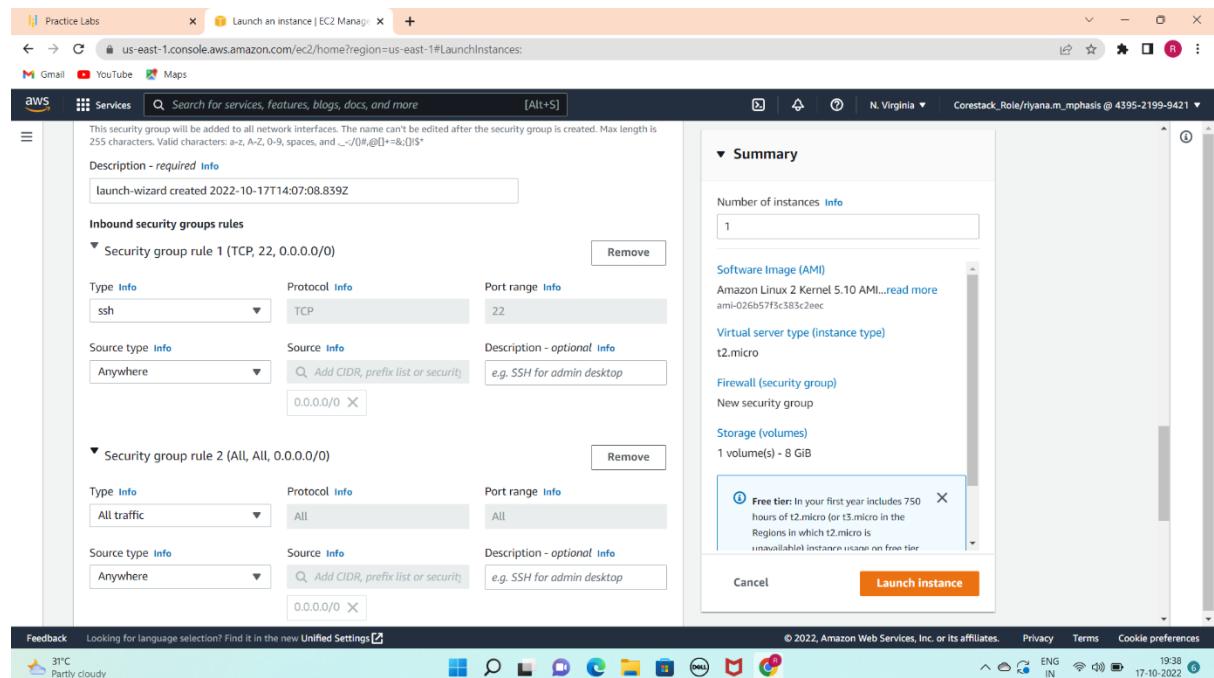
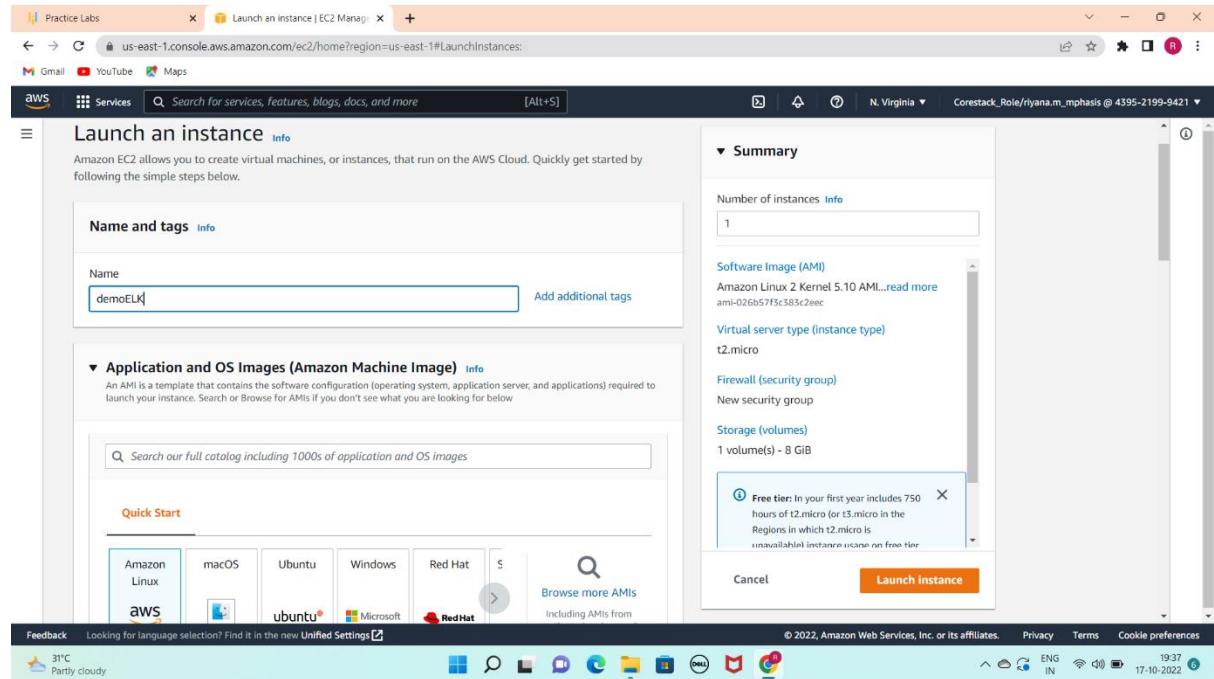


DEPLOYING ELK STACK ON DOCKER CONTAINER

Results:

1. Create ec2-instance



The screenshot shows the AWS Management Console with the EC2 Instances page open. On the left, there's a sidebar with various navigation options like EC2 Dashboard, EC2 Global View, Events, Tags, and Instances (which is currently selected). Under Instances, there are links for Instances New, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances New, Dedicated Hosts, Scheduled Instances, and Capacity Reservations. Below that is another section for Images (AMIs New, AMI Catalog). At the bottom of the sidebar is a Feedback link and a copyright notice for 2022. The main content area shows a table of instances with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. One row is selected, showing 'demoELK' with ID i-04ca543799307c2da, pending status, t2.micro type, and other details. A modal window titled 'Select an instance' is overlaid on the page, containing the same information about the selected instance. The bottom of the screen shows a Windows taskbar with icons for File Explorer, Task View, Start, and others, along with system status indicators like battery level and network connection.

2. Install java and its dependencies

The screenshot shows an EC2 Instance Connect session. The title bar says 'EC2 Instance Connect'. The main area is a terminal window showing the output of a 'sudo yum update' command on Amazon Linux 2 AMI. The output lists several packages being updated, including 'java-1.8.0-openjdk.x86_64' and various dependency packages like 'xorg-x11-fonts-type1', 'libjvm.so', and 'libasound.so.2'. The session title is 'EC2 Instance Connect' and the instance ID is 'i-04ca543799307c2da (demoELK)'. The bottom of the screen shows a Windows taskbar with icons for File Explorer, Task View, Start, and others, along with system status indicators like battery level and network connection.

```

[ec2-user@ip-172-31-27-55 ~]$ 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)
[ec2-user@ip-172-31-27-55 ~]$
```

i-04ca543799307c2da (demoELK)

PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55

3. Install elastic search on AWS server

```

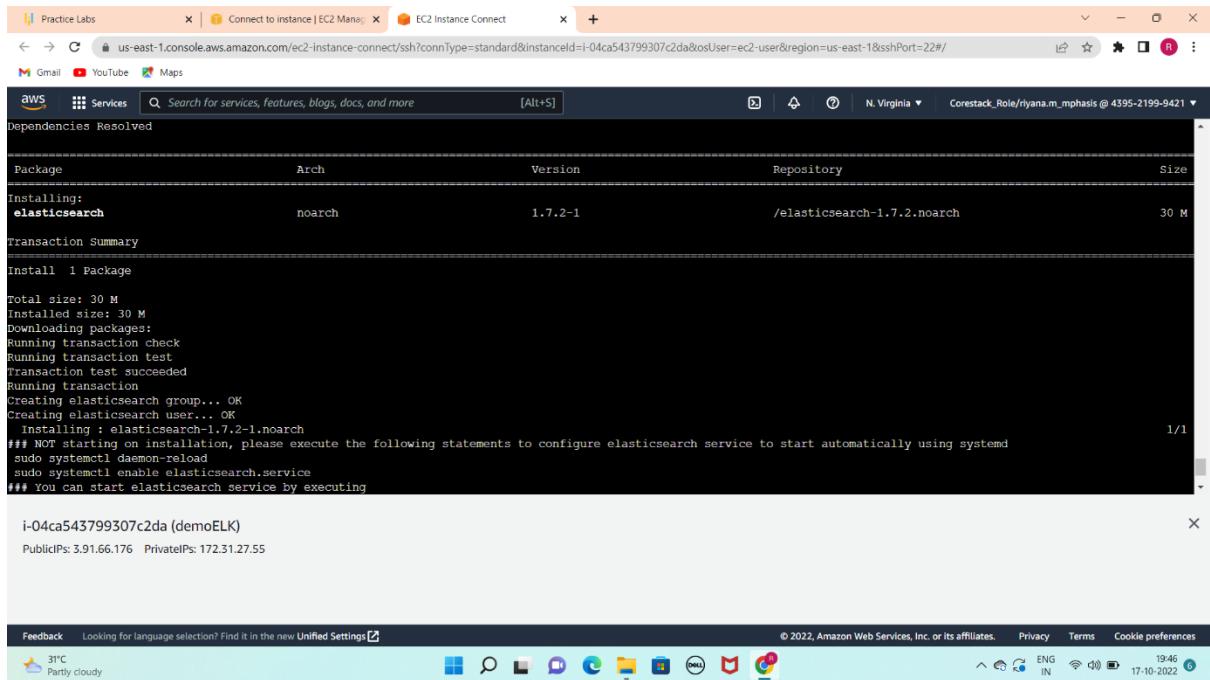
[ec2-user@ip-172-31-27-55 ~]$ sudo su
[root@ip-172-31-27-55 ec2-user]# yum install -y
Loaded plugins: extras suggestions, langpacks, priorities, update-motd
Error: Need to pass a list of pkgs to install
  Mini usage:
install PACKAGE...
Install a package or packages on your system
aliases: install-n, install-na, install-nevra
[root@ip-172-31-27-55 ec2-user]# cd /root
[root@ip-172-31-27-55 ~]# wget https://download.elastic.co/elasticsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-17 14:15:03-- https://download.elastic.co/elasticsearch/elasticsearch-1.7.2.noarch.rpm
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: 27304727 (26M) [binary/octet-stream]
Saving to: 'elasticsearch-1.7.2.noarch.rpm'

100% [=====] 27,304,727 32.9MB/s in 0.8s
2022-10-17 14:15:04 (32.9 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]

[root@ip-172-31-27-55 ~]# yum install elasticsearch-1.7.2.noarch.rpm -y
Loaded plugins: extras suggestions, langpacks, priorities, update-motd
```

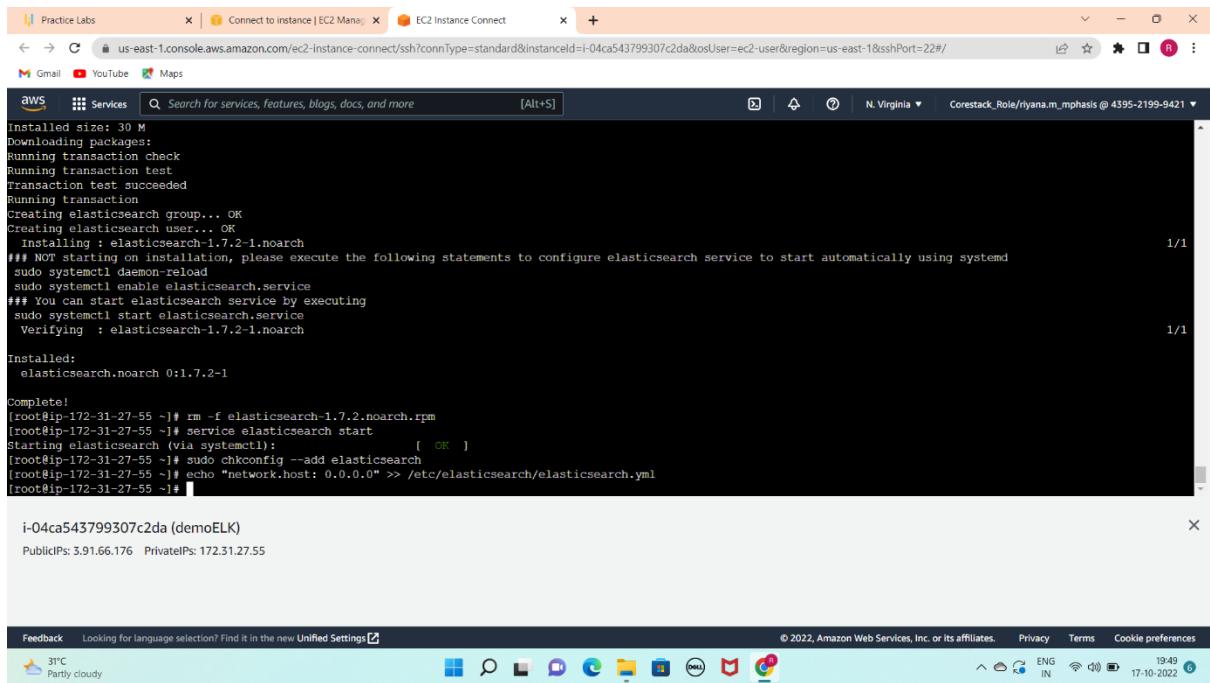
i-04ca543799307c2da (demoELK)

PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55



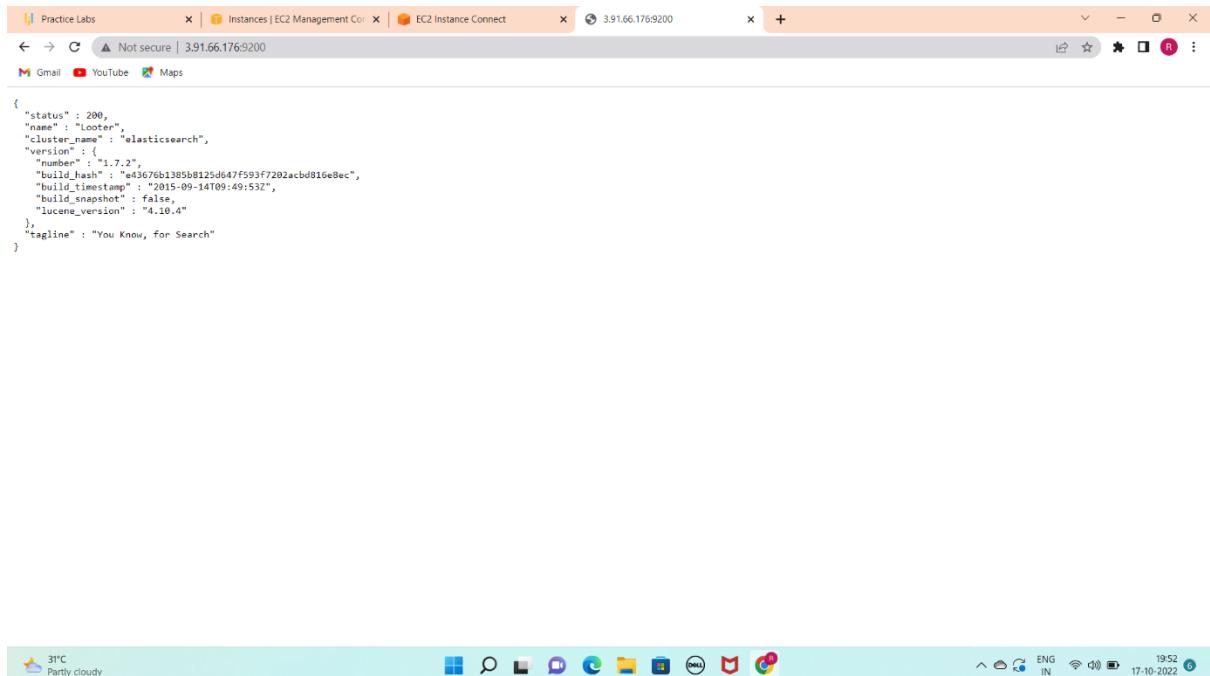
```
Practice Labs | Connect to instance | EC2 Manager | EC2 Instance Connect | + | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user&region=us-east-1&sshPort=22#/ | 🔍 | ⌛ | 🌐 | N. Virginia | Corestack_Role/ryana.m_mphasis @ 4395-2199-9421 | Gmail | YouTube | Maps | AWS Services | Search for services, features, blogs, docs, and more [Alt+S] | 🔍 | ⌛ | 🌐 | N. Virginia | Corestack_Role/ryana.m_mphasis @ 4395-2199-9421 | 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 | 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 | *** 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 | 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 | Party cloudy | ENG | IN | 19:46 | 17-10-2022 |
```

4. Start the server and configuring AWS ip



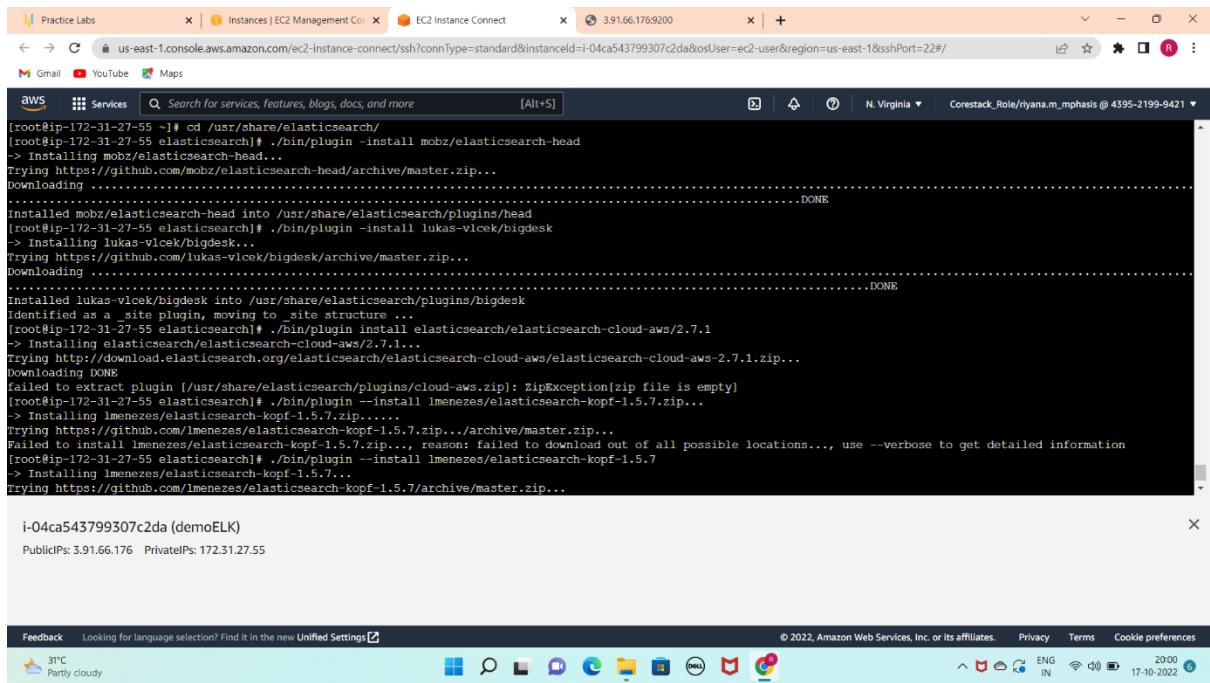
```
Practice Labs | Connect to instance | EC2 Manager | EC2 Instance Connect | + | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user&region=us-east-1&sshPort=22#/ | 🔍 | ⌛ | 🌐 | N. Virginia | Corestack_Role/ryana.m_mphasis @ 4395-2199-9421 | Gmail | YouTube | Maps | AWS Services | Search for services, features, blogs, docs, and more [Alt+S] | 🔍 | ⌛ | 🌐 | N. Virginia | Corestack_Role/ryana.m_mphasis @ 4395-2199-9421 | 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 | *** 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-172-31-27-55 ~]# rm -f elasticsearch-1.7.2.noarch.rpm | [root@ip-172-31-27-55 ~]# service elasticsearch start | Starting elasticsearch (via systemctl): | [OK] | [root@ip-172-31-27-55 ~]# sudo chkconfig --add elasticsearch | [root@ip-172-31-27-55 ~]# echo "network.host: 0.0.0.0" > /etc/elasticsearch/elasticsearch.yml | [root@ip-172-31-27-55 ~]# | 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 | Party cloudy | ENG | IN | 19:49 | 17-10-2022 |
```

5. Checking elastic search



```
{  
    "status": 200,  
    "name": "Locoter",  
    "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"  
}
```

6. Install plugins



```
[root@ip-172-31-27-55 ~]# cd /usr/share/elasticsearch/  
[root@ip-172-31-27-55 elasticsearch]# ./bin/plugin --install mobz/elasticsearch-head  
-> Installing mobz/elasticsearch-head...  
Trying https://github.com/mobz/elasticsearch-head/archive/master.zip...  
downloading .....  
installed mobz/elasticsearch-head into /usr/share/elasticsearch/plugins/head  
[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 .....  
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...  
  
i-04ca543799307c2da (demoELK)  
Public IPs: 3.91.66.176 Private IPs: 172.31.27.55
```

Practice Labs | Instances | EC2 Management Con | EC2 Instance Connect | 391.66.176.9200 | +

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user®ion=us-east-1&sshPort=22#/

Gmail YouTube Maps

aws Services Search for services, features, blogs, docs, and more [Alt+S]

```
[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 ...
Installed lukas-vlcek/bigdesk into /usr/share/elasticsearch/plugins/bigdesk
Identified as _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 ...
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...
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 ...
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 Party cloudy ENG IN 2000 17-10-2022

Practice Labs | Instances | EC2 Management Con | EC2 Instance Connect | 391.66.176.9200 | +

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-04ca543799307c2da&osUser=ec2-user®ion=us-east-1&sshPort=22#/

Gmail YouTube Maps

aws Services Search for services, features, blogs, docs, and more [Alt+S]

```
[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
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 Party cloudy ENG IN 2001 17-10-2022

```

| Practice Labs | Instances | EC2 Management Con | EC2 Instance Connect | 391.66.176.9200 | + |
← → C 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#/ EC2 Instance Connect
M Gmail YouTube Maps
aws Services Search for services, features, blogs, docs, and more [Alt+S]
cleanup : libxml2-2.9.1-6.amzn2.5.5.x86_64
cleanup : zlib-1.2.7-19.amzn2.0.1.x86_64
cleanup : initscripts-9.49.47-1.amzn2.0.2.x86_64
Verifying : libxml2-python-2.9.1-6.amzn2.5.6.x86_64
Verifying : kpatch-runtime-0.9.4-6.amzn2.noarch
Verifying : libxml2-2.9.1-6.amzn2.5.6.x86_64
verifying : tzdata-2022d-1.amzn2.0.1.noarch
Verifying : kernel-5.10.144-127.601.amzn2.x86_64
Verifying : initscripts-9.49.47-1.amzn2.0.3.x86_64
Verifying : zlib-1.2.7-19.amzn2.0.2.x86_64
Verifying : libxml2-2.9.1-6.amzn2.5.5.x86_64
Verifying : kpatch-runtime-0.9.4-3.amzn2.noarch
Verifying : initscripts-9.49.47-1.amzn2.0.2.x86_64
Verifying : tzdata-2022c-1.amzn2.noarch

Installed:
  kernel.x86_64 0:5.10.144-127.601.amzn2

Updated:
  initscripts.x86_64 0:9.49.47-1.amzn2.0.3      kpatch-runtime.noarch 0:0.9.4-6.amzn2.5.6      libxml2.x86_64 0:2.9.1-6.amzn2.5.6      libxml2-python.x86_64 0:2.9.1-6.amzn2.5.6
  tzdata.noarch 0:2022d-1.amzn2.0.1      zlib.x86_64 0:1.2.7-19.amzn2.0.2

Complete!
[root@ip-172-31-27-55 elasticsearch]# 

```

i-04ca543799307c2da (demoELK)
PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55

7. Kibana installation

```

| Practice Labs | Instances | EC2 Management Con | EC2 Instance Connect | 391.66.176.9200 | + |
← → C 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#/ EC2 Instance Connect
M Gmail YouTube Maps
aws Services Search for services, features, blogs, docs, and more [Alt+S]
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

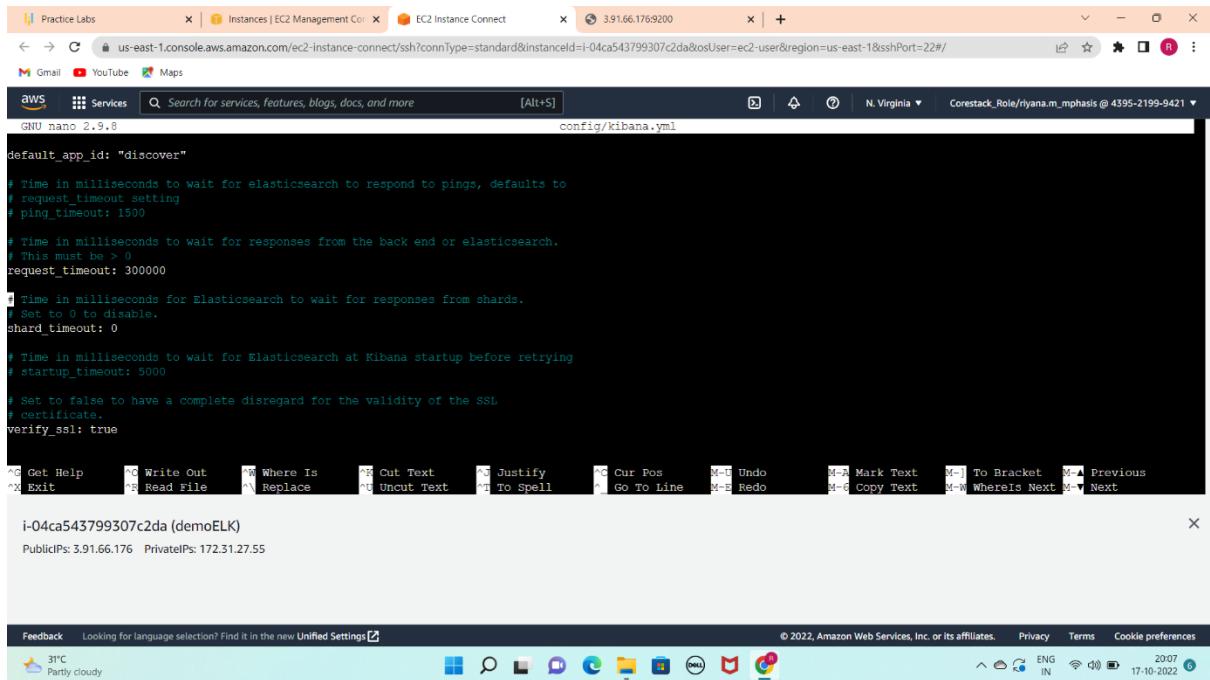
# Kibana uses an index in Elasticsearch to store saved searches, visualizations
# and dashboards. It will create a new index if it doesn't already exist.
kibana_index: ".kibana"

# If your Elasticsearch is protected with basic auth, this is the user credentials
# used by the Kibana server to perform maintenance on the kibana_index at startup. Your Kibana
# users will still need to authenticate with Elasticsearch (which is proxied through
# the Kibana server)
^G Get Help ^C Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-B Mark Text M-] To Bracket
^X Exit ^R Read File ^V Replace ^U Uncut Text ^I To Spell ^A Go To Line M-U Redo M-D Copy Text M-W Whereis Next M-V 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 Party cloudy ENG IN 2001 17-10-2022 6



```
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

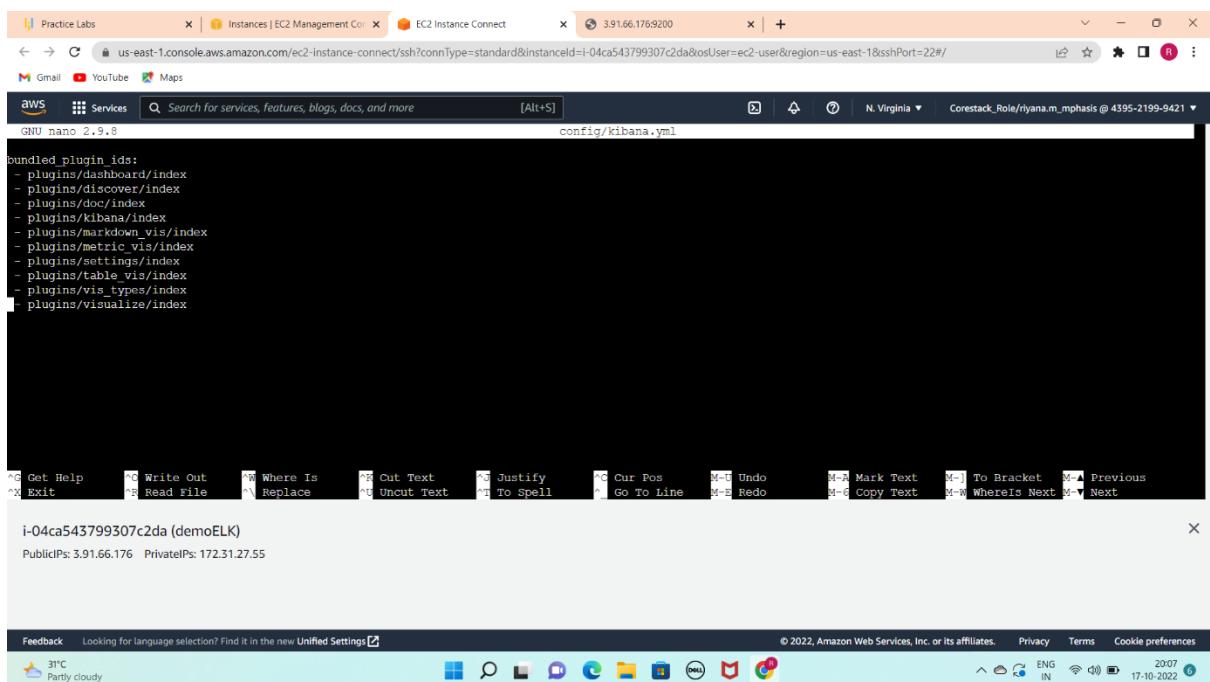
# Time in milliseconds to wait for responses from the back end or elasticsearch.
# This must be > 0
request_timeout: 300000

# Time in milliseconds for Elasticsearch to wait for responses from shards.
# Set to 0 to disable.
shard_timeout: 0

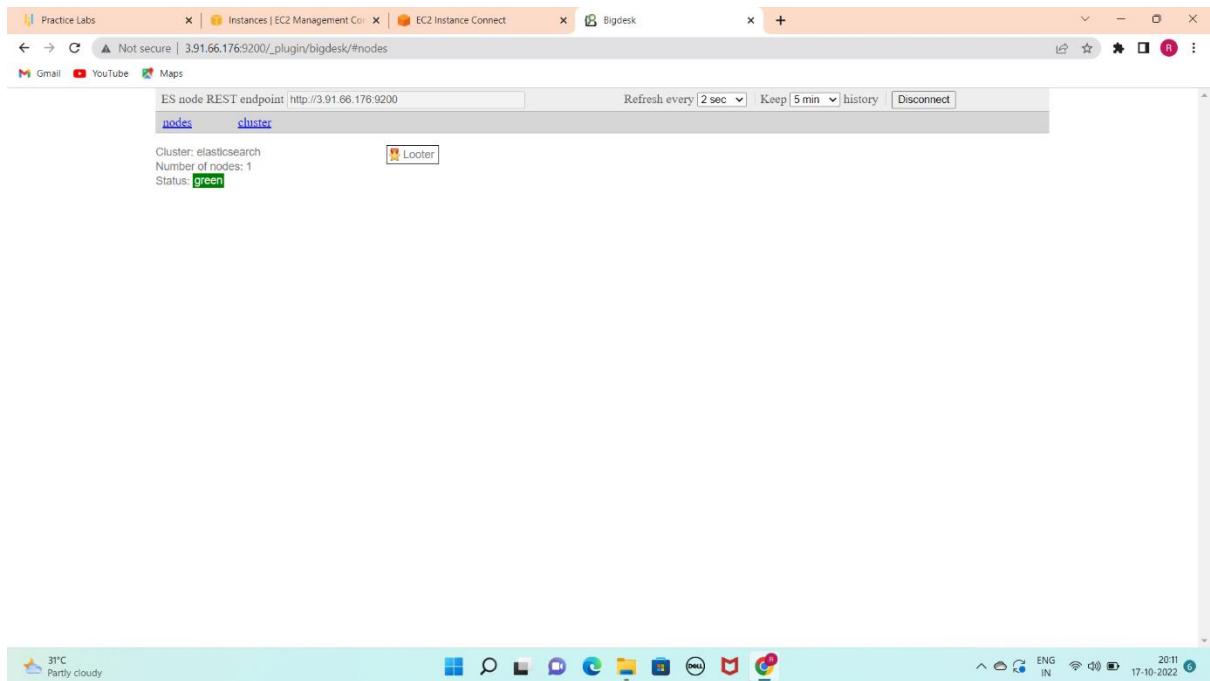
# Time in milliseconds to wait for Elasticsearch at Kibana startup before retrying
# startup_timeout: 5000

# Set to false to have a complete disregard for the validity of the SSL
# certificate.
verify_ssl: true

i-04ca543799307c2da (demoELK)
PublicIPs: 3.91.66.176 PrivateIPs: 172.31.27.55
```



```
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
```



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

ES node REST endpoint: http://3.91.66.176:9200/_plugin/bigdesk/#nodes/f1f6WaAPwToO1cxUbVneOyw

Refresh every: 2 sec | Keep: 5 min | history | Disconnect

nodes **cluster**

Cluster: elasticsearch
Number of nodes: 1
Status: green

Selected node:
Name: Looter
ID: f1f6WaAPwToO1cxUbVneOyw
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: 247.6mb
Used: 47.2mb

Non-Heap Mem
Committed: 41.4mb
Used: 41.4mb

Threads
Peak: 26
Count: 26

GC (Δ)
Total time (O/Y): 32ms / 89ms
Total count (O/Y): 1 / 2

Thread Pools

Search Index Bulk Refresh

31°C Party cloudy

20:11 17-10-2022

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

ES node REST endpoint: http://3.91.66.176:9200/_plugin/bigdesk/#nodes/f1f6WaAPwToO1cxUbVneOyw

Refresh every: 2 sec | Keep: 5 min | history | Disconnect

nodes **cluster**

Used: 48mb
Used: 41.6mb
Count: 26
Total count (O/Y): 1 / 2

Thread Pools

Search Index Bulk Refresh

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 (2399 MHz)
CPU total logical cores: 1
CPU cache: 30kb

Uptime: 1.9s
Refresh interval: 1ms
Total mem: 965.7mb (1012666368 b)
Total swap: 0b (0 b)

CPU (%)
User: 0% Sys: 0%

Mem
Free: 622mb Used: 343.7mb

Swap
Free: 0b Used: 0b

Load Average
2: 0
1: 0.02
0: 0

31°C Party cloudy

20:11 17-10-2022

