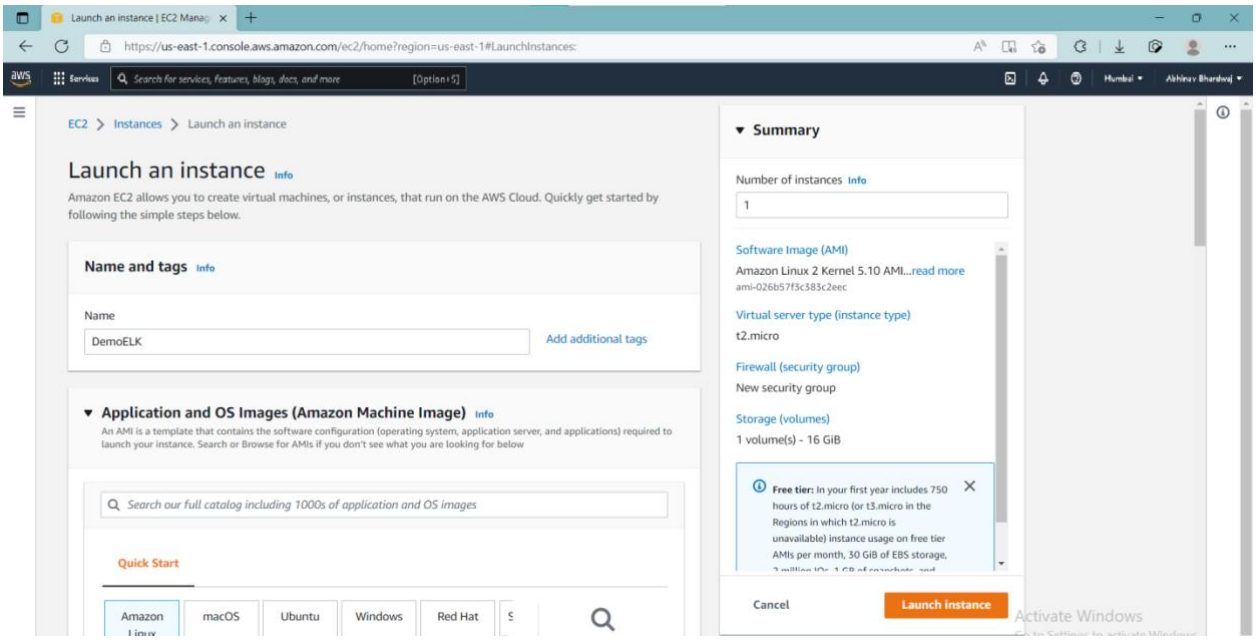
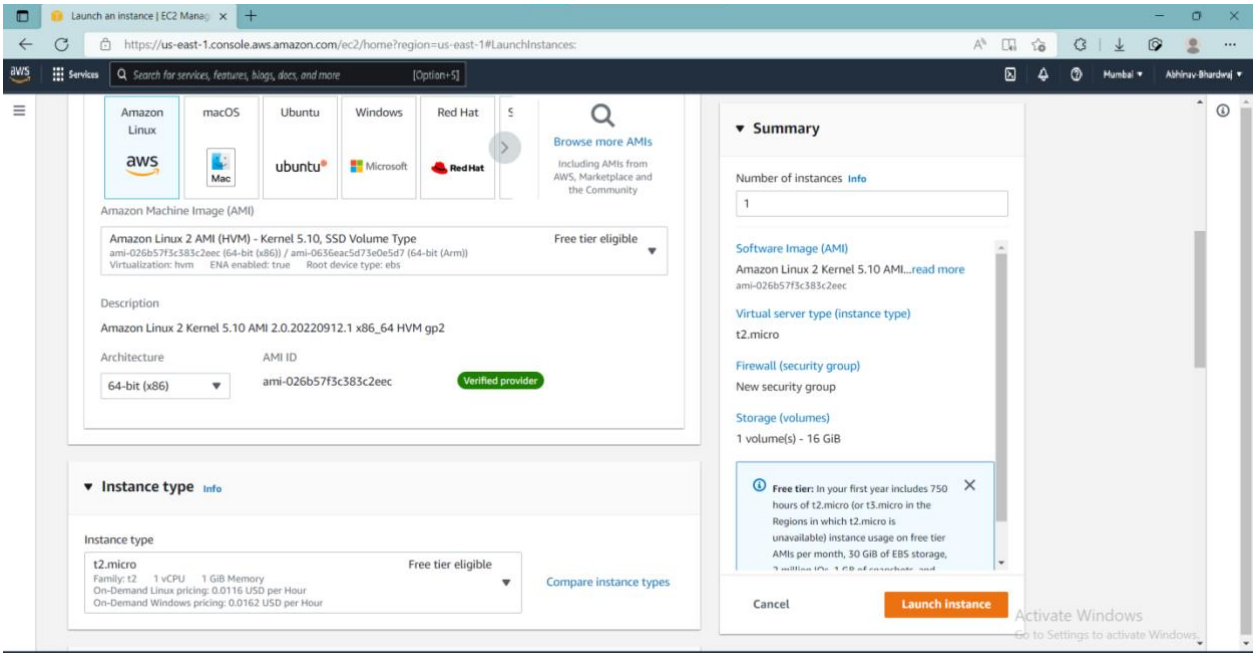
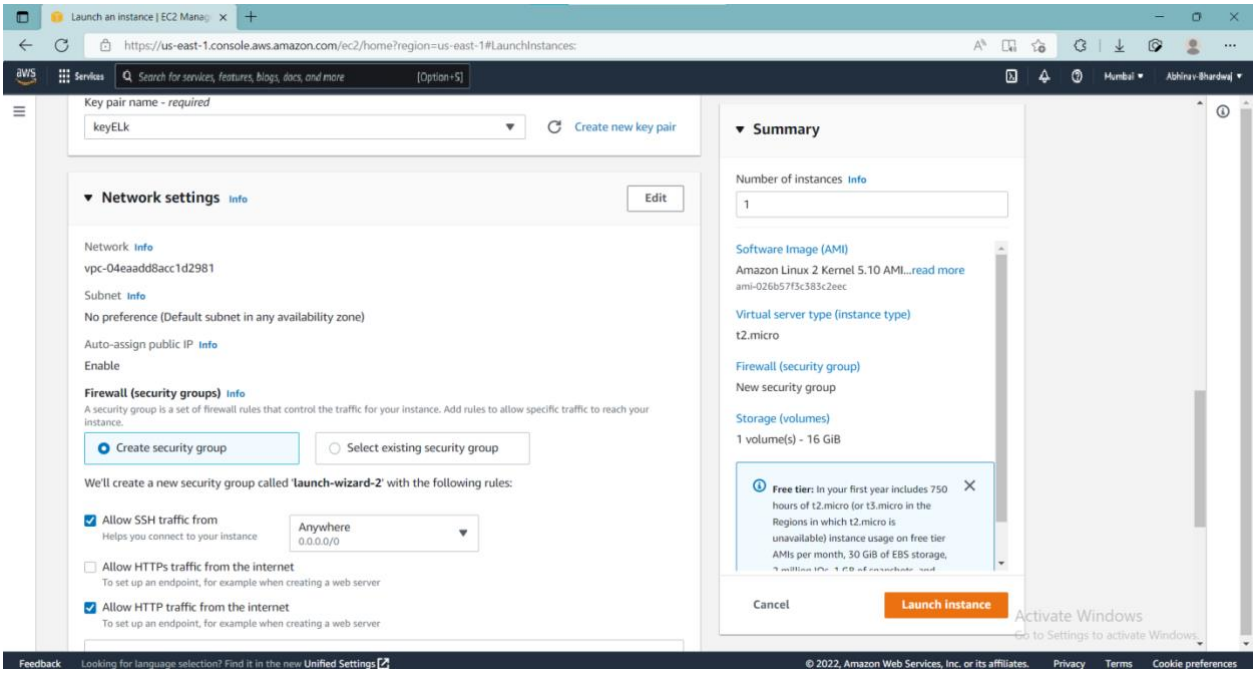
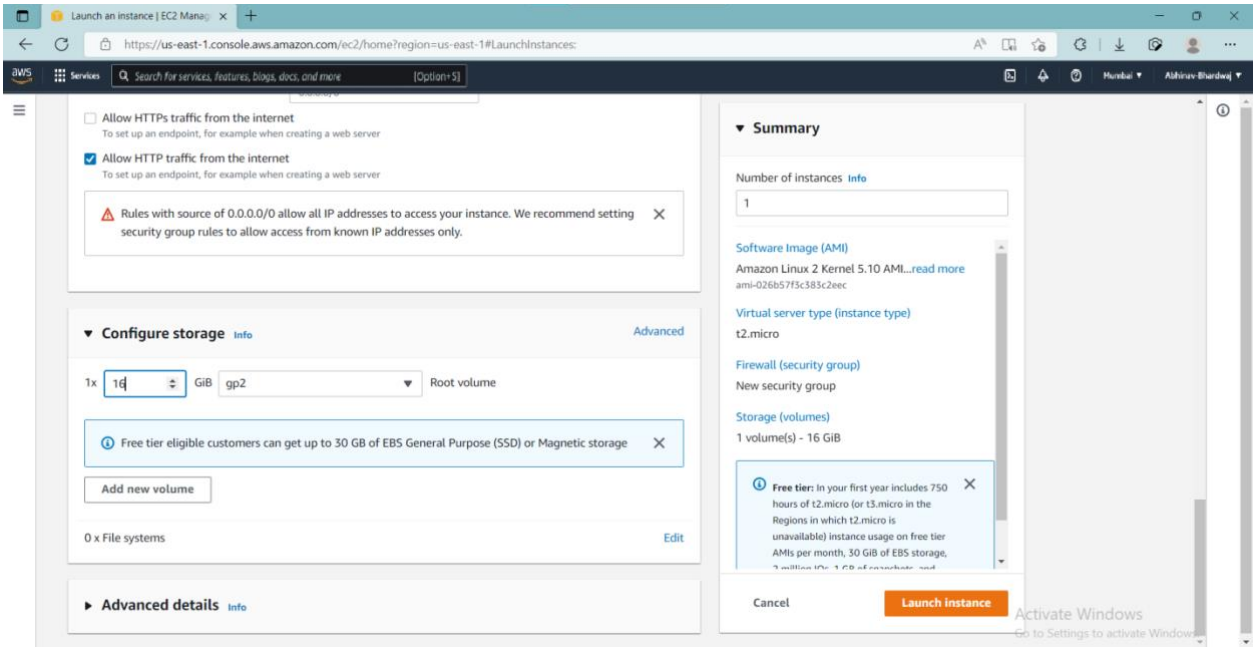
Steps to Deploy ELK Stack on Docker Container

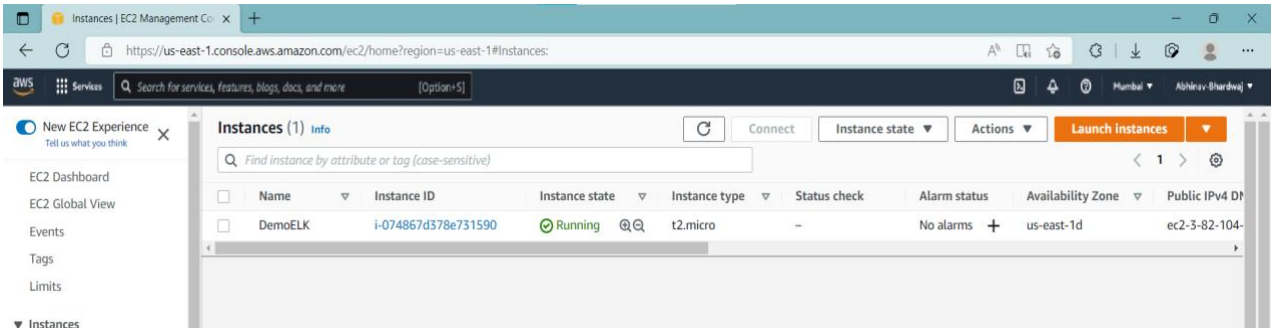
Creating EC2 instance on AWS



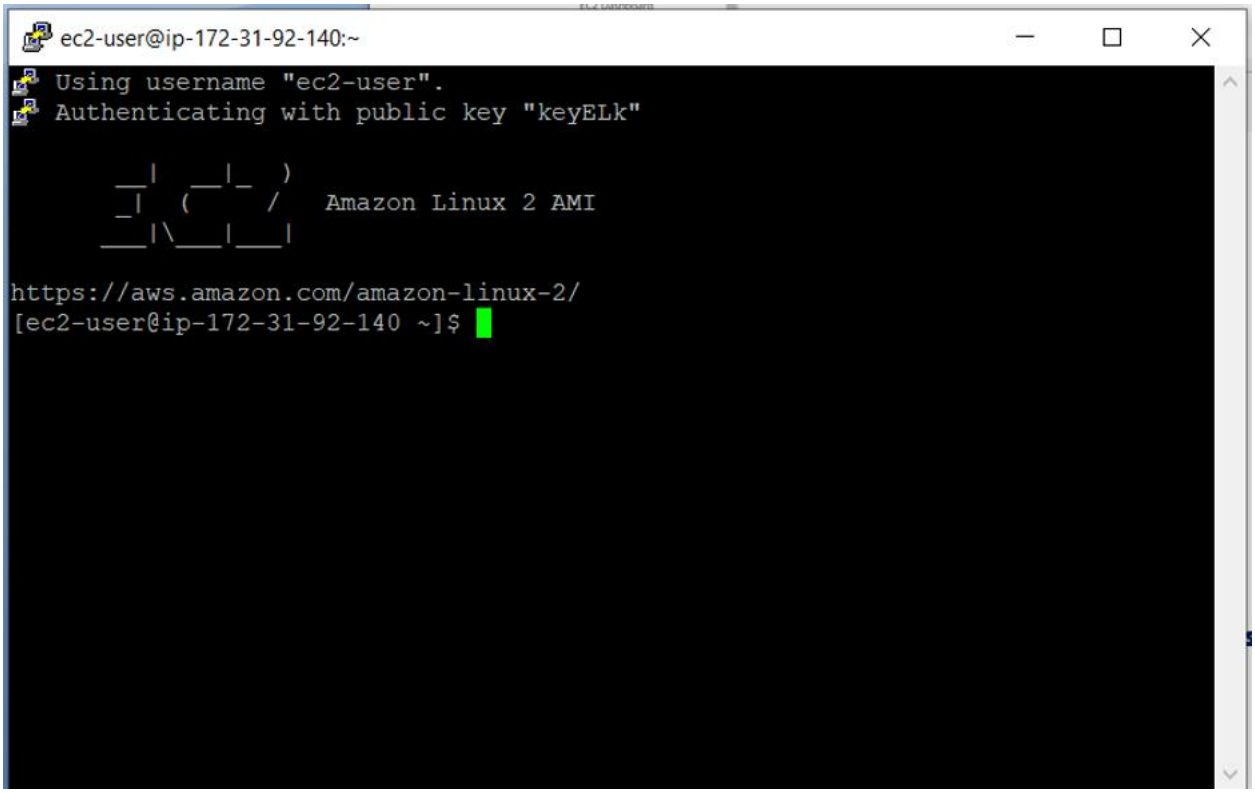



Launch an instance | EC2 Manag
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Key pair name - required
keyELk
Create new key pair
Network settings Info
Edit
Network Info
vpc-04eaadd8acc1d2981
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign 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
0.0.0.0/0
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
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
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Launch an instance | EC2 Manag
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
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


Instances | EC2 Management Co
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DN
DemoELK
i-074867d378e731590
Running
t2.micro
–
No alarms
us-east-1d
ec2-3-82-104-

Connecting local machine with the instance



Now using the instance terminal, installing requirements on instance

- Installing Java JDK

```
ec2-user@ip-172-31-92-140:~
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 insta
lled
--> Processing Dependency: java-1.8.0-openjdk-headless(x86-64) = 1:1.8.0.342.b07
-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-openjd
k-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjvm.so(SUNWprivate_1.1)(64bit) for package: 1:java
-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:jav
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:j
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-1
.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-openj
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-
1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjvm.so()(64bit) for package: 1:java-1.8.0-openjdk-
1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjava.so()(64bit) for package: 1:java-1.8.0-openjdk
-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libgif.so.4()(64bit) for package: 1:java-1.8.0-openjd
k-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libasound.so.2()(64bit) for package: 1:java-1.8.0-ope
njdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXtst.so.6()(64bit) for package: 1:java-1.8.0-openj
dk-1.8.0.342.b07-1.amzn2.0.1.x86_64
```

```
  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 0:1.3-7.amzn2
  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
  xorg-x11-fonts-Type1.noarch 0:7.5-9.amzn2

Complete!
[ec2-user@ip-172-31-92-140 ~]$
```

ec2-user@ip-172-31-92-140:~

```
[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 ~]$
```

- Installing ElasticSearch and configuring for autoboot and making is accessible via public IP

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

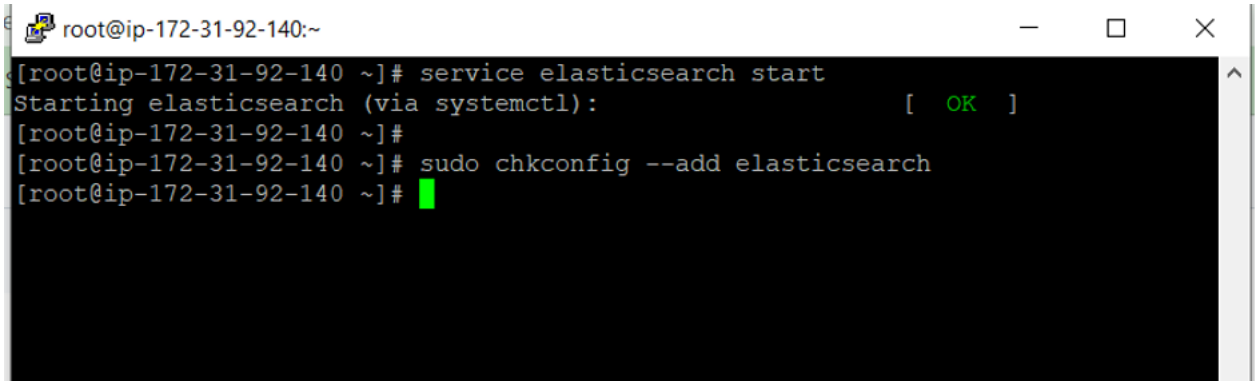
```
[ec2-user@ip-172-31-92-140 ~]$ sudo su
[root@ip-172-31-92-140 ec2-user]# yum install -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Error: Need to pass a list of pkgs to install
 Mini usage:

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
```

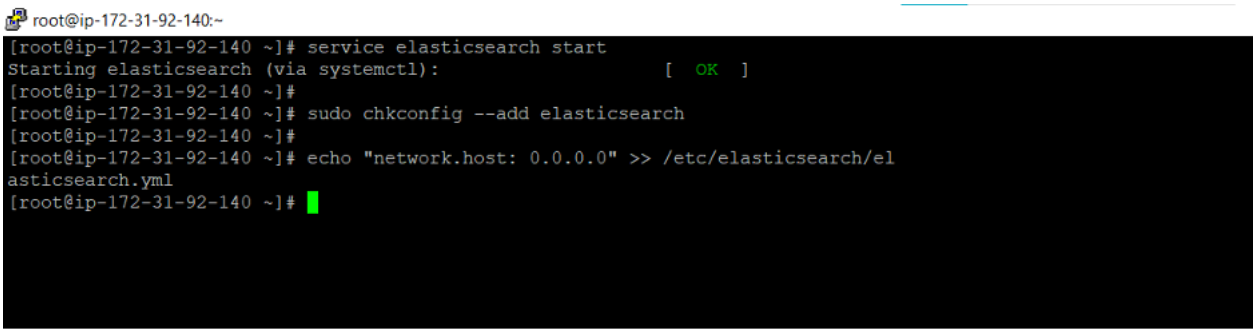
root@ip-172-31-92-140:~

```
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
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
  Verifying  : elasticsearch-1.7.2-1.noarch                                 1/1

Installed:
  elasticsearch.noarch 0:1.7.2-1

Complete!
[root@ip-172-31-92-140 ~]# rm -f elasticsearch-1.7.2.noarch.rpm
```

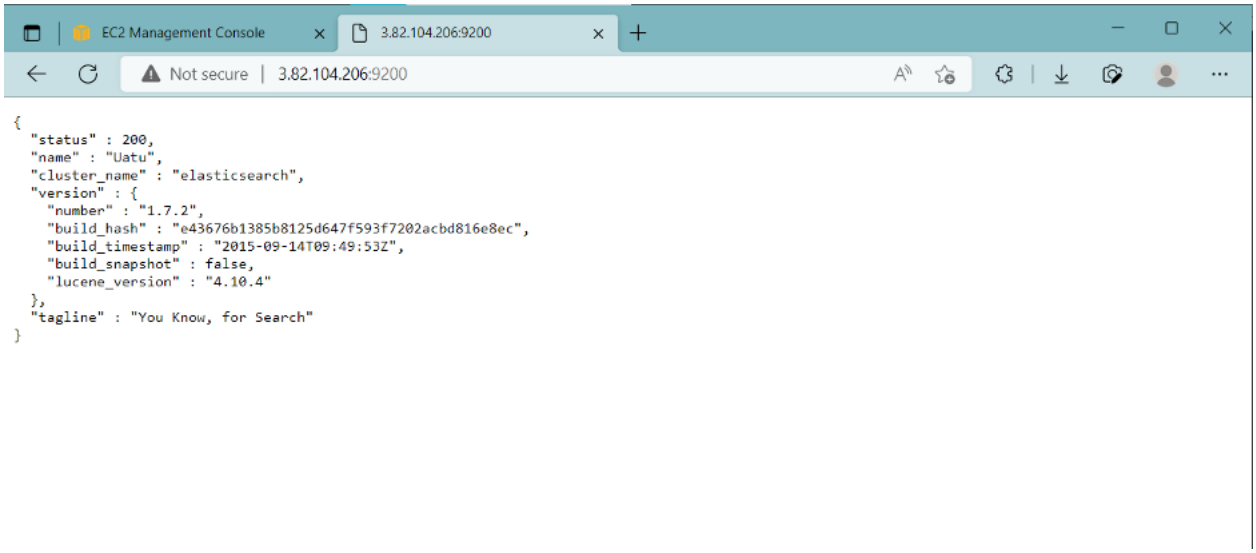
root@ip-172-31-92-140:~

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





- Checking ElasticSearch via public IP



- Installing required plugins

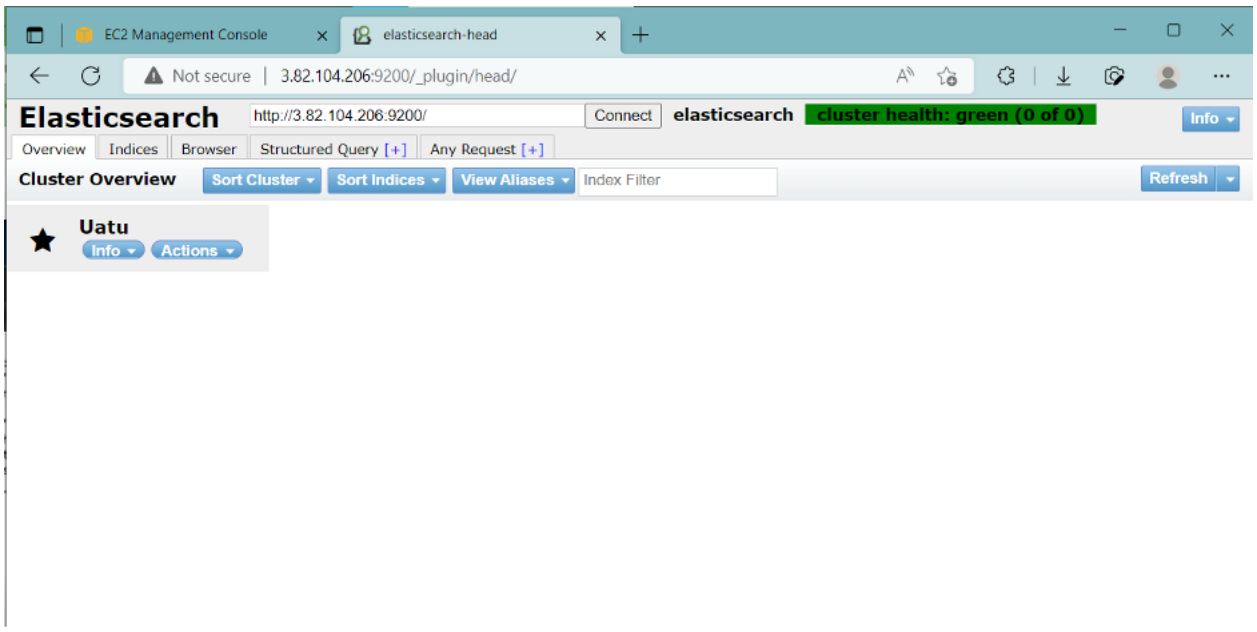
```
root@ip-172-31-92-140:/usr/share/elasticsearch
[root@ip-172-31-92-140 ~]# service elasticsearch start
Starting elasticsearch (via systemctl):                    [  OK  ]
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/el
asticsearch.yml
[root@ip-172-31-92-140 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-92-140 elasticsearch]# ./bin/plugin -install mobz/elasticsearch-head
-> Installing mobz/elasticsearch-head...
Trying https://github.com/mobz/elasticsearch-head/archive/master.zip...
Downloading ..........................................................................................................
Installed mobz/elasticsearch-head into /usr/share/elasticsearch/plugins/head
[root@ip-172-31-92-140 elasticsearch]# ./bin/plugin -install lukas-vlcek/bigdesk
-> Installing lukas-vlcek/bigdesk...
Trying https://github.com/lukas-vlcek/bigdesk/archive/master.zip...
Downloading ..........................................................................................................
.......................................................................................................DONE
Installed lukas-vlcek/bigdesk into /usr/share/elasticsearch/plugins/bigdesk
Identified as a _site plugin, moving to _site structure ...
[root@ip-172-31-92-140 elasticsearch]# ./bin/plugin install elasticsearch/elasticsearch-cloud-aws/2.7.1
-> Installing elasticsearch/elasticsearch-cloud-aws/2.7.1...
Trying http://download.elasticsearch.org/elasticsearch/elasticsearch-cloud-aws/elasticsearch-cloud-aws-2.7.1.zip...
Downloading DONE
failed to extract plugin [/usr/share/elasticsearch/plugins/cloud-aws.zip]: ZipException[zip file is empty]
[root@ip-172-31-92-140 elasticsearch]# ./bin/plugin --install lmenezes/elasticsearch-kopf/1.5.7
-> Installing lmenezes/elasticsearch-kopf/1.5.7...
Trying http://download.elasticsearch.org/lmenezes/elasticsearch-kopf/elasticsearch-kopf-1.5.7.zip...
Downloading DONE
failed to extract plugin [/usr/share/elasticsearch/plugins/kopf.zip]: ZipException[zip file is empty]
[root@ip-172-31-92-140 elasticsearch]#
```

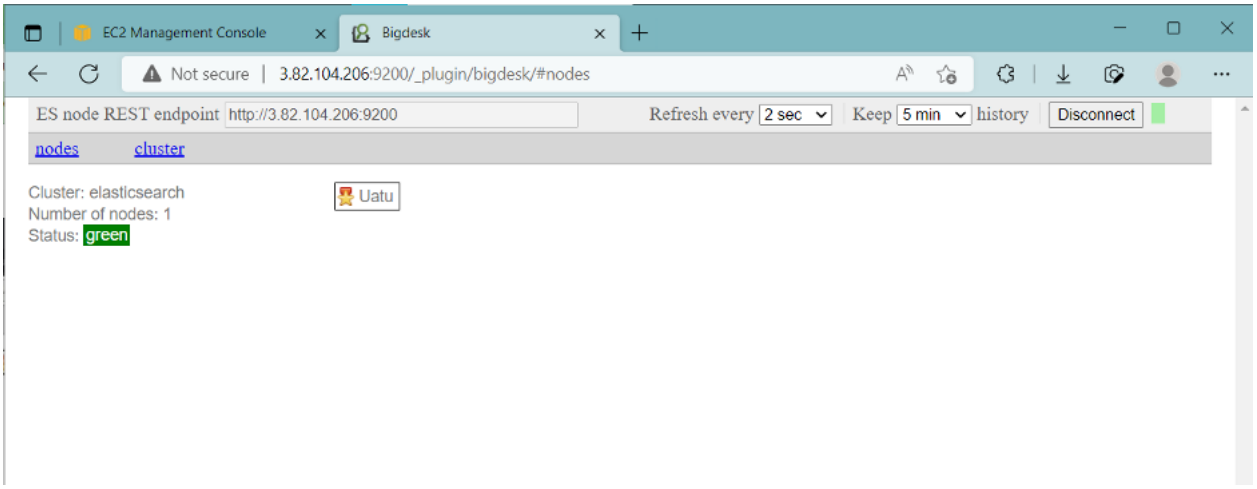
- Installing Kibana

```
root@ip-172-31-92-140:~/kibana-4.1.2-linux-x64
[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                                                                                                  | 3.7 kB  00:00:00
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: 11707239 (11M) [binary/octet-stream]
Saving to: 'kibana-4.1.2-linux-x64.tar.gz'

100%[=====================================================================================================================>] 11,707,239  9.50MB/s   in 1.2s

2022-10-09 14:17:19 (9.50 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11707239/11707239]

[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
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'

[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]#
```

Checking user interface for data analysis and data visualization deployed ELK Stack :-





EC2 Management Console | Bigdesk

Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/I3KMFR7ITRWX6lpCsLfNsw

ES node REST endpoint http://3.82.104.206:9200 Refresh every 2 sec Keep 5 min history Disconnect

nodes cluster

Cluster: elasticsearch
Number of nodes: 1
Status: green

Uatu

Selected node:

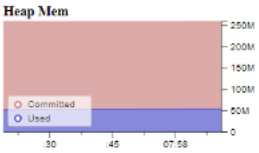
Name: Uatu
ID: I3KMFR7ITRWX6lpCsLfNsw
Hostname: ip-172-31-92-140.ec2.internal
Elasticsearch version: 1.7.2

JVM

VM name: OpenJDK 64-Bit Server VM
VM vendor: Red Hat, Inc.
VM version: 25.342-b07

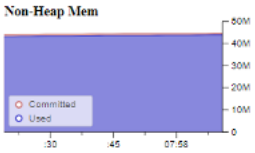
Uptime: 43m
Java version: 1.8.0_342
PID: 13373

Heap Mem



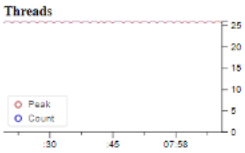
Committed: 247.6mb
Used: 51.6mb

Non-Heap Mem



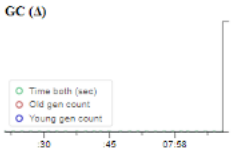
Committed: 42.5mb
Used: 41.8mb

Threads



Peak: 26
Count: 26

GC (Δ)



Total time (O/Y): 37ms / 93ms
Total count (O/Y): 1 / 2

Thread Pools

Search

Index

Bulk

Refresh

EC2 Management Console | Bigdesk

Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/I3KMFR7ITRWX6lpCsLfNsw

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]

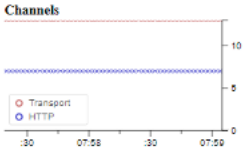
Publish address:
inet[/172.31.92.140:9200]

Transport address:
inet[/172.31.92.140:9300]

Bound address:
inet[/0:0:0:0:0:0:0:0:9300]

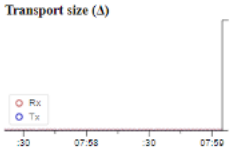
Publish address:
inet[/172.31.92.140:9300]

Channels



Transport: 13
HTTP: 7
HTTP total opened: 16

Transport size (Δ)



Series: weighted avg
Rx: 1.5kb, #6
Tx: 1.5kb, #6

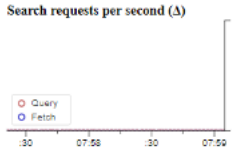
Indices

Docs count: 0
Docs deleted: 0

Flush: 0, 0s
Refresh: 0, 0s

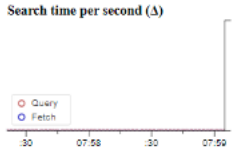
Size: 0b

Search requests per second (Δ)



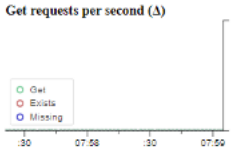
Query: 0
Fetch: 0

Search time per second (Δ)



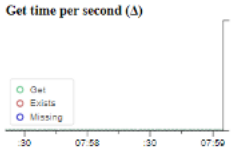
Query: 0s
Fetch: 0s

Get requests per second (Δ)



Get: 0
Exists: 0
Missing: 0

Get time per second (Δ)



Get: 0s
Exists: 0s
Missing: 0s

Cache size

Cache evictions (Δ)

Indexing requests per second (Δ)

Indexing time per second (Δ)