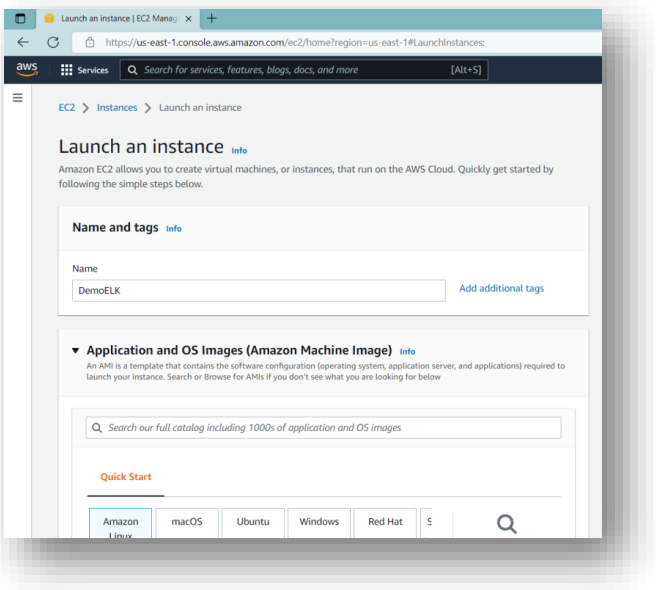
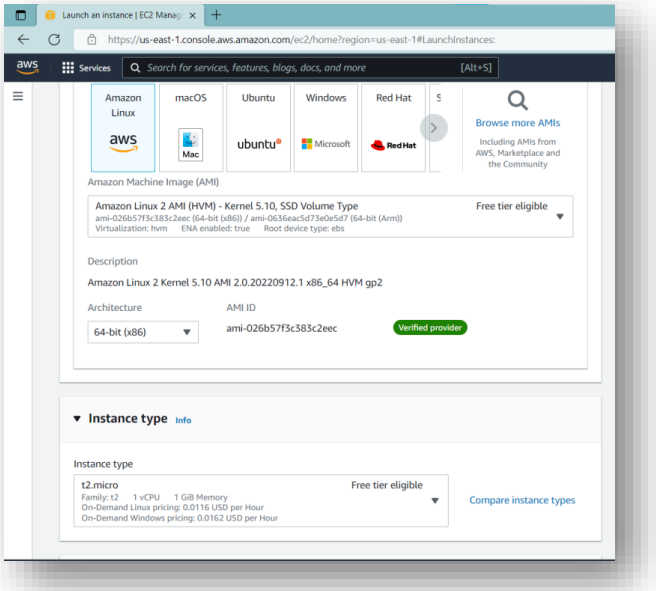
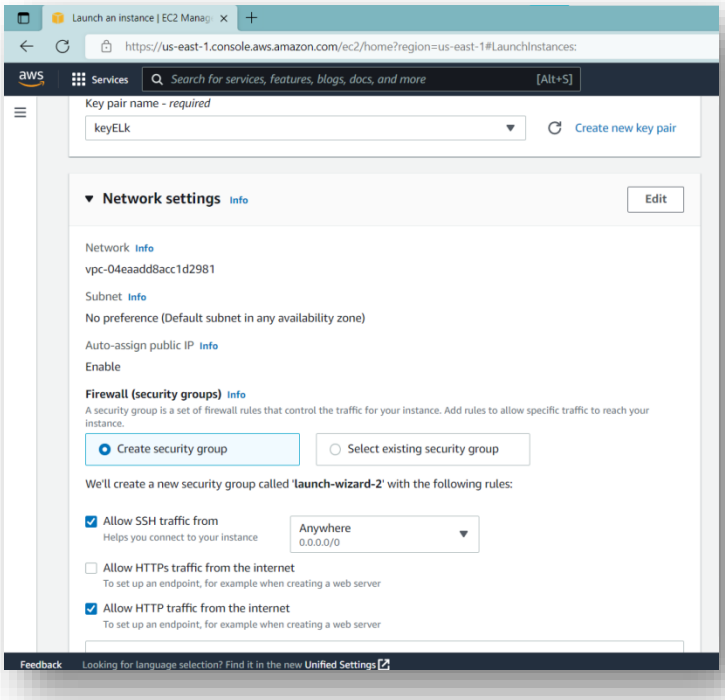
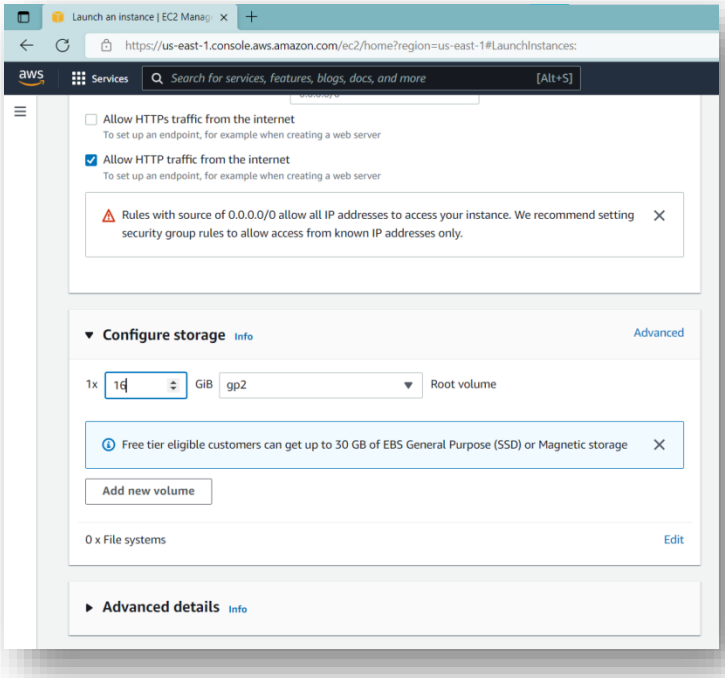
Deploying ELK Stack on Docker Container (Doc)

First we need to create an EC2- instance.

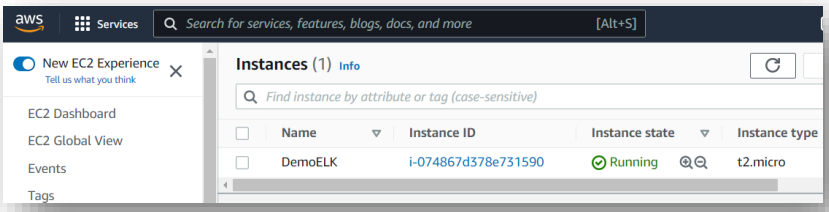


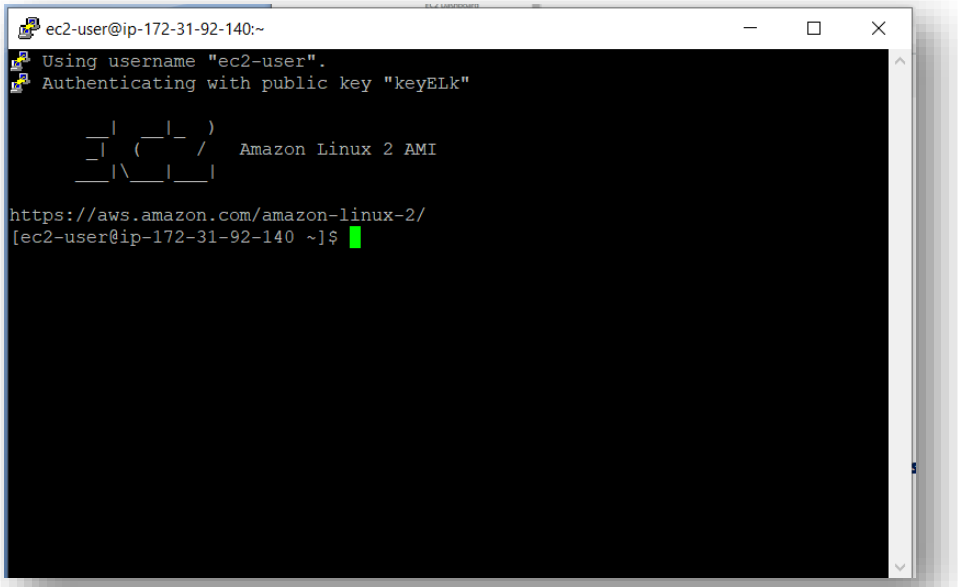



Launch an instance | EC2 Manag
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Key pair name - required
keyELk
Create new key pair
Network settings Info
Edit
Network Info
vpc-04eaadd8acc1d2981
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
Feedback
Looking for language selection? Find it in the new Unified Settings


Launch an instance | EC2 Manag
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
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

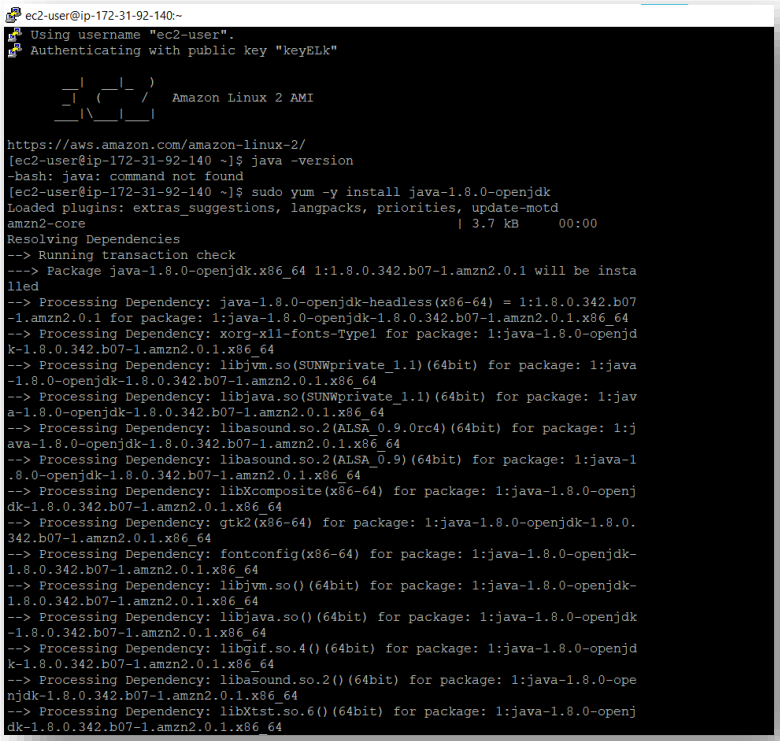
Now connect to the instance using putty

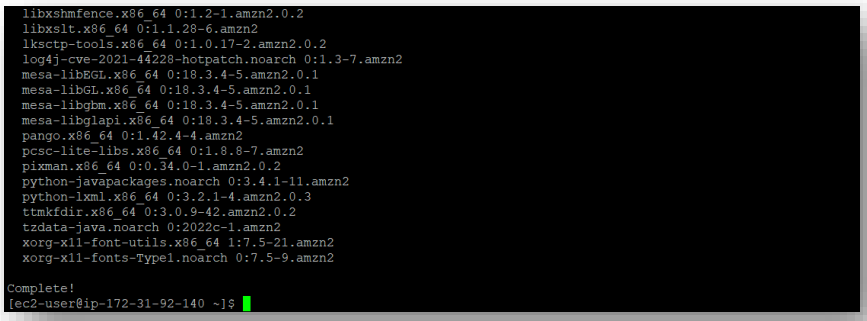


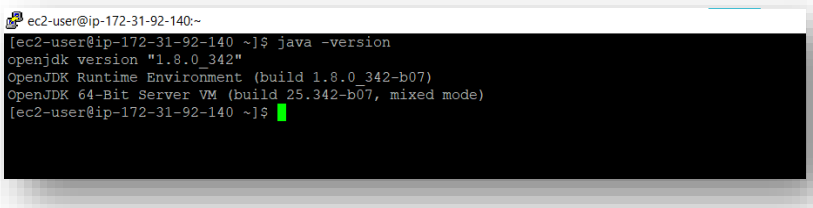


Now follow the following step

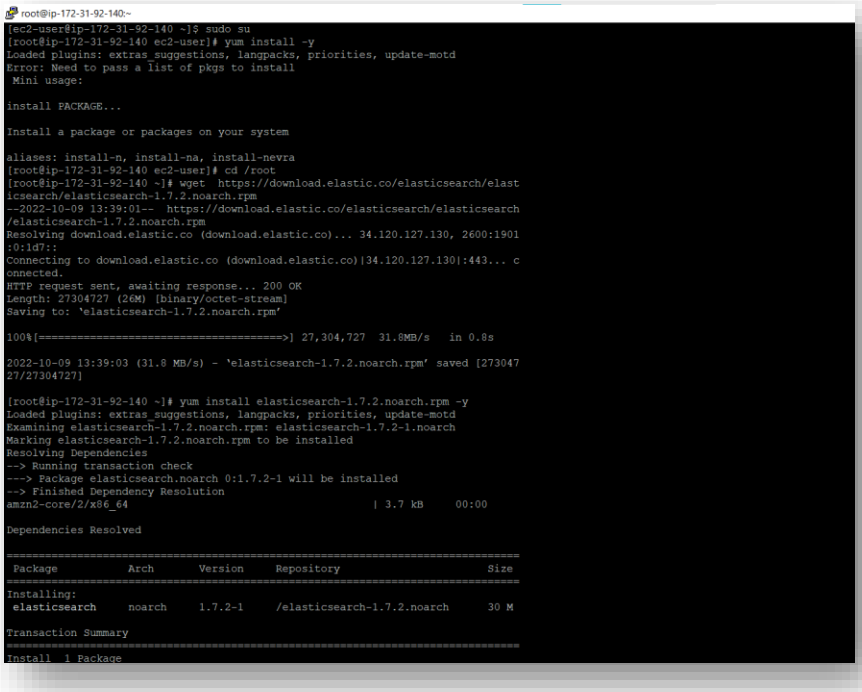
Step1: Install java and its Dependencies

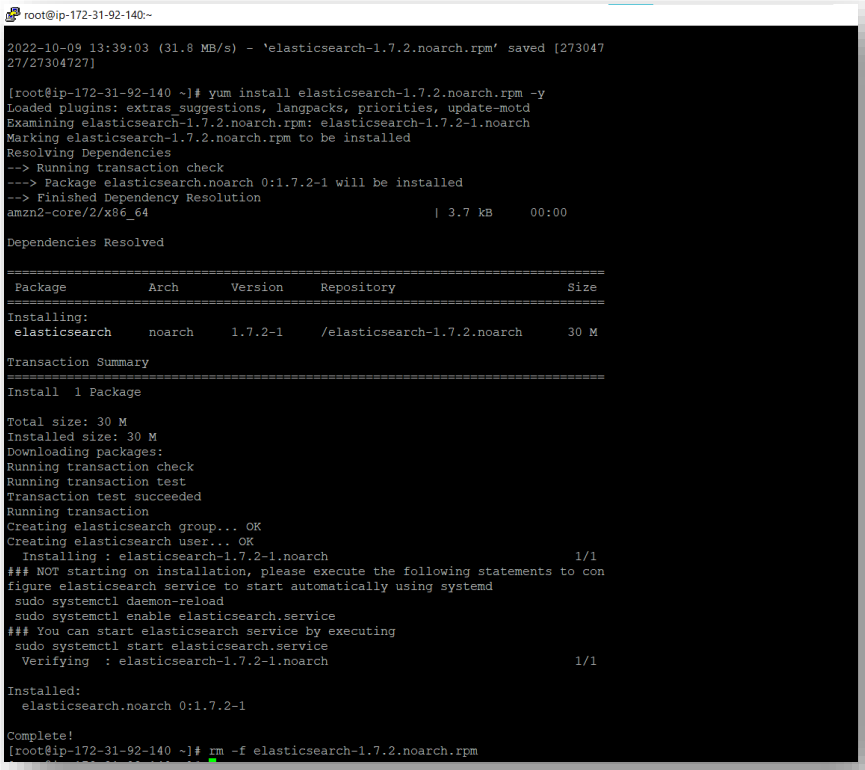




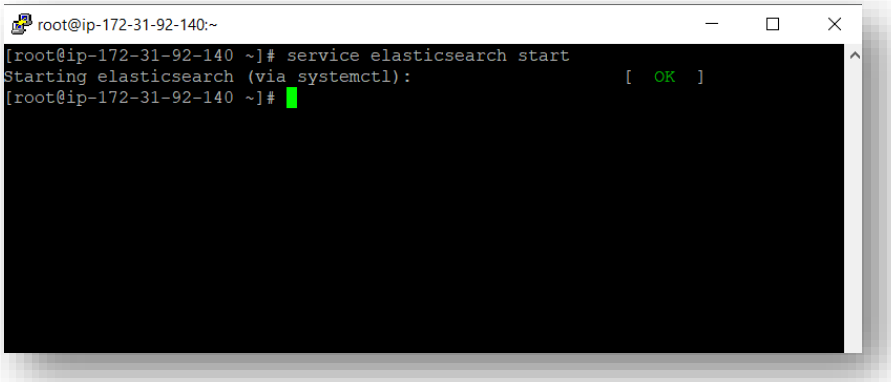


Step2: Install Elastic search on AWS Server

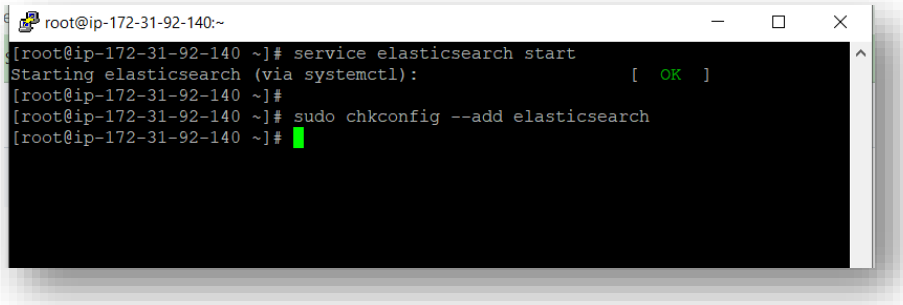




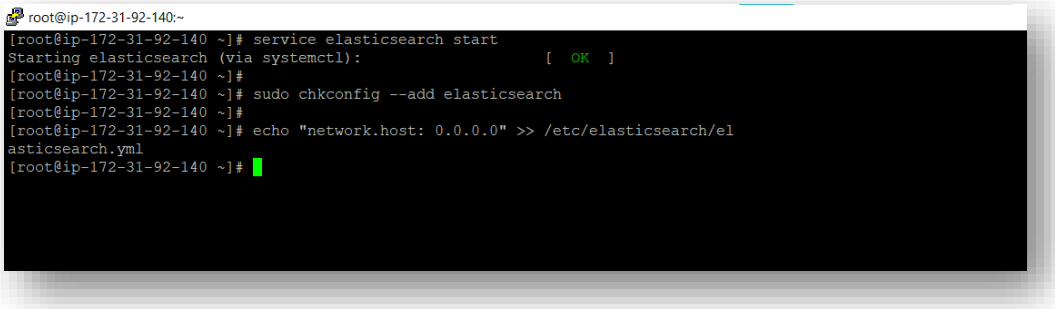
Step3: Start the Server



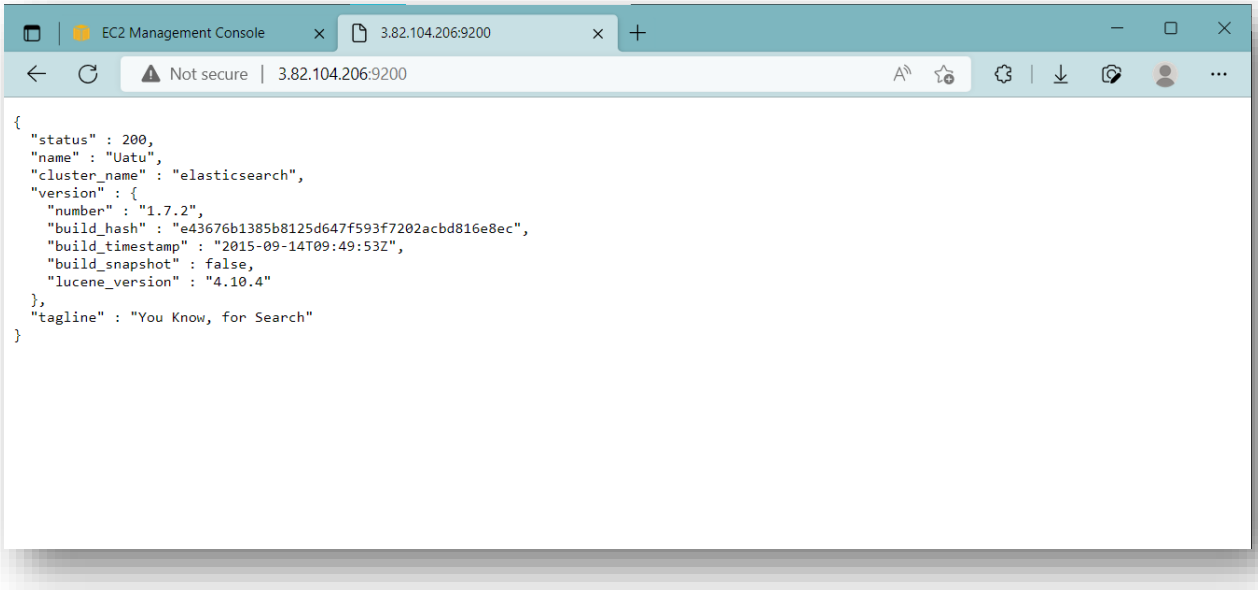
Step4: Automatically Boot u on start



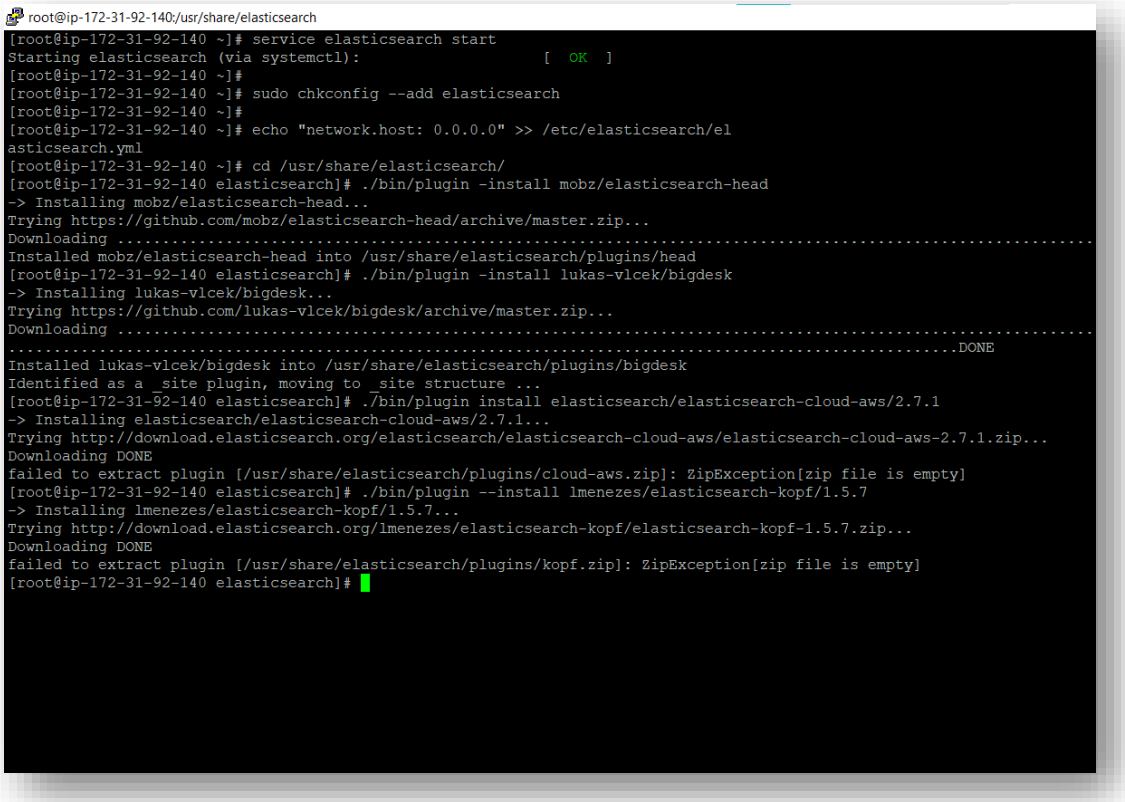
Step5:Configuring AWS IP so you can access using public IP



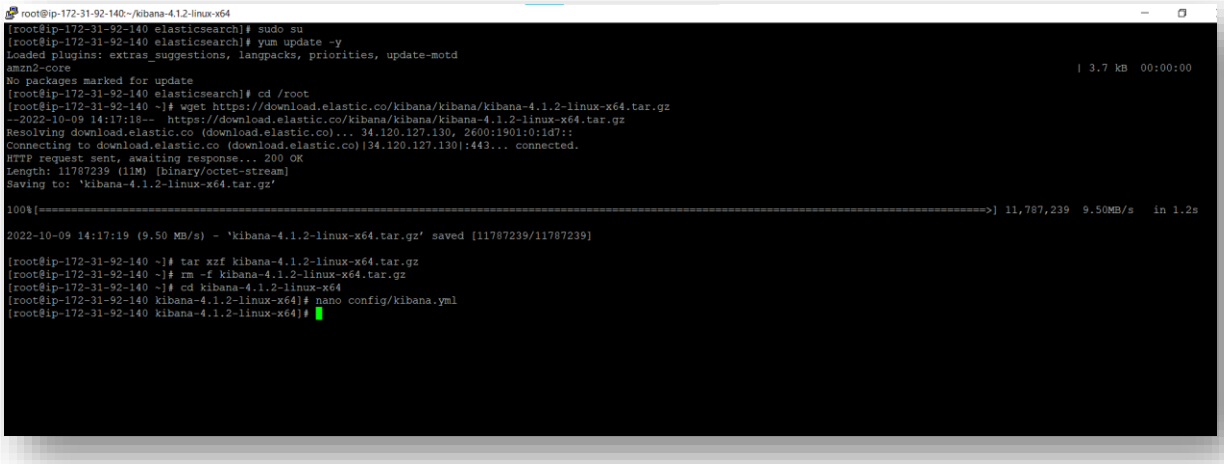
Checking Elastic Search

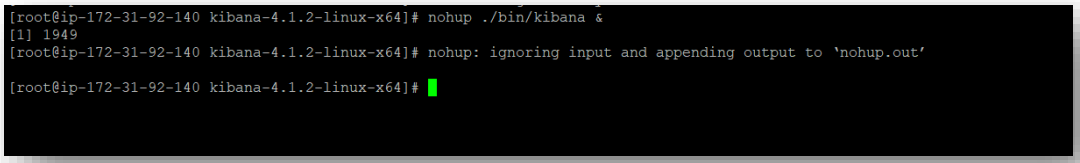


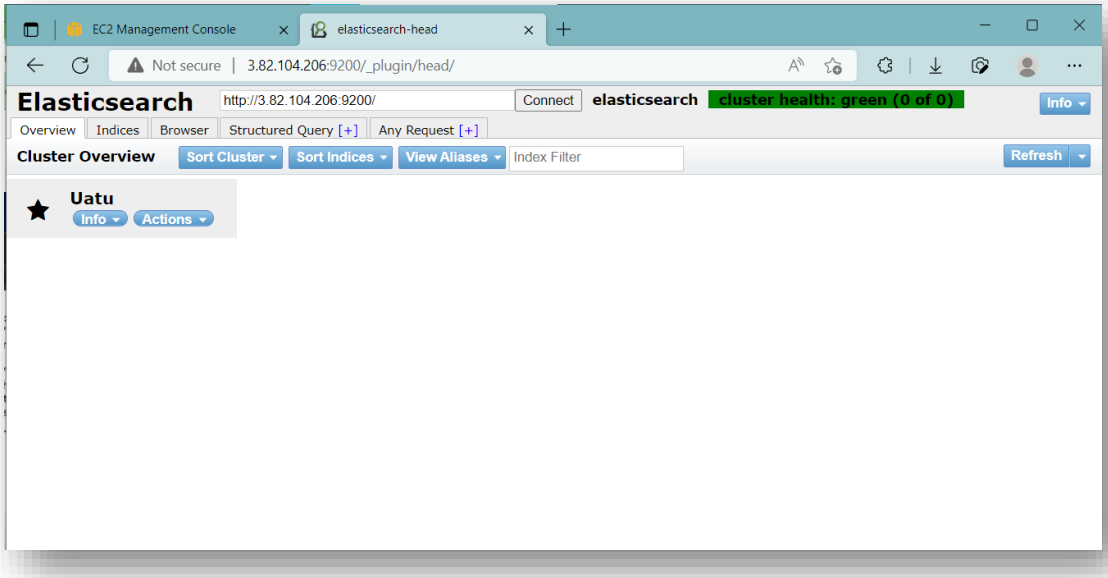
Step6:Install Plugins

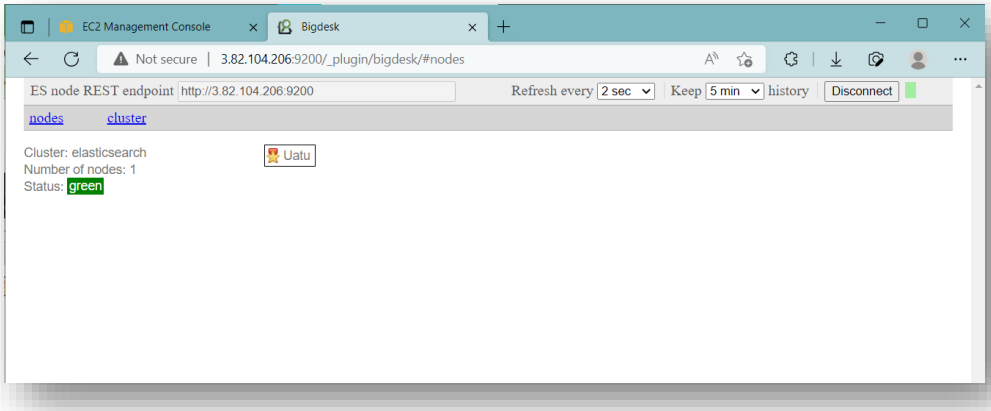


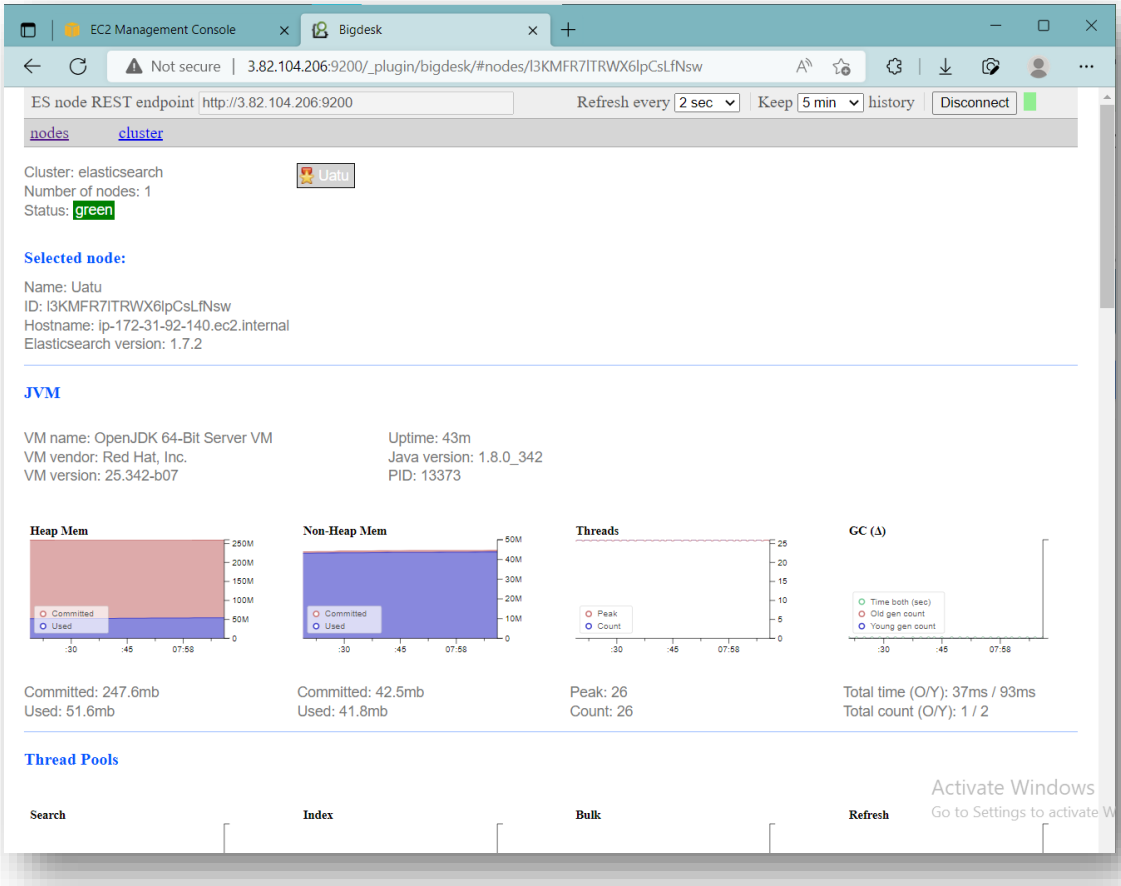
Step 7:Install Kibana

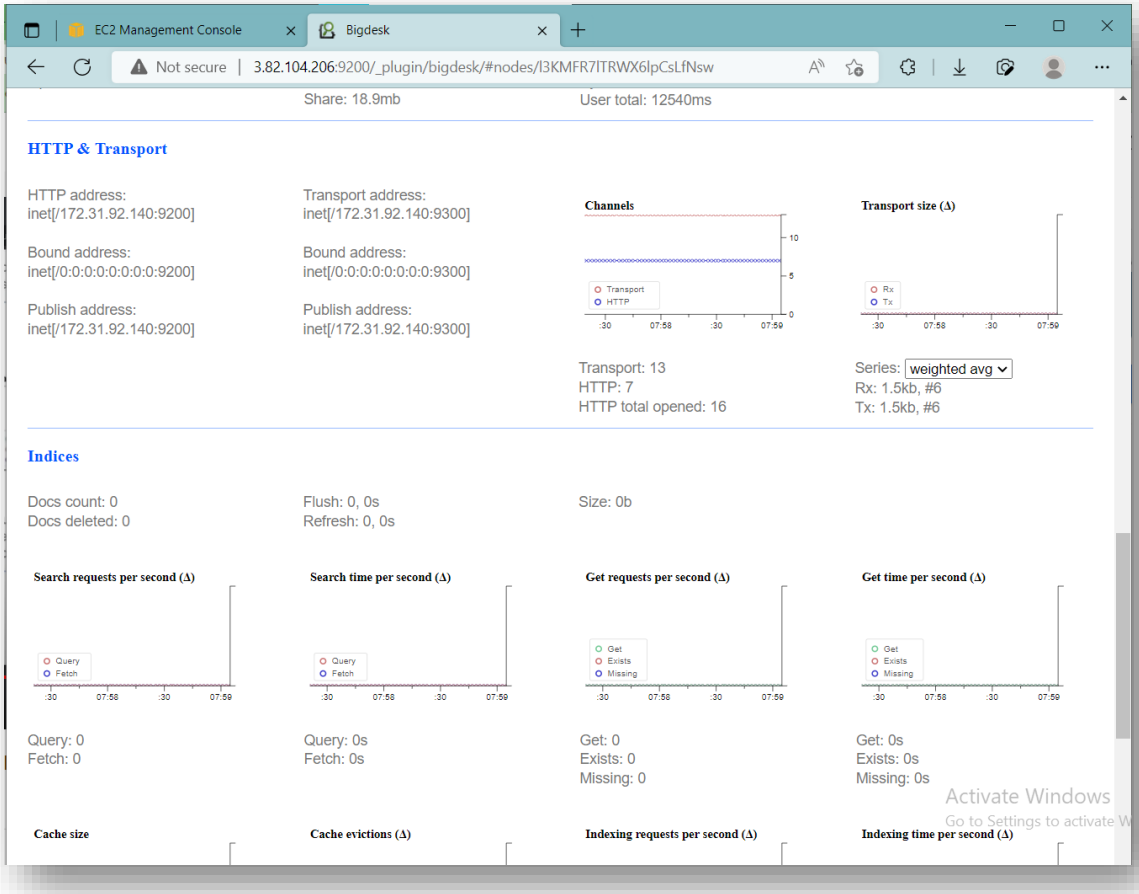







EC2 Management Console
Bigdesk
Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes
ES node REST endpoint http://3.82.104.206:9200
Refresh every 2 sec
Keep 5 min history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: green
Uatu


EC2 Management Console
Bigdesk
Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/l3KMFR7ITRWX6lpCsLfNsw
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: l3KMFR7ITRWX6lpCsLfNsw
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
Used
Committed: 247.6mb
Used: 51.6mb
Non-Heap Mem
Committed
Used
Committed: 42.5mb
Used: 41.8mb
Threads
Peak
Count
Peak: 26
Count: 26
GC (Δ)
Time both (sec)
Old gen count
Young gen count
Total time (O/Y): 37ms / 93ms
Total count (O/Y): 1 / 2
Thread Pools
Search
Index
Bulk
Refresh
Activate Windows
Go to Settings to activate W


EC2 Management Console
Bigdesk
Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/l3KMFR7lTRWX6lpCsLfNsw
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
HTTP
Transport size (Δ)
Rx
Tx
Transport: 13
HTTP: 7
HTTP total opened: 16
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
Fetch
Search time per second (Δ)
Get requests per second (Δ)
Get
Exists
Missing
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
Activate Windows
Cache size
Cache evictions (Δ)
Indexing requests per second (Δ)
Indexing time per second (Δ)