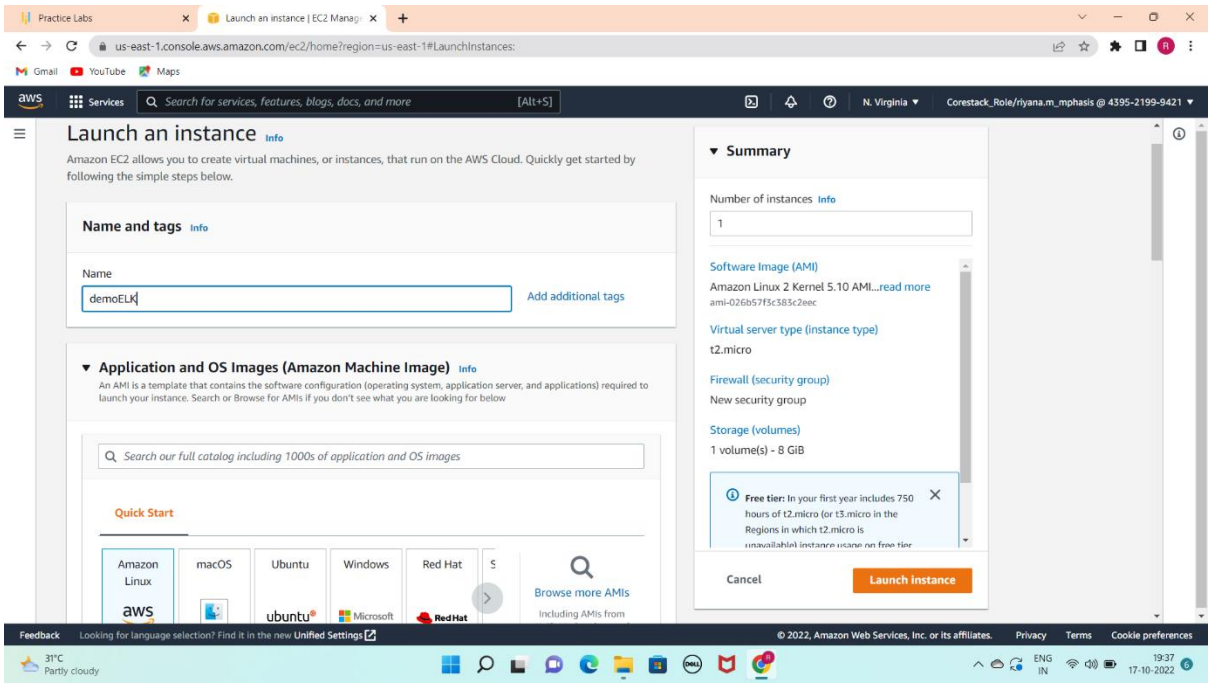
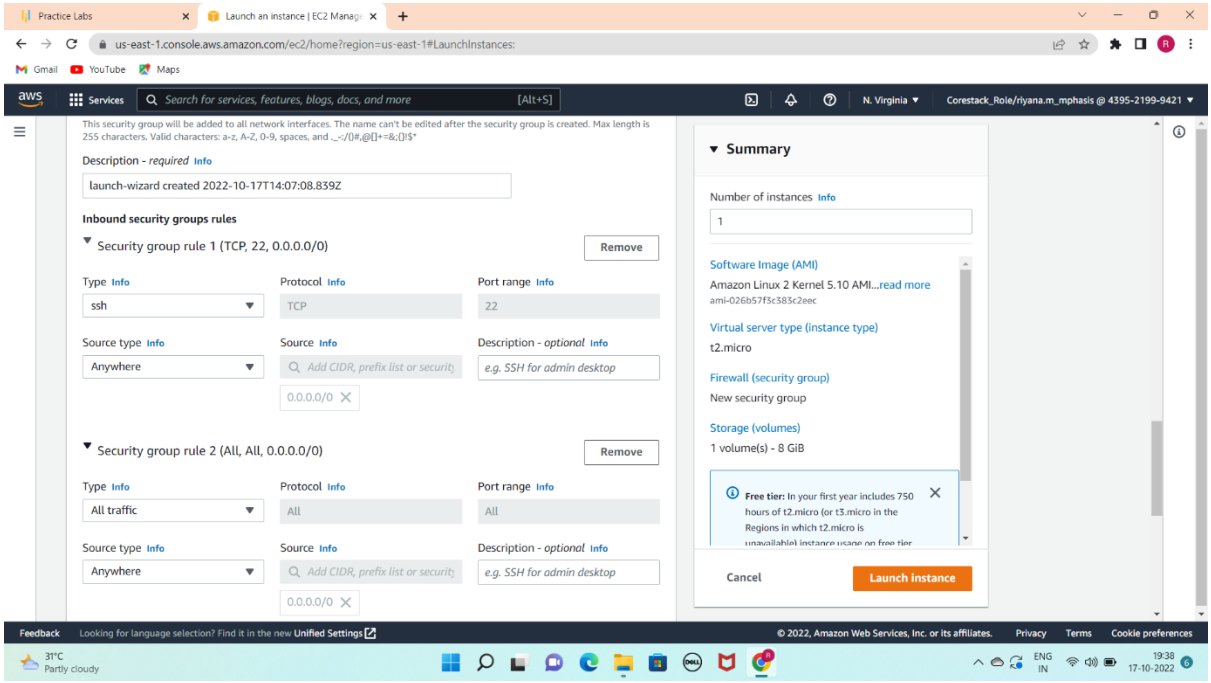
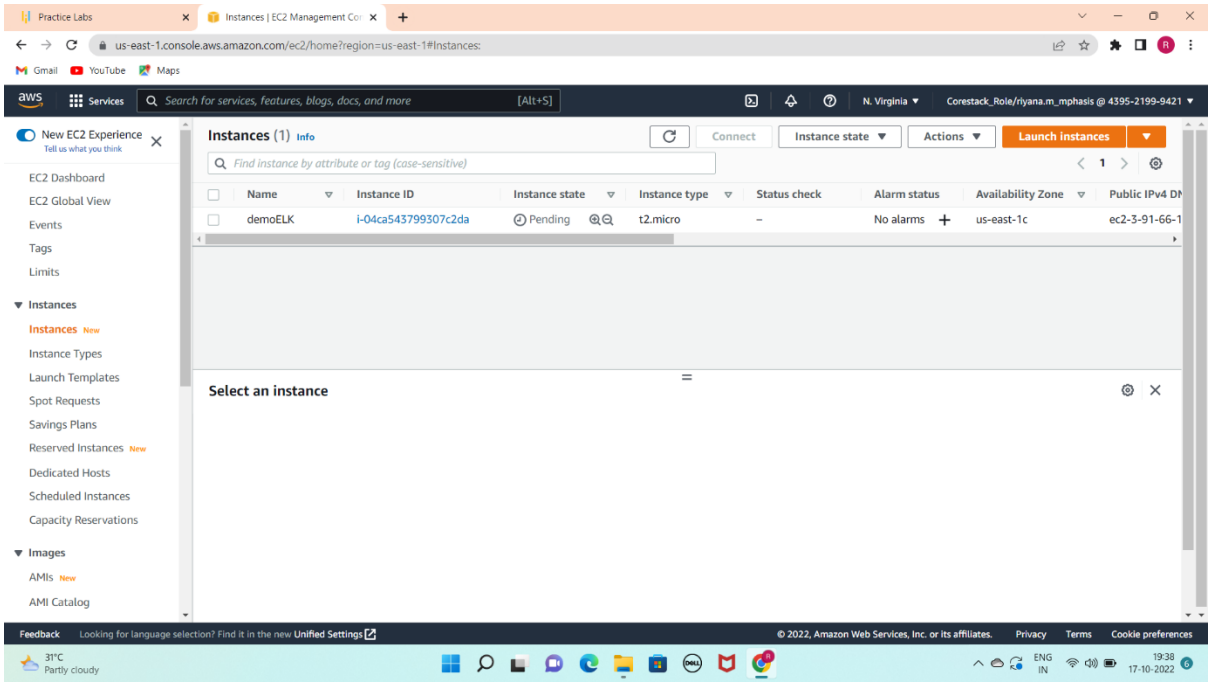
# DELPOYING ELK STACK ON DOCKER CONTAINER

## Results:

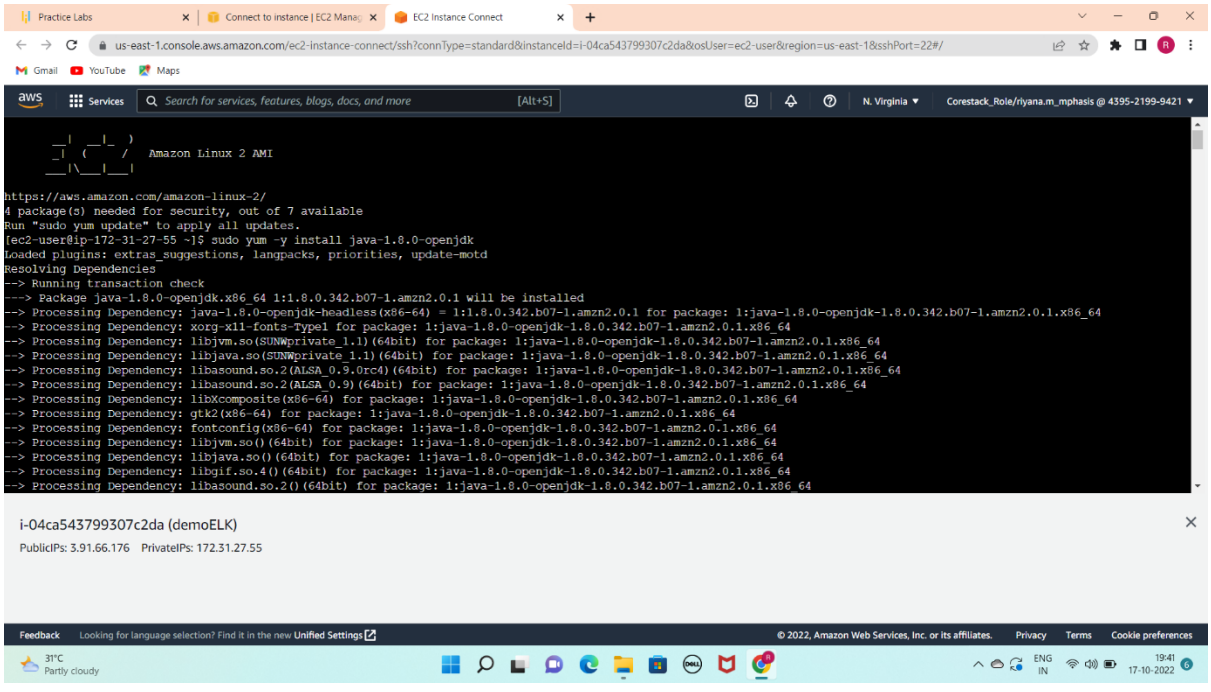
1. Create ec2-instance

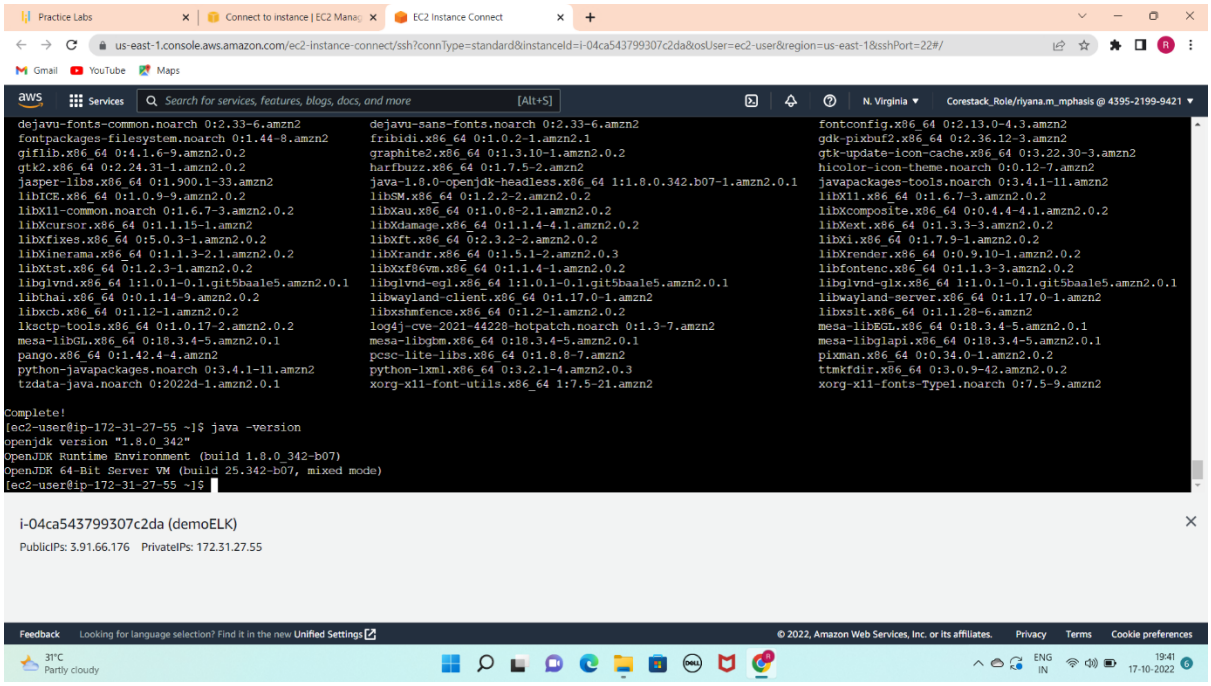


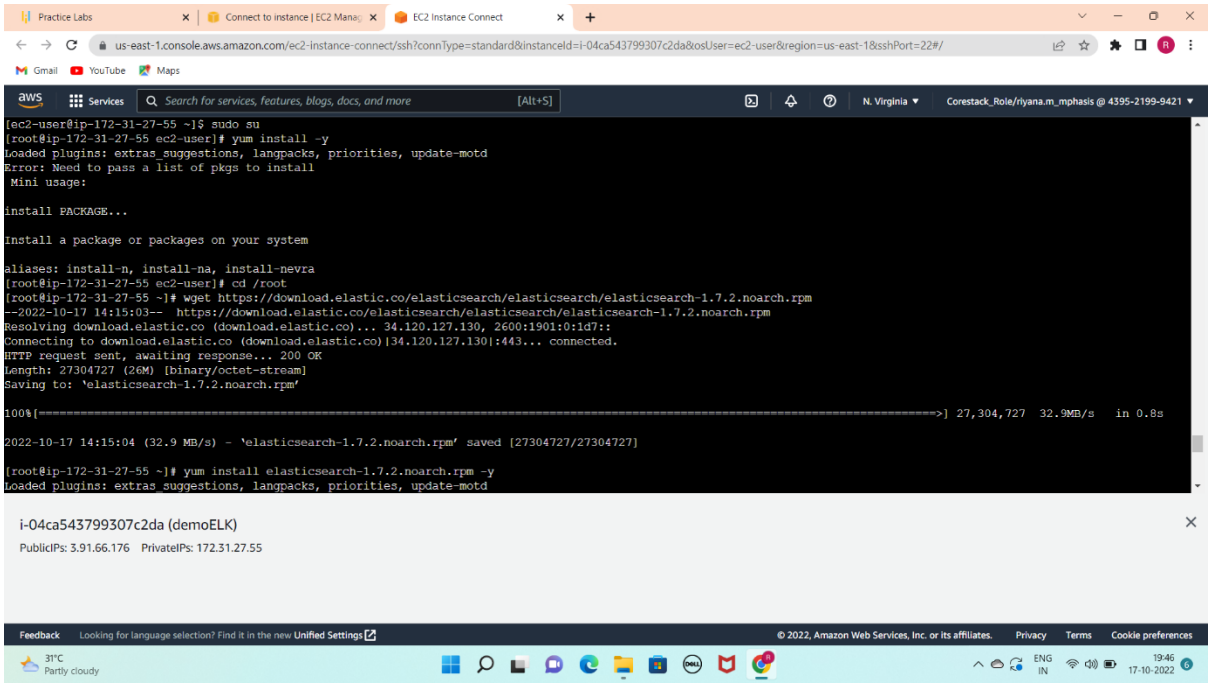


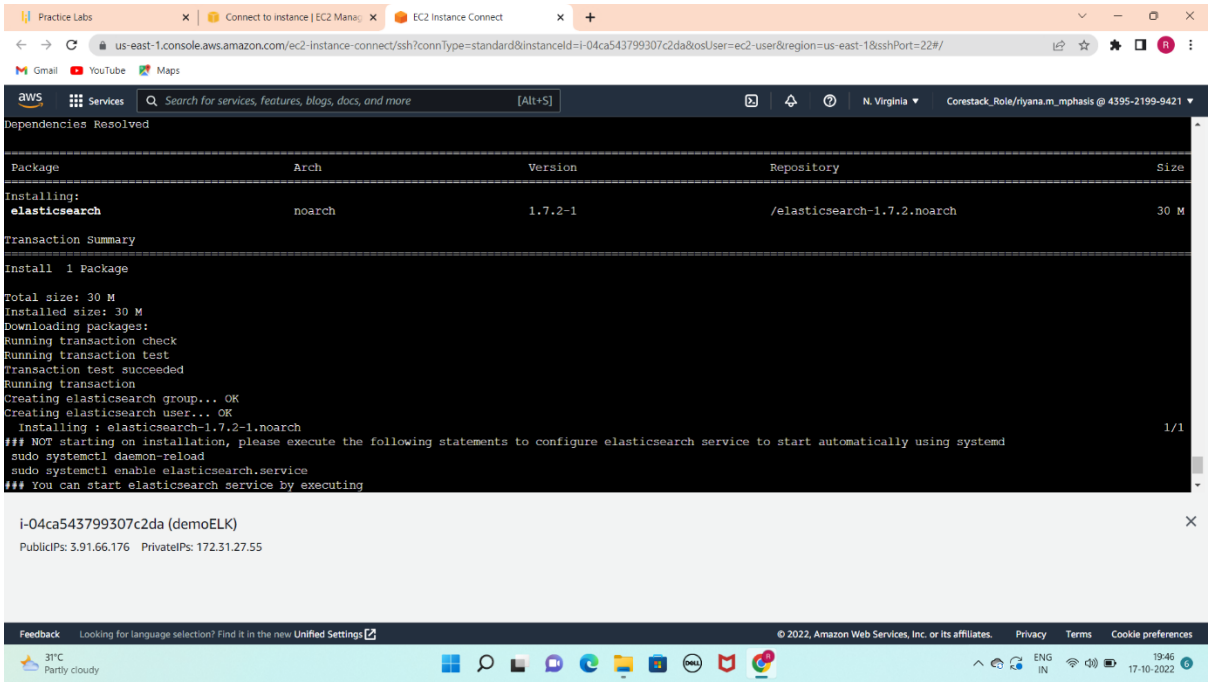

## 2. Install java and its dependencies



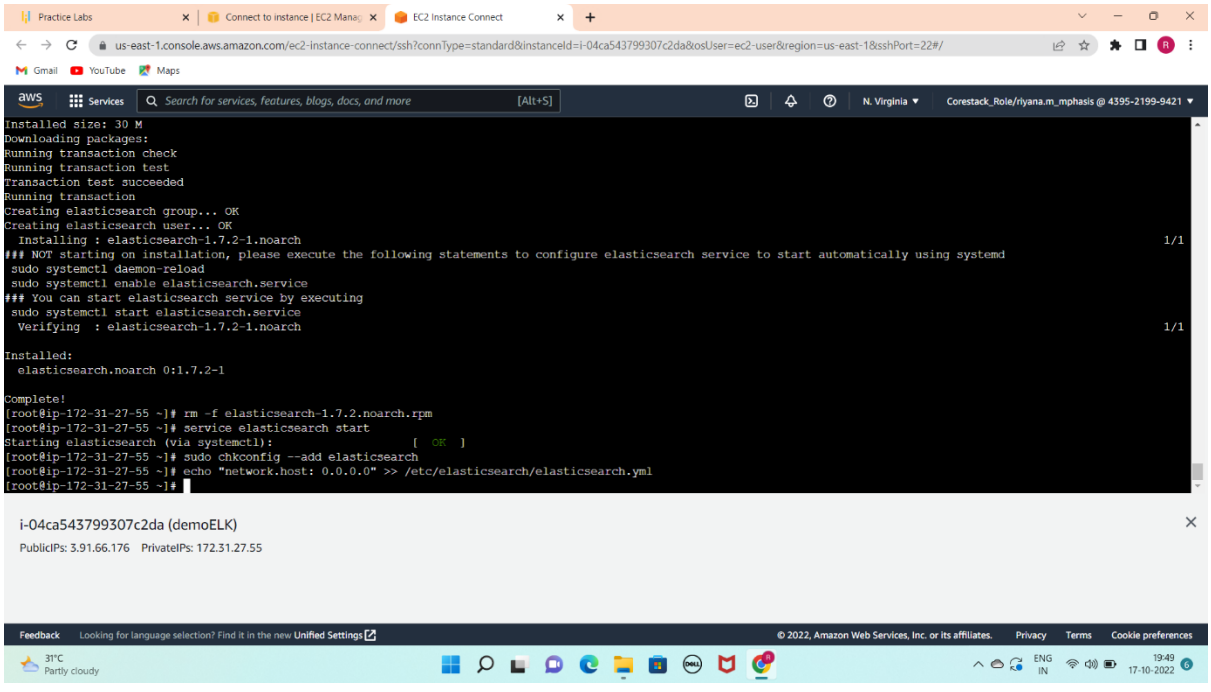



# 3. Install elastic search on AWS server

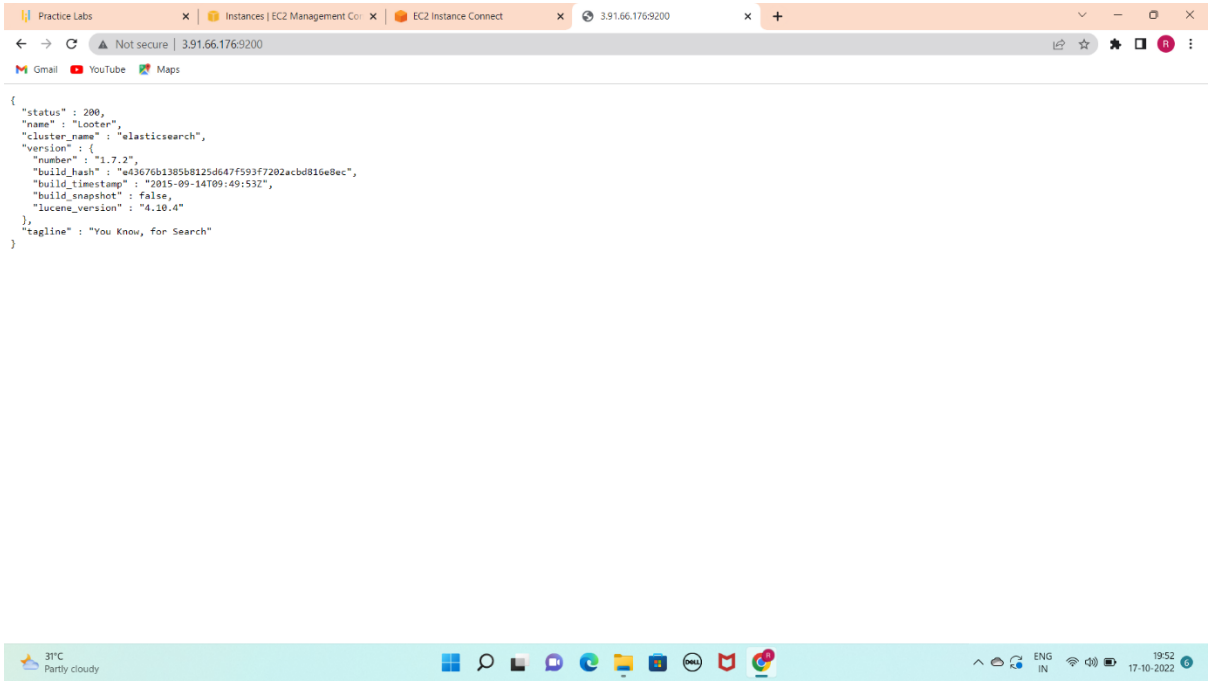




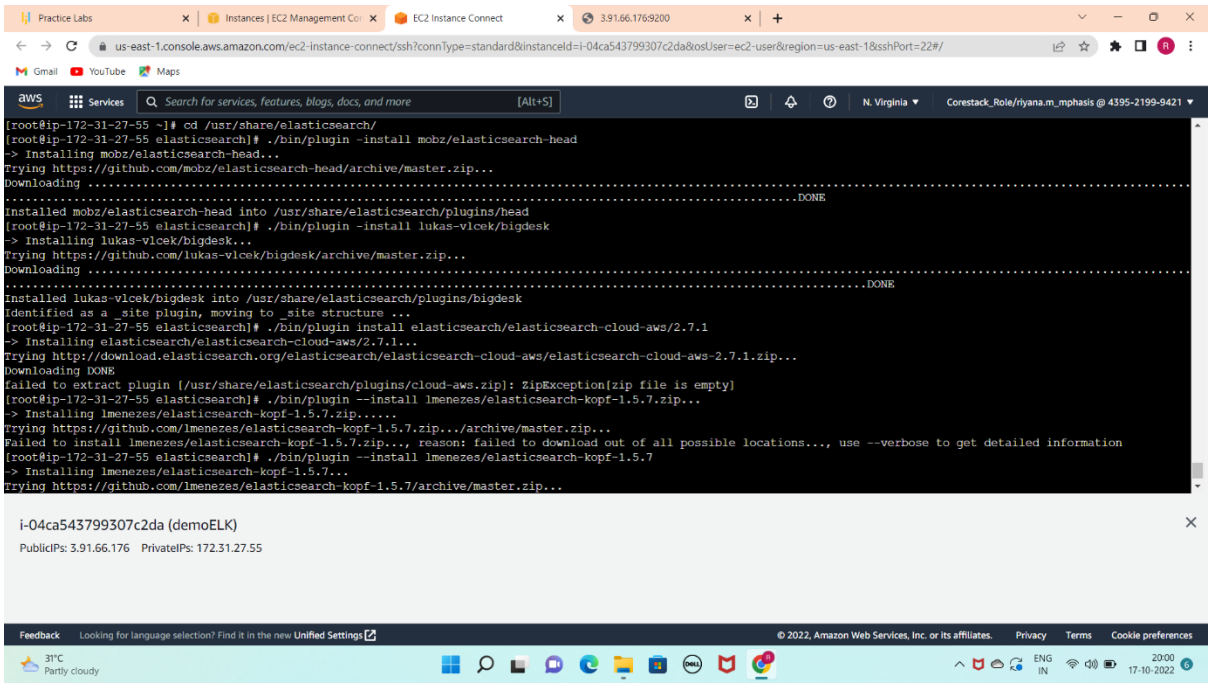

# 4. Start the server and configuring AWS ip

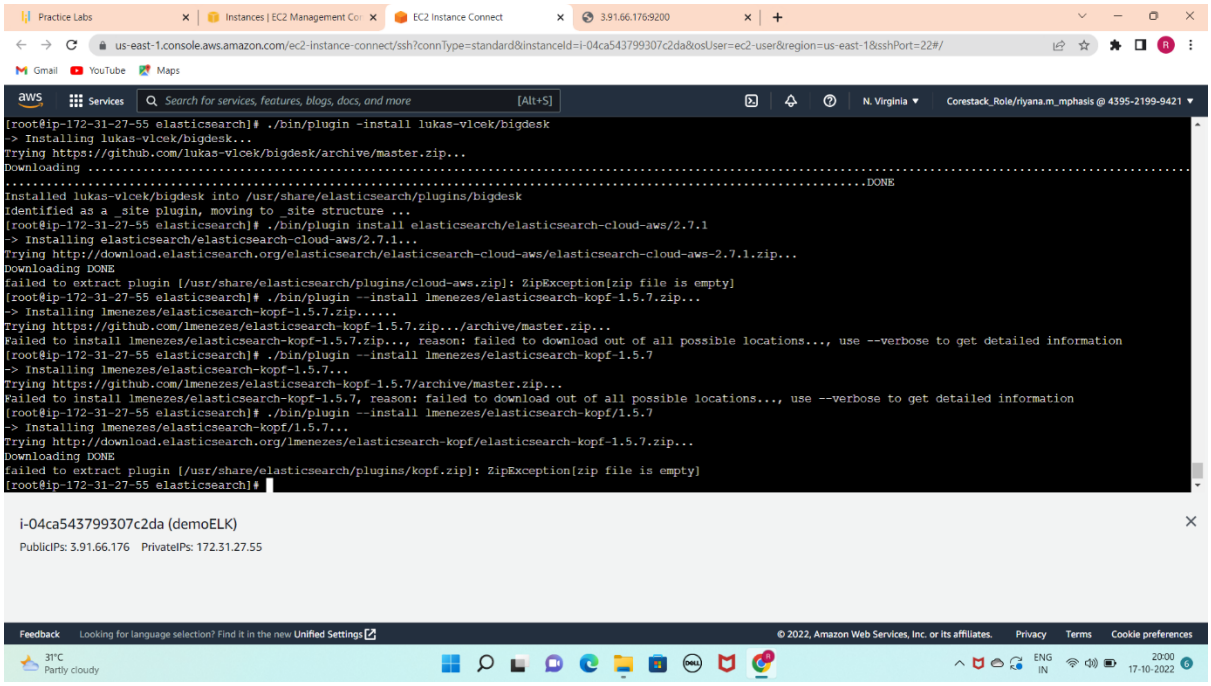


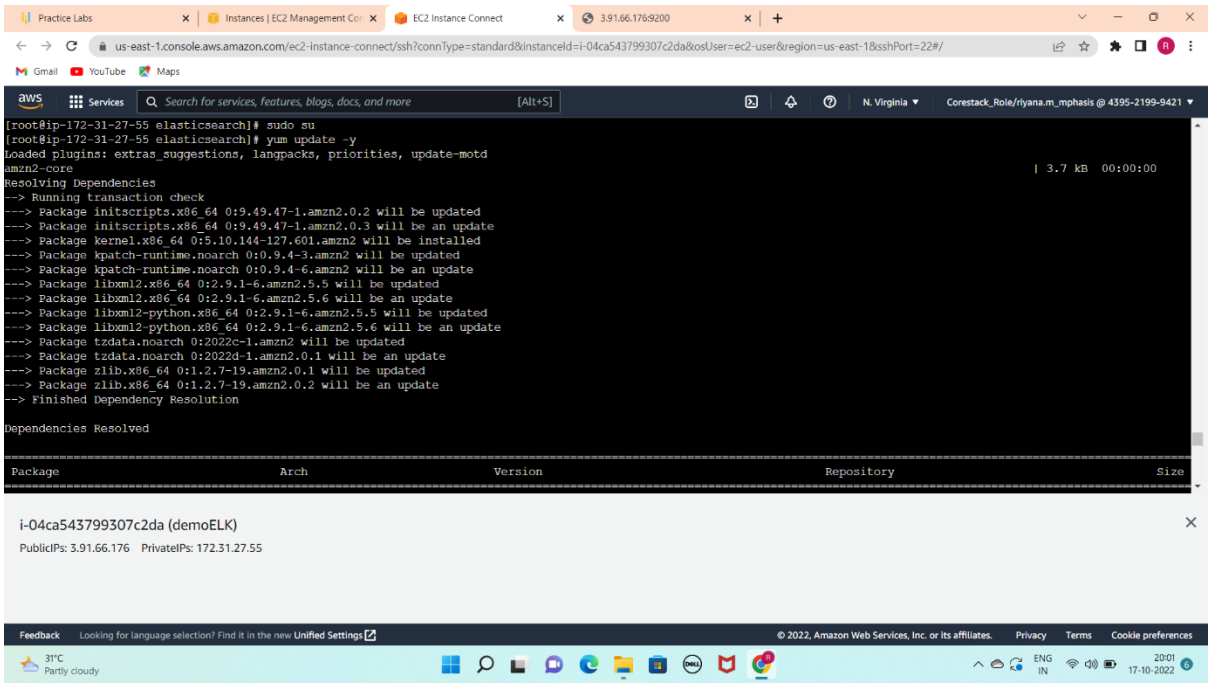
# 5. Checking elastic search

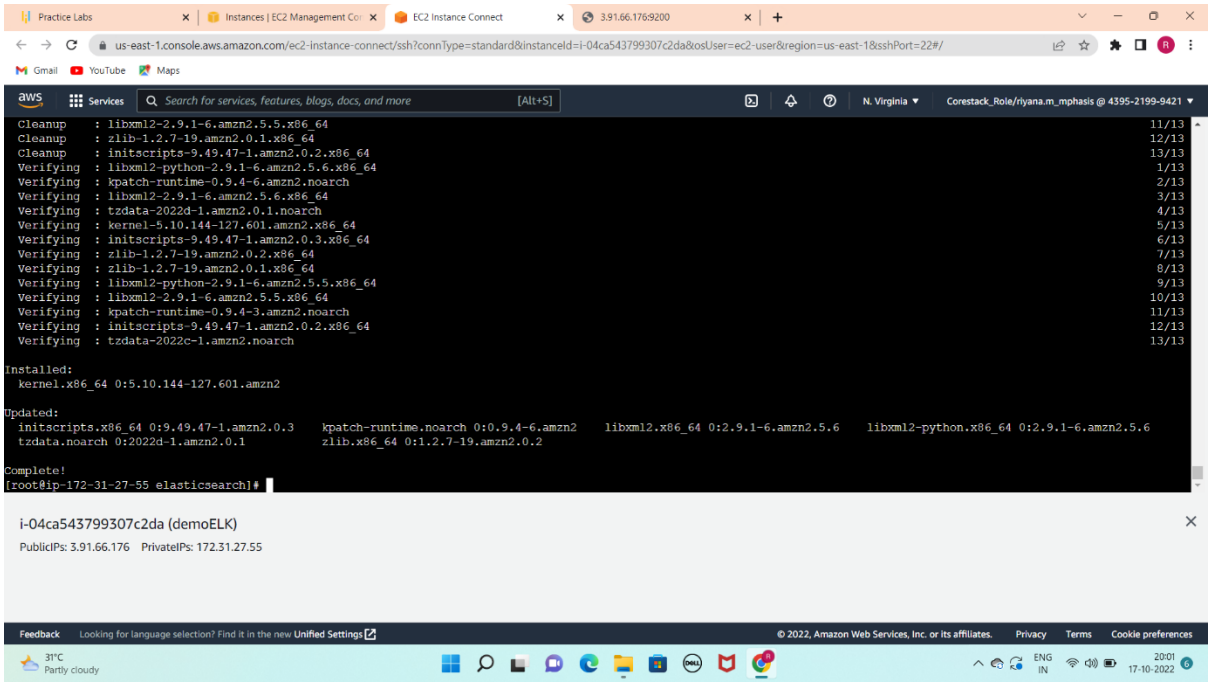



# 6. Install plugins

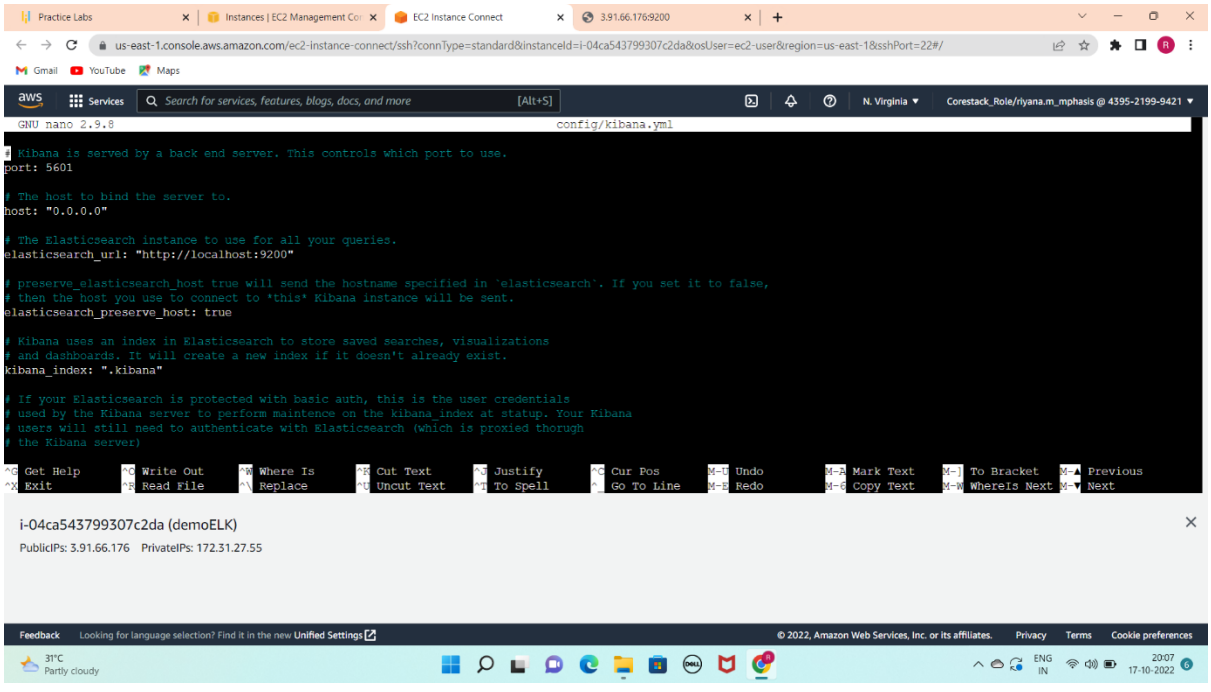


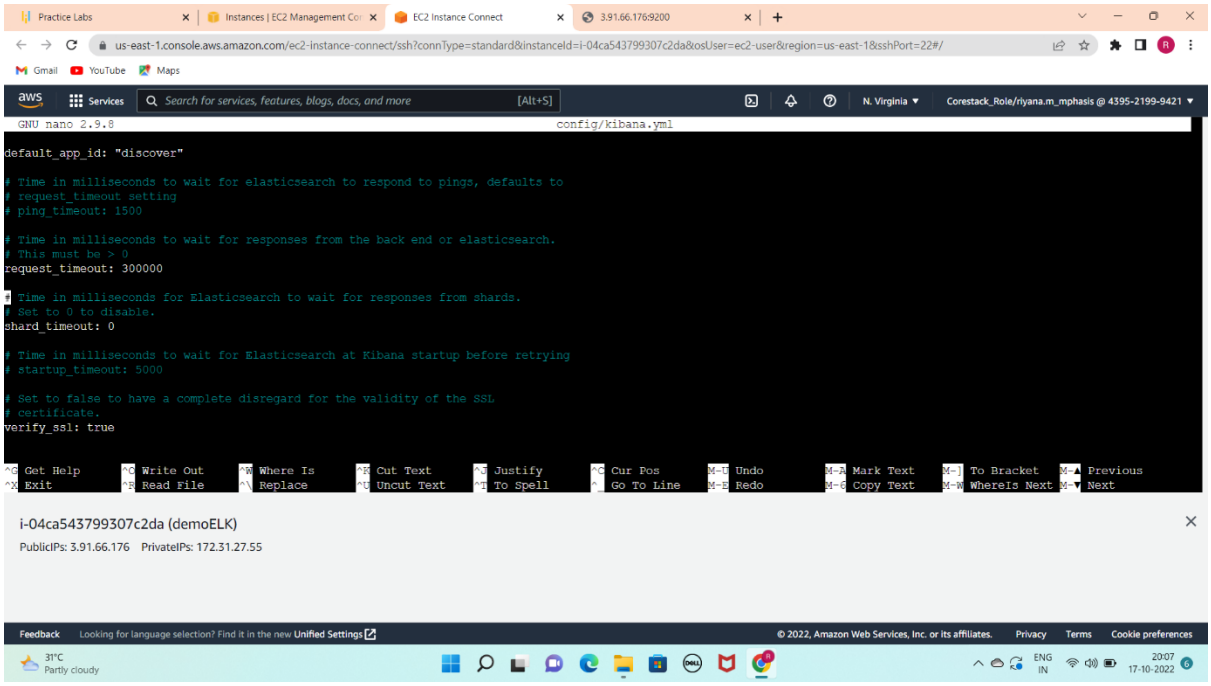

Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
3.91.66.176:9200
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user&region=us-east-1&sshPort=22#/
Gmail
YouTube
Maps
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/riyana.m_mphasis @ 4395-2199-9421
[root@ip-172-31-27-55 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-172-31-27-55 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-172-31-27-55 elasticsearch]# ./bin/plugin --install lmenezes/elasticsearch-kopf-1.5.7.zip...
-> Installing lmenezes/elasticsearch-kopf-1.5.7.zip.....
Trying https://github.com/lmenezes/elasticsearch-kopf-1.5.7.zip.../archive/master.zip...
Failed to install lmenezes/elasticsearch-kopf-1.5.7.zip..., reason: failed to download out of all possible locations..., use --verbose to get detailed information
[root@ip-172-31-27-55 elasticsearch]# ./bin/plugin --install lmenezes/elasticsearch-kopf-1.5.7
-> Installing lmenezes/elasticsearch-kopf-1.5.7...
Trying https://github.com/lmenezes/elasticsearch-kopf-1.5.7/archive/master.zip...
Failed to install lmenezes/elasticsearch-kopf-1.5.7, reason: failed to download out of all possible locations..., use --verbose to get detailed information
[root@ip-172-31-27-55 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-172-31-27-55 elasticsearch]#
i-04ca543799307c2da (demoELK)
PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
31°C
Partly cloudy
ENG
IN
20:00
17-10-2022

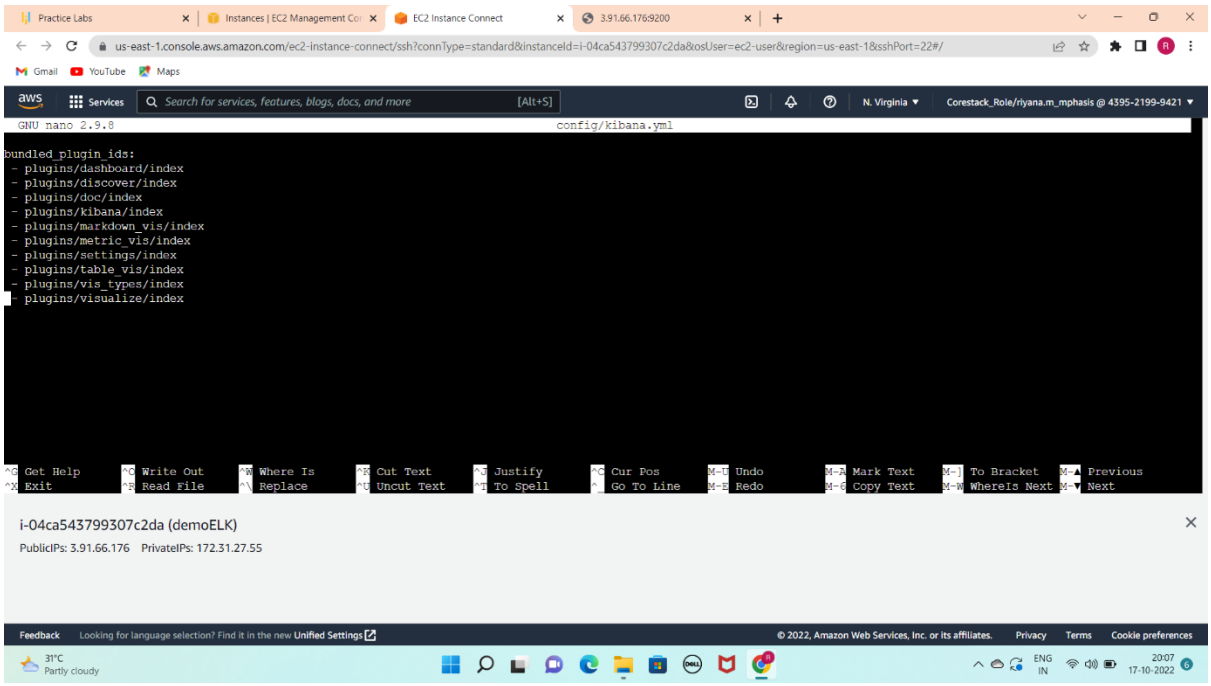

Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
3.91.66.176:9200
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user&region=us-east-1&sshPort=22#/
Gmail
YouTube
Maps
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/riyana.m_mphasis @ 4395-2199-9421
[root@ip-172-31-27-55 elasticsearch]# sudo su
[root@ip-172-31-27-55 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.7 kB 00:00:00
Resolving Dependencies
--> Running transaction check
---> Package initscripts.x86_64 0:9.49.47-1.amzn2.0.2 will be updated
---> Package initscripts.x86_64 0:9.49.47-1.amzn2.0.3 will be an update
---> Package kernel.x86_64 0:5.10.144-127.601.amzn2 will be installed
---> Package kpatch-runtime.noarch 0:0.9.4-3.amzn2 will be updated
---> Package kpatch-runtime.noarch 0:0.9.4-6.amzn2 will be an update
---> Package libxml2.x86_64 0:2.9.1-6.amzn2.5.5 will be updated
---> Package libxml2.x86_64 0:2.9.1-6.amzn2.5.6 will be an update
---> Package libxml2-python.x86_64 0:2.9.1-6.amzn2.5.5 will be updated
---> Package libxml2-python.x86_64 0:2.9.1-6.amzn2.5.6 will be an update
---> Package tzdata.noarch 0:2022c-1.amzn2 will be updated
---> Package tzdata.noarch 0:2022d-1.amzn2.0.1 will be an update
---> Package zlib.x86_64 0:1.2.7-19.amzn2.0.1 will be updated
---> Package zlib.x86_64 0:1.2.7-19.amzn2.0.2 will be an update
--> Finished Dependency Resolution
Dependencies Resolved
Package Arch Version Repository Size
i-04ca543799307c2da (demoELK)
PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
31°C
Partly cloudy
ENG
IN
20:01
17-10-2022

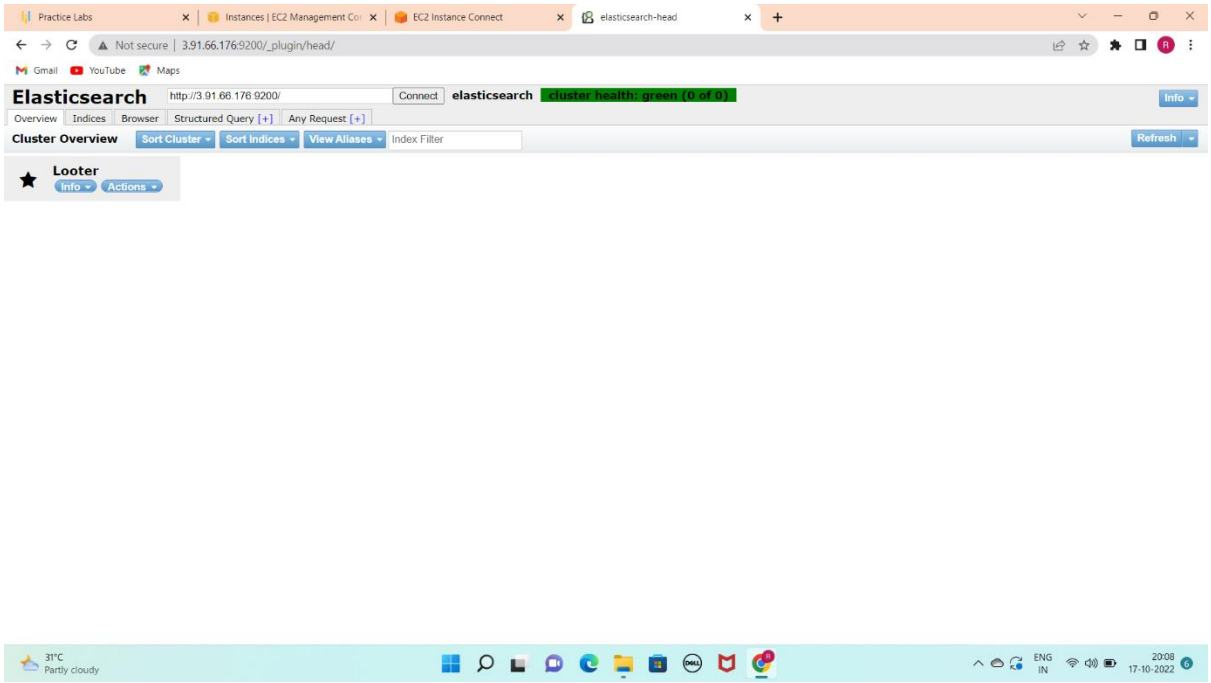


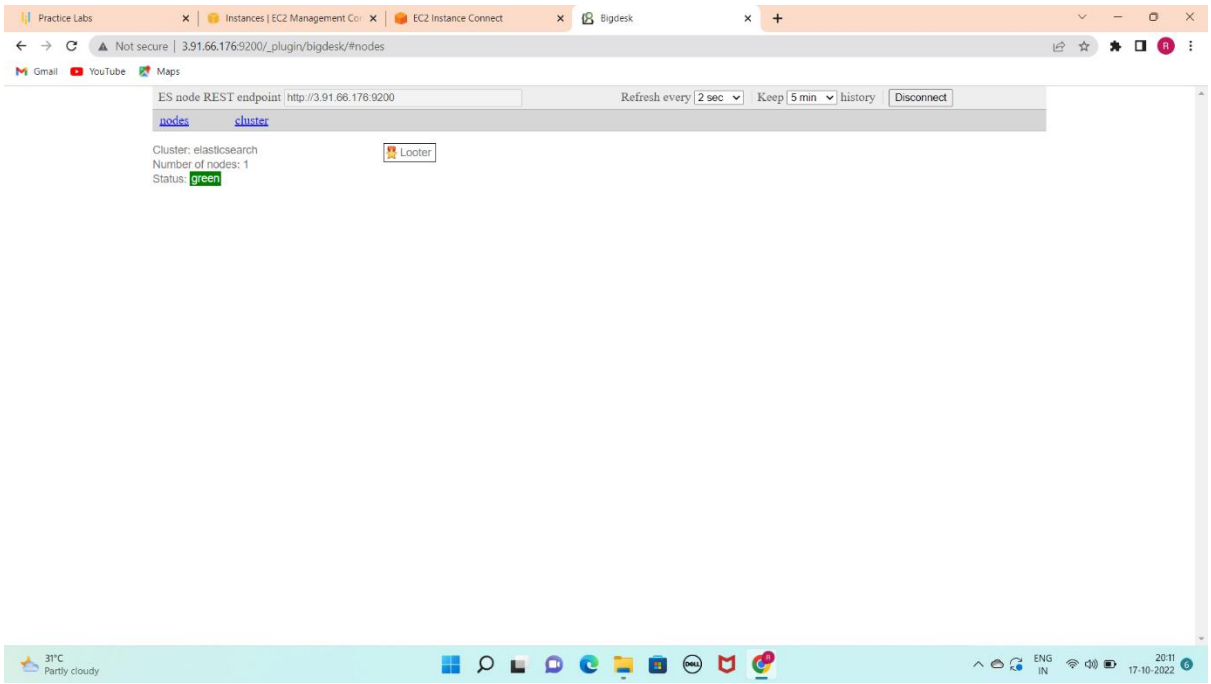

# 7. Kibana installation

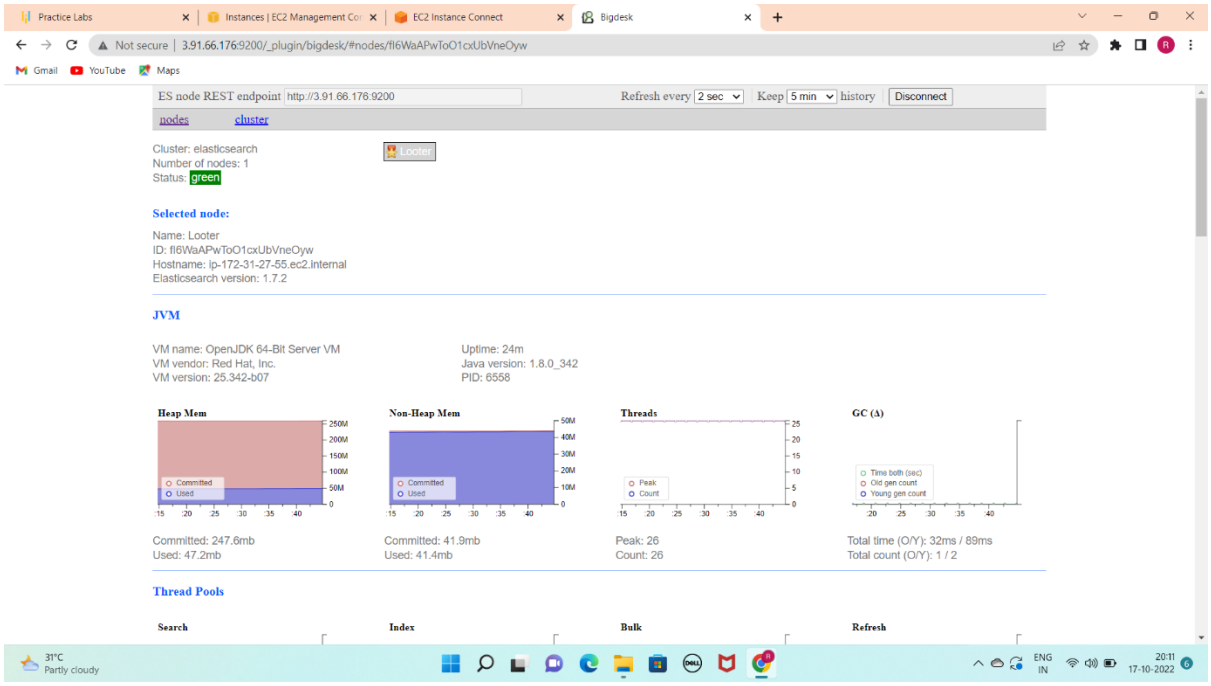


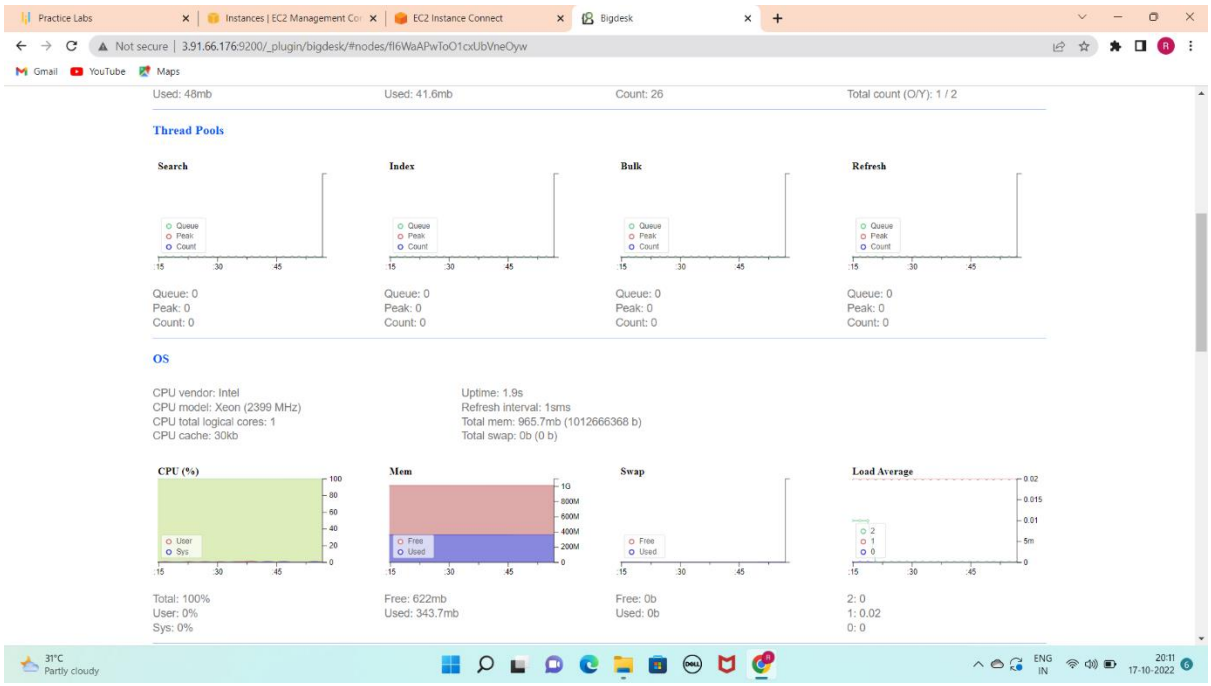

Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
3.91.66.176:9200
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user&region=us-east-1&sshPort=22#/
Gmail
YouTube
Maps
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Corestack_Role/riyana.m_mphasis @ 4395-2199-9421
GNU nano 2.9.8 config/kibana.yml
default_app_id: "discover"
# Time in milliseconds to wait for elasticsearch to respond to pings, defaults to
# request_timeout setting
# ping_timeout: 1500
# Time in milliseconds to wait for responses from the back end or elasticsearch.
# This must be > 0
request_timeout: 300000
# Time in milliseconds for Elasticsearch to wait for responses from shards.
# Set to 0 to disable.
shard_timeout: 0
# Time in milliseconds to wait for Elasticsearch at Kibana startup before retrying
# startup_timeout: 5000
# Set to false to have a complete disregard for the validity of the SSL
# certificate.
verify_ssl: true
^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
i-04ca543799307c2da (demoELK)
PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
31°C
Partly cloudy
ENG
IN
20:07
17-10-2022


Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
3.91.66.176:9200
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user&region=us-east-1&sshPort=22#/
Gmail
YouTube
Maps
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Corestack_Role/riyana.m_mphasis @ 4395-2199-9421
GNU nano 2.9.8 config/kibana.yml
bundled_plugin_ids:
- plugins/dashboard/index
- plugins/discover/index
- plugins/doc/index
- plugins/kibana/index
- plugins/markdown_vis/index
- plugins/metric_vis/index
- plugins/settings/index
- plugins/table_vis/index
- plugins/vis_types/index
- plugins/visualize/index
^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
i-04ca543799307c2da (demoELK)
PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
31°C
Partly cloudy
ENG
IN
20:07
17-10-2022


Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
elasticsearch-head
Not secure | 3.91.66.176:9200/_plugin/head/
Gmail
YouTube
Maps
Elasticsearch
http://3.91.66.176:9200/
Connect
elasticsearch
cluster health: green (0 of 0)
Info
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
Sort Indices
View Aliases
Index Filter
Refresh
Looter
Info
Actions
31°C
Partly cloudy
ENG
IN
20:08
17-10-2022


Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
Bigdesk
Not secure | 3.91.66.176:9200/_plugin/bigdesk/#nodes
Gmail
YouTube
Maps
ES node REST endpoint
http://3.91.66.176:9200
Refresh every
2 sec
Keep
5 min
history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Looter
31°C
Partly cloudy
ENG
IN
20:11
17-10-2022


Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
Bigdesk
Not secure | 3.91.66.176:9200/_plugin/bigdesk/#nodes/fI6WaAPwToO1cxUbVneOyw
Gmail
YouTube
Maps
ES node REST endpoint http://3.91.66.176:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Looter
Selected node:
Name: Looter
ID: fI6WaAPwToO1cxUbVneOyw
Hostname: ip-172-31-27-55.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: 24m
Java version: 1.8.0_342
PID: 6558
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: 47.2mb
Committed: 41.9mb
Used: 41.4mb
Peak: 26
Count: 26
Total time (O/Y): 32ms / 89ms
Total count (O/Y): 1 / 2
Thread Pools
Search
Index
Bulk
Refresh
31°C
Partly cloudy
ENG
IN
20:11
17-10-2022

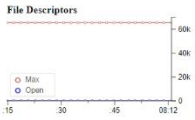

Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
Bigdesk
Not secure | 3.91.66.176:9200/_plugin/bigdesk/#nodes/fI6WaAPwToO1cxUbVneOyw
Gmail
YouTube
Maps
Used: 48mb
Used: 41.6mb
Count: 26
Total count (O/Y): 1 / 2
Thread Pools
Search
Index
Bulk
Refresh
Queue
Peak
Count
Queue: 0
Peak: 0
Count: 0
OS
CPU vendor: Intel
CPU model: Xeon (2399 MHz)
CPU total logical cores: 1
CPU cache: 30kb
Uptime: 1.9s
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: 0%
Sys: 0%
Free: 622mb
Used: 343.7mb
Free: 0b
Used: 0b
2: 0
1: 0.02
0: 0
31°C
Partly cloudy
ENG
IN
20:11
17-10-2022

Practice Labs | Instances | EC2 Management Co | EC2 Instance Connect | Bigdesk

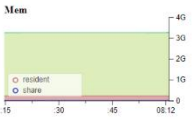
Not secure | 3.91.66.176:9200/_plugin/bigdesk/#nodes/fl6WaAPwToO1cxUbVneOyw

Gmail YouTube Maps

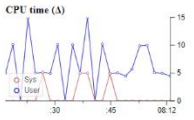
## Process



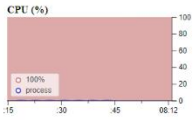

Max: 65535
Open: 104




Total virtual: 3gb
Resident: 224.6mb
Share: 19.3mb




Series: weighted avg
Sys total: 570ms
User total: 10100ms




Total: 100%
Process: 0%

## HTTP & Transport

HTTP address: inet[/172.31.27.55:9200]

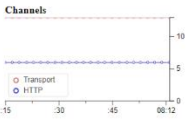
Bound address:
inet[/0:0:0:0:0:0:0:0:9200]

Publish address:
inet[/172.31.27.55:9200]

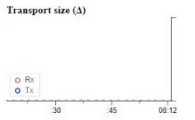
Transport address:
inet[/172.31.27.55:9300]

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

Publish address:
inet[/172.31.27.55:9300]




Transport: 13
HTTP: 6
HTTP total opened: 9




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

31°C Partly cloudy

ENG IN 20:12 17-10-2022

Practice Labs | Instances | EC2 Management Co | EC2 Instance Connect | Bigdesk

Not secure | 3.91.66.176:9200/_plugin/bigdesk/#nodes/fl6WaAPwToO1cxUbVneOyw

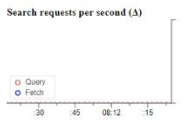
Gmail YouTube Maps

## Indices

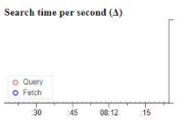
Docs count: 0
Docs deleted: 0

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

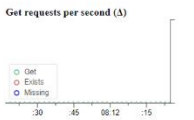
Size: 0b



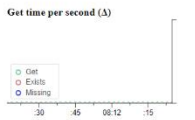

Query: 0
Fetch: 0



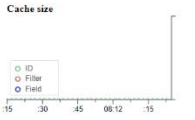

Query: 0s
Fetch: 0s



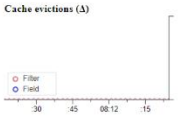

Get: 0
Exists: 0
Missing: 0



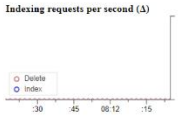

Get: 0s
Exists: 0s
Missing: 0s



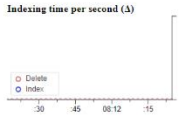

ID: 0b
Filter: 0b
Field: 0b




Filter: 0
Field: 0



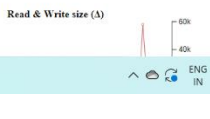

Delete: 0
Index: 0




Delete: 0s
Index: 0s

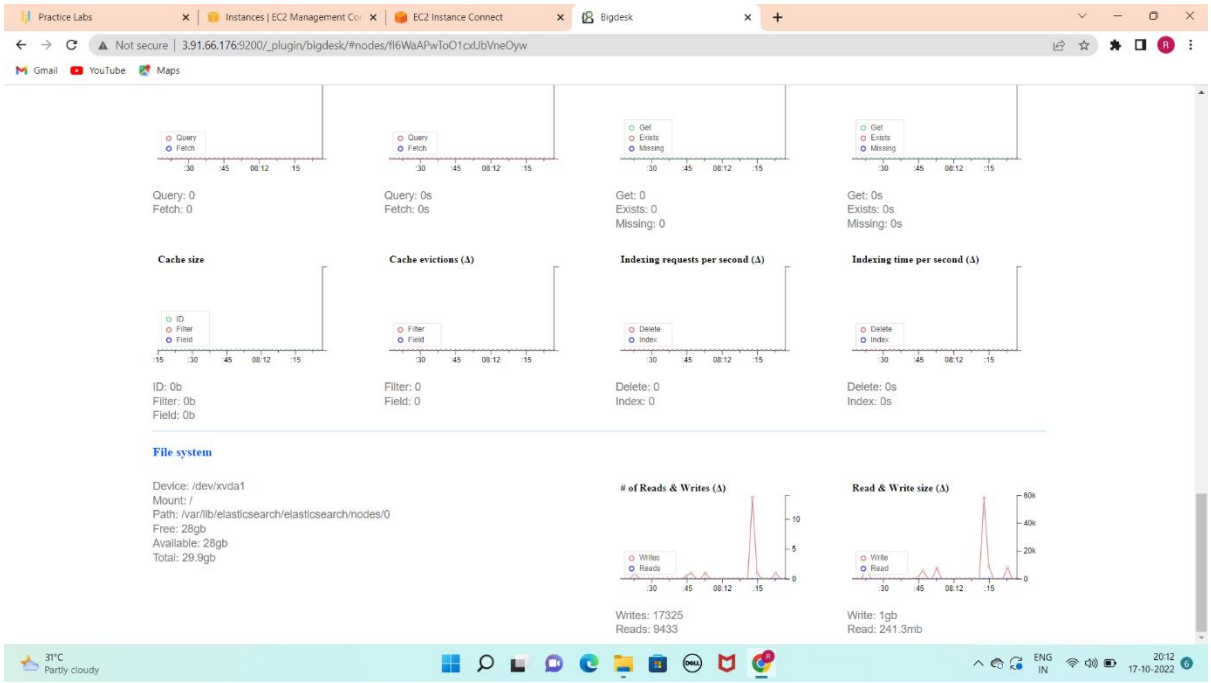
## File system

Device: /dev/xvda1
Mount: /
Path: /var/lib/elasticsearch/elasticsearch/nodes/0
Free: 28gb


31°C Partly cloudy

ENG IN 20:12 17-10-2022


Practice Labs
Instances | EC2 Management Co
EC2 Instance Connect
Bigdesk
Not secure | 3.91.66.176:9200/_plugin/bigdesk/#nodes/fl6WaAPwToO1cxUbVneOyw
Gmail
YouTube
Maps
Query
Fetch
Query: 0
Fetch: 0
Query: 0s
Fetch: 0s
Get
Exists
Missing
Get: 0
Exists: 0
Missing: 0
Get: 0s
Exists: 0s
Missing: 0s
Cache size
ID
Filter
Field
ID: 0b
Filter: 0b
Field: 0b
Cache evictions (Δ)
Filter: 0
Field: 0
Indexing requests per second (Δ)
Delete
Index
Delete: 0
Index: 0
Indexing time per second (Δ)
Delete: 0s
Index: 0s
File system
Device: /dev/xvda1
Mount: /
Path: /var/lib/elasticsearch/elasticsearch/nodes/0
Free: 28gb
Available: 28gb
Total: 29.9gb
# of Reads & Writes (Δ)
Writes
Reads
Writes: 17325
Reads: 9433
Read & Write size (Δ)
Write
Read
Write: 1gb
Read: 241.3mb
31°C
Partly cloudy
ENG
IN
20:12
17-10-2022