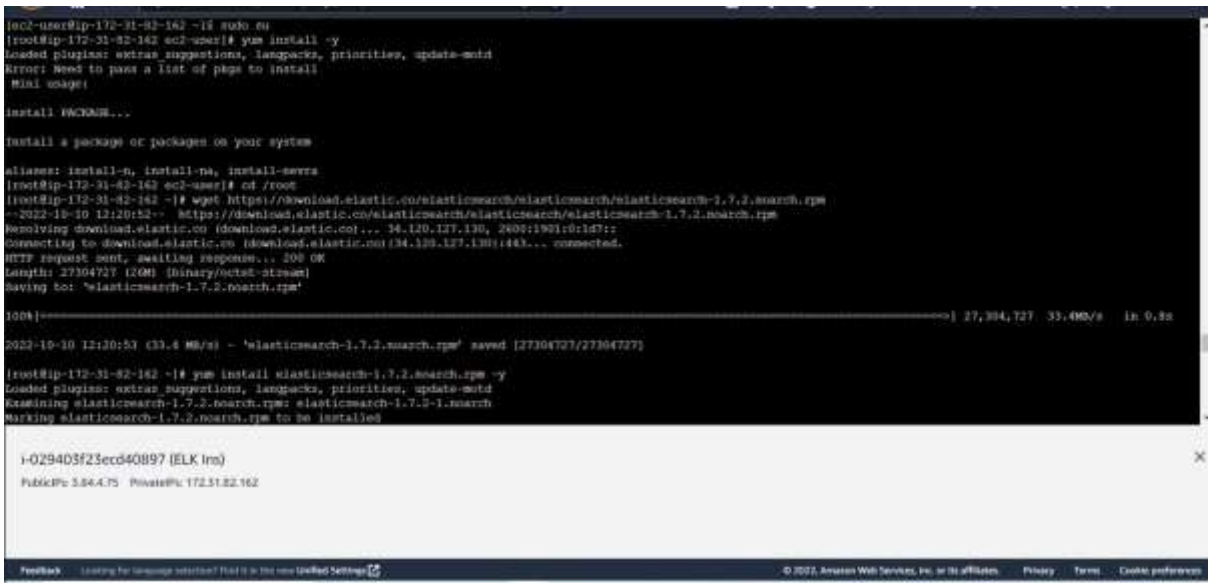
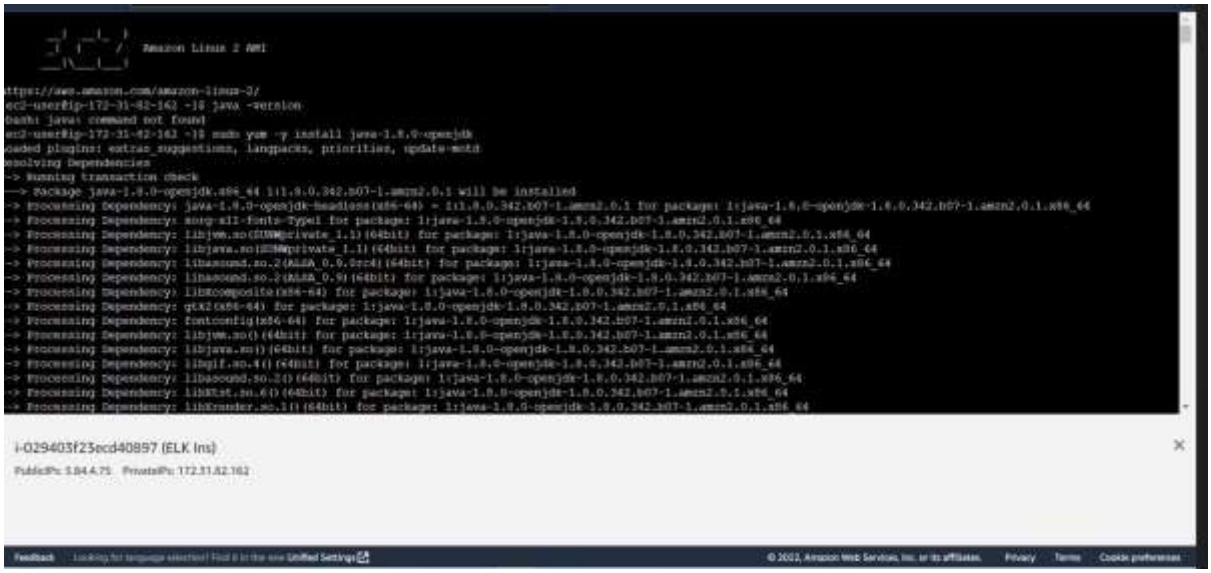
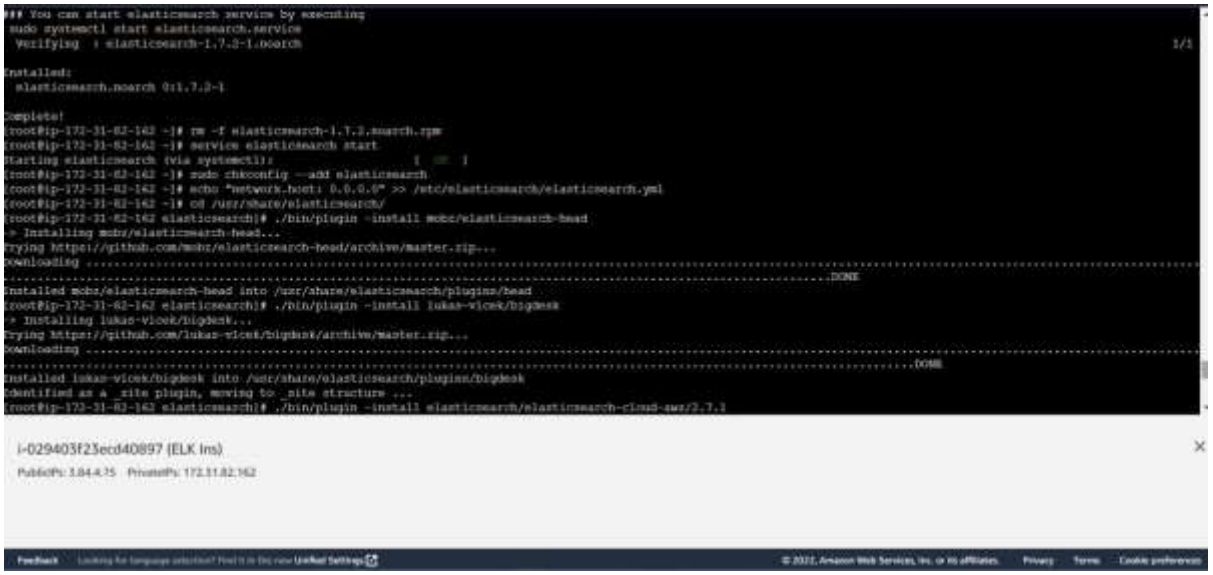
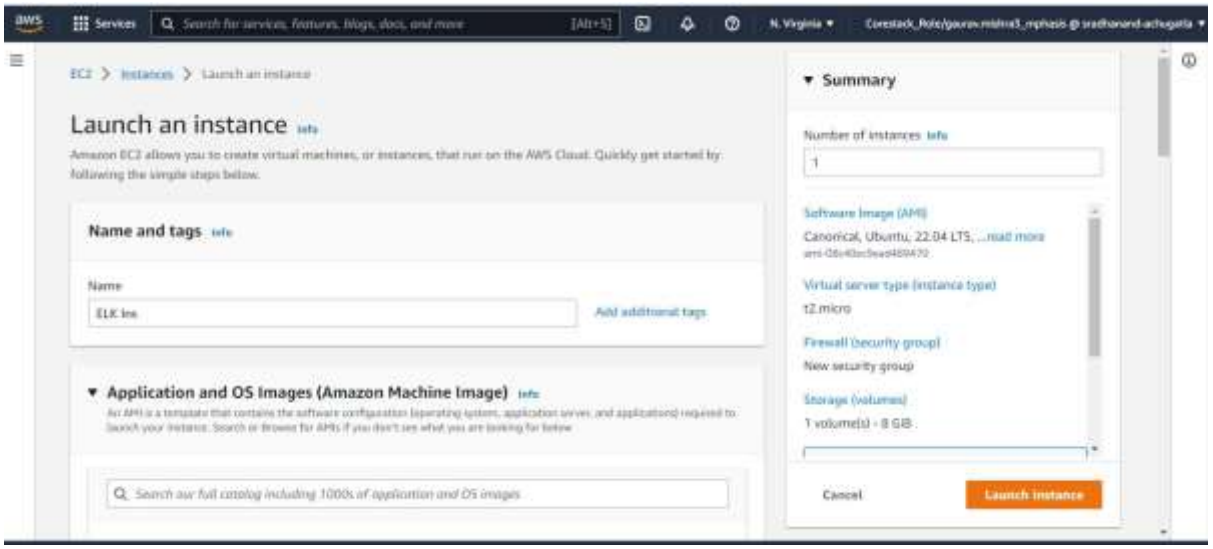
Project: Deploying ELK Stack on Docker Container.

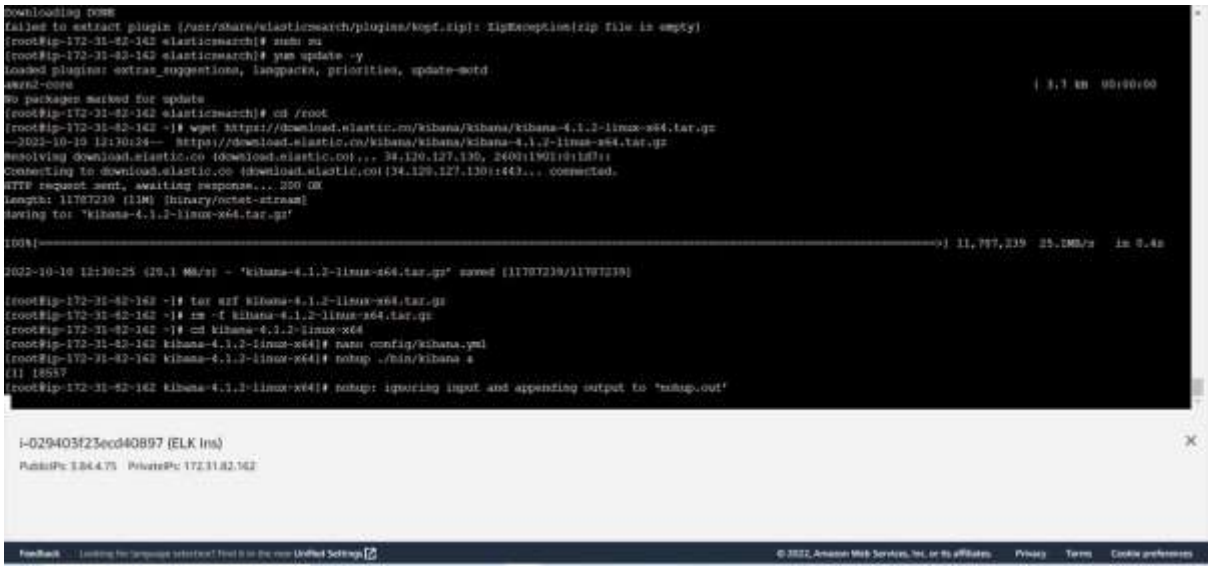
Screenshots:

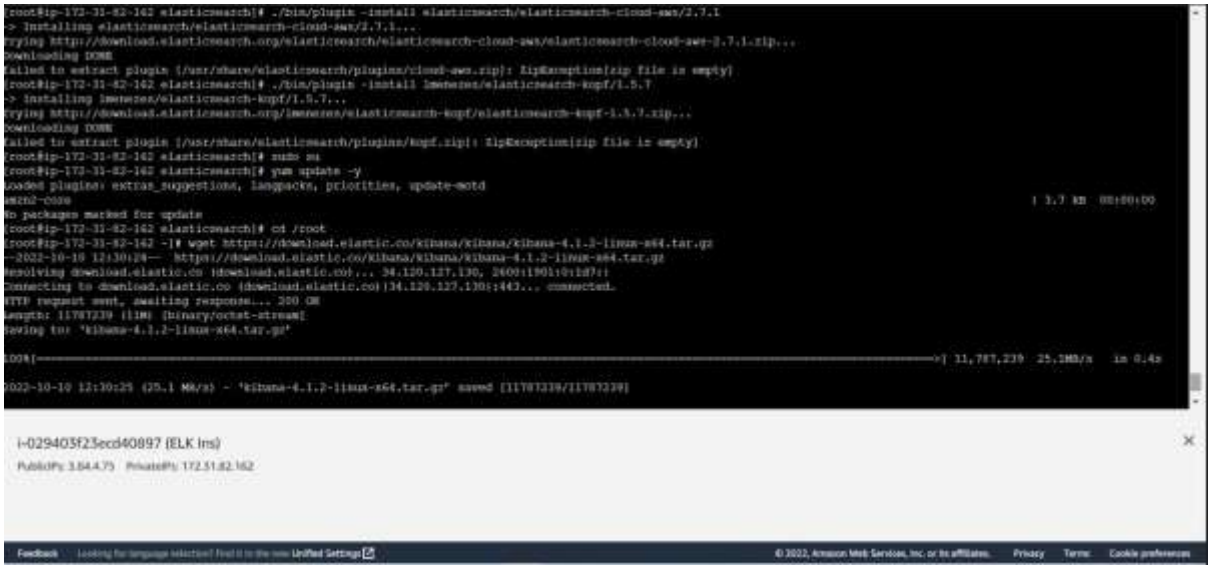


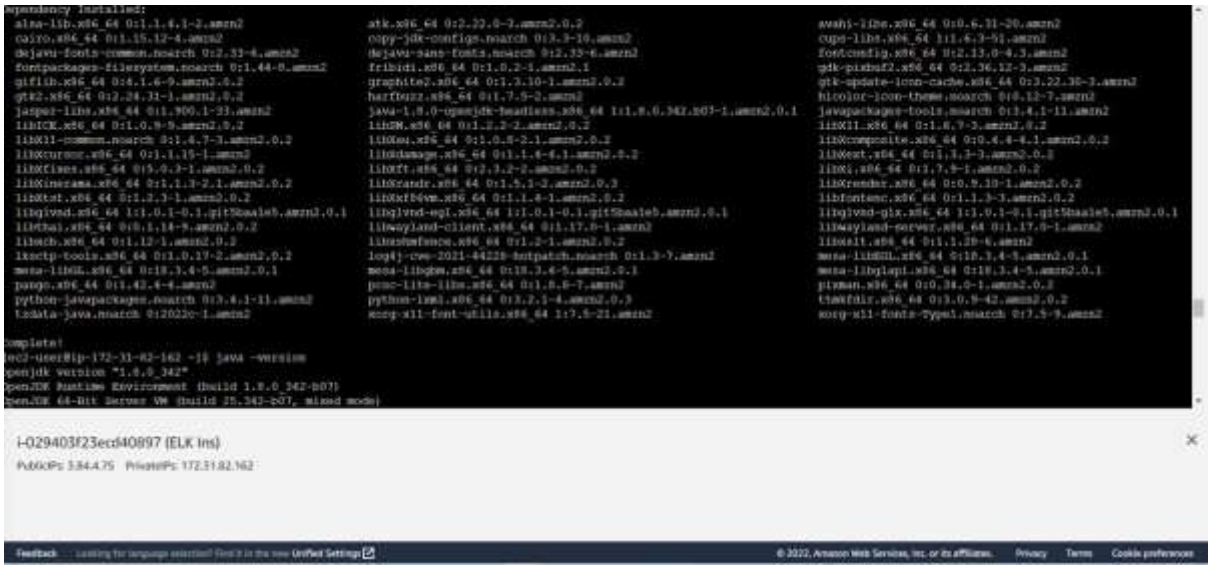


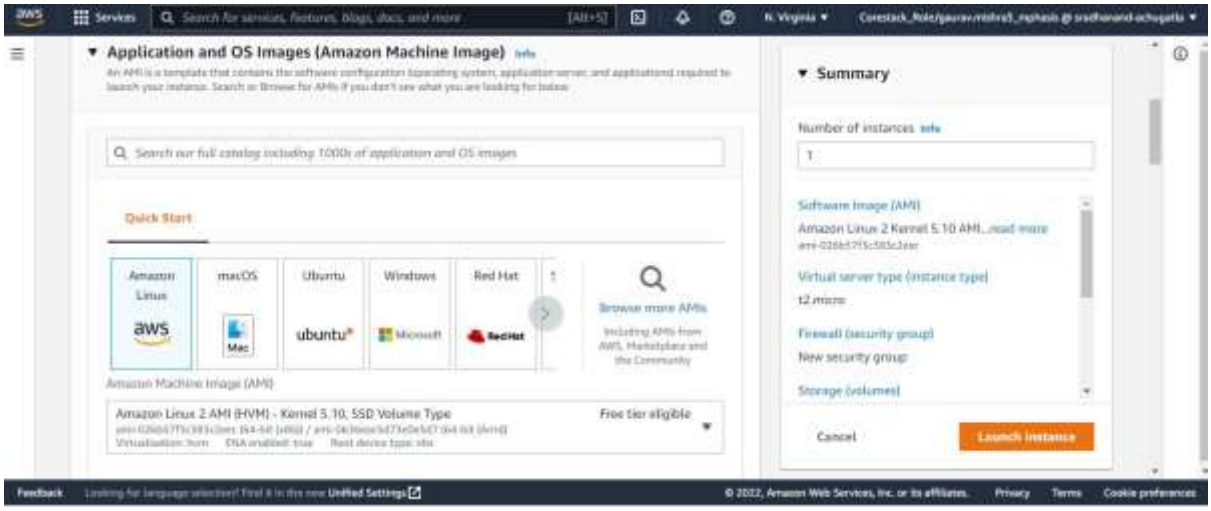

You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Verifying : elasticsearch-1.7.2-1.noarch 1/1
Installed:
elasticsearch.noarch 0:1.7.2-1
Complete!
[root@ip-172-31-82-162 ~]# rm -f elasticsearch-1.7.2.noarch.rpm
[root@ip-172-31-82-162 ~]# service elasticsearch start
Starting elasticsearch (via systemctl): [OK]
[root@ip-172-31-82-162 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-82-162 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-82-162 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-82-162 elasticsearch]# ./bin/plugin -install mobz/elasticsearch-head
-> Installing mobz/elasticsearch-head...
Trying https://github.com/mobz/elasticsearch-head/archive/master.zip...
Downloading .....DONE
Installed mobz/elasticsearch-head into /usr/share/elasticsearch/plugins/head
[root@ip-172-31-82-162 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-172-31-82-162 elasticsearch]# ./bin/plugin -install elasticsearch/elasticsearch-cloud-aws/2.7.1
i-029403f23ecd40897 (ELK ins)
PublicIPs: 3.84.4.75 PrivateIPs: 172.31.82.162

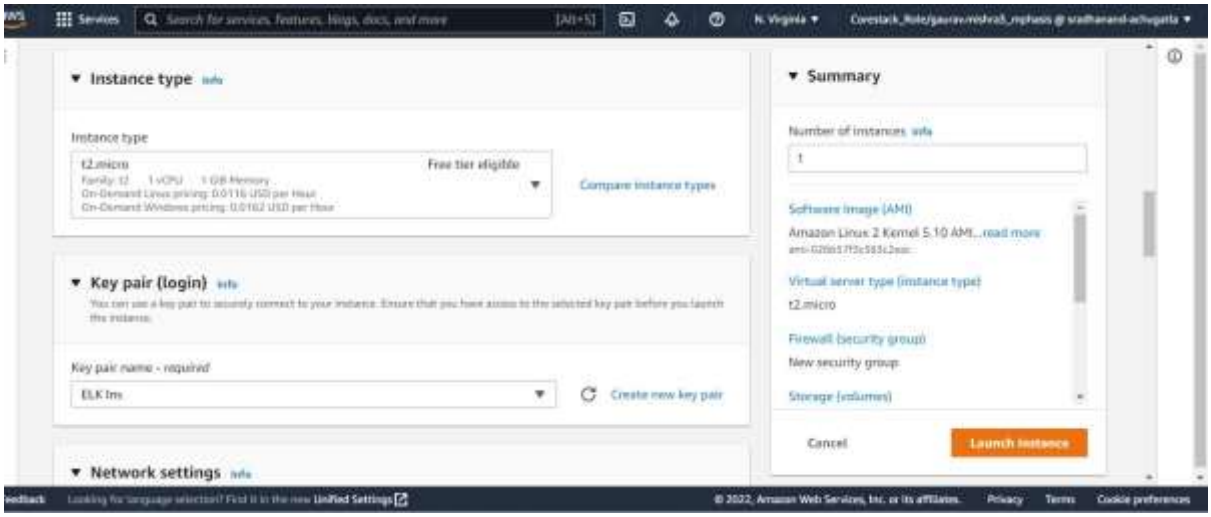

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
ELK ins
Add additional tags
Application and OS Images (Amazon Machine Image) Info
Search our full catalog including 1000s of application and OS images
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance

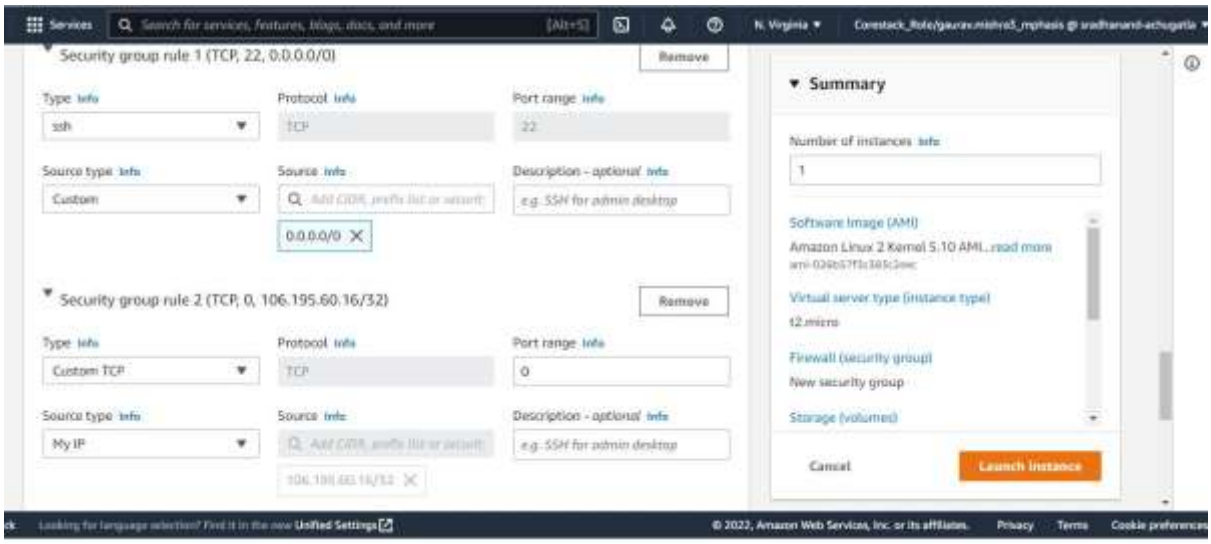

Downloading DONE
Failed to extract plugin [/usr/share/elasticsearch/plugins/kopf.zip]: ZipException[zip file is empty]
[root@ip-172-31-82-162 elasticsearch]# sudo su
[root@ip-172-31-82-162 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.7 kB 00:00:00
No packages marked for update
[root@ip-172-31-82-162 elasticsearch]# cd /root
[root@ip-172-31-82-162 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-10 12:30:24-- 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 25.1MB/s in 0.4s
2022-10-10 12:30:25 (25.1 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]
[root@ip-172-31-82-162 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-82-162 ~]# rm -f kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-82-162 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-82-162 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-82-162 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 18557
[root@ip-172-31-82-162 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'
i-029403f23ecd40897 (ELK ins)
PublicIPs: 3.84.4.75 PrivateIPs: 172.31.82.162

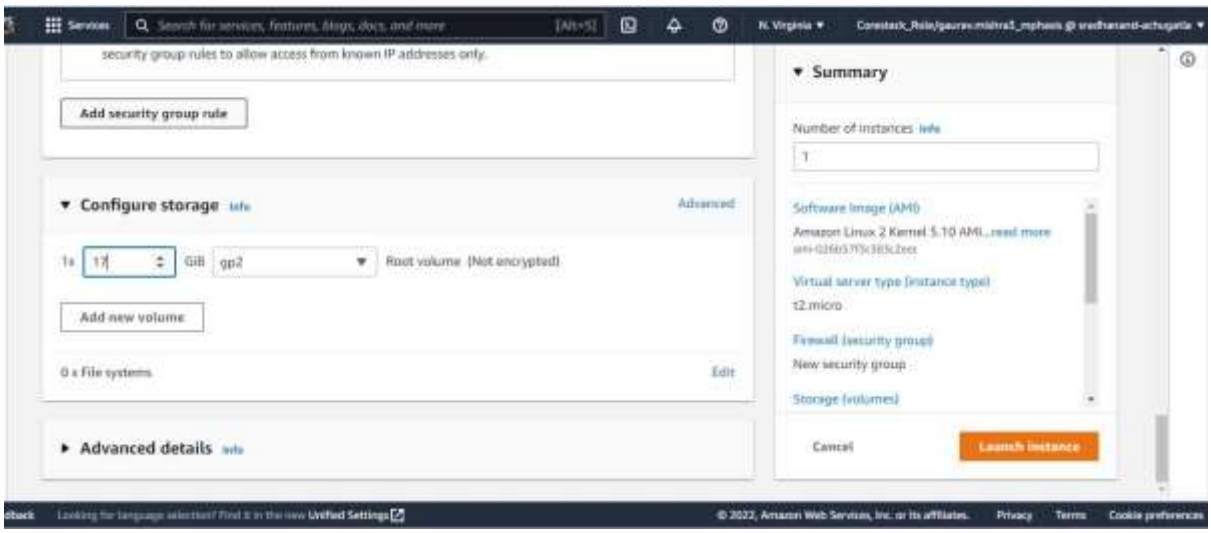

[root@ip-172-31-82-162 elasticsearch]# ./bin/plugin -install elasticsearch/elasticsearch-cloud-aws/2.7.1
-> Installing elasticsearch/elasticsearch-cloud-aws/2.7.1...
Trying http://download.elasticsearch.org/elasticsearch/elasticsearch-cloud-aws/elasticsearch-cloud-aws-2.7.1.zip...
Downloading DONE
Failed to extract plugin [/usr/share/elasticsearch/plugins/cloud-aws.zip]: ZipException[zip file is empty]
[root@ip-172-31-82-162 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-172-31-82-162 elasticsearch]# sudo su
[root@ip-172-31-82-162 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-172-31-82-162 elasticsearch]# cd /root
[root@ip-172-31-82-162 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-10 12:30:24-- 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 25.1MB/s in 0.4s
2022-10-10 12:30:25 (25.1 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]
i-029403f23ecd40897 (ELK ins)
PublicIPs: 3.84.4.75 PrivateIPs: 172.31.82.162
Feedback
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

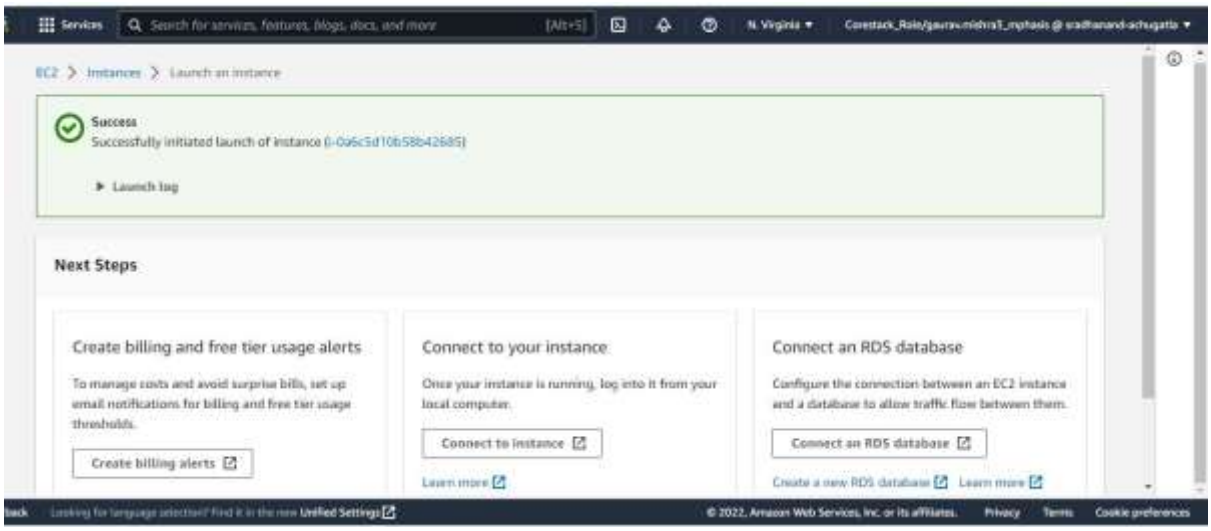

Dependency Installed:
alsa-lib.x86_64 0:1.1.6.1-2.amzn2
atk.x86_64 0:2.22.0-3.amzn2.0.2
avahi-libs.x86_64 0:0.6.31-20.amzn2
cairo.x86_64 0:1.15.12-4.amzn2
copy-jdk-configs.noarch 0:3.3-10.amzn2
cups-libs.x86_64 1:1.6.3-51.amzn2
dejavu-fonts-common.noarch 0:2.33-6.amzn2
dejavu-sans-fonts.noarch 0:2.33-6.amzn2
fontconfig.x86_64 0:2.13.0-4.3.amzn2
fontpackages-filesystem.noarch 0:1.44-8.amzn2
fribidi.x86_64 0:1.0.2-1.amzn2.1
gdk-pixbuf2.x86_64 0:2.36.12-3.amzn2
gtk2.x86_64 0:2.24.31-1.amzn2.0.2
graphite2.x86_64 0:1.3.10-1.amzn2.0.2
gtk-update-icon-cache.x86_64 0:3.22.30-3.amzn2
harfbuzz.x86_64 0:1.7.5-2.amzn2
hicolor-icon-theme.noarch 0:0.12-7.amzn2
jasper-libs.x86_64 0:1.900.1-33.amzn2
java-1.8.0-openjdk-headless.x86_64 1:1.8.0.342.b07-1.amzn2.0.1
javapackages-tools.noarch 0:3.4.1-11.amzn2
libICE.x86_64 0:1.0.9-9.amzn2.0.2
libSM.x86_64 0:1.2.2-2.amzn2.0.2
libX11.x86_64 0:1.6.7-3.amzn2.0.2
libX11-common.noarch 0:1.6.7-3.amzn2.0.2
libXau.x86_64 0:1.0.8-2.1.amzn2.0.2
libXcomposite.x86_64 0:0.4.4-4.1.amzn2.0.2
libXcursor.x86_64 0:1.1.15-1.amzn2
libXdamage.x86_64 0:1.1.4-6.1.amzn2.0.2
libXext.x86_64 0:1.3.3-3.amzn2.0.2
libXfixes.x86_64 0:5.0.3-1.amzn2.0.2
libXft.x86_64 0:2.3.2-2.amzn2.0.2
libXi.x86_64 0:1.7.9-1.amzn2.0.2
libXinerama.x86_64 0:1.1.3-2.1.amzn2.0.2
libXrandr.x86_64 0:1.5.1-2.amzn2.0.3
libXrender.x86_64 0:0.9.10-1.amzn2.0.2
libXtst.x86_64 0:1.2.3-1.amzn2.0.2
libXxf86vm.x86_64 0:1.1.4-1.amzn2.0.2
libfontenc.x86_64 0:1.1.3-3.amzn2.0.2
libglvnd.x86_64 1:1.0.1-0.1.git5baa1e5.amzn2.0.1
libglvnd-egl.x86_64 1:1.0.1-0.1.git5baa1e5.amzn2.0.1
libglvnd-glx.x86_64 1:1.0.1-0.1.git5baa1e5.amzn2.0.1
libthai.x86_64 0:0.1.14-9.amzn2.0.2
libwayland-client.x86_64 0:1.17.0-1.amzn2
libwayland-server.x86_64 0:1.17.0-1.amzn2
libxcb.x86_64 0:1.12-1.amzn2.0.2
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-libGL.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
pcre-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
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-172-31-82-162 ~]$ 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)
i-029403f23ecd40897 (ELK ins)
PublicIPs: 3.84.4.75 PrivateIPs: 172.31.82.162
Feedback
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Application and OS Images (Amazon Machine Image)
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
Free tier eligible
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance
Feedback
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Instance type
Instance type
t2.micro
Free tier eligible
Compare instance types
Key pair (login)
Key pair name - required
ELK Ins
Create new key pair
Network settings
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance


Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type
ssh
Protocol
TCP
Port range
22
Source type
Custom
Source
0.0.0.0/0
Description - optional
e.g. SSH for admin desktop
Security group rule 2 (TCP, 0, 106.195.60.16/32)
Remove
Type
Custom TCP
Protocol
TCP
Port range
0
Source type
My IP
Source
Description - optional
e.g. SSH for admin desktop
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance


security group rules to allow access from known IP addresses only.
Add security group rule
Configure storage
Advanced
1x
17
GiB
gp2
Root volume (Not encrypted)
Add new volume
0 x File systems
Edit
Advanced details
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance



EC2 > Instances > i-029403f23ecd40897 > Connect to instance

Connect to instance Info

Connect to your instance i-029403f23ecd40897 (ELK Ins) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID

i-029403f23ecd40897 (ELK Ins)

Public IP address

3.84.4.75

User name

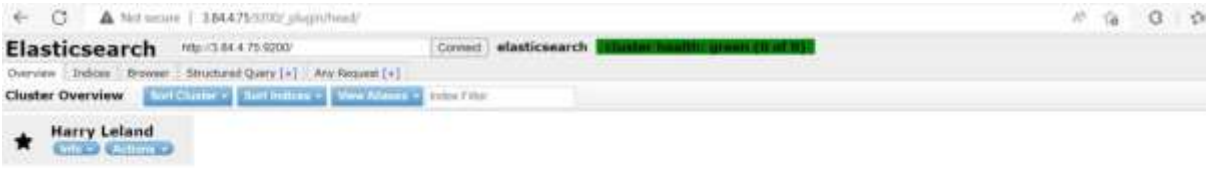
ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

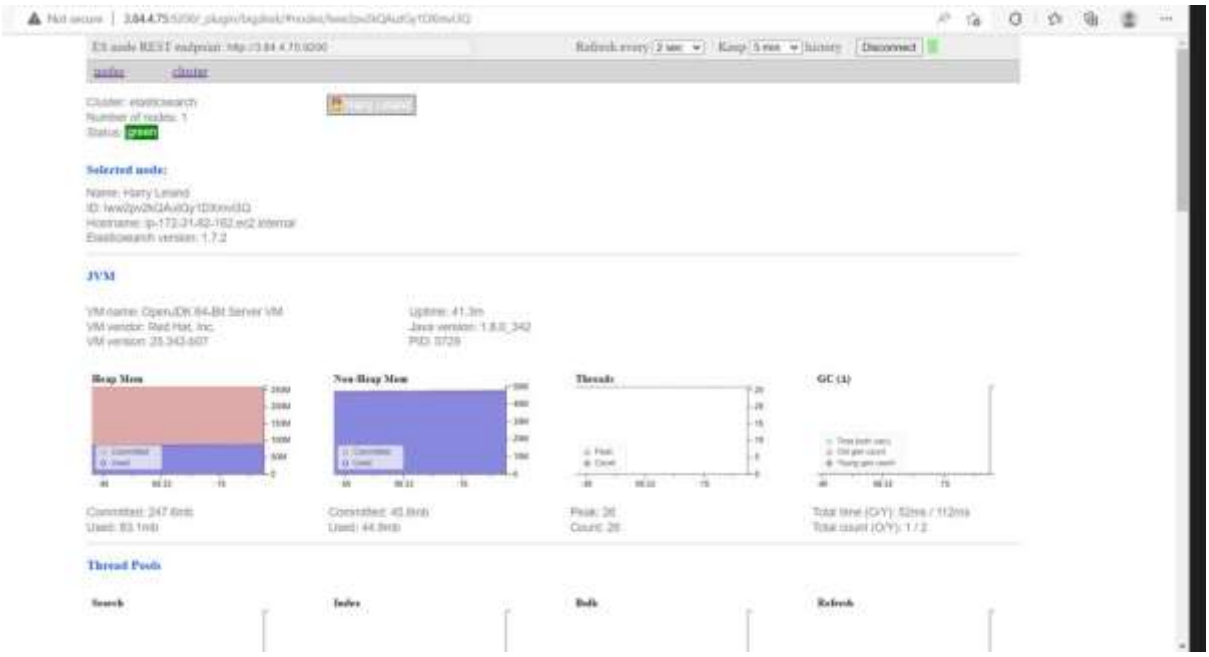
Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel Connect

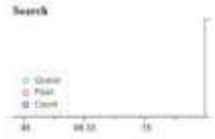

Not secure | 3.84.4.75:9200
{
"status" : 200,
"name" : "Harry Leland",
"cluster_name" : "elasticsearch",
"version" : {
"number" : "1.7.2",
"build_hash" : "e43676b1385b8125d647f593f7202acbd816e8ec",
"build_timestamp" : "2015-09-14T09:49:53Z",
"build_snapshot" : false,
"lucene_version" : "4.10.4"
},
"tagline" : "You Know, for Search"
}


Not secure | 3.84.4.75:9200/_plugin/head/
Elasticsearch
http://3.84.4.75:9200/
Connect
elasticsearch
cluster health: green (5 of 5)
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Harry Leland
Info
Actions

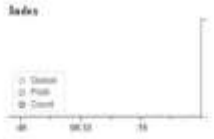

Not secure
ES node REST endpoint: http://3.84.4.75:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Harry Leland


Not secure
ES node REST endpoint: http://3.84.4.75:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Selected node:
Name: Harry Leland
Hostname: ip-172-31-82-162.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: 41.3m
Java version: 1.8.0_342
PID: 9729
Heap Mem
Non-Heap Mem
Threads
GC (1)
Committed: 247.6mb
Used: 83.1mb
Committed: 45.6mb
Used: 44.8mb
Peak: 26
Count: 26
Total time (O/Y): 52ms / 112ms
Total count (O/Y): 1 / 2
Thread Pools
Search
Index
Bulk
Refresh

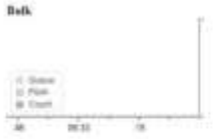
Thread Pools



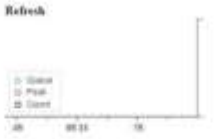
Queue: 0
Peak: 0
Count: 0



Queue: 0
Peak: 0
Count: 0



Queue: 0
Peak: 0
Count: 0

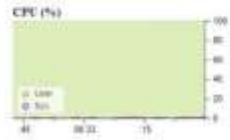


Queue: 0
Peak: 0
Count: 0

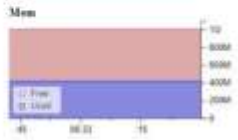
OS

CPU vendor: Intel
CPU model: Xeon (2299 MHz)
CPU total logical cores: 1
CPU cache: 30kb

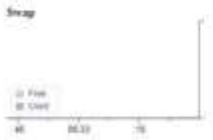
Uptime: 2.0s
Refresh interval: 1sms
Total mem: 965.7mb (1012666368 b)
Total swap: 0b (0 b)



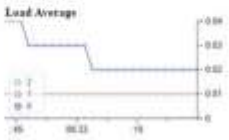
Total: 100%
User: 1%
Sys: 1%



Free: 561.6mb
Used: 404mb

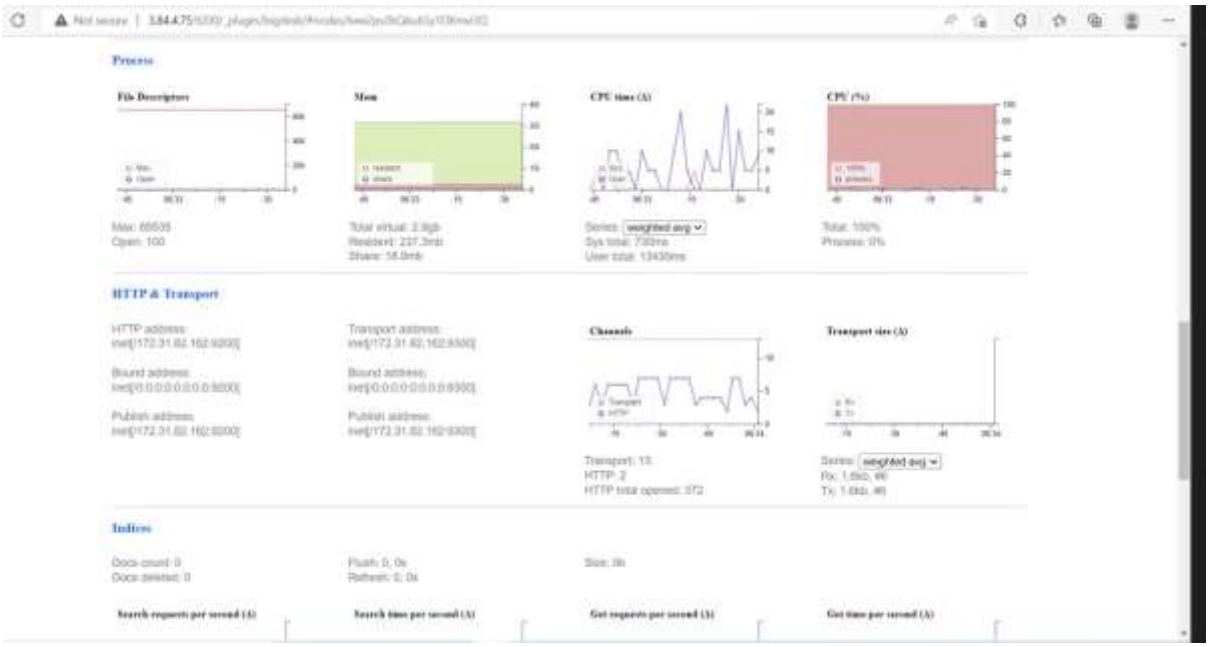


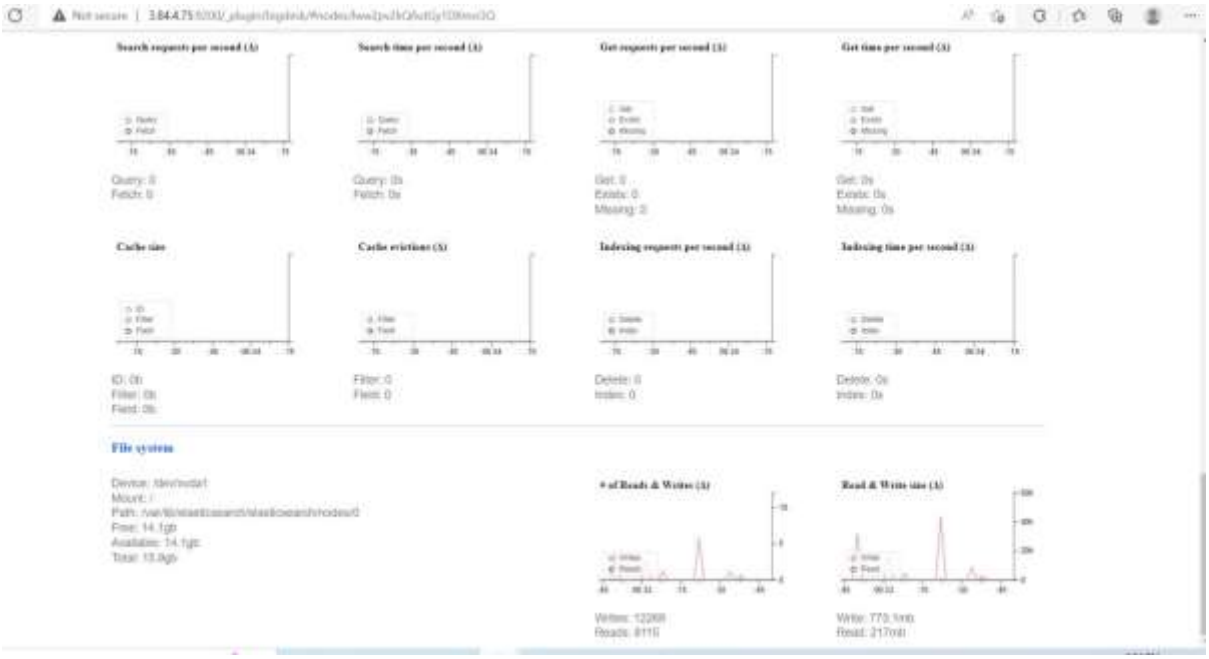
Free: 0b
Used: 0b



2: 0
1: 0.01
0: 0.02

Process




Search requests per second (1)
Search time per second (1)
Get requests per second (1)
Get time per second (1)
Query: 0
Fetch: 0
Query: 0s
Fetch: 0s
Get: 0
Exists: 0
Missing: 0
Get: 0s
Exists: 0s
Missing: 0s
Cache size
Cache evictions (1)
Indexing requests per second (1)
Indexing time per second (1)
ID: 0b
Filter: 0b
Field: 0b
Filter: 0
Field: 0
Delete: 0
Index: 0
Delete: 0s
Index: 0s
File system
Device: /dev/nvme1
Mount: /
Path: /var/lib/elasticsearch/elasticsearch/nodes/0
Free: 14.1gb
Available: 14.1gb
Total: 13.8gb
# of Reads & Writes (1)
Read & Write size (1)
Writes: 12269
Reads: 8115
Write: 773.1mb
Read: 217mb