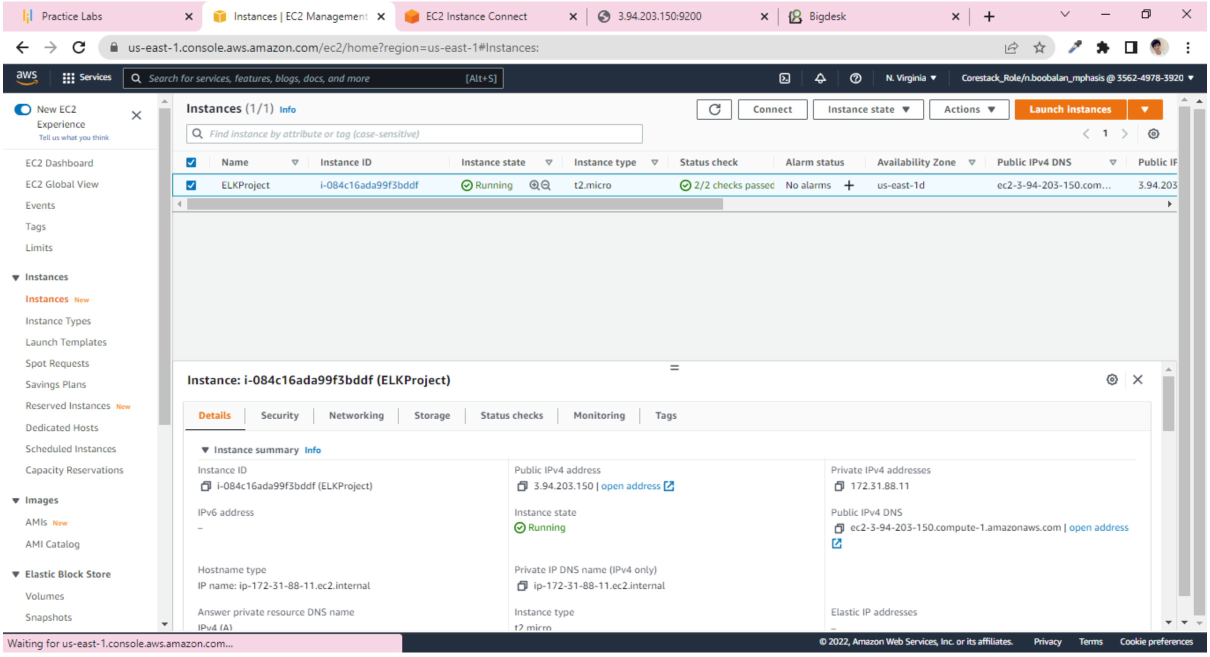
Deploying ELK Stack on Docker Container(Screenshots)

Screenshots:



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:

Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IF
☑	ELKProject	i-084c16ada99f3bddf	Running	t2.micro	2/2 checks passed	No alarms	us-east-1d	ec2-3-94-203-150.com...	3.94.203

Instance: i-084c16ada99f3bddf (ELKProject)

Instance summary Info

Instance ID
i-084c16ada99f3bddf (ELKProject)

Public IPv4 address
3.94.203.150 | open address

Private IPv4 addresses
172.31.88.11

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-3-94-203-150.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-172-31-88-11.ec2.internal

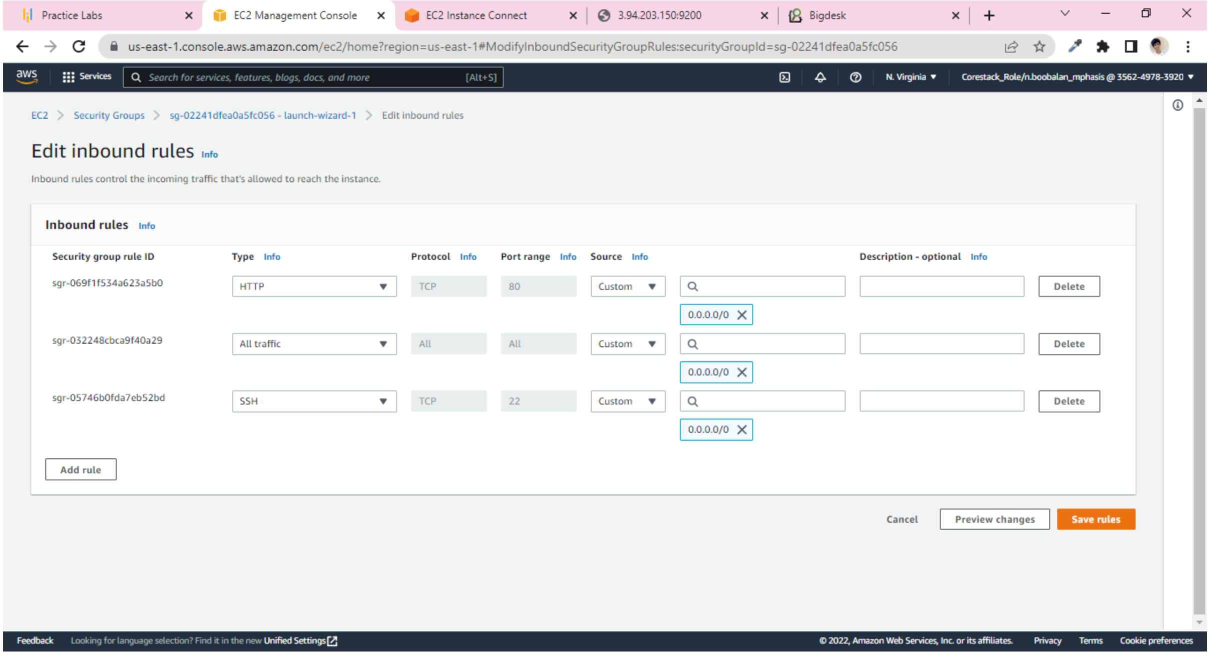
Private IP DNS name (IPv4 only)
ip-172-31-88-11.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

Elastic IP addresses
–

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


Practice Labs
EC2 Management Console
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920
EC2 > Security Groups > sg-02241dfea0a5fc056 - launch-wizard-1 > Edit inbound rules
Add rule
Cancel
Preview changes
Save rules
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/home?region=us-east-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-02241dfea0a5fc056

Edit inbound rules Info

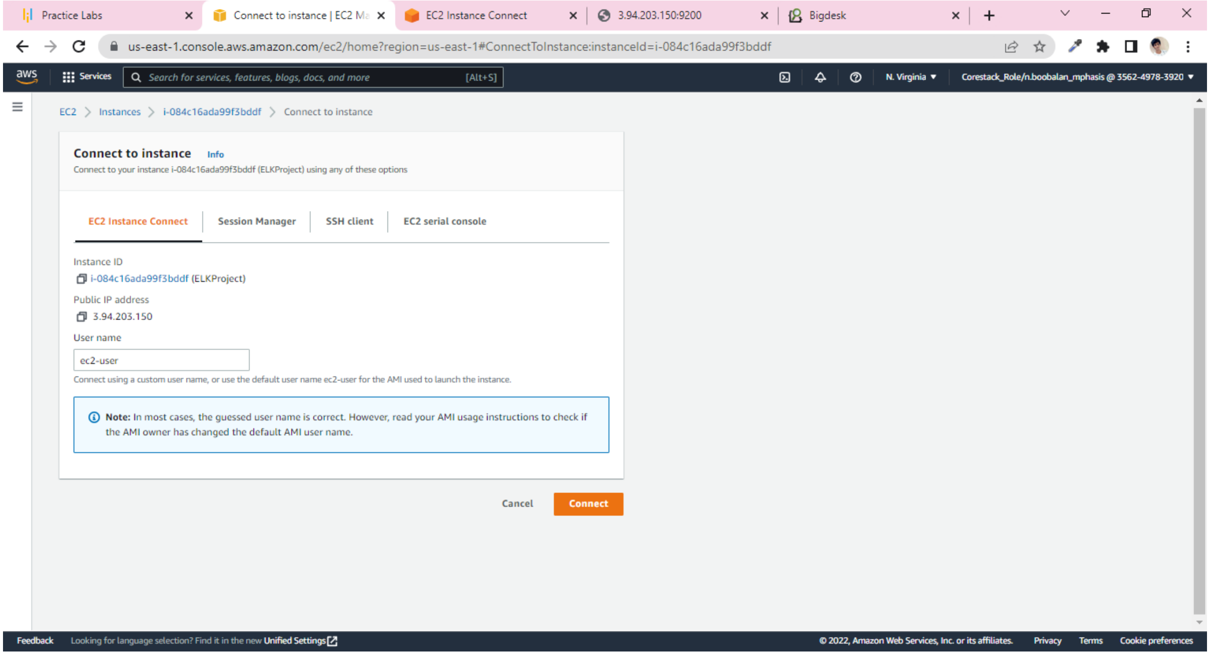
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-069f1f534a623a5b0	HTTP	TCP	80	Custom	0.0.0.0/0		Delete
sgr-032248cbca9f40a29	All traffic	All	All	Custom	0.0.0.0/0		Delete
sgr-05746b0fda7eb52bd	SSH	TCP	22	Custom	0.0.0.0/0		Delete

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

Deploying ELK Stack on Docker Container(Screenshots)



EC2 > Instances > i-084c16ada99f3bddf > Connect to instance

Connect to instance Info

Connect to your instance i-084c16ada99f3bddf (ELKProject) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-084c16ada99f3bddf (ELKProject)

Public IP address
3.94.203.150

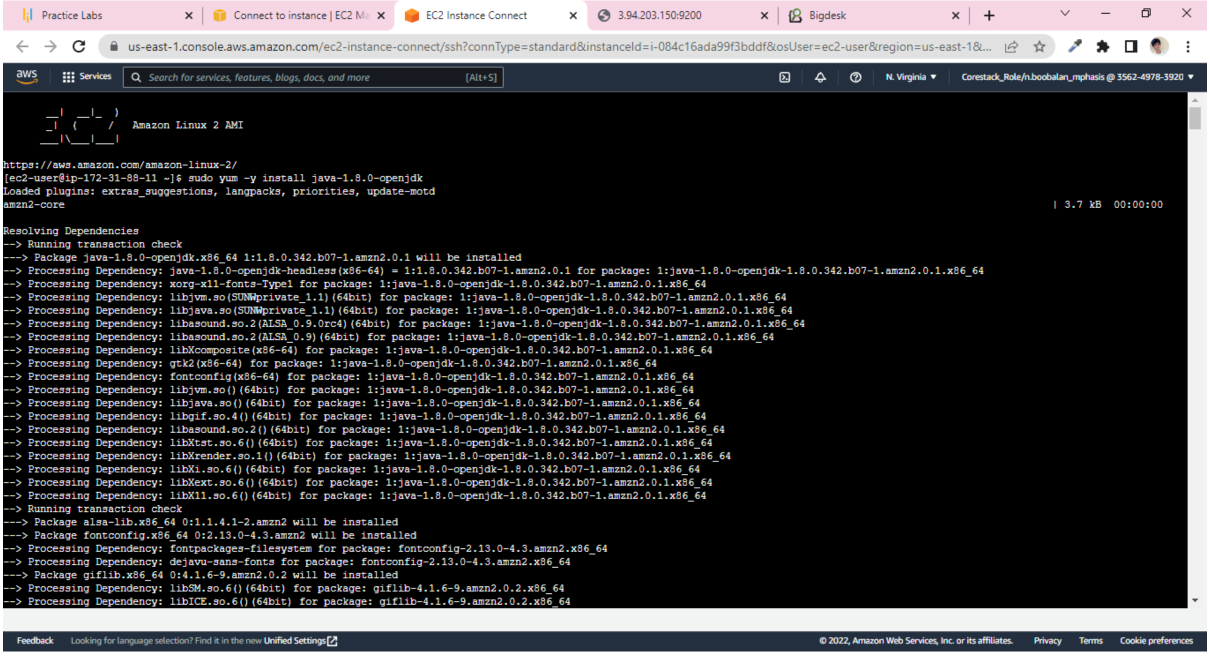
User name
ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel | Connect

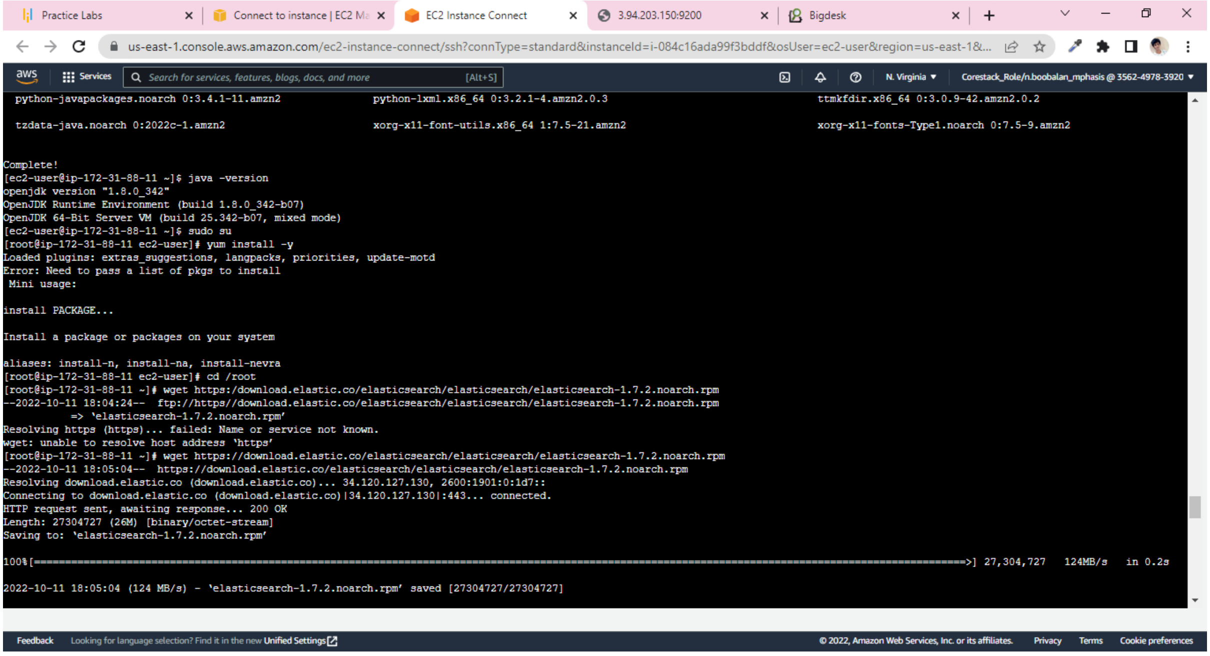
Select your instance->connect->to work on AWS terminal



```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-88-11 ~]$ sudo yum -y install java-1.8.0-openjdk
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                                                                    | 3.7 kB  00:00:00

Resolving Dependencies
--> Running transaction check
---> Package java-1.8.0-openjdk.x86_64 1:1.8.0.342.b07-1.amzn2.0.1 will be installed
--> Processing Dependency: java-1.8.0-openjdk-headless(x86-64) = 1:1.8.0.342.b07-1.amzn2.0.1 for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: xorg-x11-fonts-Type1 for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjvm.so(SUNWprivate_1.1)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjava.so(SUNWprivate_1.1)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libasound.so.2(ALSA_0.9.0rc4)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libasound.so.2(ALSA_0.9)(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXcomposite(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: gtk2(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: fontconfig(x86-64) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjvm.so()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libjava.so()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libgif.so.4()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libasound.so.2()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXtst.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXrender.so.1()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXi.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libXext.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Processing Dependency: libX11.so.6()(64bit) for package: 1:java-1.8.0-openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64
--> Running transaction check
---> Package alsa-lib.x86_64 0:1.1.4.1-2.amzn2 will be installed
---> Package fontconfig.x86_64 0:2.13.0-4.3.amzn2 will be installed
--> Processing Dependency: fontpackages-filesystem for package: fontconfig-2.13.0-4.3.amzn2.x86_64
--> Processing Dependency: dejavu-sans-fonts for package: fontconfig-2.13.0-4.3.amzn2.x86_64
---> Package giflib.x86_64 0:4.1.6-9.amzn2.0.2 will be installed
--> Processing Dependency: libSM.so.6()(64bit) for package: giflib-4.1.6-9.amzn2.0.2.x86_64
--> Processing Dependency: libICE.so.6()(64bit) for package: giflib-4.1.6-9.amzn2.0.2.x86_64
```

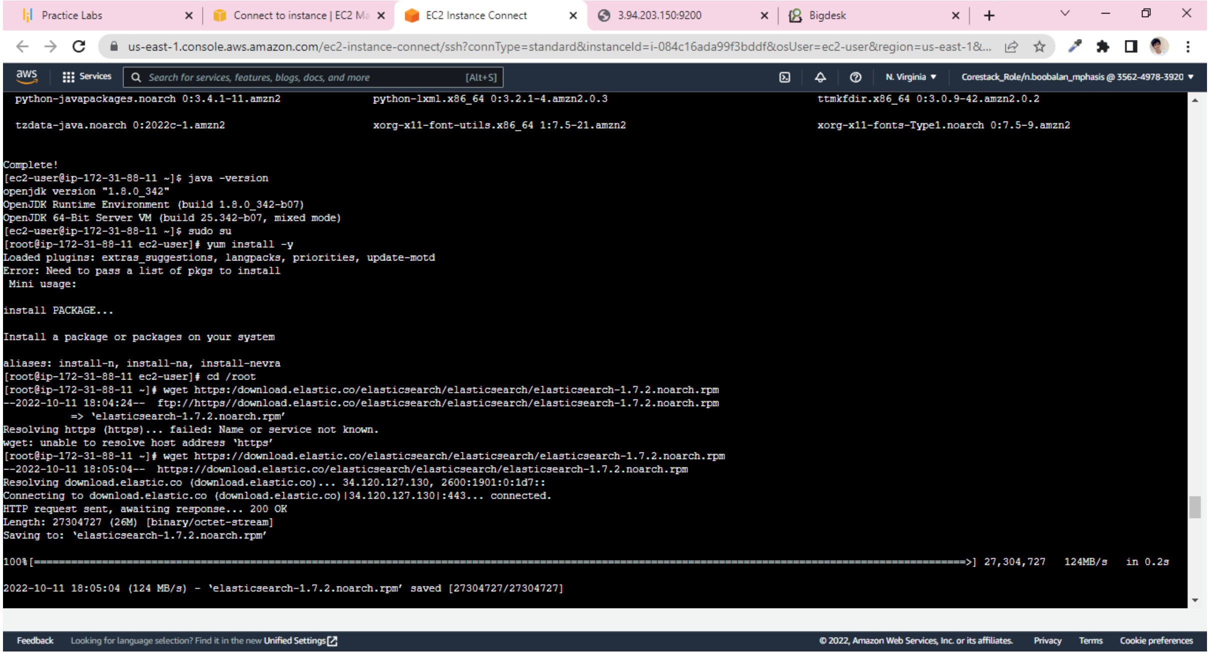
Check the java version , if there is no java version → just install it using “sudo yum -y install java”

Deploying ELK Stack on Docker Container(Screenshots)



```
  python-javapackages.noarch 0:3.4.1-11.amzn2              python-lxml.x86_64 0:3.2.1-4.amzn2.0.3                      ttmkfdir.x86_64 0:3.0.9-42.amzn2.0.2

  tzdata-java.noarch 0:2022c-1.amzn2                       xorg-x11-font-utils.x86_64 1:7.5-21.amzn2                   xorg-x11-fonts-Type1.noarch 0:7.5-9.amzn2


Complete!
[ec2-user@ip-172-31-88-11 ~]$ 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-172-31-88-11 ~]$ sudo su
[root@ip-172-31-88-11 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-172-31-88-11 ec2-user]# cd /root
[root@ip-172-31-88-11 ~]# wget https:/download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-11 18:04:24--  ftp://https//download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
           => 'elasticsearch-1.7.2.noarch.rpm'
Resolving https (https)... failed: Name or service not known.
wget: unable to resolve host address 'https'
[root@ip-172-31-88-11 ~]# wget https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-11 18:05:04--  https://download.elastic.co/elasticsearch/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   124MB/s   in 0.2s

2022-10-11 18:05:04 (124 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]
```

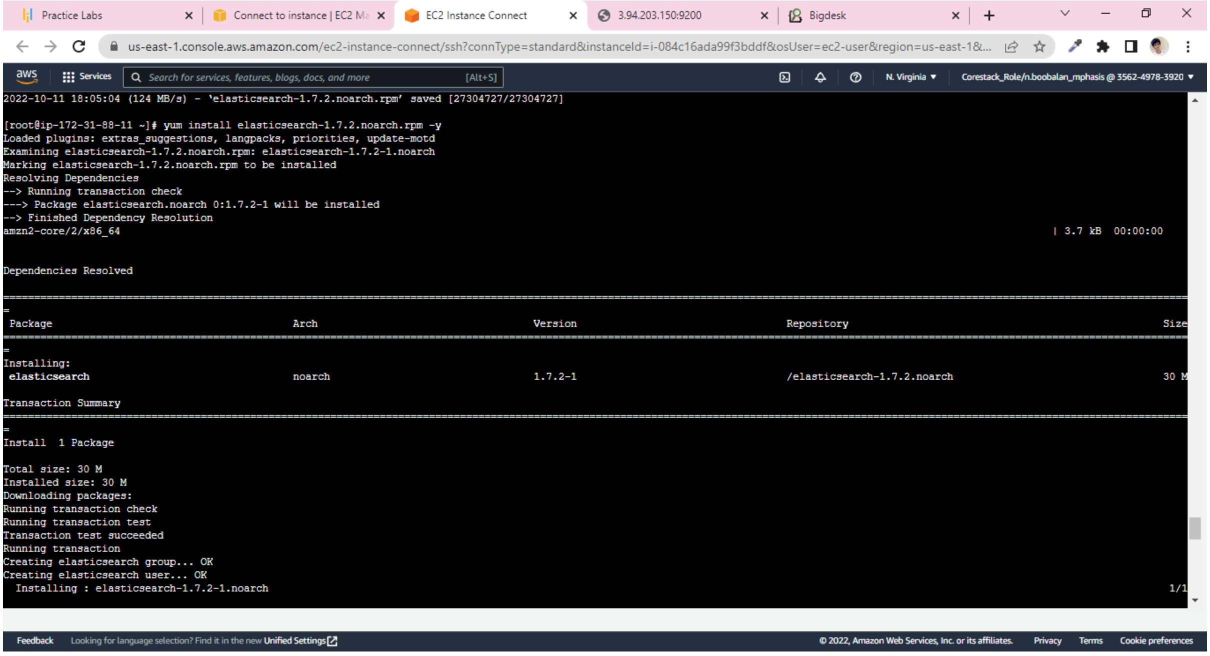
Check for java—version



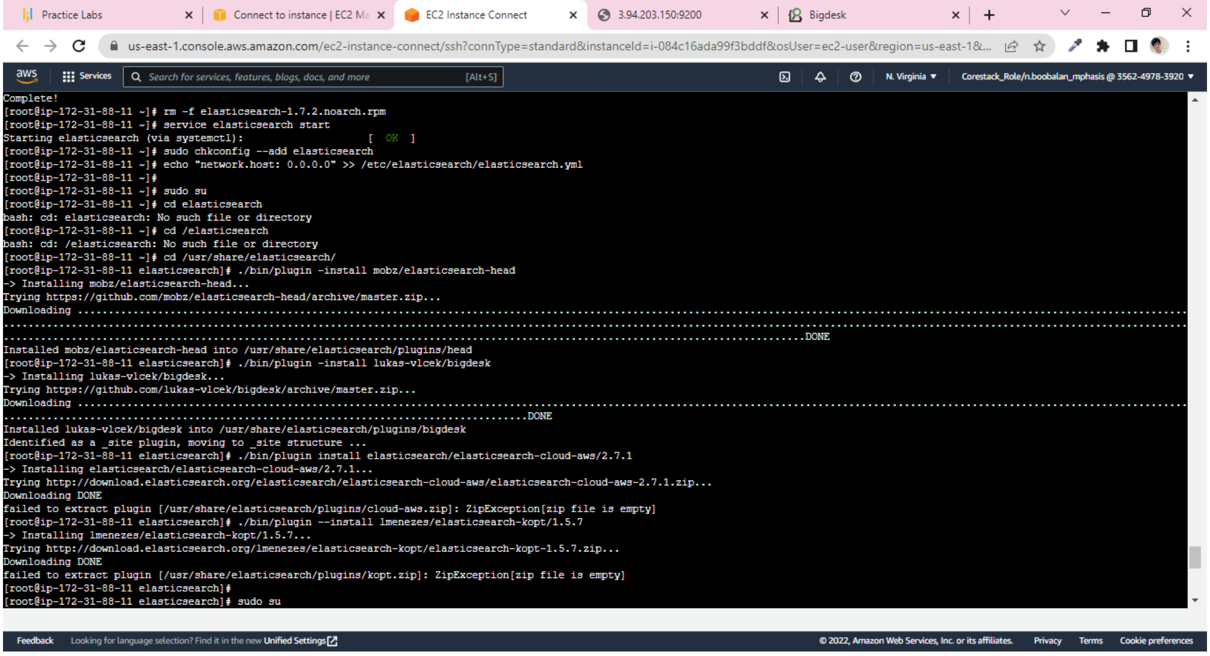
```
  python-javapackages.noarch 0:3.4.1-11.amzn2              python-lxml.x86_64 0:3.2.1-4.amzn2.0.3                      ttmkfdir.x86_64 0:3.0.9-42.amzn2.0.2

  tzdata-java.noarch 0:2022c-1.amzn2                       xorg-x11-font-utils.x86_64 1:7.5-21.amzn2                   xorg-x11-fonts-Type1.noarch 0:7.5-9.amzn2


Complete!
[ec2-user@ip-172-31-88-11 ~]$ 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-172-31-88-11 ~]$ sudo su
[root@ip-172-31-88-11 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-172-31-88-11 ec2-user]# cd /root
[root@ip-172-31-88-11 ~]# wget https:/download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-11 18:04:24--  ftp://https//download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
           => 'elasticsearch-1.7.2.noarch.rpm'
Resolving https (https)... failed: Name or service not known.
wget: unable to resolve host address 'https'
[root@ip-172-31-88-11 ~]# wget https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-11 18:05:04--  https://download.elastic.co/elasticsearch/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   124MB/s   in 0.2s

2022-10-11 18:05:04 (124 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]
```

Install Elastic Stack on AWS Server

Deploying ELK Stack on Docker Container(Screenshots)

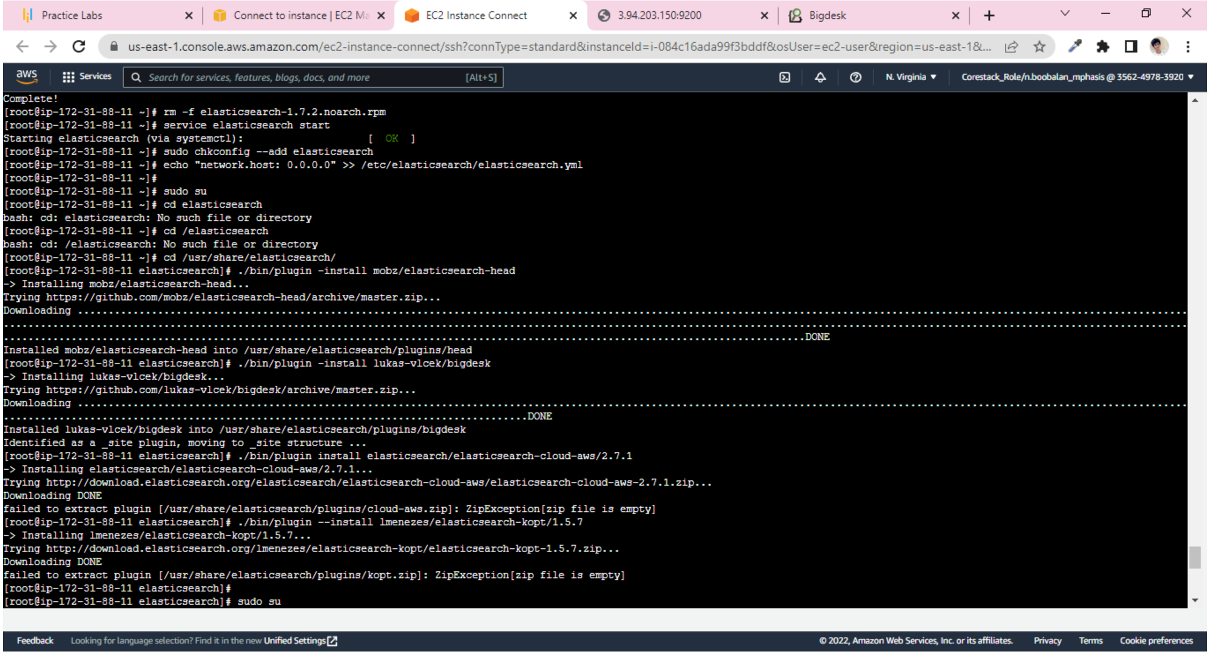

Practice Labs
Connect to instance | EC2 Ma
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

```
2022-10-11 18:05:04 (124 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]

[root@ip-172-31-88-11 ~]# 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
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
```


Practice Labs
Connect to instance | EC2 Ma
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

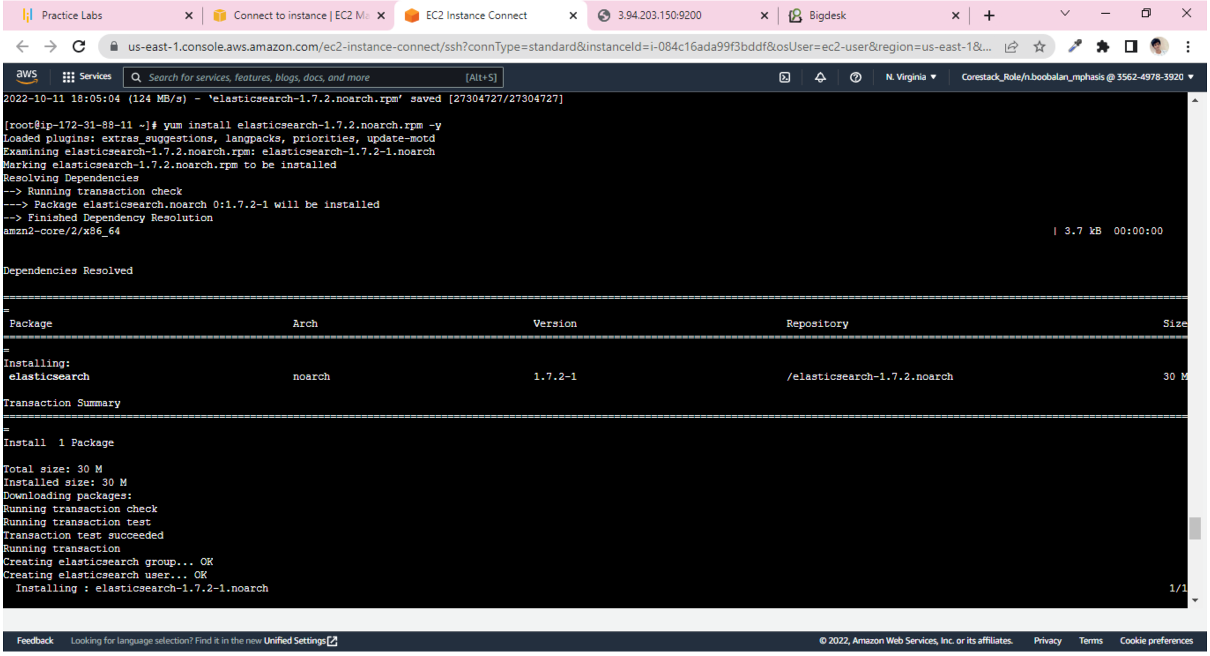
```
Complete!
[root@ip-172-31-88-11 ~]# rm -f elasticsearch-1.7.2.noarch.rpm
[root@ip-172-31-88-11 ~]# service elasticsearch start
Starting elasticsearch (via systemctl):                    [  OK  ]
[root@ip-172-31-88-11 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-88-11 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-88-11 ~]#
[root@ip-172-31-88-11 ~]# sudo su
[root@ip-172-31-88-11 ~]# cd elasticsearch
bash: cd: elasticsearch: No such file or directory
[root@ip-172-31-88-11 ~]# cd /elasticsearch
bash: cd: /elasticsearch: No such file or directory
[root@ip-172-31-88-11 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-88-11 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-172-31-88-11 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-172-31-88-11 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-172-31-88-11 elasticsearch]# ./bin/plugin --install lmenezes/elasticsearch-kopt/1.5.7
-> Installing lmenezes/elasticsearch-kopt/1.5.7...
Trying http://download.elasticsearch.org/lmenezes/elasticsearch-kopt/elasticsearch-kopt-1.5.7.zip...
Downloading DONE
failed to extract plugin [/usr/share/elasticsearch/plugins/kopt.zip]: ZipException[zip file is empty]
[root@ip-172-31-88-11 elasticsearch]#
[root@ip-172-31-88-11 elasticsearch]# sudo su
```

Deploying ELK Stack on Docker Container(Screenshots)


Practice Labs
Connect to instance | EC2 Ma
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

```
Complete!
[root@ip-172-31-88-11 ~]# rm -f elasticsearch-1.7.2.noarch.rpm
[root@ip-172-31-88-11 ~]# service elasticsearch start
Starting elasticsearch (via systemctl):                    [  OK  ]
[root@ip-172-31-88-11 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-88-11 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-88-11 ~]#
[root@ip-172-31-88-11 ~]# sudo su
[root@ip-172-31-88-11 ~]# cd elasticsearch
bash: cd: elasticsearch: No such file or directory
[root@ip-172-31-88-11 ~]# cd /elasticsearch
bash: cd: /elasticsearch: No such file or directory
[root@ip-172-31-88-11 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-88-11 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-172-31-88-11 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-172-31-88-11 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-172-31-88-11 elasticsearch]# ./bin/plugin --install lmenezes/elasticsearch-kopt/1.5.7
-> Installing lmenezes/elasticsearch-kopt/1.5.7...
Trying http://download.elasticsearch.org/lmenezes/elasticsearch-kopt/elasticsearch-kopt-1.5.7.zip...
Downloading DONE
failed to extract plugin [/usr/share/elasticsearch/plugins/kopt.zip]: ZipException[zip file is empty]
[root@ip-172-31-88-11 elasticsearch]#
[root@ip-172-31-88-11 elasticsearch]# sudo su
```

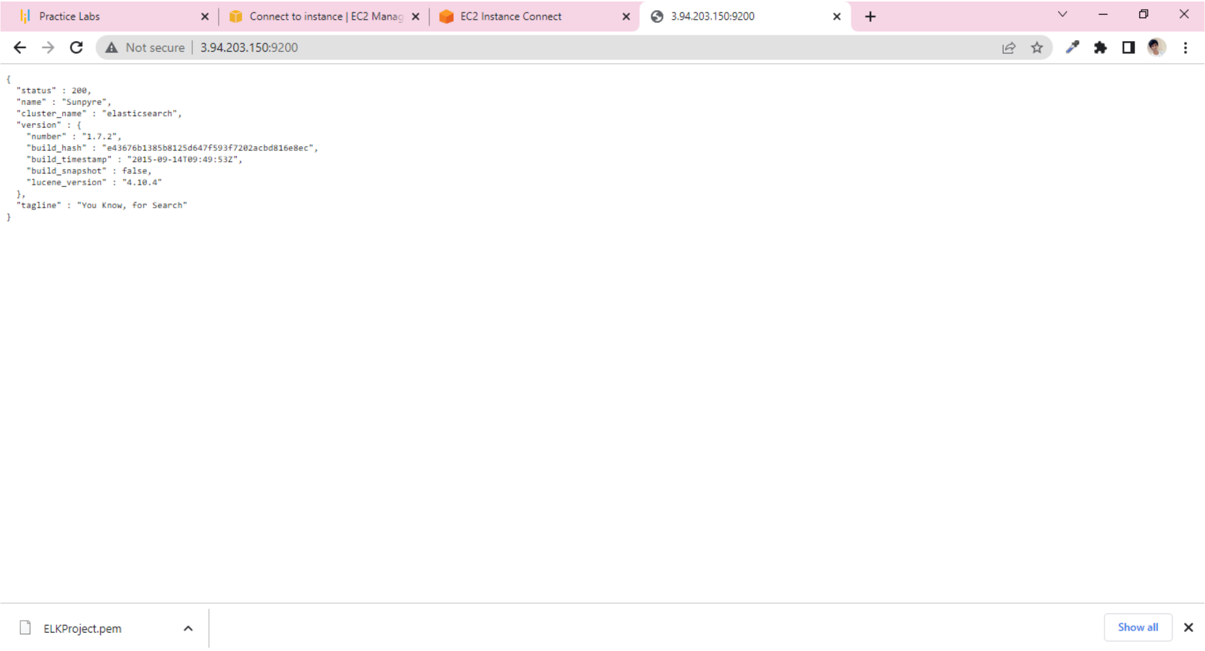
After Installation Start the Server


Practice Labs
Connect to instance | EC2 Ma
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

```
2022-10-11 18:05:04 (124 MB/s) - ‘elasticsearch-1.7.2.noarch.rpm’ saved [27304727/27304727]

[root@ip-172-31-88-11 ~]# 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
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
```

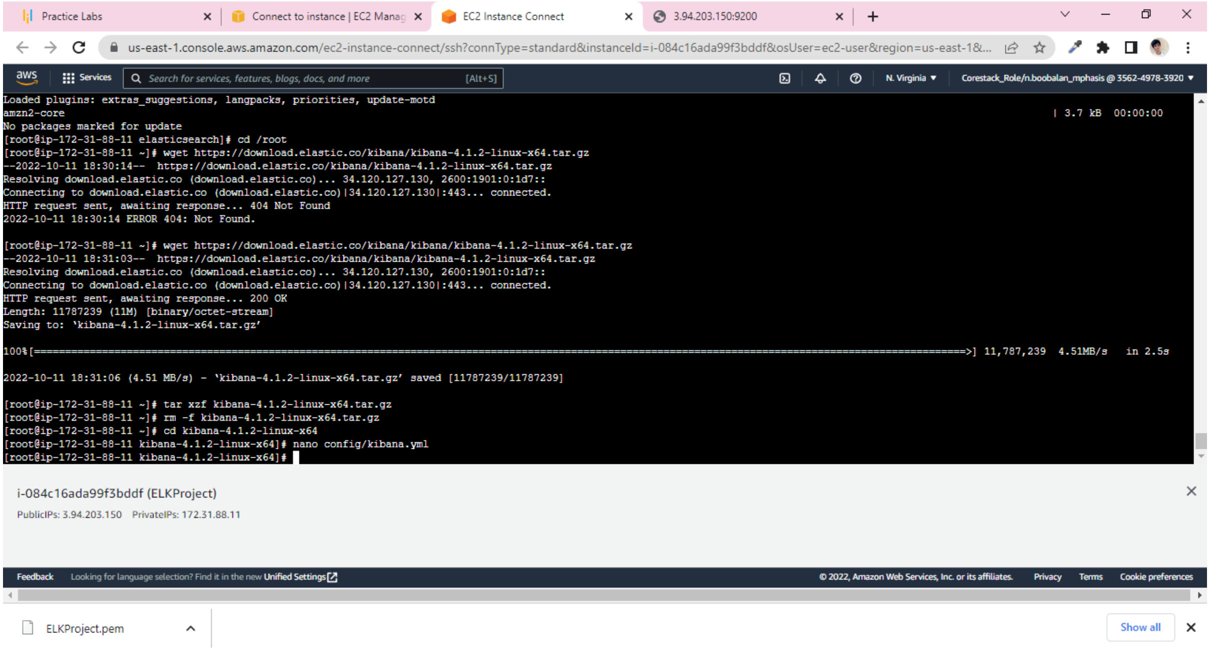
It Automatically Boot on you to start and configure Aws IP so you an access using your public IP

Deploying ELK Stack on Docker Container(Screenshots)



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

Checking Elastic Search:


Practice Labs
Connect to instance | EC2 Manag
EC2 Instance Connect
3.94.203.150:9200
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ELKProject.pem
Show all

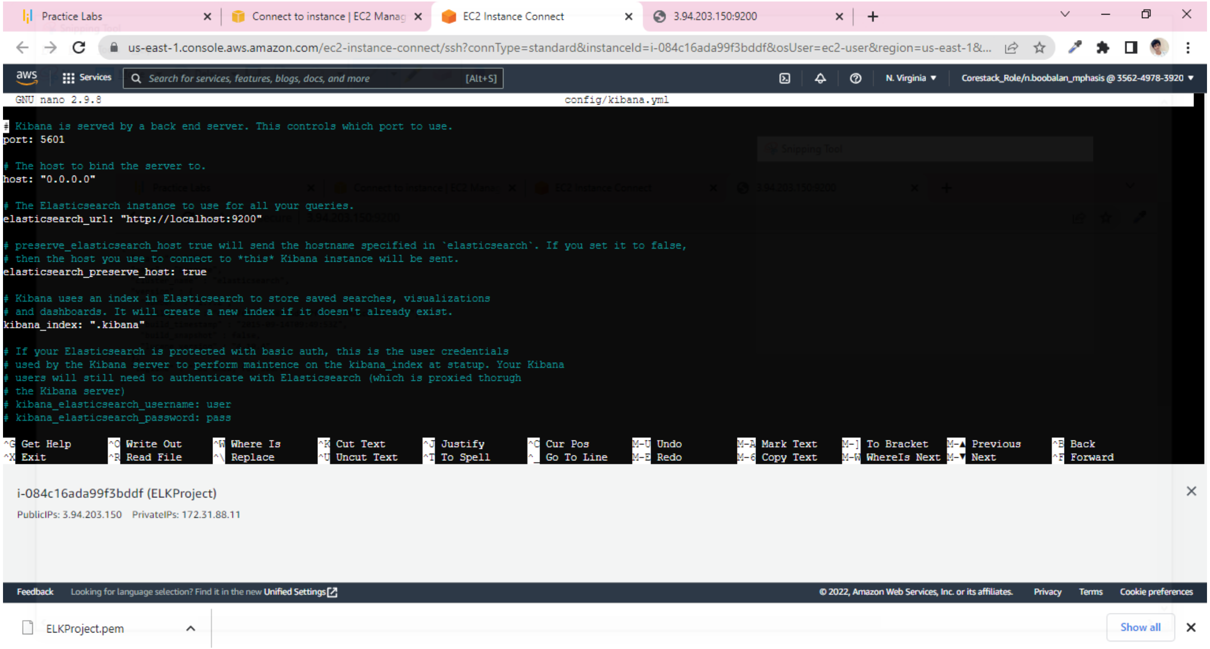
```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                                                               | 3.7 kB  00:00:00
No packages marked for update
[root@ip-172-31-88-11 elasticsearch]# cd /root
[root@ip-172-31-88-11 ~]# wget https://download.elastic.co/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-11 18:30:14--  https://download.elastic.co/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... 404 Not Found
2022-10-11 18:30:14 ERROR 404: Not Found.

[root@ip-172-31-88-11 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-11 18:31:03--  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  4.51MB/s   in 2.5s

2022-10-11 18:31:06 (4.51 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]

[root@ip-172-31-88-11 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-88-11 ~]# rm -f kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-88-11 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-88-11 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-88-11 kibana-4.1.2-linux-x64]#
```

i-084c16ada99f3bddf (ELKProject)

PublicIPs: 3.94.203.150   PrivateIPs: 172.31.88.11

Install Plugins and Kibana

Deploying ELK Stack on Docker Container(Screenshots)



Practice Labs
Connect to instance | EC2 Manag
EC2 Instance Connect
3.94.203.150:9200
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920

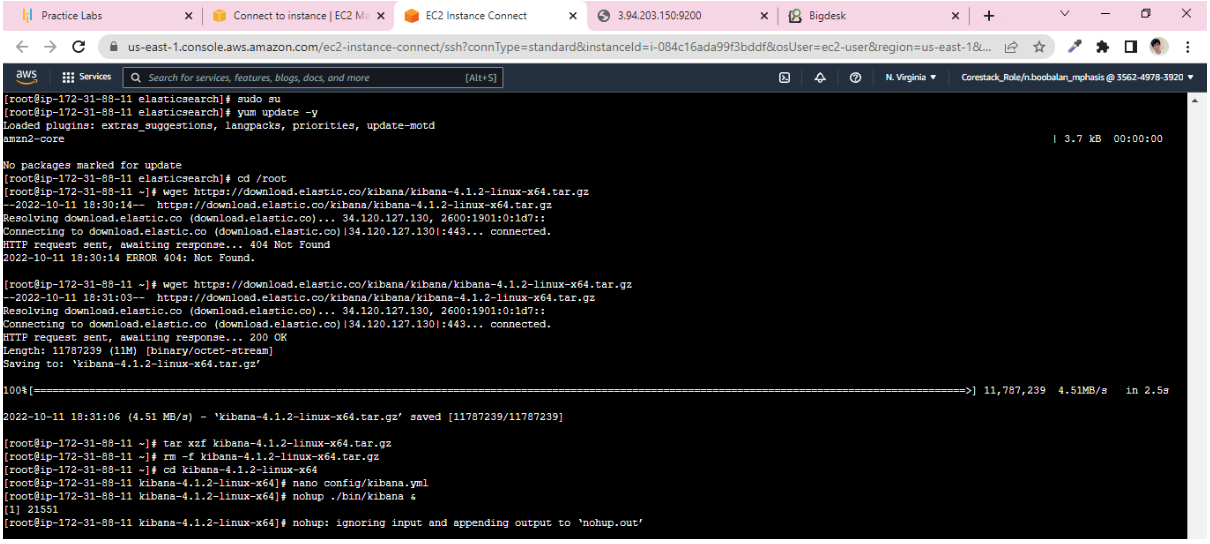
```
  GNU nano 2.9.8                                                            config/kibana.yml

# 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

^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   ^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 M-▼ Next     ^F Forward
```

i-084c16ada99f3bddf (ELKProject)

PublicIPs: 3.94.203.150   PrivateIPs: 172.31.88.11

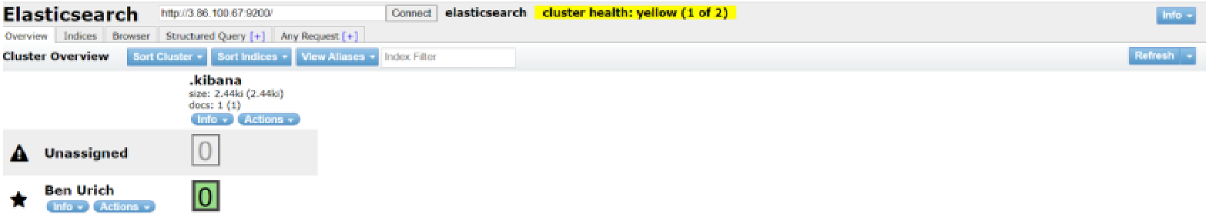
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ELKProject.pem
Show all

Deploying ELK Stack on Docker Container(Screenshots)



Practice Labs
Connect to instance | EC2 Ma
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada99f3bddf&osUser=ec2-user&region=us-east-1&...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
Corestack_Role/n.boobalan_mphasis @ 3562-4978-3920

```
[root@ip-172-31-88-11 elasticsearch]# sudo su
[root@ip-172-31-88-11 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                                                              | 3.7 kB  00:00:00

No packages marked for update
[root@ip-172-31-88-11 elasticsearch]# cd /root
[root@ip-172-31-88-11 ~]# wget https://download.elastic.co/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-11 18:30:14--  https://download.elastic.co/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... 404 Not Found
2022-10-11 18:30:14 ERROR 404: Not Found.

[root@ip-172-31-88-11 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-11 18:31:03--  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  4.51MB/s   in 2.5s

2022-10-11 18:31:06 (4.51 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]

[root@ip-172-31-88-11 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-88-11 ~]# rm -f kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-88-11 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-88-11 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-88-11 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 21551
[root@ip-172-31-88-11 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'
```



http://3.86.100.67:9200/

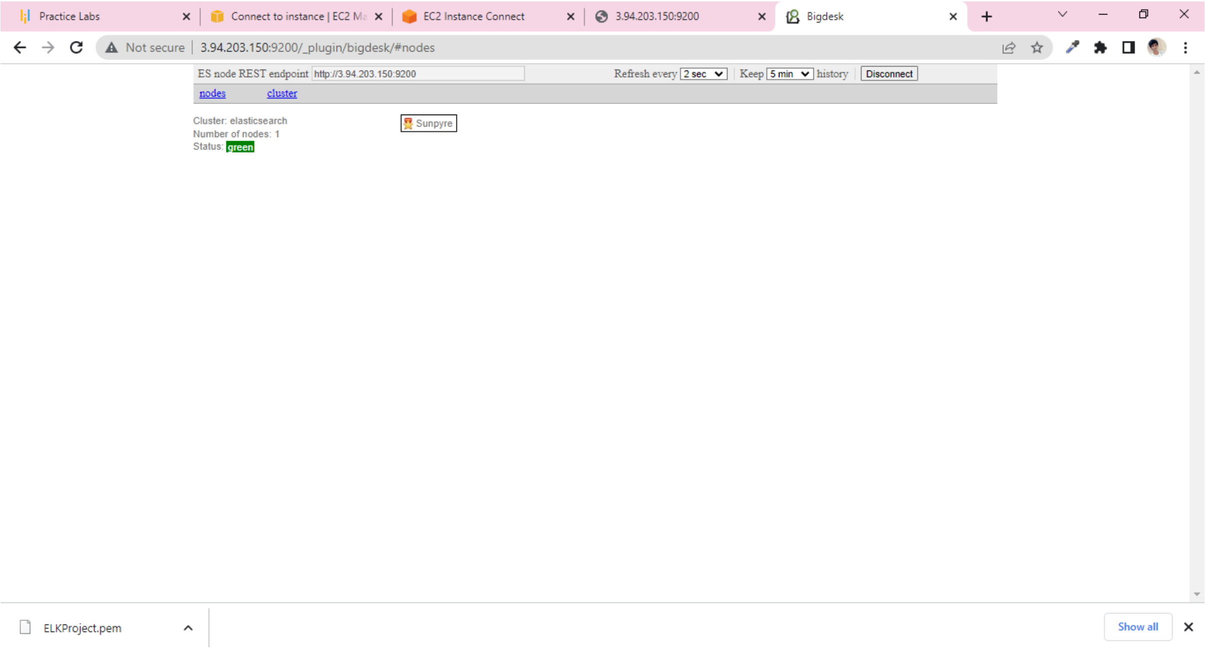
elasticsearch cluster health: yellow (1 of 2)

.kibana
size: 2.44ki (2.44ki)
docs: 1 (1)

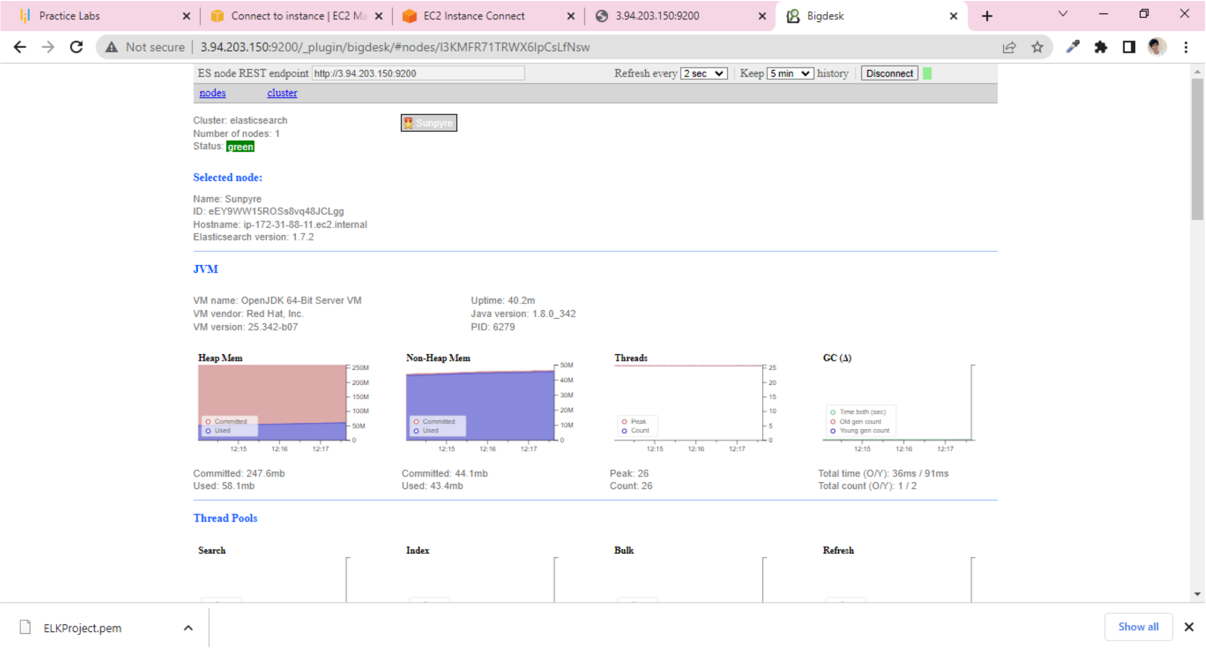
Unassigned 0

Ben Urich 0

Deploying ELK Stack on Docker Container(Screenshots)



Cluster: elasticsearch
Number of nodes: 1
Status: green



Cluster: elasticsearch
Number of nodes: 1
Status: green

Selected node:

Name: Sunpyre
ID: eEY9WW15ROSs8vq48JCLgg
Hostname: ip-172-31-88-11.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: 40.2m
Java version: 1.8.0_342
PID: 6279

Committed: 247.6mb
Used: 58.1mb

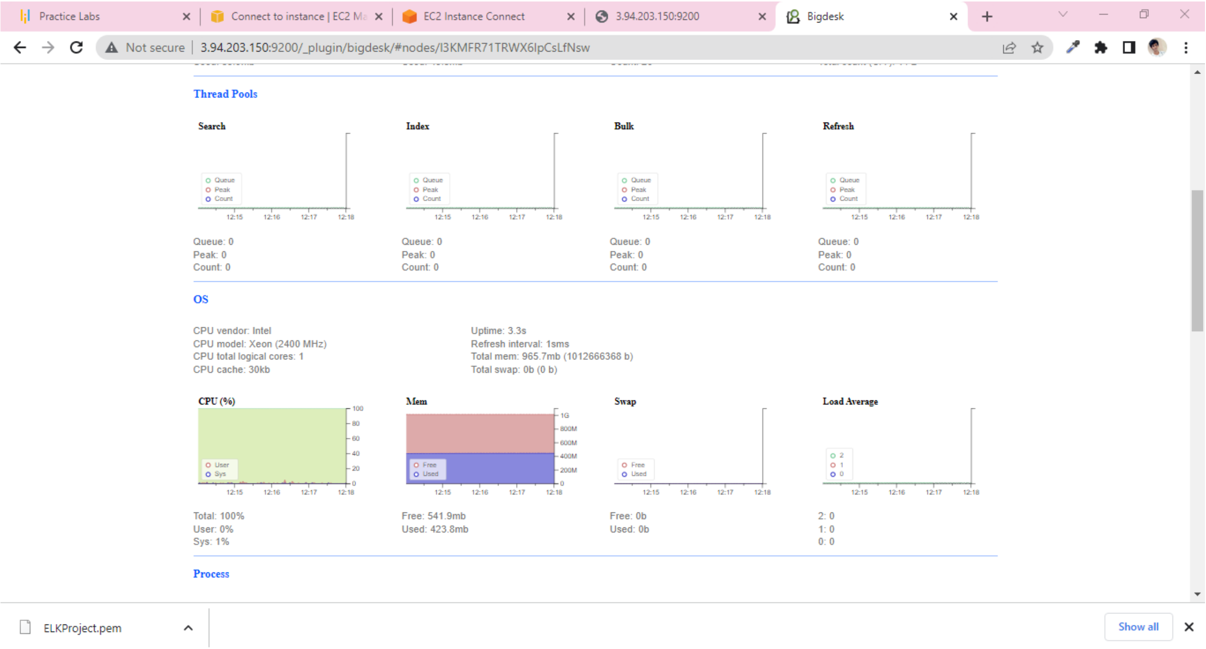
Committed: 44.1mb
Used: 43.4mb

Peak: 26
Count: 26

Total time (O/Y): 36ms / 91ms
Total count (O/Y): 1 / 2

Thread Pools

Deploying ELK Stack on Docker Container(Screenshots)



3.94.203.150:9200/_plugin/bigdesk/#nodes/I3KMFR71TRWX6lpCsLfNsw

Thread Pools

Search

Queue: 0
Peak: 0
Count: 0

Index

Queue: 0
Peak: 0
Count: 0

Bulk

Queue: 0
Peak: 0
Count: 0

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: 3.3s
Refresh interval: 1sms
Total mem: 965.7mb (1012666368 b)
Total swap: 0b (0 b)

CPU (%)

Total: 100%
User: 0%
Sys: 1%

Mem

Free: 541.9mb
Used: 423.8mb

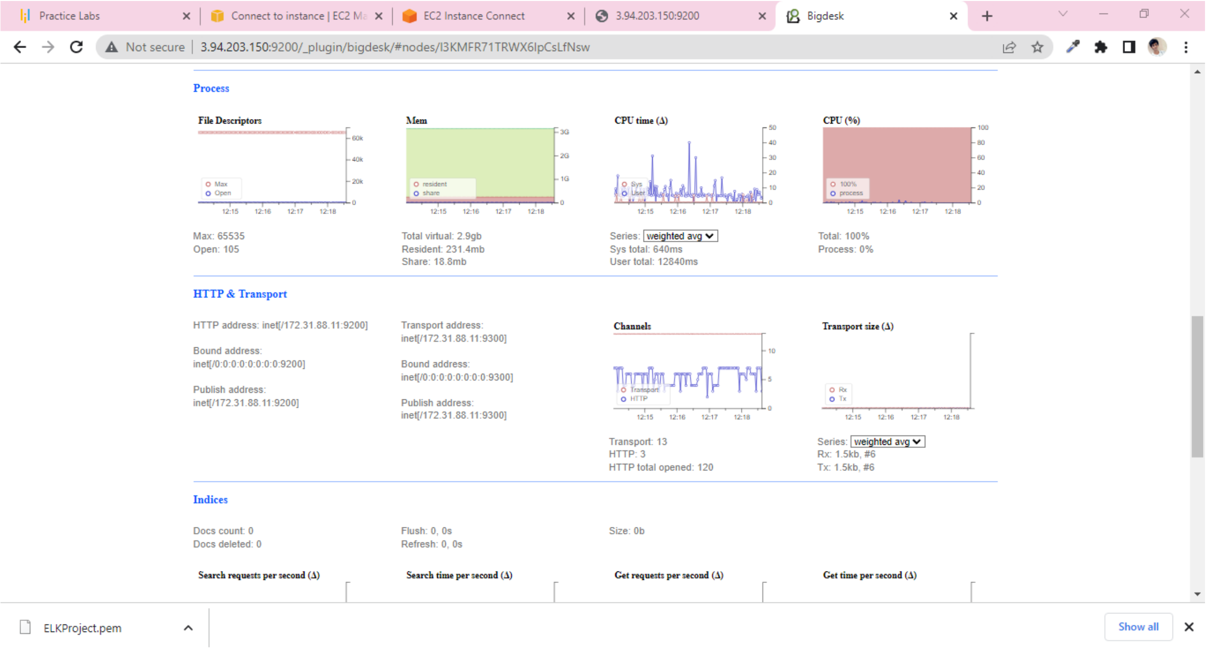
Swap

Free: 0b
Used: 0b

Load Average

2: 0
1: 0
0: 0

Process



3.94.203.150:9200/_plugin/bigdesk/#nodes/I3KMFR71TRWX6lpCsLfNsw

Process

File Descriptors

Max: 65535
Open: 105

Mem

Total virtual: 2.9gb
Resident: 231.4mb
Share: 18.8mb

CPU time (Δ)

Series: weighted avg
Sys total: 640ms
User total: 12840ms

CPU (%)

Total: 100%
Process: 0%

HTTP & Transport

HTTP address: inet[/172.31.88.11:9200]

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

Publish address:
inet[/172.31.88.11:9200]

Transport address:
inet[/172.31.88.11:9300]

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

Publish address:
inet[/172.31.88.11:9300]

Channels

Transport: 13
HTTP: 3
HTTP total opened: 120

Transport size (Δ)

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

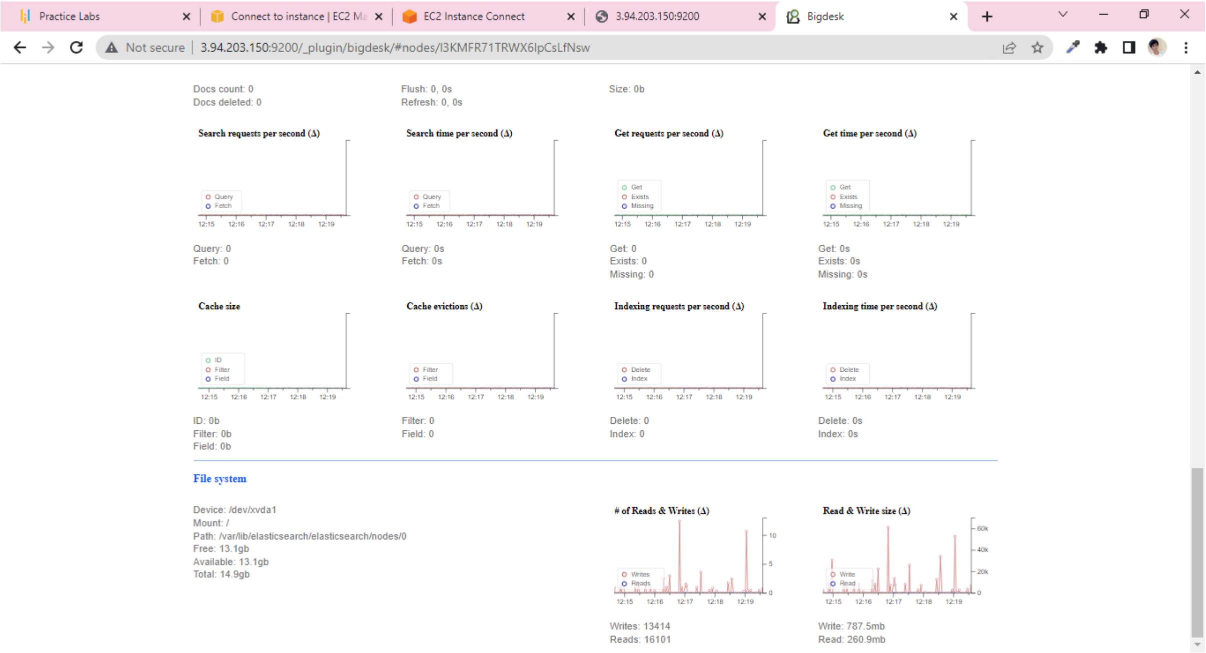
Search requests per second (Δ)

Search time per second (Δ)

Get requests per second (Δ)

Get time per second (Δ)

Deploying ELK Stack on Docker Container(Screenshots)


Practice Labs
Connect to instance | EC2 Ma
EC2 Instance Connect
3.94.203.150:9200
Bigdesk
Not secure
3.94.203.150:9200/_plugin/bigdesk/#nodes/I3KMFR71TRWX6lpCsLfNsw

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: 13.1gb
Available: 13.1gb
Total: 14.9gb

Writes: 13414
Reads: 16101

Write: 787.5mb
Read: 260.9mb