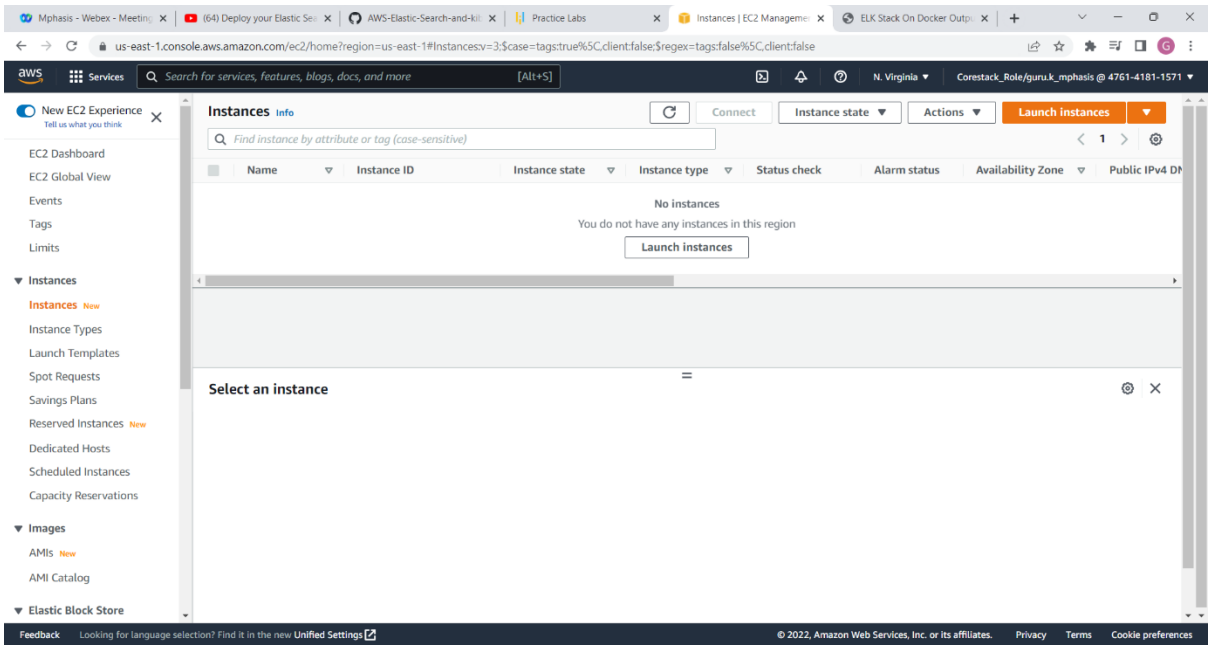
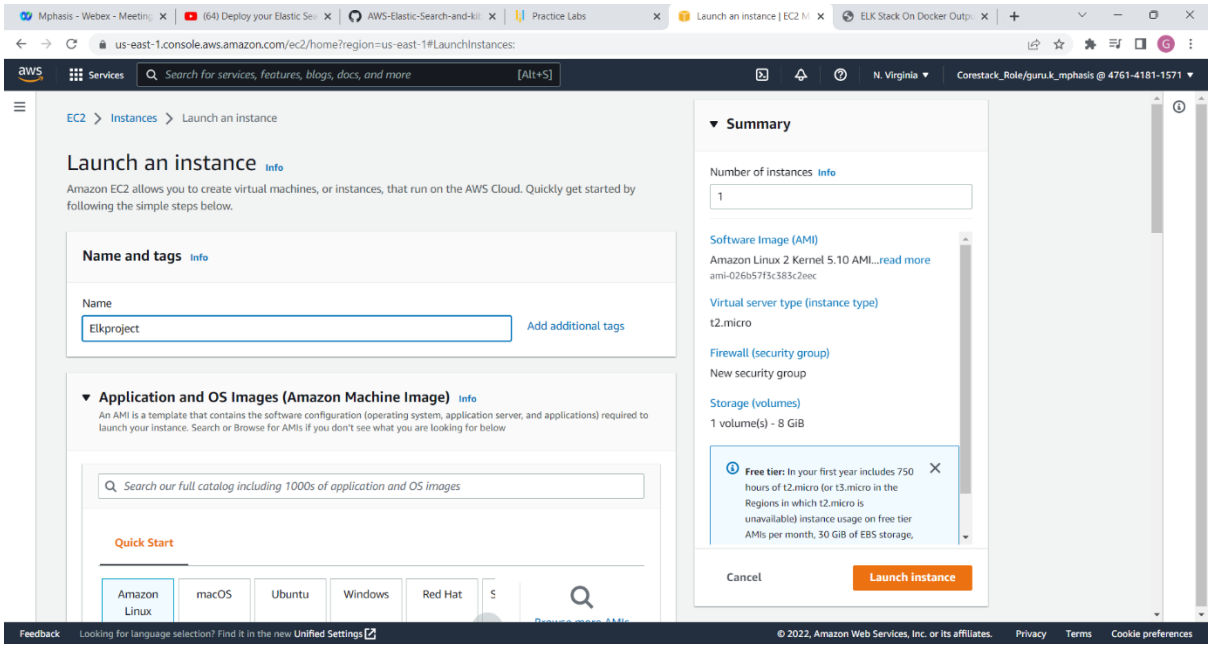
SCREENSHOT

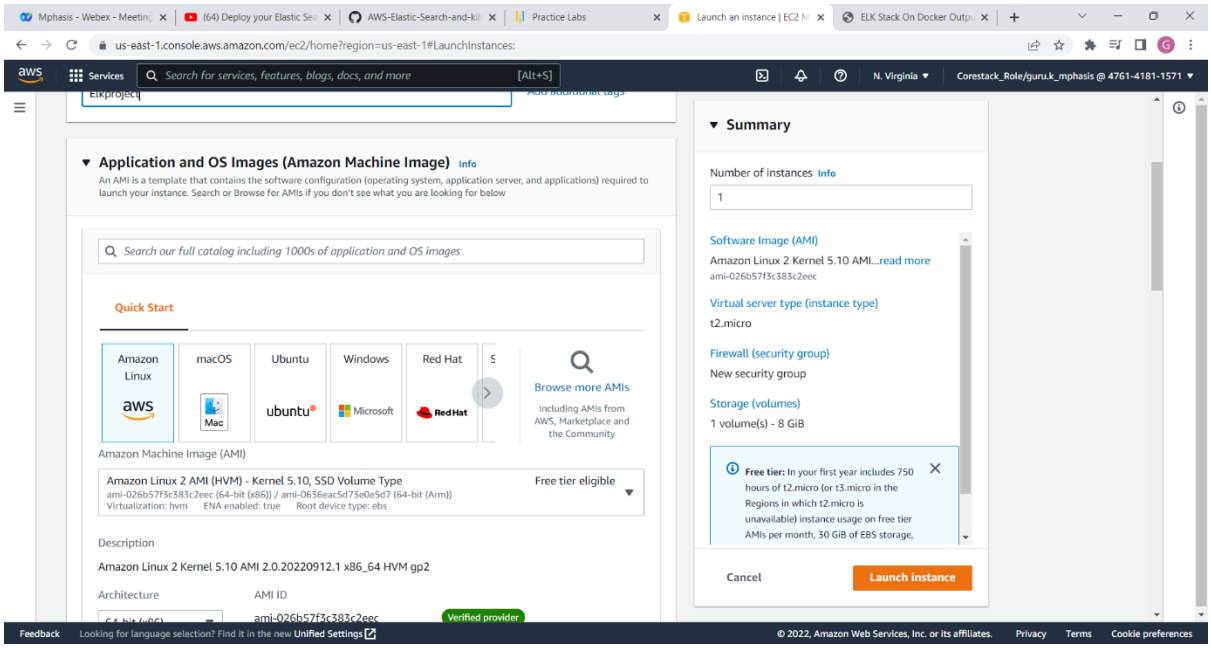
To Create a new AWS instance choose Launch instance:



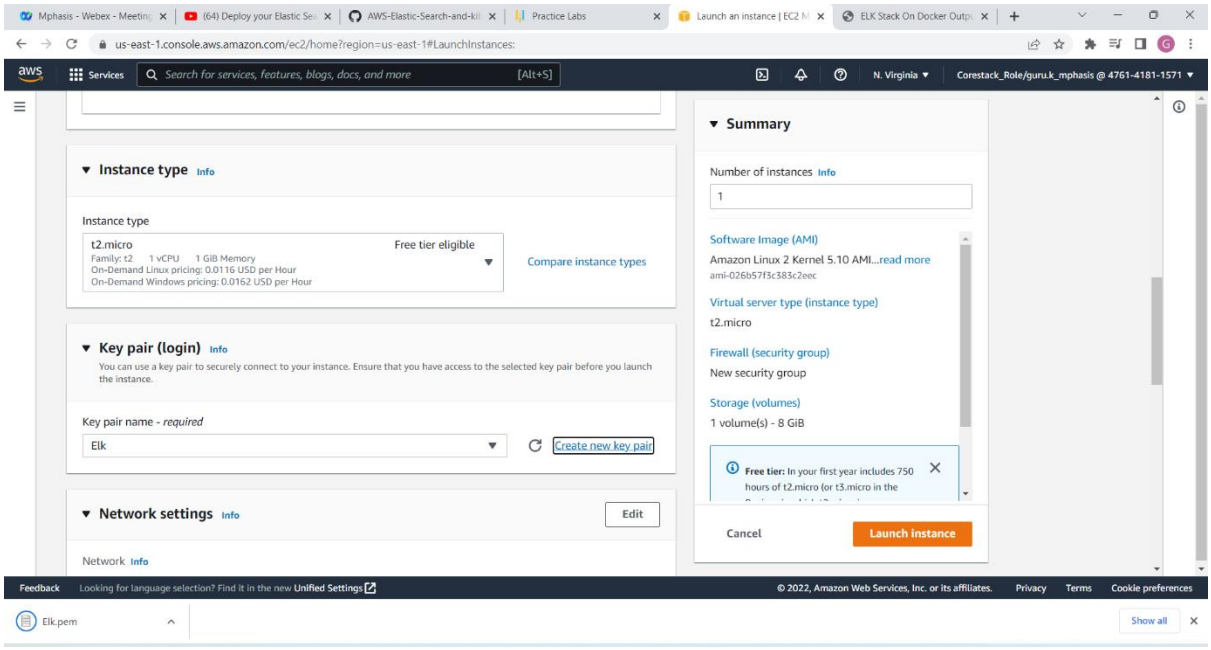
Give name of your instance:



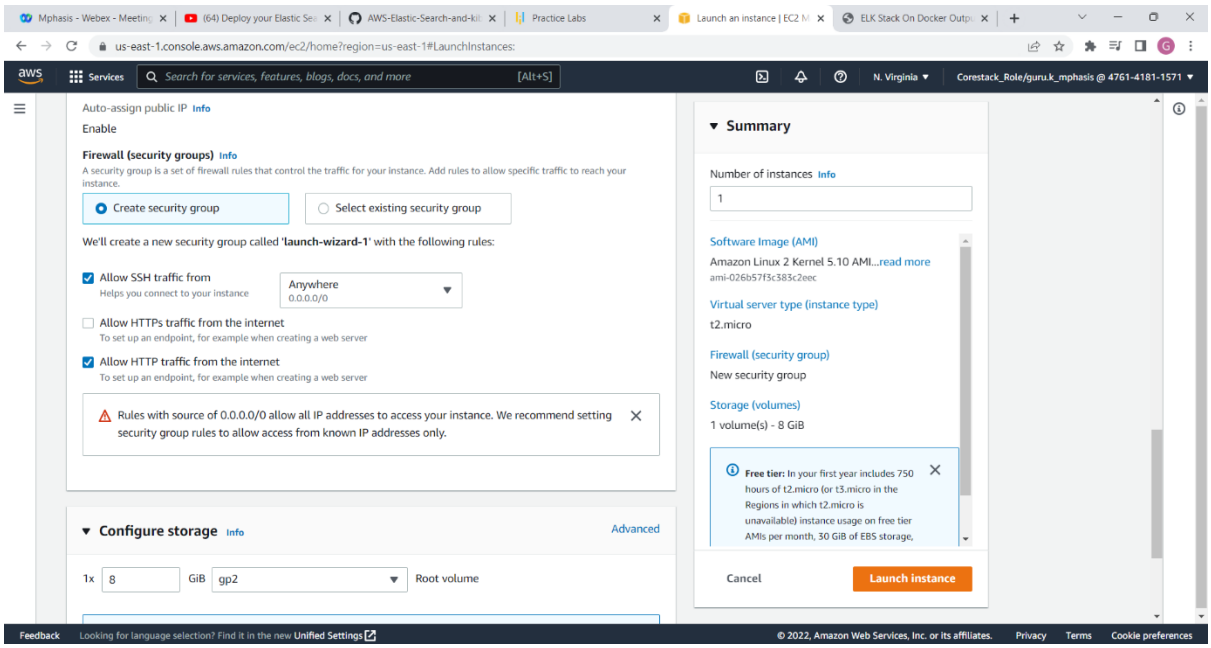
Choose AWS option:



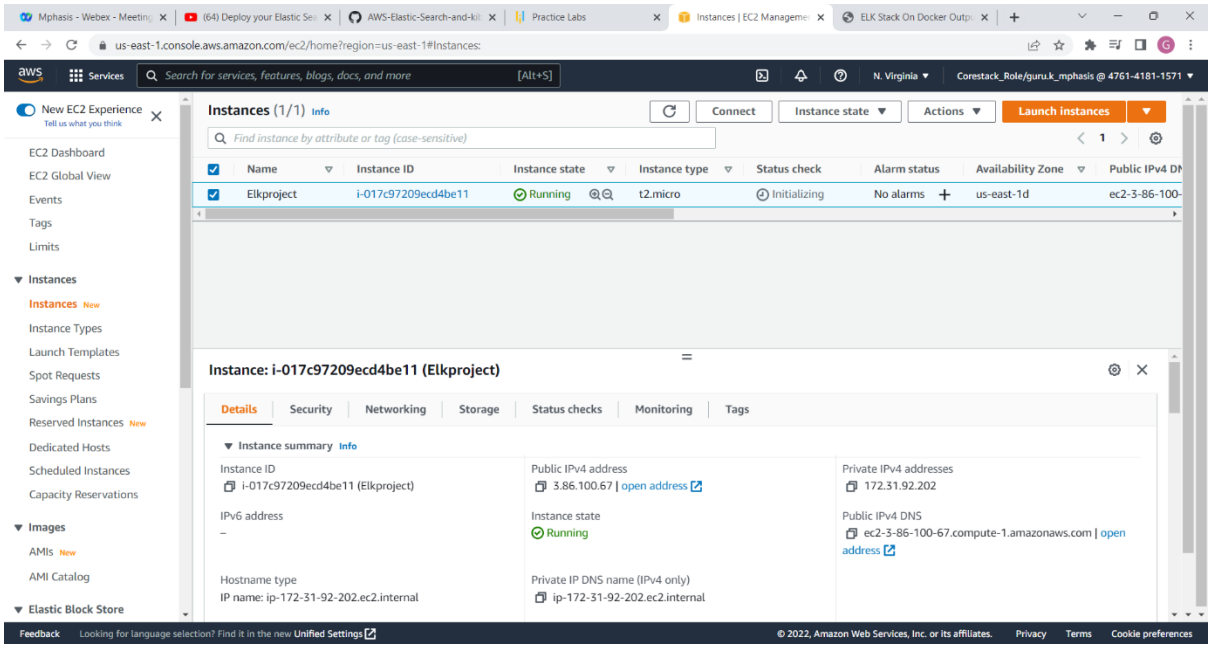
Click the keypair and add a name for it → select the Pem File now its download



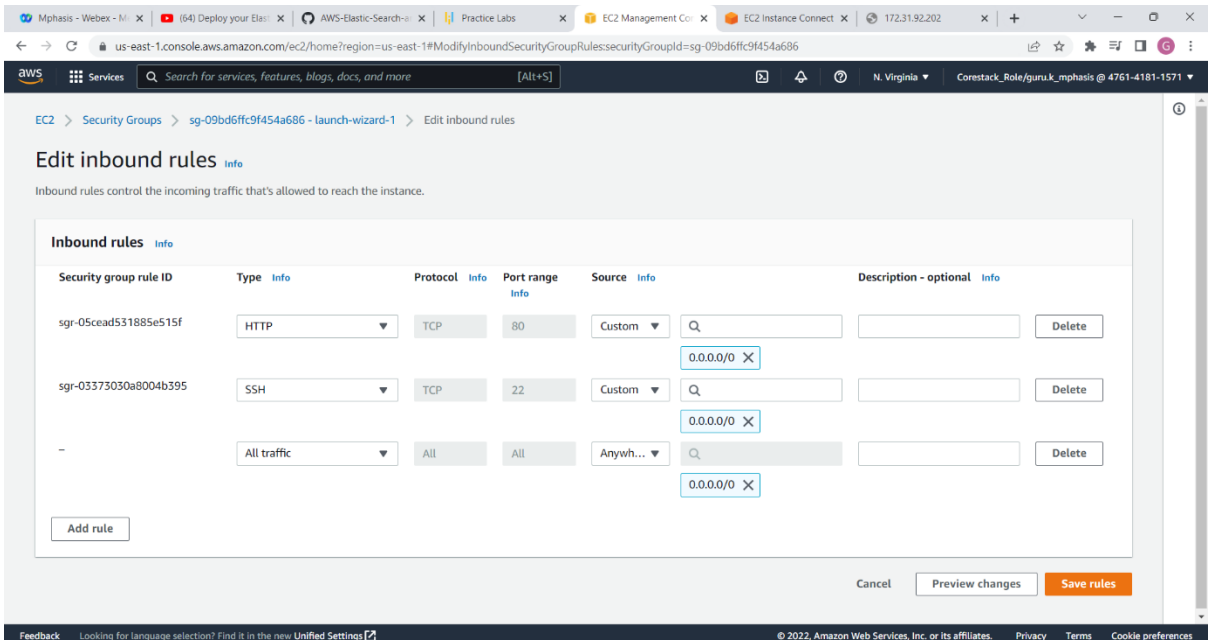
Select the http traffic check box → help to run 8080 port



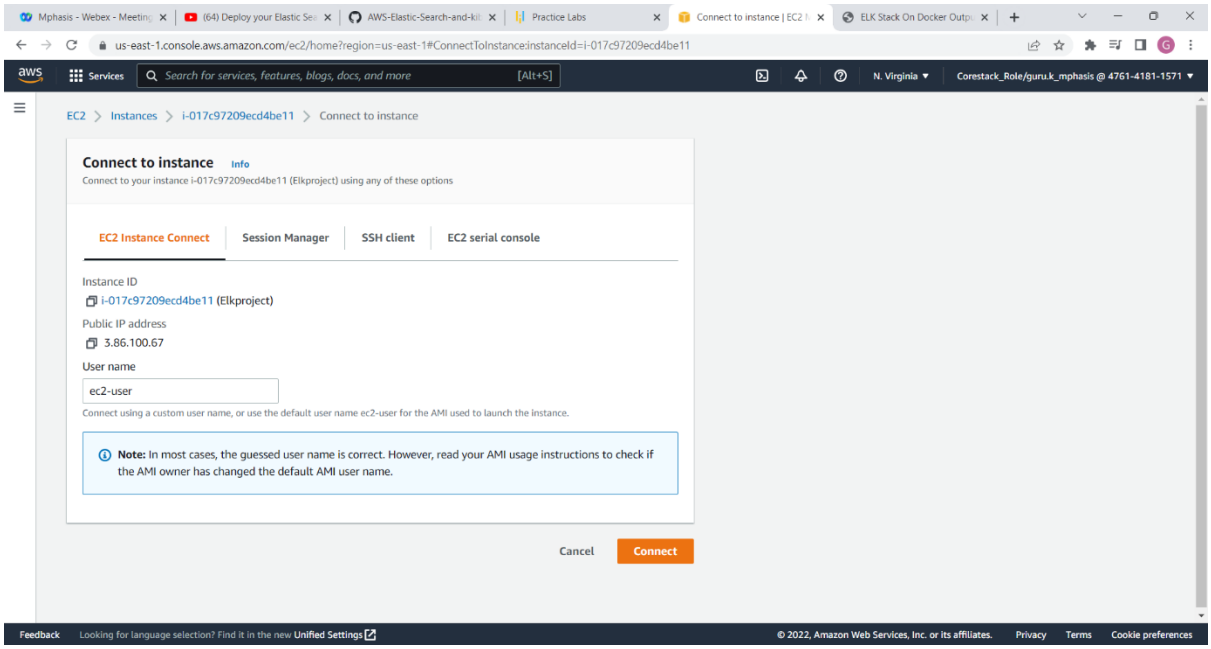
Now the instance created Successfully → refresh it until our instance change pending state to run state.



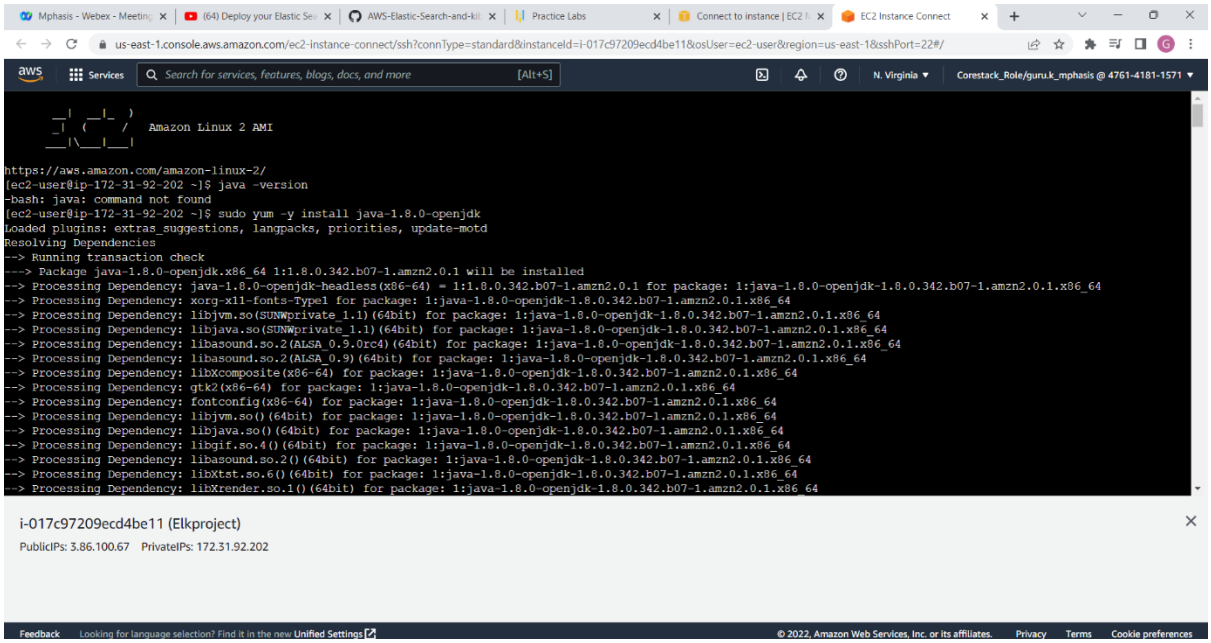
SELECT instance go to SECURITY->security groups-.>edit inbound rules->add new rule set network type All traffic and give port range and source set

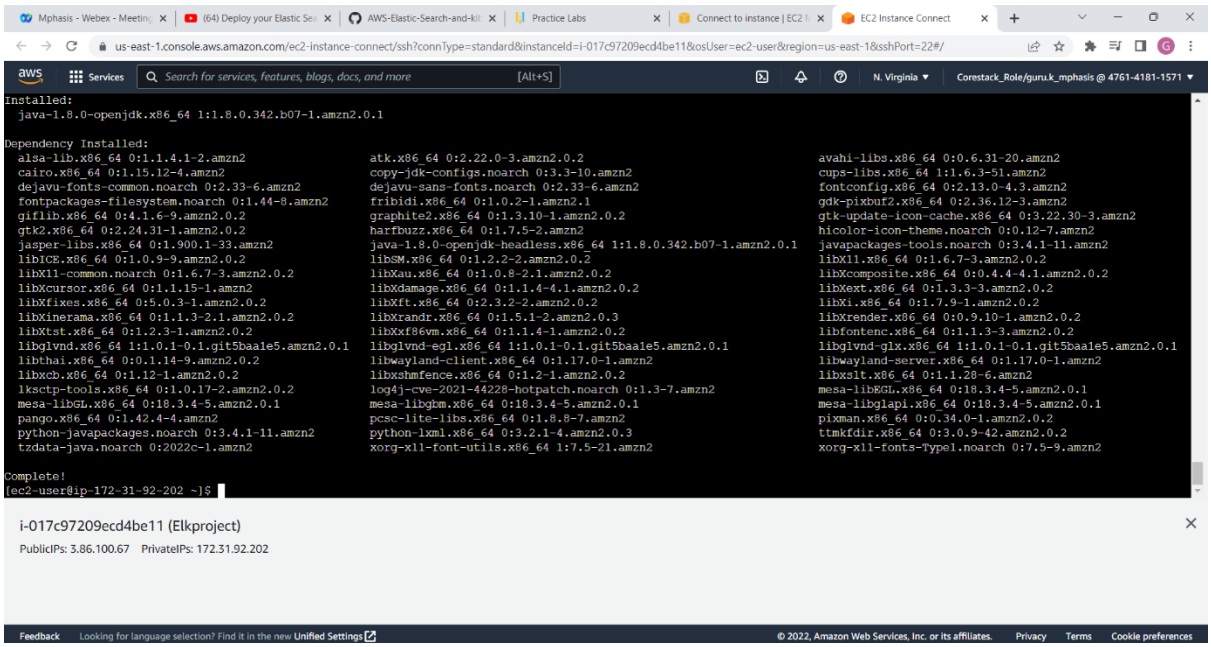


Select your instance->connect->to work on AWS terminal

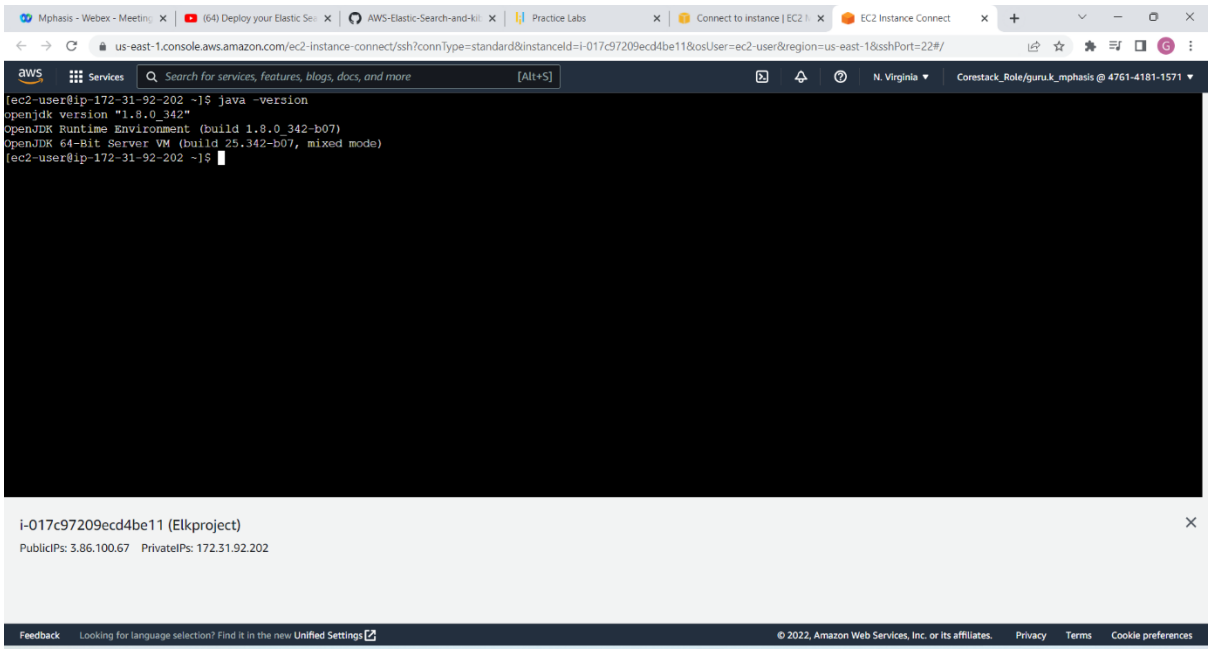


Check the java version , if there is no java version → just install it using “sudo yum -y install java”

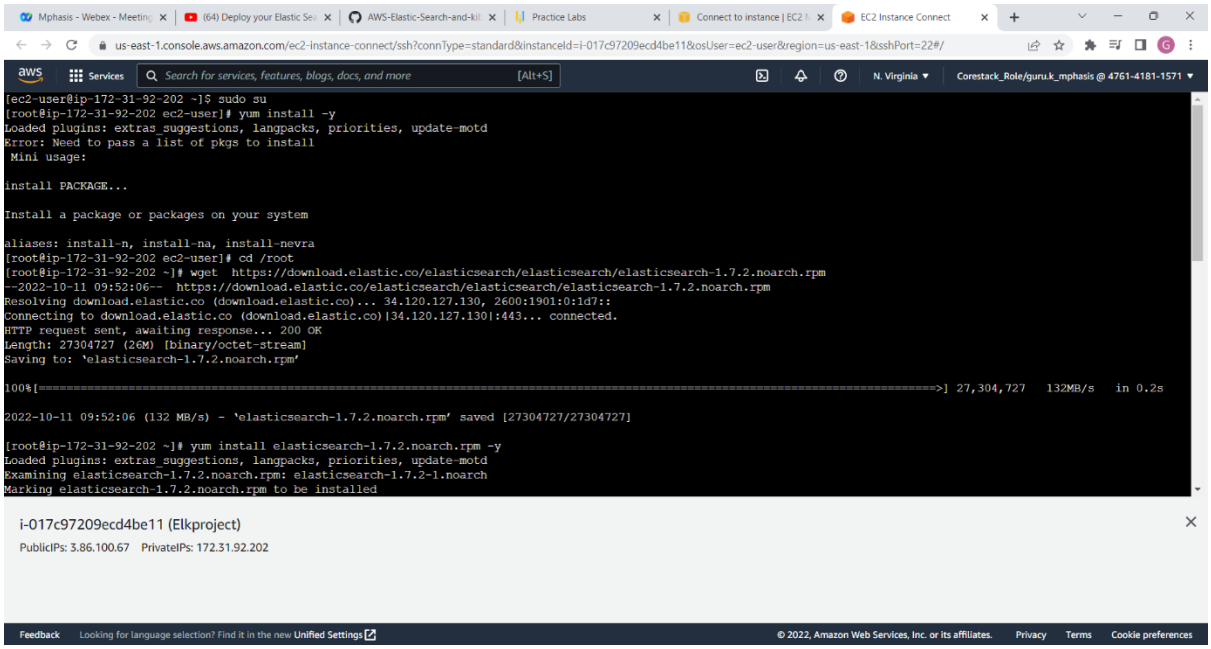


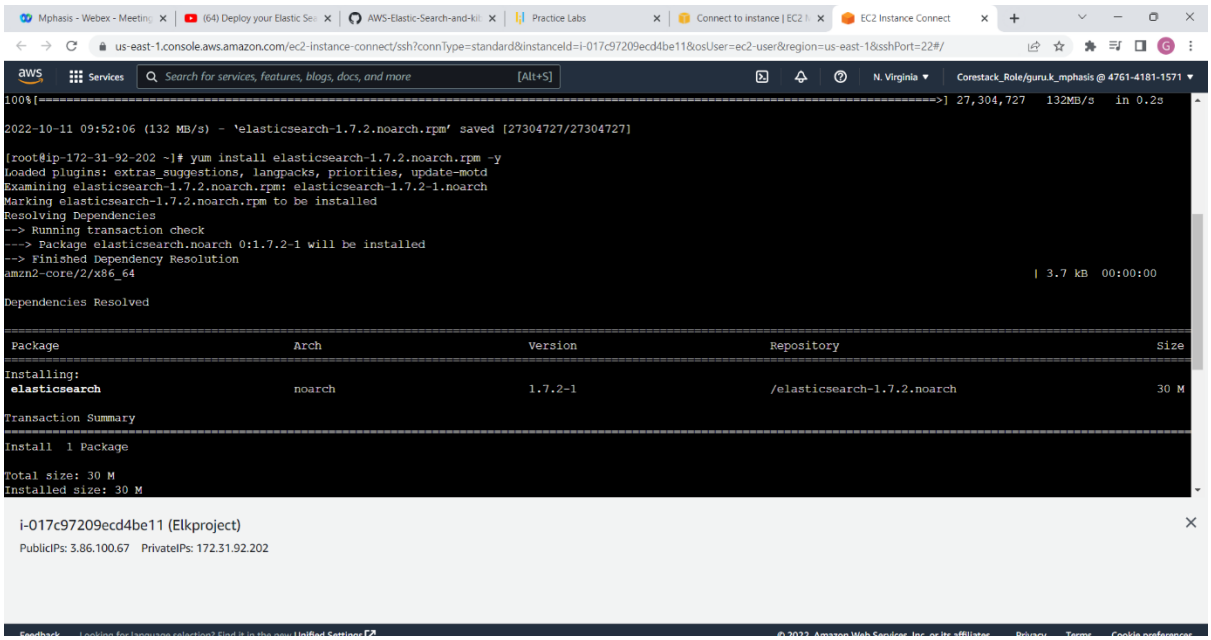


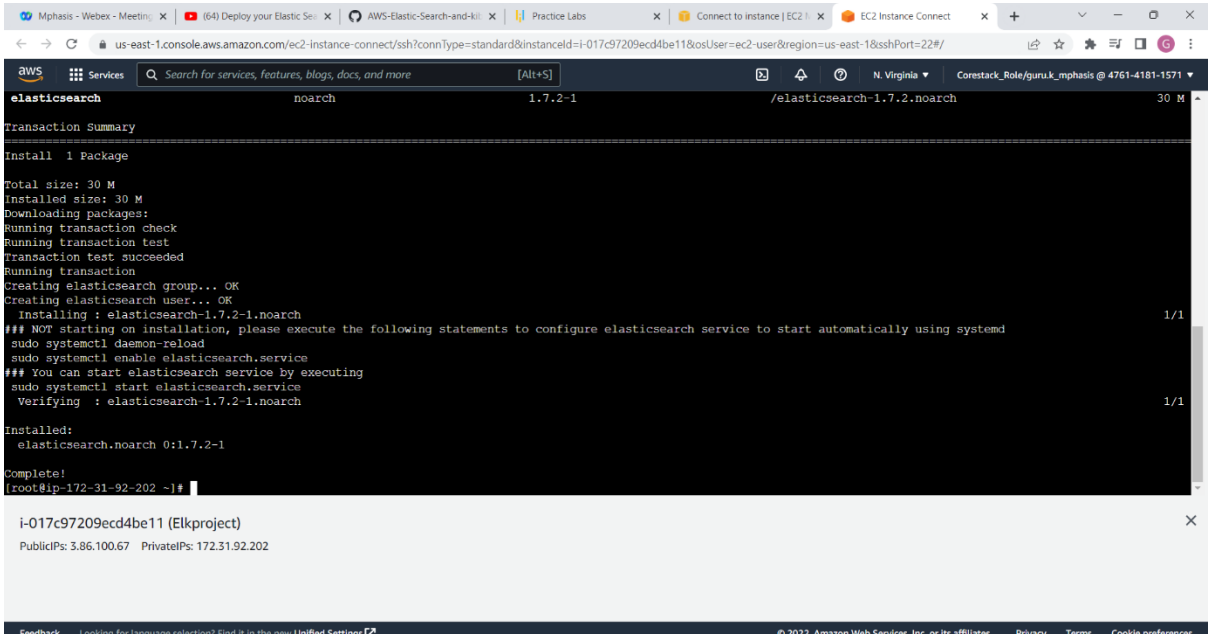
Check for java--version



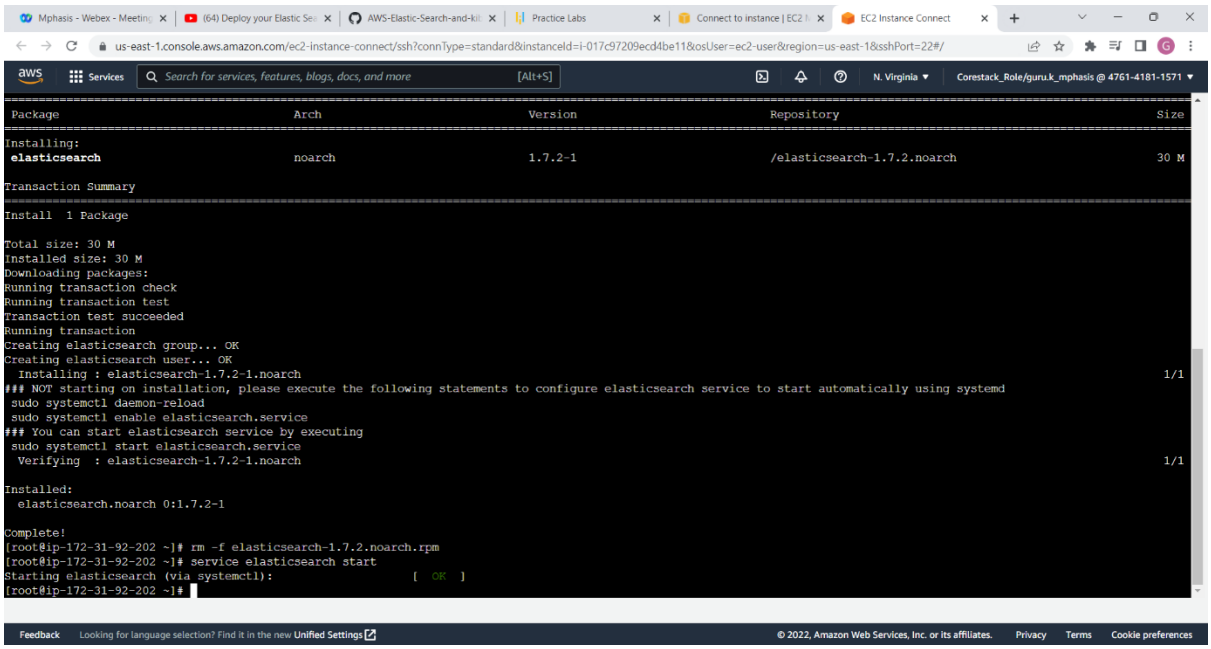
Install Elastic Stack on AWS Server:



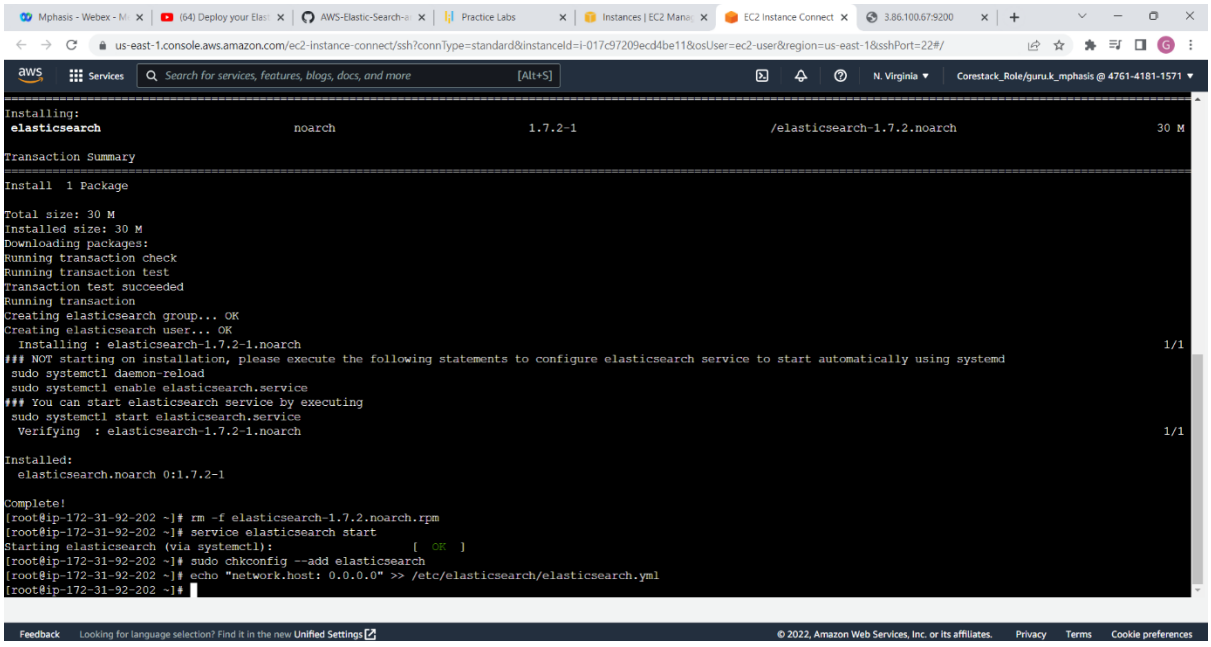

Mphasis - Webex - Meeting
(64) Deploy your Elastic Se
AWS-Elastic-Search-and-kil
Practice Labs
Connect to instance | EC2 I
EC2 Instance Connect
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-017c97209ecd4be11&osUser=ec2-user&region=us-east-1&sshPort=22#/
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/guru.k_mphasis @ 4761-4181-1571
100%[==========>] 27,304,727 132MB/s in 0.2s
2022-10-11 09:52:06 (132 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]
[root@ip-172-31-92-202 ~]# 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 00:00:00
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
i-017c97209ecd4be11 (Elkproject)
PublicIPs: 3.86.100.67 PrivateIPs: 172.31.92.202


Mphasis - Webex - Meeting
(64) Deploy your Elastic Se
AWS-Elastic-Search-and-kil
Practice Labs
Connect to instance | EC2 I
EC2 Instance Connect
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-017c97209ecd4be11&osUser=ec2-user&region=us-east-1&sshPort=22#/
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/guru.k_mphasis @ 4761-4181-1571
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 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
Verifying : elasticsearch-1.7.2-1.noarch 1/1
Installed:
elasticsearch.noarch 0:1.7.2-1
Complete!
[root@ip-172-31-92-202 ~]#
i-017c97209ecd4be11 (Elkproject)
PublicIPs: 3.86.100.67 PrivateIPs: 172.31.92.202

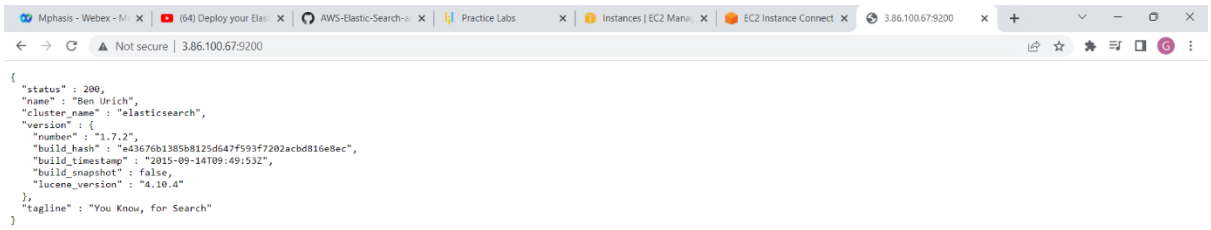
After Installation Start the Server:



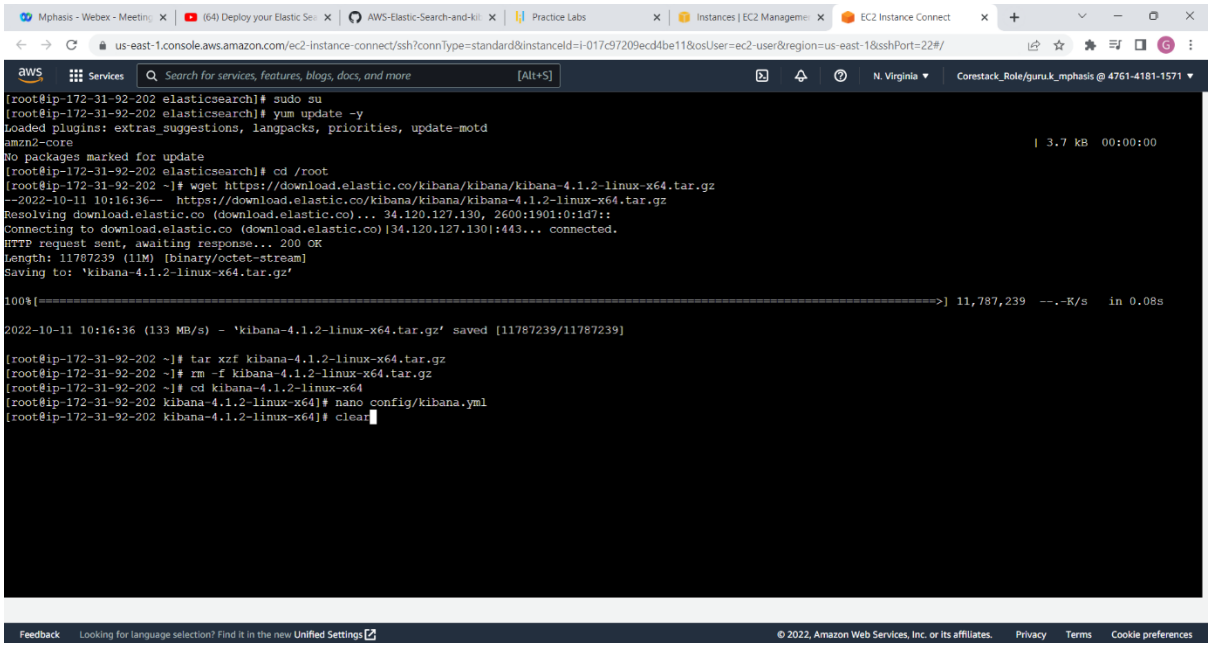
It Automatically Boot on you to start and configure Aws IP so you an access using your public IP

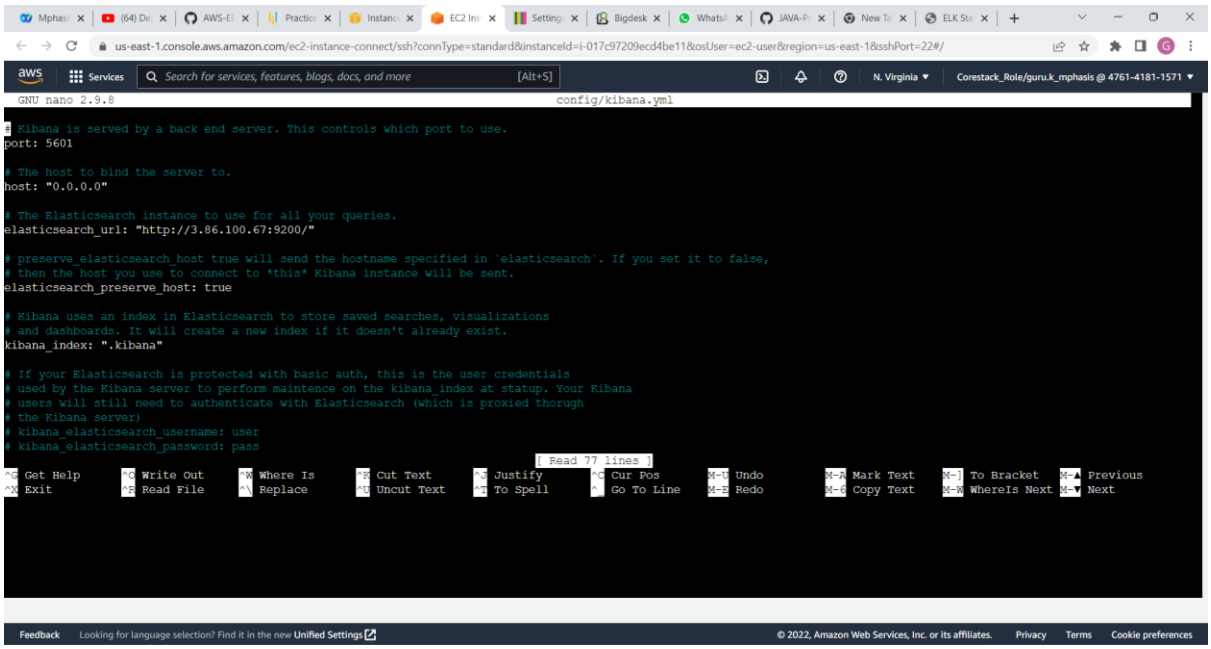


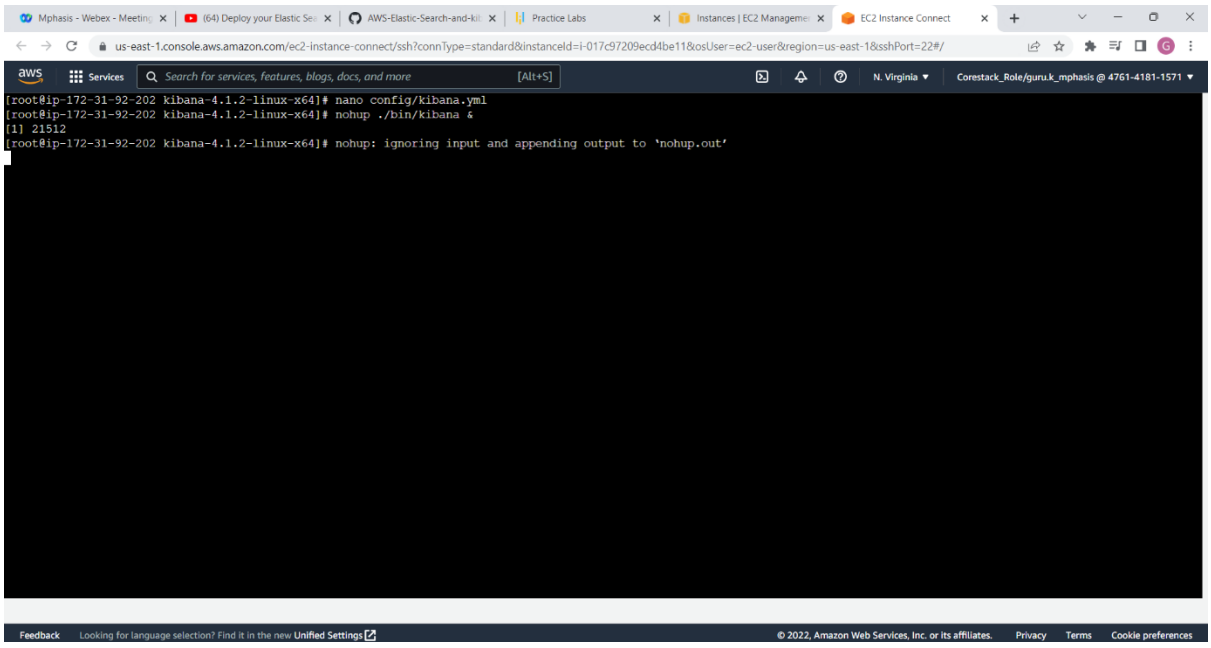
Checking Elastic Search:

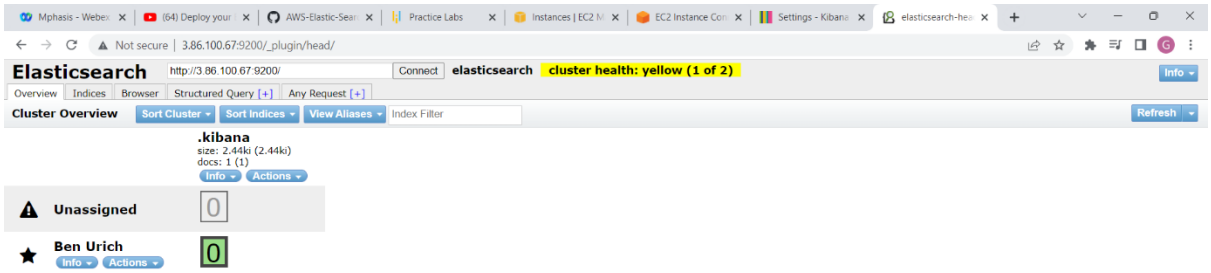


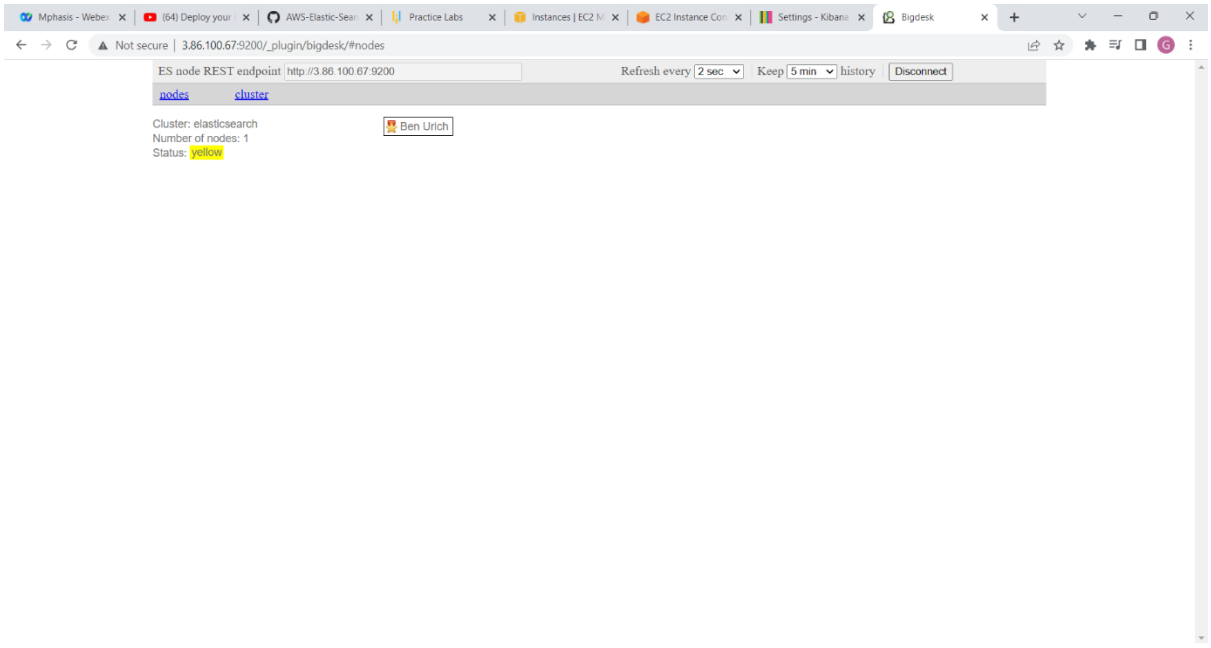
Install Plugins and Kibana:

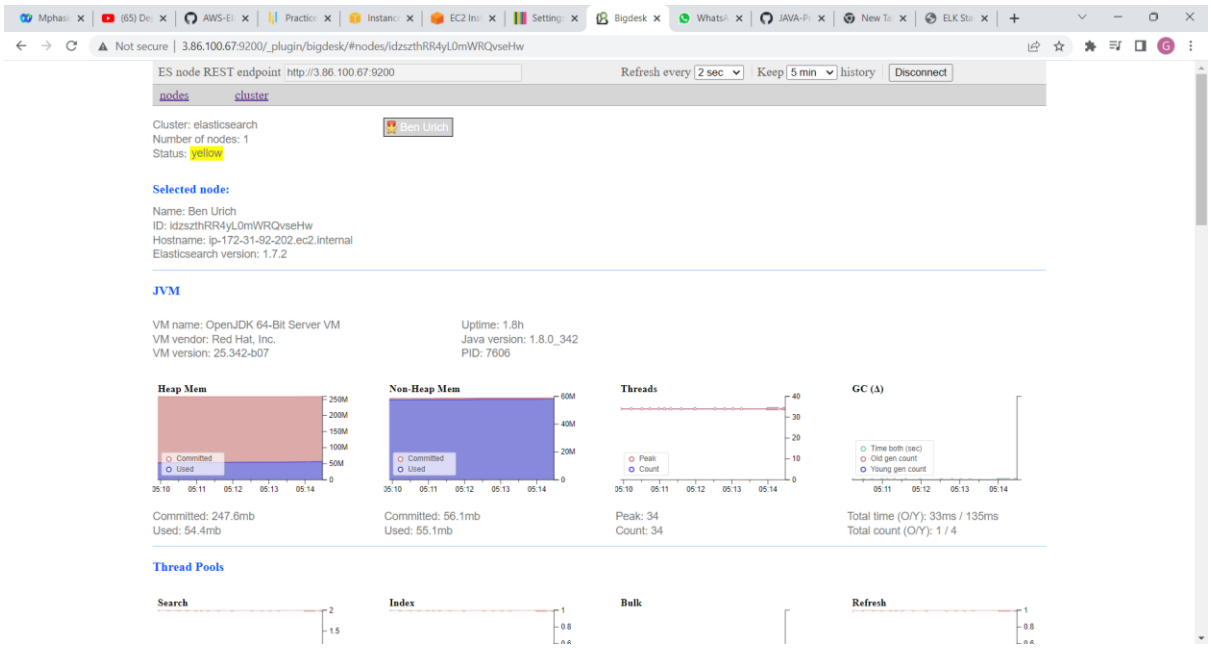


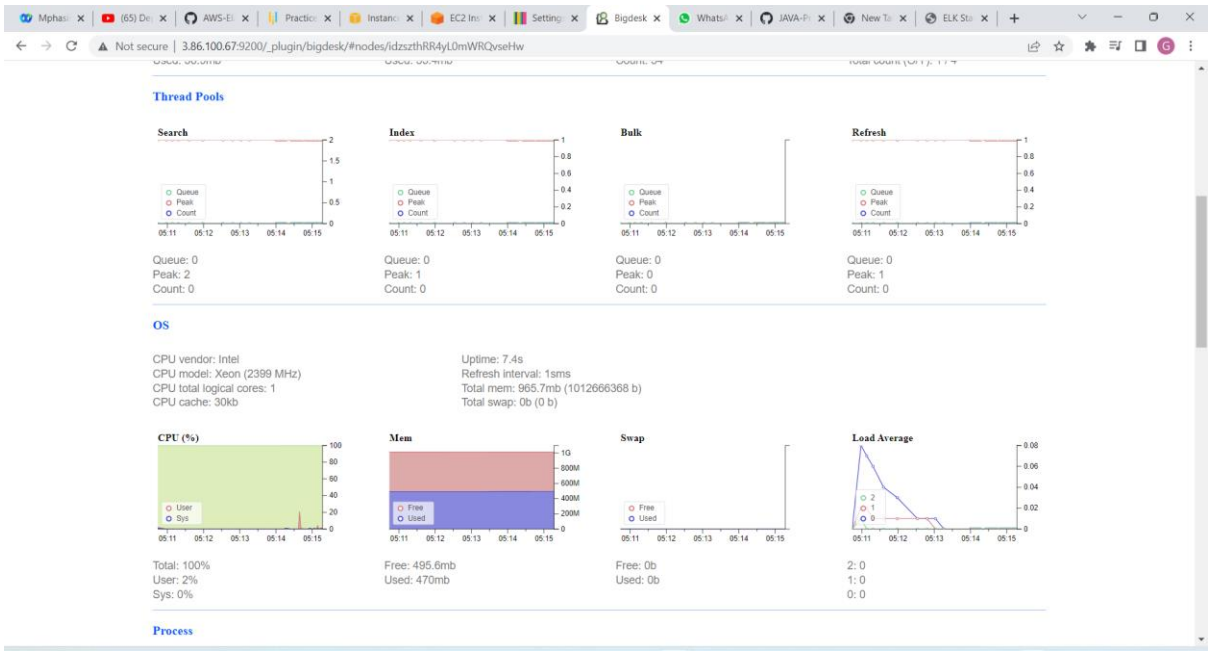

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-017c97209ecd4be11&osUser=ec2-user&region=us-east-1&sshPort=22#/
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Corestack_Role/guru.k_mphasis @ 4761-4181-1571
GNU nano 2.9.8 config/kibana.yml
Kibana is served by a back end server. This controls which port to use.
port: 5601
The host to bind the server to.
host: "0.0.0.0"
The Elasticsearch instance to use for all your queries.
elasticsearch_url: "http://3.86.100.67:9200/"
preserve_elasticsearch_host true will send the hostname specified in `elasticsearch`. If you set it to false,
then the host you use to connect to *this* Kibana instance will be sent.
elasticsearch_preserve_host: true
Kibana uses an index in Elasticsearch to store saved searches, visualizations
and dashboards. It will create a new index if it doesn't already exist.
kibana_index: ".kibana"
If your Elasticsearch is protected with basic auth, this is the user credentials
used by the Kibana server to perform maintence on the kibana_index at statup. Your Kibana
users will still need to authenticate with Elasticsearch (which is proxied thorugh
the Kibana server)
kibana_elasticsearch_username: user
kibana_elasticsearch_password: pass
[Read 77 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-▲ Previous
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text M-W WhereIs Next M-▼ Next
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

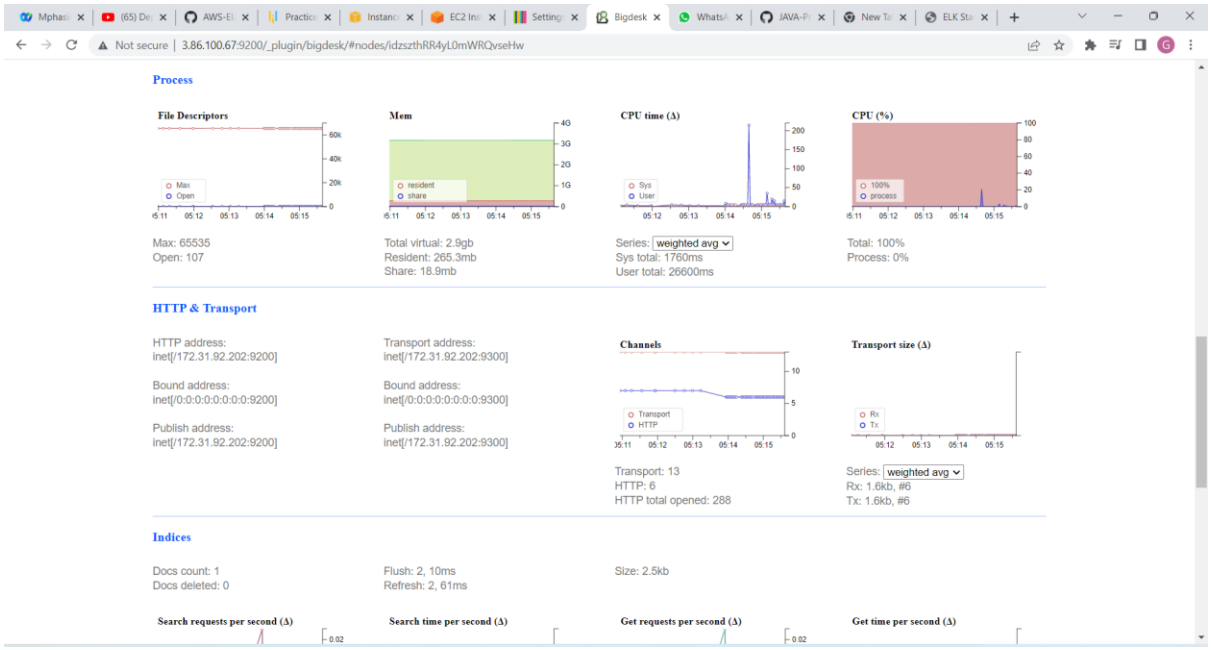

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-017c97209ecd4be11&osUser=ec2-user&region=us-east-1&sshPort=22#/
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Corestack_Role/guru.k_mphasis @ 4761-4181-1571
[root@ip-172-31-92-202 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-92-202 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 21512
[root@ip-172-31-92-202 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

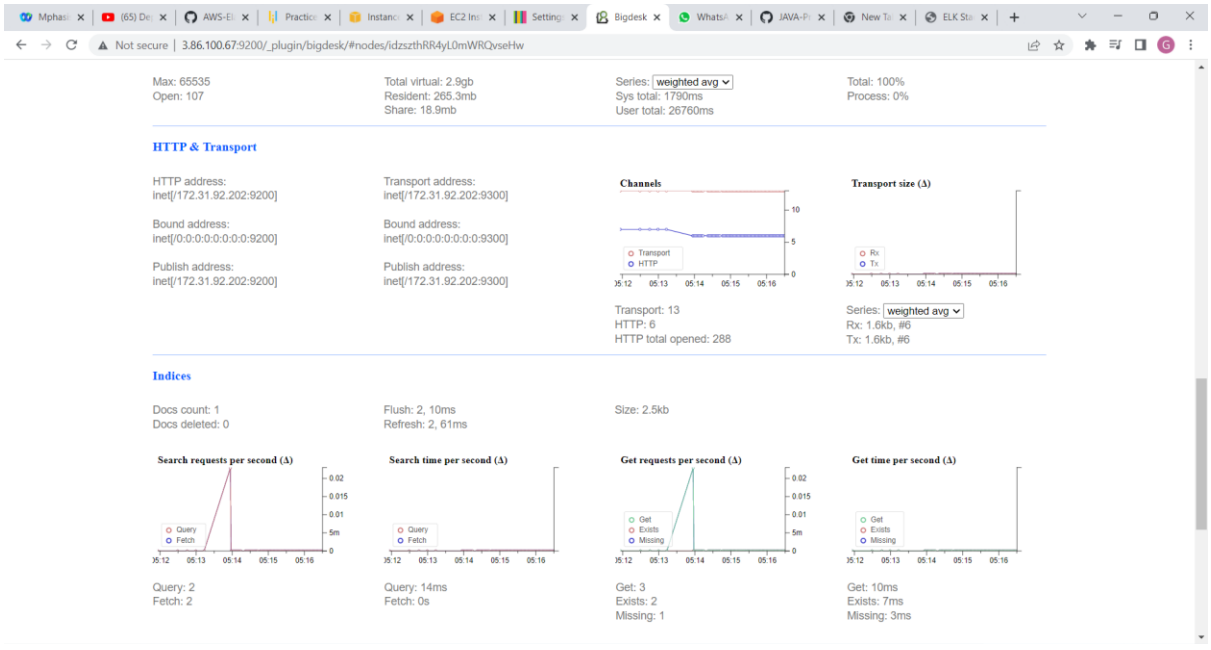

Not secure | 3.86.100.67:9200/_plugin/head/
Elasticsearch
http://3.86.100.67:9200/
Connect
elasticsearch
cluster health: yellow (1 of 2)
Info
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
Sort Indices
View Aliases
Index Filter
Refresh
.kibana
size: 2.44ki (2.44ki)
docs: 1 (1)
Info
Actions
Unassigned
0
Ben Urich
Info
Actions
0


Not secure | 3.86.100.67:9200/_plugin/bigdesk/#nodes
ES node REST endpoint http://3.86.100.67:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: yellow
Ben Urich


Not secure | 3.86.100.67:9200/_plugin/bigdesk/#nodes/idzszthRR4yL0mWRQvseHw
ES node REST endpoint http://3.86.100.67:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: yellow
Ben Urich
Selected node:
Name: Ben Urich
ID: idzszthRR4yL0mWRQvseHw
Hostname: ip-172-31-92-202.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: 1.8h
Java version: 1.8.0_342
PID: 7606
Heap Mem
Committed
Used
Non-Heap Mem
Committed
Used
Threads
Peak
Count
GC (Δ)
Time both (sec)
Old gen count
Young gen count
Committed: 247.6mb
Used: 54.4mb
Committed: 56.1mb
Used: 55.1mb
Peak: 34
Count: 34
Total time (O/Y): 33ms / 135ms
Total count (O/Y): 1 / 4
Thread Pools
Search
Index
Bulk
Refresh


Not secure | 3.86.100.67:9200/_plugin/bigdesk/#nodes/idzszthRR4yL0mWRQvseHw
Thread Pools
Search
Index
Bulk
Refresh
Queue
Peak
Count
Queue: 0
Peak: 2
Count: 0
Queue: 0
Peak: 1
Count: 0
Queue: 0
Peak: 0
Count: 0
Queue: 0
Peak: 1
Count: 0
OS
CPU vendor: Intel
CPU model: Xeon (2399 MHz)
CPU total logical cores: 1
CPU cache: 30kb
Uptime: 7.4s
Refresh interval: 1sms
Total mem: 965.7mb (1012666368 b)
Total swap: 0b (0 b)
CPU (%)
User
Sys
Mem
Free
Used
Swap
Free
Used
Load Average
Total: 100%
User: 2%
Sys: 0%
Free: 495.6mb
Used: 470mb
Free: 0b
Used: 0b
2: 0
1: 0
0: 0
Process


Bigdesk
Not secure | 3.86.100.67:9200/_plugin/bigdesk/#nodes/idzszthRR4yL0mWRQvseHw
Process
File Descriptors
Max
Open
Mem
resident
share
CPU time (Δ)
Sys
User
CPU (%)
100%
process
Max: 65535
Open: 107
Total virtual: 2.9gb
Resident: 265.3mb
Share: 18.9mb
Series: weighted avg
Sys total: 1760ms
User total: 26600ms
Total: 100%
Process: 0%
HTTP & Transport
HTTP address:
inet[/172.31.92.202:9200]
Bound address:
inet[/0:0:0:0:0:0:0:0:9200]
Publish address:
inet[/172.31.92.202:9200]
Transport address:
inet[/172.31.92.202:9300]
Bound address:
inet[/0:0:0:0:0:0:0:0:9300]
Publish address:
inet[/172.31.92.202:9300]
Channels
Transport
HTTP
Transport size (Δ)
Rx
Tx
Transport: 13
HTTP: 6
HTTP total opened: 288
Series: weighted avg
Rx: 1.6kb, #6
Tx: 1.6kb, #6
Indices
Docs count: 1
Docs deleted: 0
Flush: 2, 10ms
Refresh: 2, 61ms
Size: 2.5kb
Search requests per second (Δ)
Search time per second (Δ)
Get requests per second (Δ)
Get time per second (Δ)


Bigdesk
Not secure | 3.86.100.67:9200/_plugin/bigdesk/#nodes/idzszthRR4yL0mWRQvseHw
Max: 65535
Open: 107
Total virtual: 2.9gb
Resident: 265.3mb
Share: 18.9mb
Series: weighted avg
Sys total: 1790ms
User total: 26760ms
Total: 100%
Process: 0%
HTTP & Transport
HTTP address:
inet[/172.31.92.202:9200]
Bound address:
inet[/0:0:0:0:0:0:0:0:9200]
Publish address:
inet[/172.31.92.202:9200]
Transport address:
inet[/172.31.92.202:9300]
Bound address:
inet[/0:0:0:0:0:0:0:0:9300]
Publish address:
inet[/172.31.92.202:9300]
Channels
Transport
HTTP
Transport size (Δ)
Rx
Tx
Transport: 13
HTTP: 6
HTTP total opened: 288
Series: weighted avg
Rx: 1.6kb, #6
Tx: 1.6kb, #6
Indices
Docs count: 1
Docs deleted: 0
Flush: 2, 10ms
Refresh: 2, 61ms
Size: 2.5kb
Search requests per second (Δ)
Query
Fetch
Search time per second (Δ)
Query
Fetch
Get requests per second (Δ)
Get
Exists
Missing
Get time per second (Δ)
Get
Exists
Missing
Query: 2
Fetch: 2
Query: 14ms
Fetch: 0s
Get: 3
Exists: 2
Missing: 1
Get: 10ms
Exists: 7ms
Missing: 3ms