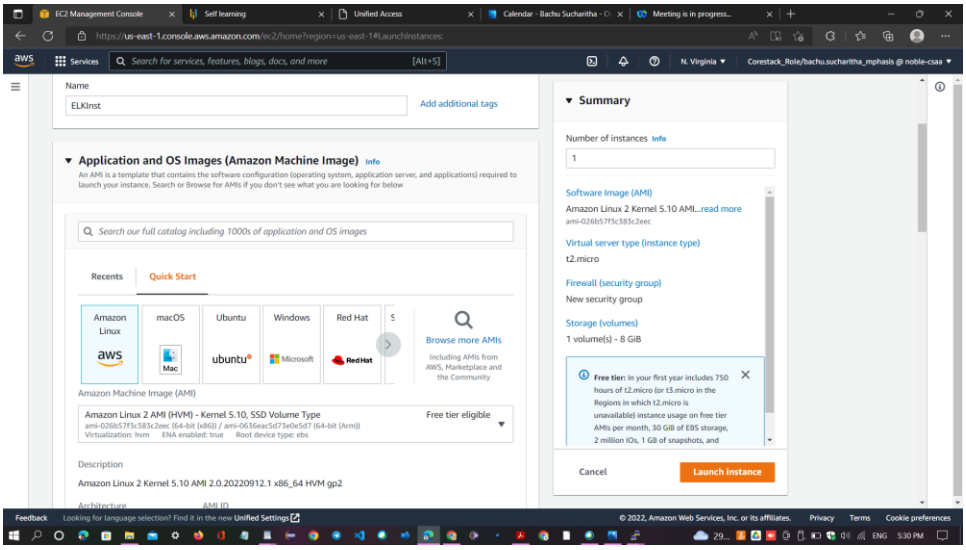
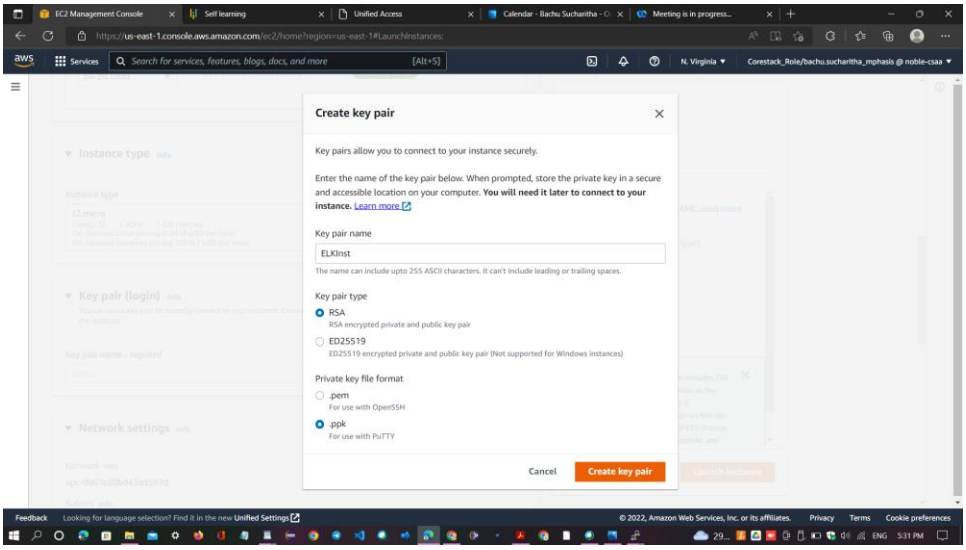
Screenshots

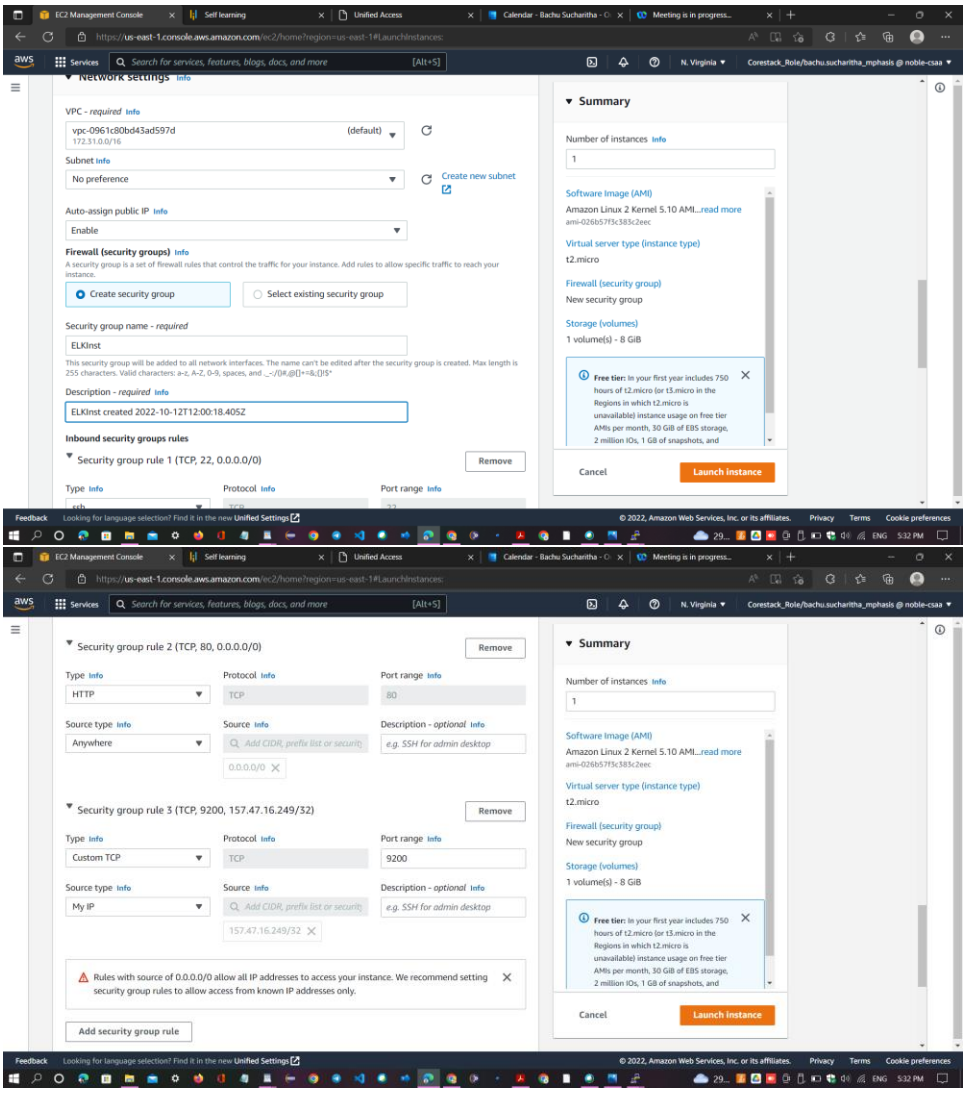
Create an instance and choose Amazon Linux:



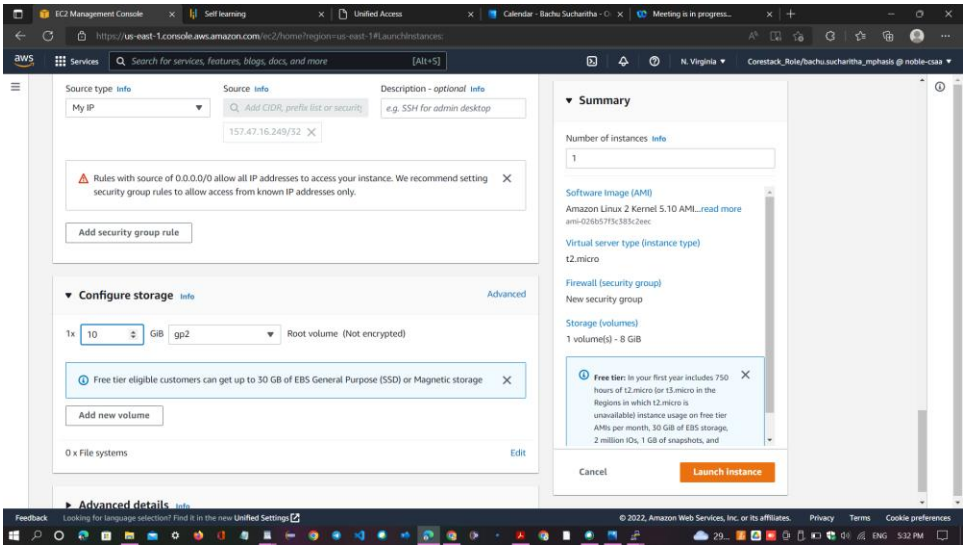
Create Key Pair:



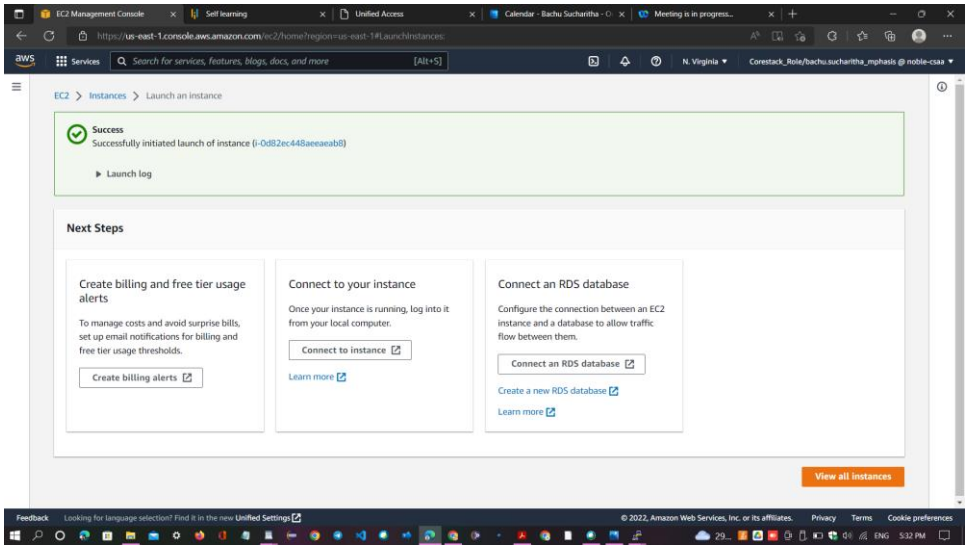
Edit the Network Settings:



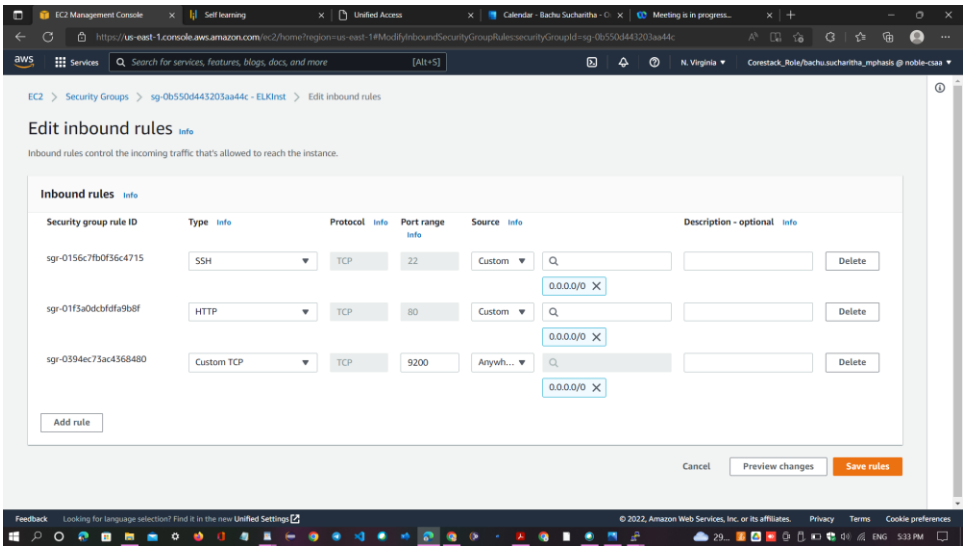
Configure the storage:



The instance is successful:

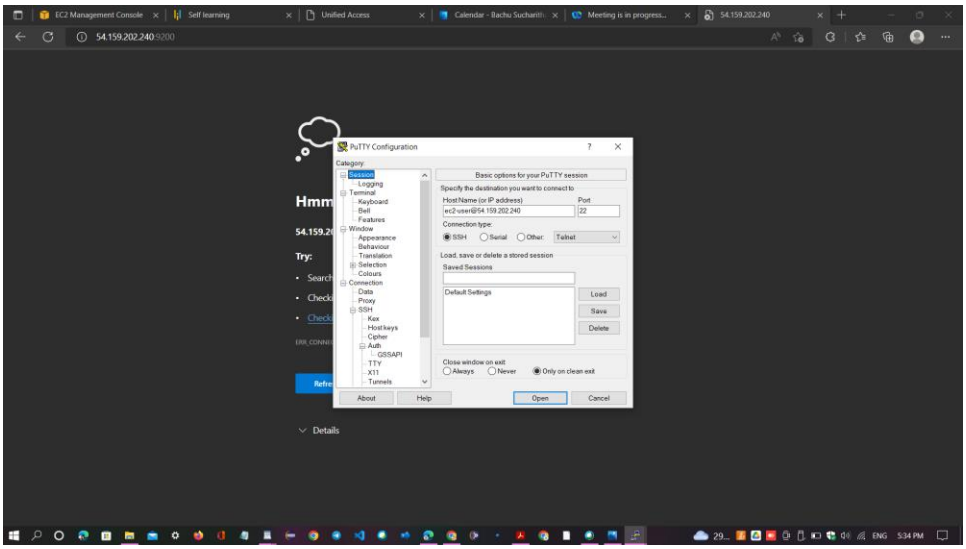


Edit the inbound rules using security details:

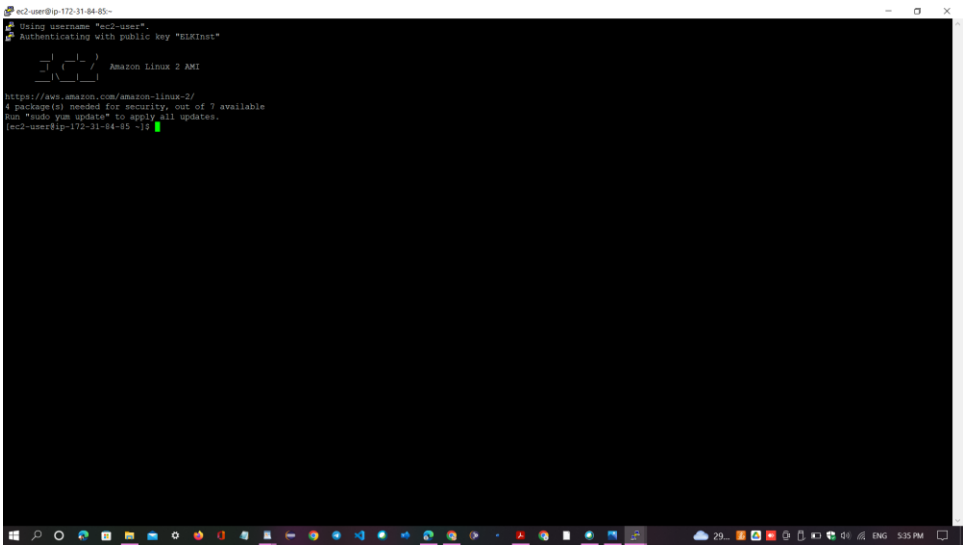


Configure using PuTTY Configuration:

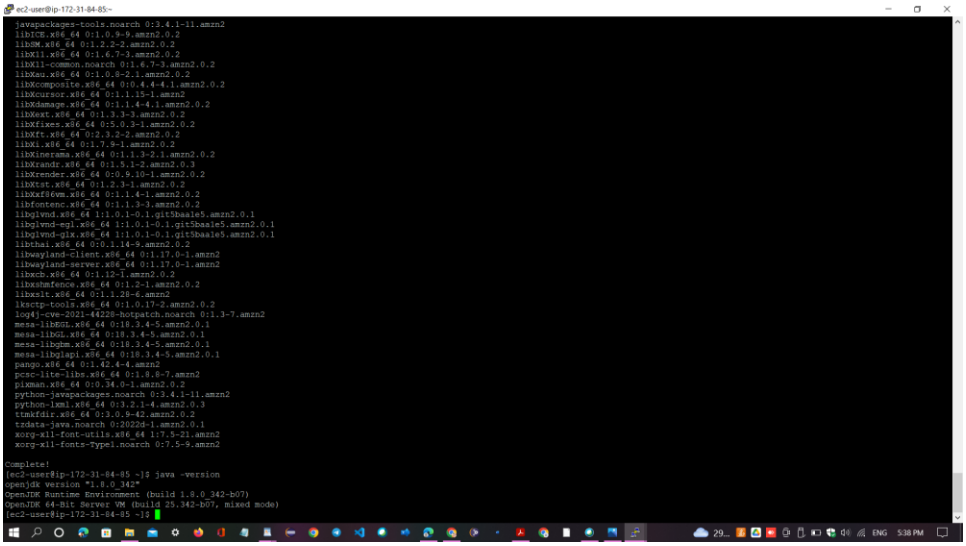
Now connect to the instance using putty



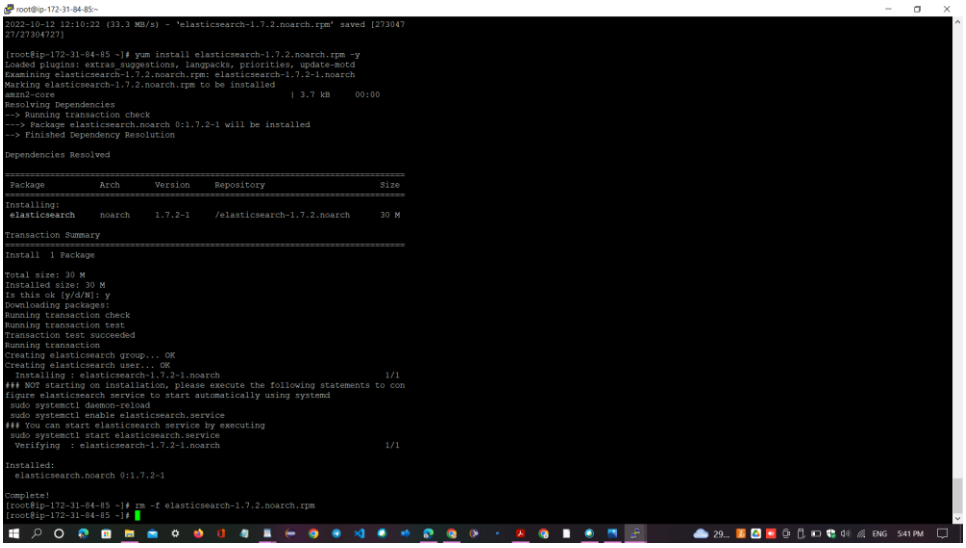
Amazon Linux:



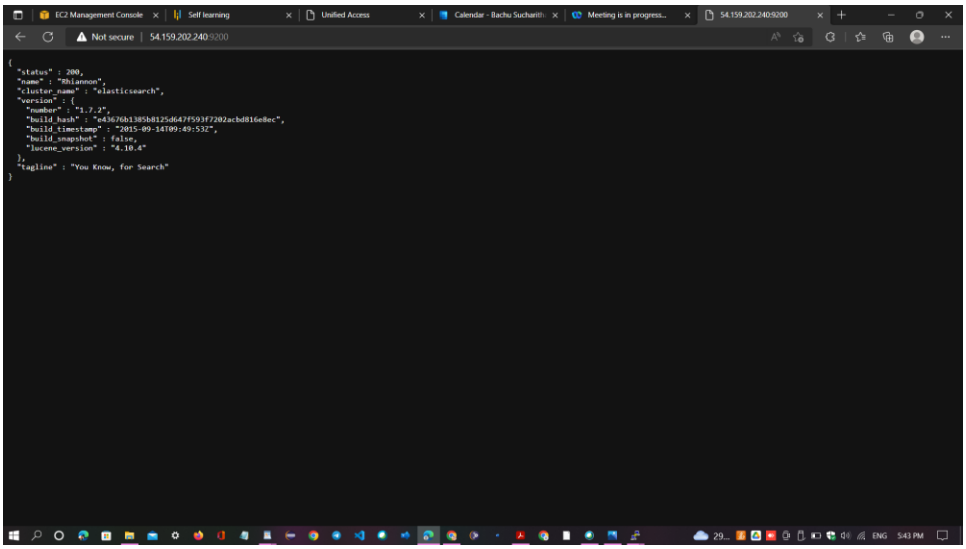
Install java and its Dependencies:



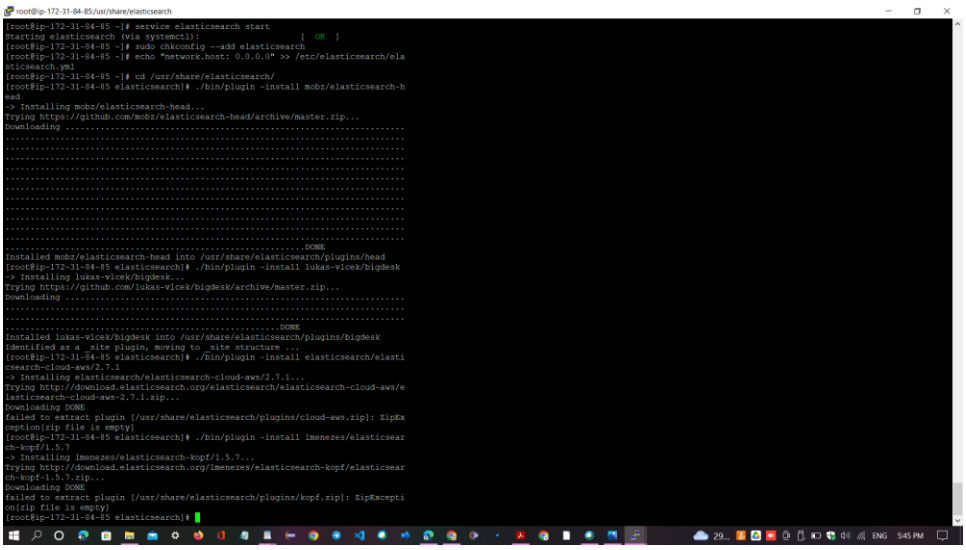
Install Elastic search on AWS Server



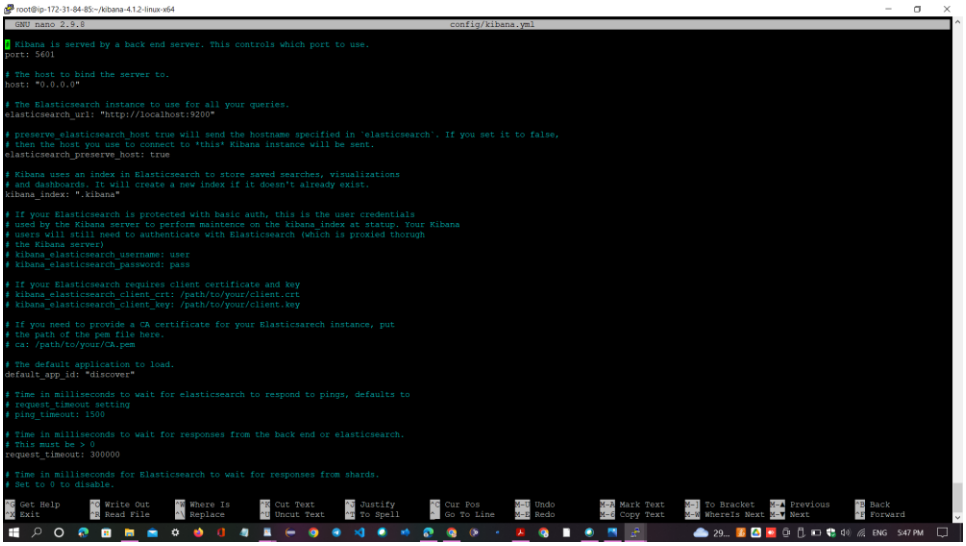
Public ip address:9200 :

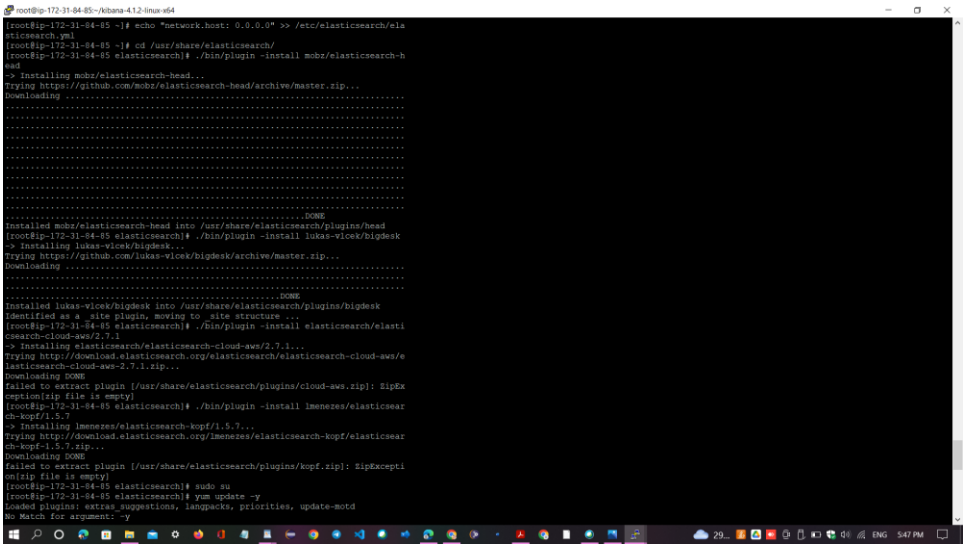


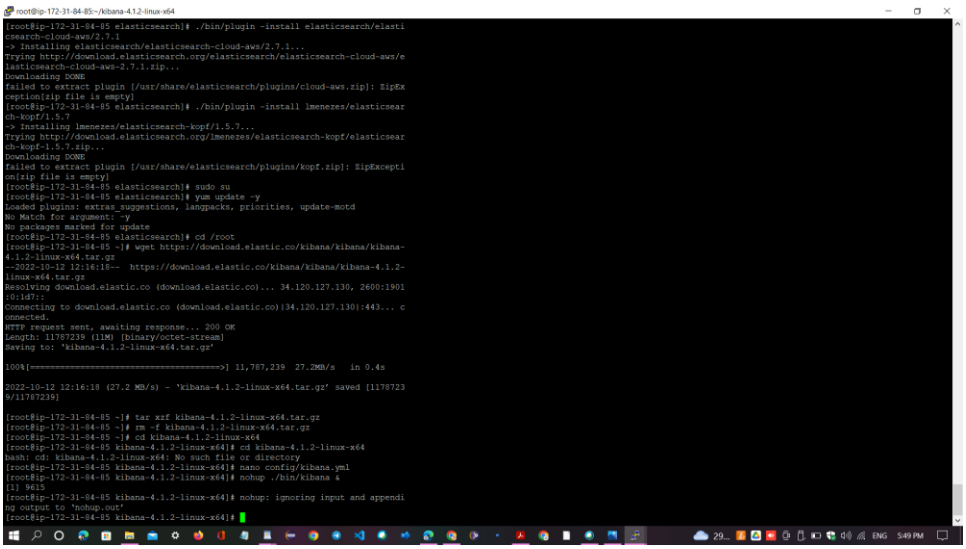
Installing Elasticsearch:

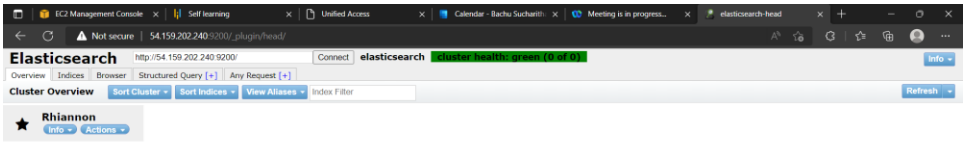


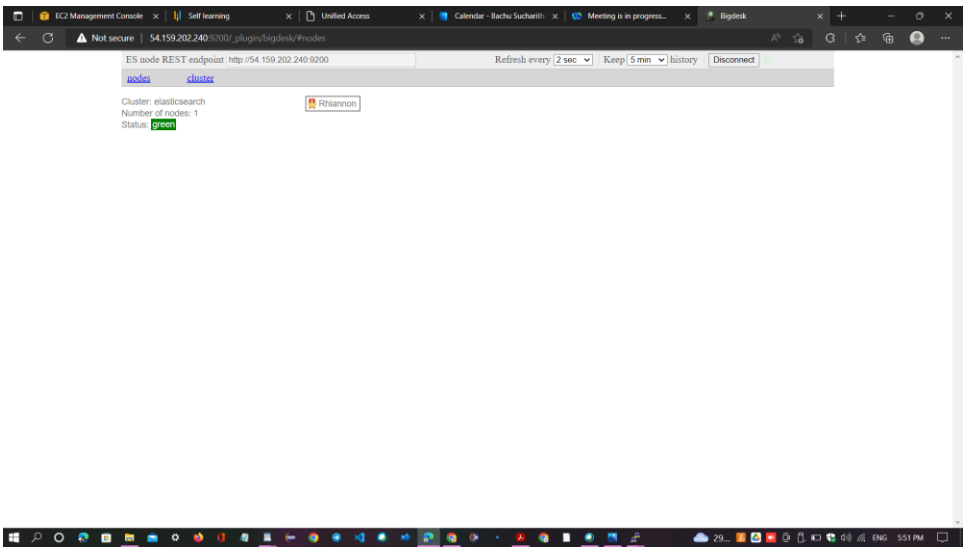
Installing kibana:

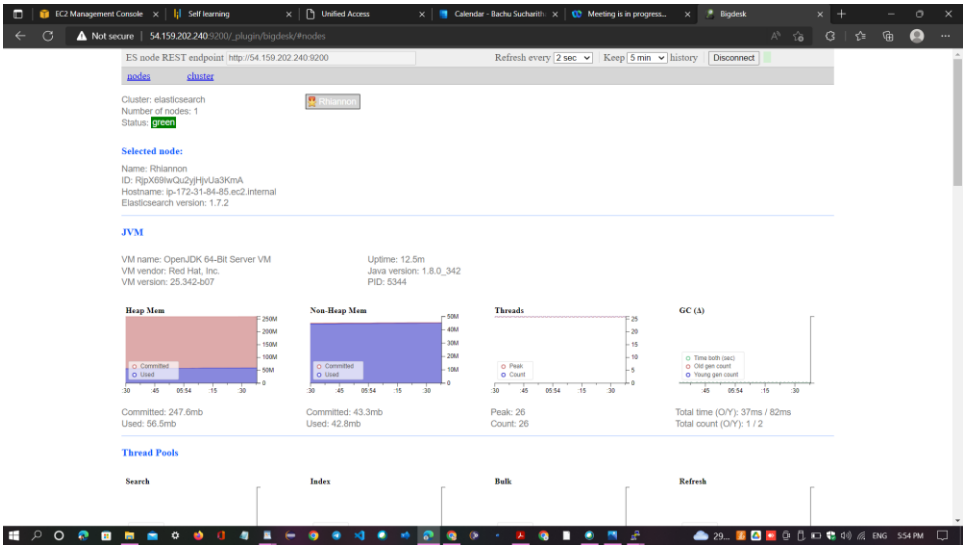

root@ip-172-31-84-85:~/kibana-4.1.2-linux-x64
GNU nano 2.9.8 config/kibana.yml
Kibana is served by a back end server. This controls which port to use.
port: 5601
The host to bind the server to.
host: "0.0.0.0"
The Elasticsearch instance to use for all your queries.
elasticsearch_url: "http://localhost:9200"
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
If your Elasticsearch requires client certificate and key
kibana_elasticsearch_client_crt: /path/to/your/client.crt
kibana_elasticsearch_client_key: /path/to/your/client.key
If you need to provide a CA certificate for your Elasticsarech instance, put
the path of the pem file here.
ca: /path/to/your/CA.pem
The default application to load.
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.
^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-Q Previous ^B Back
^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 ^F Next ^V Forward
29... ENG 5:47 PM

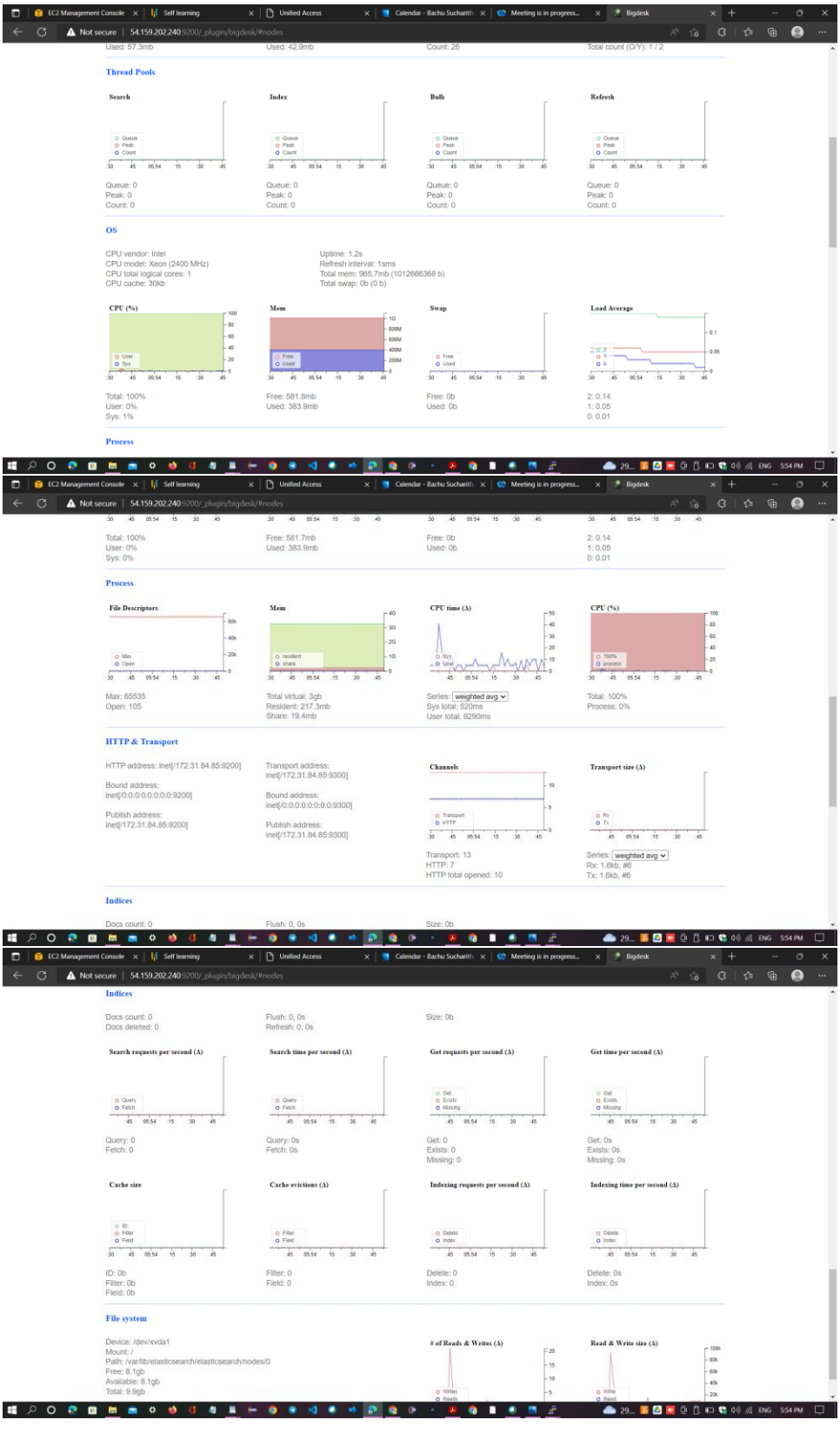

root@ip-172-31-84-85:~/kibana-4.1.2-linux-x64
[root@ip-172-31-84-85 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-84-85 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-84-85 elasticsearch]# ./bin/plugin -install mobz/elasticsearch-head
-> Installing mobz/elasticsearch-head...
Trying https://github.com/mobz/elasticsearch-head/archive/master.zip...
Downloading .....DONE
Installed mobz/elasticsearch-head into /usr/share/elasticsearch/plugins/head
[root@ip-172-31-84-85 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-172-31-84-85 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-172-31-84-85 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-172-31-84-85 elasticsearch]# sudo su
[root@ip-172-31-84-85 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No Match for argument: -y
29... ENG 5:47 PM

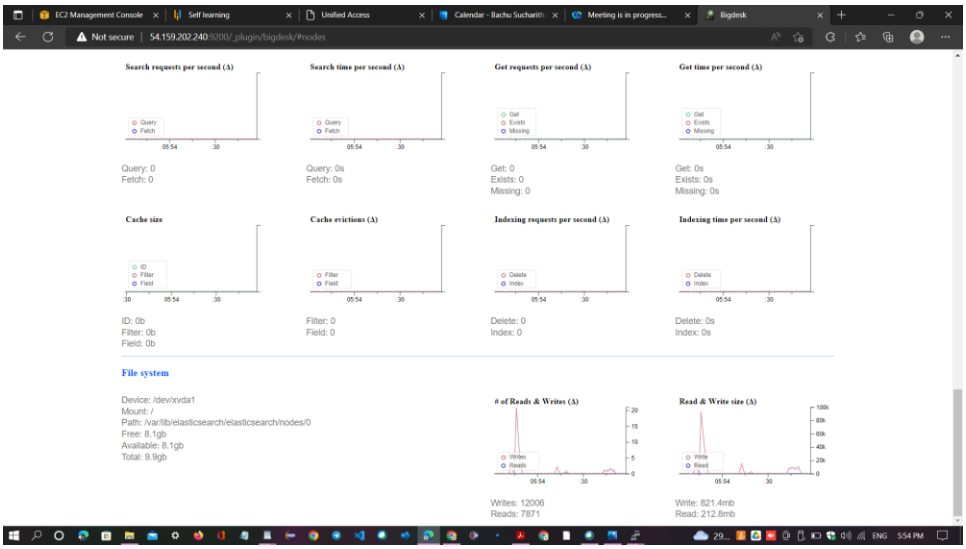

root@ip-172-31-84-85:~/kibana-4.1.2-linux-x64
[root@ip-172-31-84-85 elasticsearch]# ./bin/plugin -install elasticsearch/elasticsearch-cloud-aws/2.7.1
-> Installing elasticsearch/elasticsearch-cloud-aws/2.7.1...
Trying http://download.elasticsearch.org/elasticsearch/elasticsearch-cloud-aws/elasticsearch-cloud-aws-2.7.1.zip...
Downloading DONE
failed to extract plugin [/usr/share/elasticsearch/plugins/cloud-aws.zip]: ZipException[zip file is empty]
[root@ip-172-31-84-85 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-172-31-84-85 elasticsearch]# sudo su
[root@ip-172-31-84-85 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No Match for argument: -y
No packages marked for update
[root@ip-172-31-84-85 elasticsearch]# cd /root
[root@ip-172-31-84-85 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-12 12:16:18-- 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 27.2MB/s in 0.4s
2022-10-12 12:16:18 (27.2 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]
[root@ip-172-31-84-85 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-84-85 ~]# rm -f kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-84-85 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-84-85 kibana-4.1.2-linux-x64]# cd kibana-4.1.2-linux-x64
bash: cd: kibana-4.1.2-linux-x64: No such file or directory
[root@ip-172-31-84-85 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-84-85 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 9615
[root@ip-172-31-84-85 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'
[root@ip-172-31-84-85 kibana-4.1.2-linux-x64]#
29... ENG 5:49 PM


EC2 Management Console
Self learning
Unified Access
Calendar - Bachu Sucharith
Meeting is in progress...
elasticsearch-head
Not secure | 54.159.202.240:9200/_plugin/head/
Elasticsearch
http://54.159.202.240:9200/
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
Rhiannon
Info
Actions


EC2 Management Console
Self learning
Unified Access
Calendar - Bachu Sucharith
Meeting is in progress...
Bigdesk
Not secure | 54.159.202.240:9200/_plugin/bigdesk/#nodes
ES node REST endpoint http://54.159.202.240:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Rhiannon


EC2 Management Console
Self learning
Unified Access
Calendar - Bachu Sucharith
Meeting is in progress...
Bigdesk
Not secure | 54.159.202.240:9200/_plugin/bigdesk/#nodes
ES node REST endpoint http://54.159.202.240:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Rhiannon
Selected node:
Name: Rhiannon
ID: RgX6lIwQuQyjHjvUa3KmA
Hostname: ip-172-31-84-85.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: 12.5m
Java version: 1.8.0_342
PID: 5344
Heap Mem
Committed
Used
Committed: 247.6mb
Used: 56.5mb
Non-Heap Mem
Committed
Used
Committed: 43.3mb
Used: 42.8mb
Threads
Peak
Count
Peak: 26
Count: 26
GC (Δ)
Time both (sec)
Old gen count
Young gen count
Total time (O/Y): 37ms / 82ms
Total count (O/Y): 1 / 2
Thread Pools
Search
Index
Bulk
Refresh


EC2 Management Console
Self learning
Unified Access
Calendar - Bachu Sucharith
Meeting is in progress...
Bigdesk
Not secure | 54.159.202.240:9200/_plugin/bigdesk/#nodes
Used: 57.3mb
Used: 42.9mb
Count: 26
Total count (O/Y): 1 / 2
Thread Pools
Search
Index
Bulk
Refresh
Queue: 0
Peak: 0
Count: 0
OS
CPU vendor: Intel
CPU model: Xeon (2400 MHz)
CPU total logical cores: 1
CPU cache: 30kb
Uptime: 1.2s
Refresh interval: 1sms
Total mem: 965.7mb (1012666368 b)
Total swap: 0b (0 b)
CPU (%)
Mem
Swap
Load Average
Total: 100%
User: 0%
Sys: 1%
Free: 581.8mb
Used: 383.9mb
Free: 0b
Used: 0b
2: 0.14
1: 0.05
0: 0.01
Process
Total: 100%
User: 0%
Sys: 0%
Free: 581.7mb
Used: 383.9mb
Free: 0b
Used: 0b
2: 0.14
1: 0.05
0: 0.01
Process
File Descriptors
Mem
CPU time (Δ)
CPU (%)
Max: 65535
Open: 105
Total virtual: 3gb
Resident: 217.3mb
Share: 19.4mb
Series: weighted avg
Sys total: 520ms
User total: 9290ms
Total: 100%
Process: 0%
HTTP & Transport
HTTP address: inet[/172.31.84.85:9200]
Bound address: inet[/0:0:0:0:0:0:0:0:9200]
Publish address: inet[/172.31.84.85:9200]
Transport address: inet[/172.31.84.85:9300]
Bound address: inet[/0:0:0:0:0:0:0:0:9300]
Publish address: inet[/172.31.84.85:9300]
Channels
Transport size (Δ)
Transport: 13
HTTP: 7
HTTP total opened: 10
Series: weighted avg
Rx: 1.6kb, #6
Tx: 1.6kb, #6
Indices
Docs count: 0
Docs deleted: 0
Flush: 0, 0s
Refresh: 0, 0s
Size: 0b
Search requests per second (Δ)
Search time per second (Δ)
Get requests per second (Δ)
Get time per second (Δ)
Query: 0
Fetch: 0
Query: 0s
Fetch: 0s
Get: 0
Exists: 0
Missing: 0
Get: 0s
Exists: 0s
Missing: 0s
Cache size
Cache evictions (Δ)
Indexing requests per second (Δ)
Indexing time per second (Δ)
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: 8.1gb
Available: 8.1gb
Total: 9.9gb
# of Reads & Writes (Δ)
Read & Write size (Δ)


EC2 Management Console
Self learning
Unified Access
Calendar - Bachu Sucharith
Meeting is in progress...
Bigdesk
Not secure
54.159.202.240:9200/_plugin/bigdesk/#nodes
Search requests per second (Δ)
Query
Fetch
05:54
:30
Query: 0
Fetch: 0
Search time per second (Δ)
Query: 0s
Fetch: 0s
Get requests per second (Δ)
Get
Exists
Missing
Get: 0
Exists: 0
Missing: 0
Get time per second (Δ)
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: 8.1gb
Available: 8.1gb
Total: 9.9gb
# of Reads & Writes (Δ)
Writes
Reads
Writes: 12006
Reads: 7871
Read & Write size (Δ)
Write
Read
Write: 821.4mb
Read: 212.8mb
ENG
5:54 PM