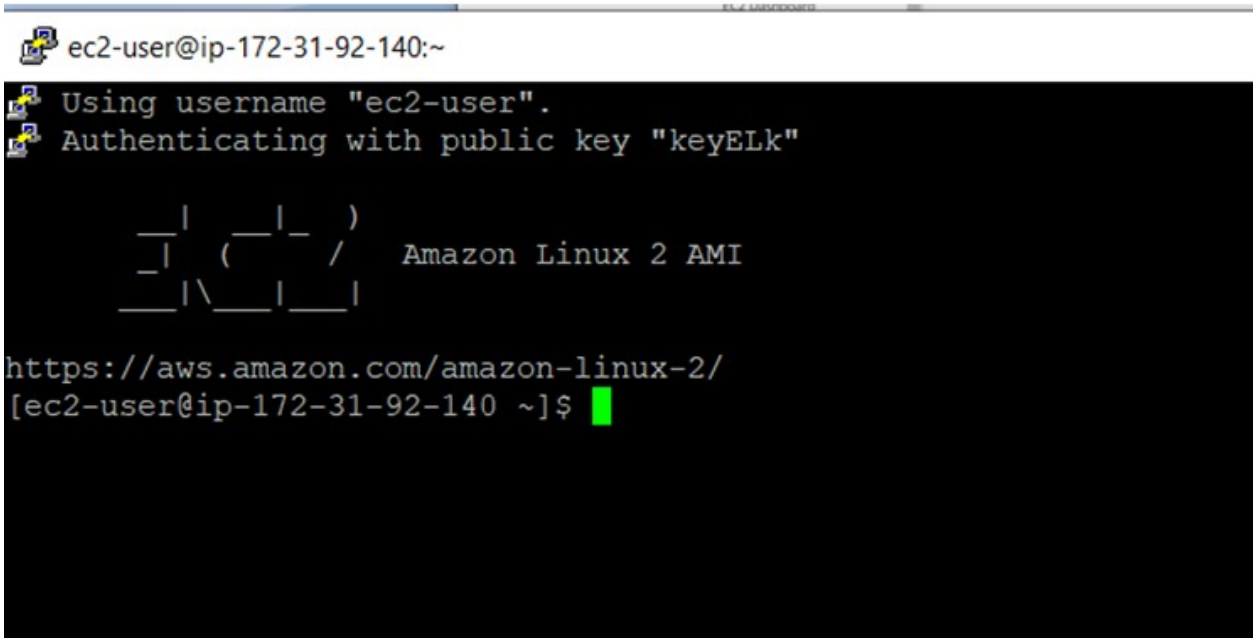





Key pair name - required
keyELk
Create new key pair
Network settings Info
Edit
Network Info
vpc-04eaadd8acc1d2981
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-2' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-026b57f3c383c2eec
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 16 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier


Allow HTTPs traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage Info
Advanced
1x
16
GiB
gp2
Root volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
0 x File systems
Edit
Advanced details Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-026b57f3c383c2eec
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 16 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage,
Cancel
Launch instance

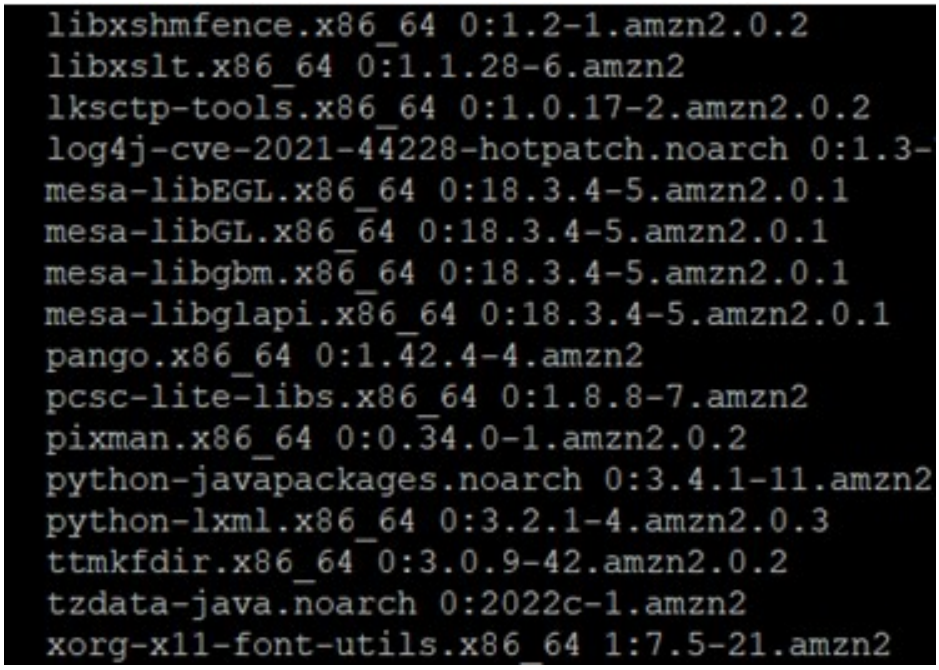




Now follow the following step

Step1: Install java and its Dependencies

```
Using username "ec2-user".
Authenticating with public key "keyELk"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-92-140 ~]$ java -version
-bash: java: command not found
[ec2-user@ip-172-31-92-140 ~]$ sudo yum -y install java-1.8.0-openjdk
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                               | 3.7 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package java-1.8.0-openjdk.x86_64 1:1.8.0.342.b07-1.amzn2.0.1 will be inst
lled
--> Processing Dependency: java-1.8.0-openjdk-headless(x86-64) = 1:1.8.0.342.b0
-1.amzn2.0.1 for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: xorg-x11-fonts-Type1 for package: 1:java-1.8.0-openj
k-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjvm.so(SUNWprivate_1.1)(64bit) for package: 1:jav
-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjava.so(SUNWprivate_1.1)(64bit) for package: 1:ja
a-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libasound.so.2(ALSA_0.9.0rc4)(64bit) for package: 1:
ava-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libasound.so.2(ALSA_0.9)(64bit) for package: 1:java-
.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXcomposite(x86-64) for package: 1:java-1.8.0-open
dk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: gtk2(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0
342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: fontconfig(x86-64) for package: 1:java-1.8.0-openjdk
```


libxshmfence.x86_64 0:1.2-1.amzn2.0.2
libxslt.x86_64 0:1.1.28-6.amzn2
lksctp-tools.x86_64 0:1.0.17-2.amzn2.0.2
log4j-cve-2021-44228-hotpatch.noarch 0:1.3-
mesa-libEGL.x86_64 0:18.3.4-5.amzn2.0.1
mesa-libGL.x86_64 0:18.3.4-5.amzn2.0.1
mesa-libgbm.x86_64 0:18.3.4-5.amzn2.0.1
mesa-libglapi.x86_64 0:18.3.4-5.amzn2.0.1
pango.x86_64 0:1.42.4-4.amzn2
pcsc-lite-libs.x86_64 0:1.8.8-7.amzn2
pixman.x86_64 0:0.34.0-1.amzn2.0.2
python-javapackages.noarch 0:3.4.1-11.amzn2
python-lxml.x86_64 0:3.2.1-4.amzn2.0.3
ttmkfdir.x86_64 0:3.0.9-42.amzn2.0.2
tzdata-java.noarch 0:2022c-1.amzn2
xorg-x11-font-utils.x86_64 1:7.5-21.amzn2

```
[ec2-user@ip-172-31-92-140 ~]$ java -version
openjdk version "1.8.0_342"
OpenJDK Runtime Environment (build 1.8.0_342-b07)
OpenJDK 64-Bit Server VM (build 25.342-b07, mixed mode)
[ec2-user@ip-172-31-92-140 ~]$
```

Step2: Install Elastic search on AWS Server

root@ip-172-31-92-140:~

```
[ec2-user@ip-172-31-92-140 ~]$ sudo su
[root@ip-172-31-92-140 ec2-user]# yum install -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Error: Need to pass a list of pkgs to install
 Mini usage:

install PACKAGE...

Install a package or packages on your system

aliases: install-n, install-na, install-nevra
[root@ip-172-31-92-140 ec2-user]# cd /root
[root@ip-172-31-92-140 ~]# wget  https://download.elastic.co/elasticsearch/elast
icsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-09 13:39:01--  https://download.elastic.co/elasticsearch/elasticsearch
/elasticsearch-1.7.2.noarch.rpm
Resolving download.elastic.co (download.elastic.co)... 34.120.127.130, 2600:1901
:0:1d7::
Connecting to download.elastic.co (download.elastic.co)|34.120.127.130|:443... c
onnected.
HTTP request sent, awaiting response... 200 OK
Length: 27304727 (26M) [binary/octet-stream]
Saving to: 'elasticsearch-1.7.2.noarch.rpm'

100%[======================================>] 27,304,727  31.8MB/s   in 0.8s
```

```
2022-10-09 13:39:03 (31.8 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [273047
27/27304727]

[root@ip-172-31-92-140 ~]# yum install elasticsearch-1.7.2.noarch.rpm -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Examining elasticsearch-1.7.2.noarch.rpm: elasticsearch-1.7.2-1.noarch
Marking elasticsearch-1.7.2.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package elasticsearch.noarch 0:1.7.2-1 will be installed
--> Finished Dependency Resolution
amzn2-core/2/x86_64                                      | 3.7 kB     00:00

Dependencies Resolved

================================================================================
 Package           Arch       Version     Repository                       Size
================================================================================
Installing:
 elasticsearch     noarch     1.7.2-1     /elasticsearch-1.7.2.noarch      30 M

Transaction Summary
================================================================================
Install  1 Package

Total size: 30 M
Installed size: 30 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Creating elasticsearch group... OK
Creating elasticsearch user... OK
  Installing : elasticsearch-1.7.2-1.noarch                                 1/1
### 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
```

Step3: Start the Server

```
[root@ip-172-31-92-140 ~]# service elasticsearch start
Starting elasticsearch (via systemctl):                    [  OK
[root@ip-172-31-92-140 ~]#
```

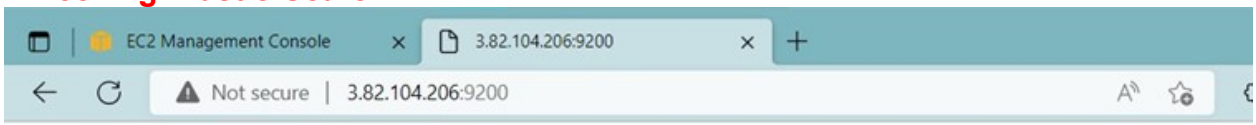
Step4: Automatically Boot u on start

```
[root@ip-172-31-92-140 ~]# service elasticsearch start
Starting elasticsearch (via systemctl):                    [  OK
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-92-140 ~]#
```

Step5:Configuring AWS IP so you can access using public IP

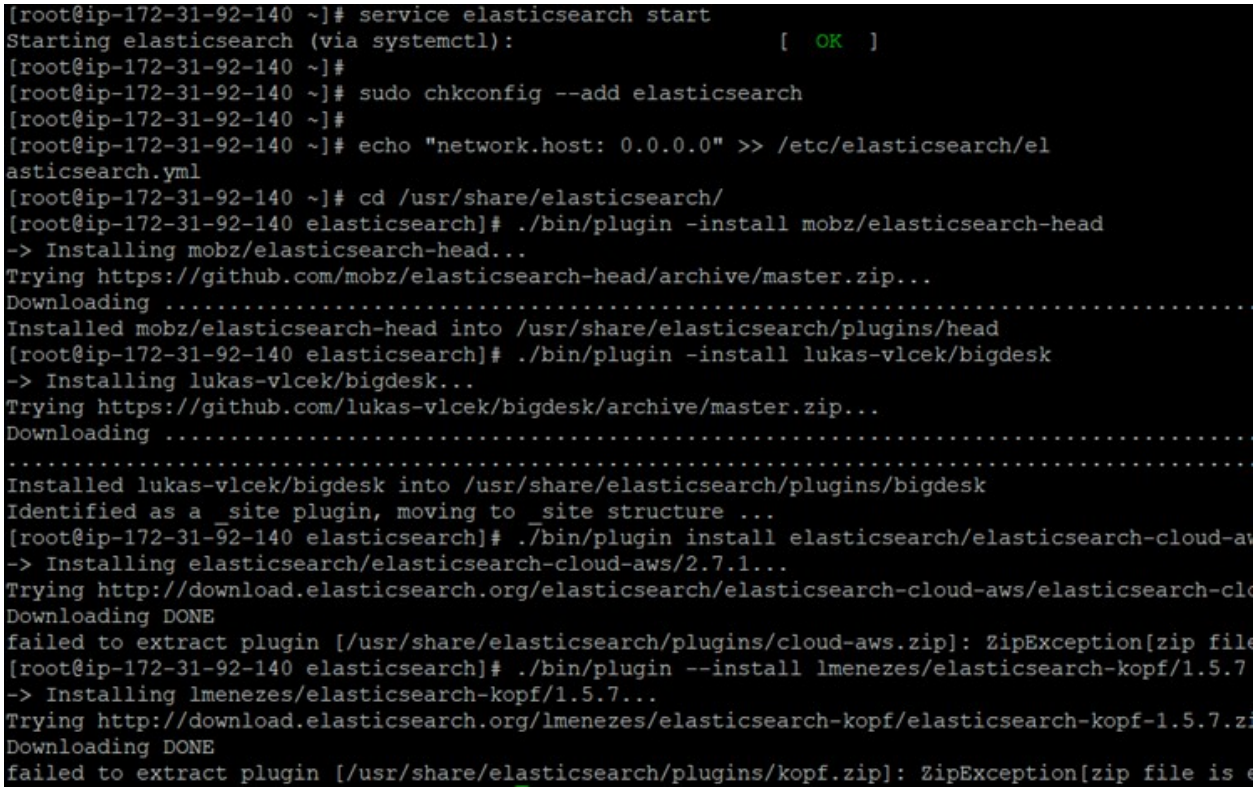
```
[root@ip-172-31-92-140 ~]# service elasticsearch start
Starting elasticsearch (via systemctl):                    [  OK  ]
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/el
asticsearch.yml
[root@ip-172-31-92-140 ~]#
```

Checking Elastic Search




```
{
  "status" : 200,
  "name" : "Uatu",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.7.2",
    "build_hash" : "e43676b1385b8125d647f593f7202acbd816e8ec",
    "build_timestamp" : "2015-09-14T09:49:53Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
```

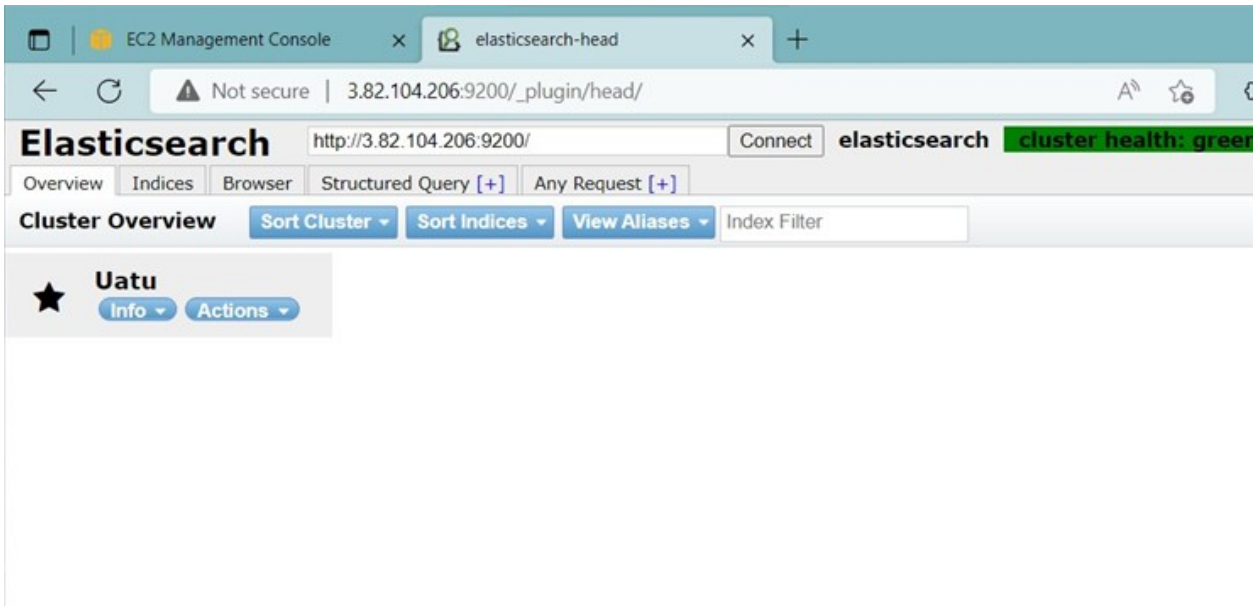

Step6:Install Plugins

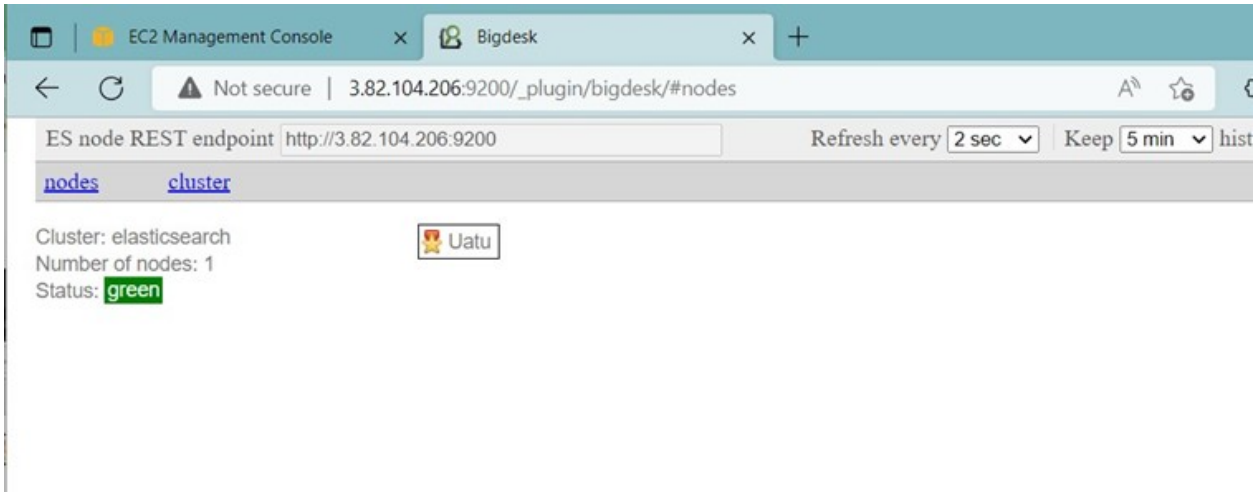


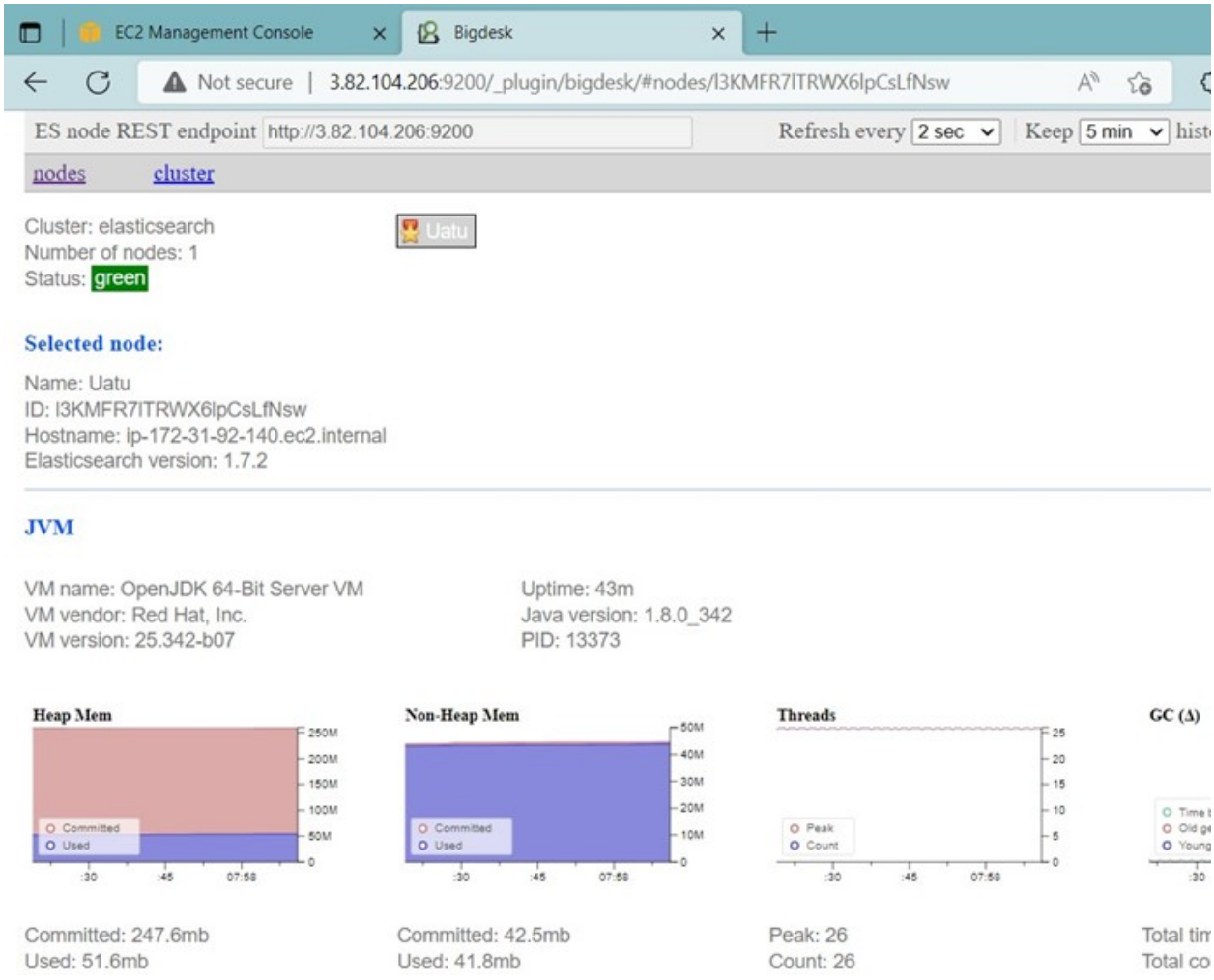
Step 7:Install Kibana

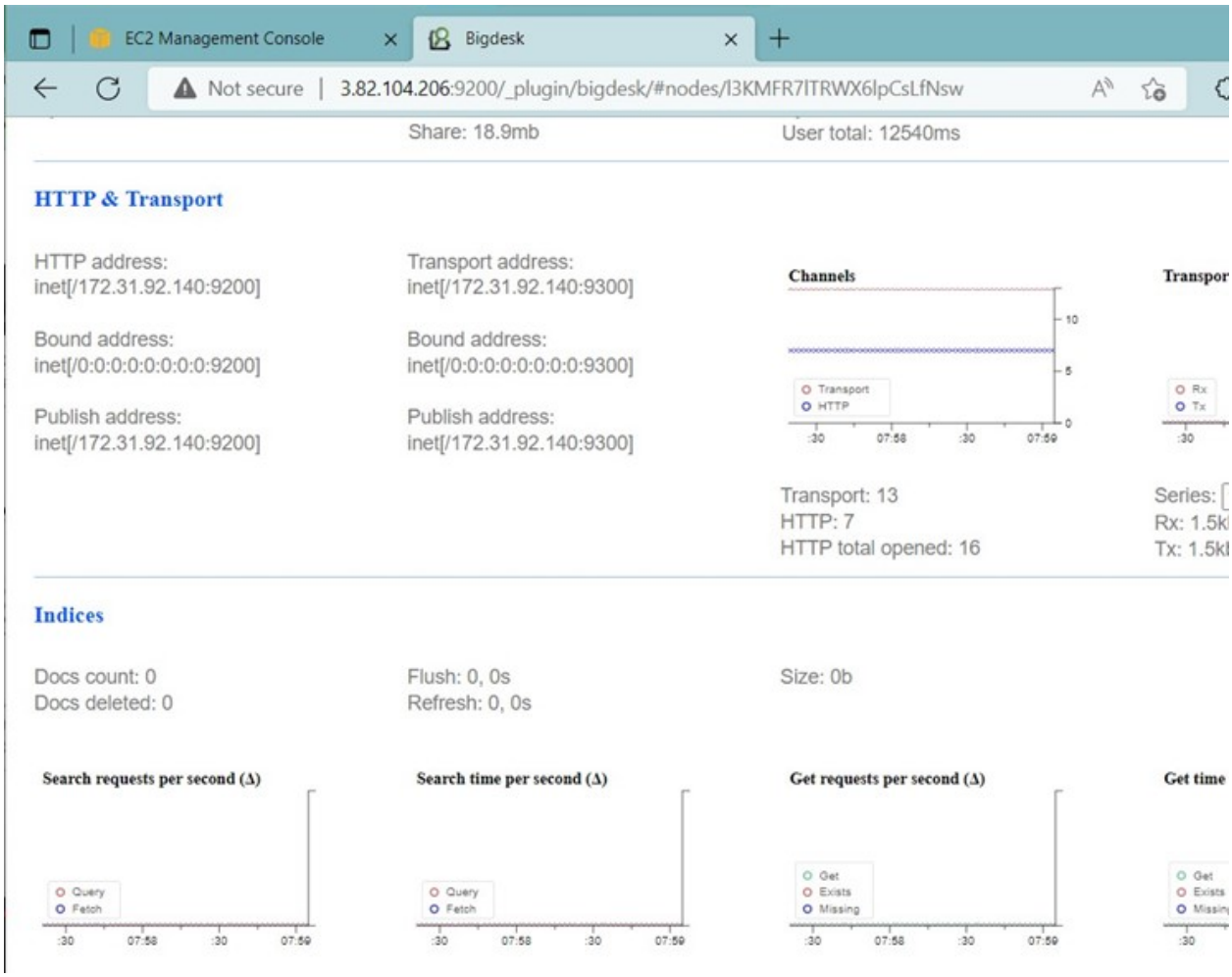
```
[root@ip-172-31-92-140 elasticsearch]# sudo su
[root@ip-172-31-92-140 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No packages marked for update
[root@ip-172-31-92-140 elasticsearch]# cd /root
[root@ip-172-31-92-140 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-09 14:17:18--  https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
Resolving download.elastic.co (download.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to download.elastic.co (download.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11787239 (11M) [binary/octet-stream]
Saving to: 'kibana-4.1.2-linux-x64.tar.gz'

100%[======================================================================================================================================================>] 11,787,239  --.-K/s   in 1.2s

2022-10-09 14:17:19 (9.50 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]

[root@ip-172-31-92-140 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-92-140 ~]# rm -f kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-92-140 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]#
```

```
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 1949
```




EC2 Management Console
Bigdesk
Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes
ES node REST endpoint http://3.82.104.206:9200
Refresh every 2 sec
Keep 5 min
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Uatu


EC2 Management Console
Bigdesk
Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/l3KMFR7ITRWX6lpCsLfNsw
ES node REST endpoint http://3.82.104.206:9200
Refresh every 2 sec
Keep 5 min
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Uatu
Selected node:
Name: Uatu
ID: l3KMFR7ITRWX6lpCsLfNsw
Hostname: ip-172-31-92-140.ec2.internal
Elasticsearch version: 1.7.2
JVM
VM name: OpenJDK 64-Bit Server VM
VM vendor: Red Hat, Inc.
VM version: 25.342-b07
Uptime: 43m
Java version: 1.8.0_342
PID: 13373
Heap Mem
Committed
Used
Committed: 247.6mb
Used: 51.6mb
Non-Heap Mem
Committed
Used
Committed: 42.5mb
Used: 41.8mb
Threads
Peak
Count
Peak: 26
Count: 26
GC (Δ)


EC2 Management Console
Bigdesk
Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/l3KMFR7ITRWX6lpCsLfNsw
Share: 18.9mb
User total: 12540ms
HTTP & Transport
HTTP address:
inet[/172.31.92.140:9200]
Bound address:
inet[/0:0:0:0:0:0:0:0:9200]
Publish address:
inet[/172.31.92.140:9200]
Transport address:
inet[/172.31.92.140:9300]
Bound address:
inet[/0:0:0:0:0:0:0:0:9300]
Publish address:
inet[/172.31.92.140:9300]
Channels
Transport
HTTP
Transport: 13
HTTP: 7
HTTP total opened: 16
Rx
Tx
Series:
Rx: 1.5k
Tx: 1.5k
Indices
Docs count: 0
Docs deleted: 0
Flush: 0, 0s
Refresh: 0, 0s
Size: 0b
Search requests per second (Δ)
Query
Fetch
Search time per second (Δ)
Query
Fetch
Get requests per second (Δ)
Get
Exists
Missing
Get time
Get
Exists
:30
07:58
:30
07:59