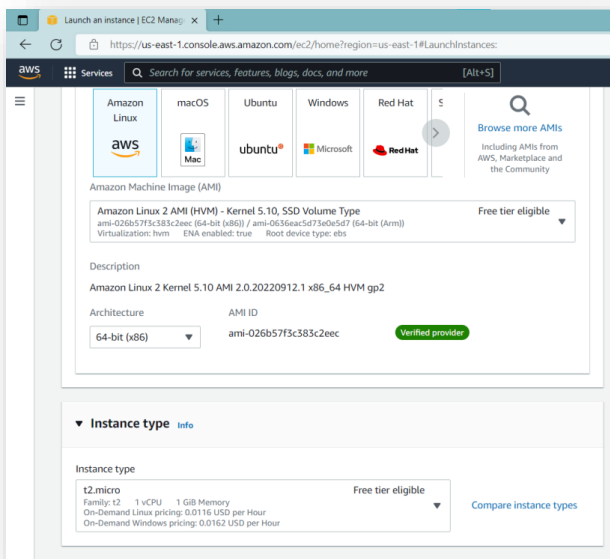
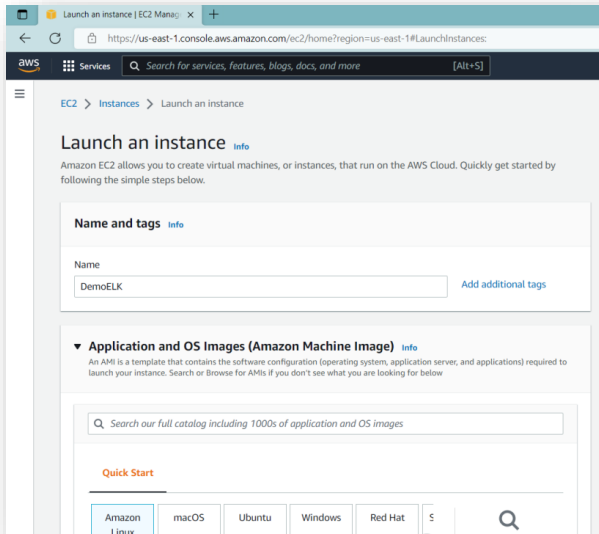


# Deploying ELK Stack on Docker Container (Doc)

First we need to create an EC2- instance.



Launch an instance | EC2 Manager | x

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

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-04eadd8acc1d2981  
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 HTTP 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 Manager | x

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

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

☐ Allow HTTP 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  

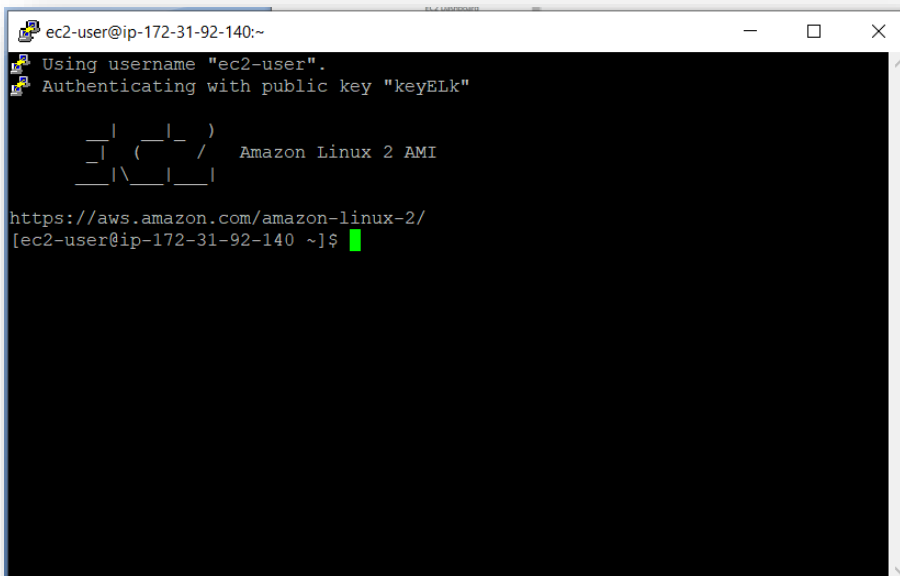
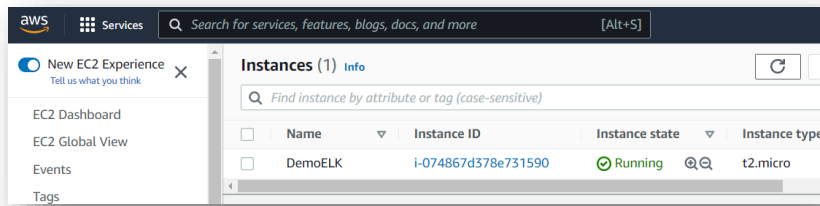
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

0 x File systems Edit

► Advanced details Info

Now connect to the instance using putty



## Step1: Install java and its Dependencies

```
libxshmfence.x86_64 0:1.2-1.amzn2.0.2
libxslt.x86_64 0:1.1.28-6.amzn2
libkcptools.x86_64 0:0.1.0.17-2.amzn2.0.2
log4j-core-2.12-47228-hotpatch.noarch 0:1.3-7.amzn2
mesa-libGL.x86_64 0:18.3.4-5.amzn2.0.1
mesa-libGL.i686 0:18.3.4-5.amzn2.0.1
mesa-libgbm.x86_64 0:18.3.4-5.amzn2.0.1
mesa-libglapi.x86_64 0:18.3.4-5.amzn2.0.1
pango.x86_64 0:1.42.4-4.amzn2
pcsc-lite-libs.x86_64 0:1.8.7.amzn2
pixman.x86_64 0:0.34.0-1.amzn2.0.2
python-javapackages.noarch 0:3.4.1-11.amzn2
python-lxml.x86_64 0:3.2.1-4.amzn2.0.3
tkmfdiff.x86_64 0:3.0.9-42.amzn2.0.2
tzdata-java.noarch 0:2022c-1.amzn2
xorg-x11-font-util.x86_64 1:7.5-21.amzn2
xorg-x11-fonts-Type1.noarch 0:7.5-9.amzn2
```

```
ec2-user@ip-172-31-92-140:~$ 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)
```

## Step2: Install Elastic search on AWS Server

```
root@ip-172-31-92-140~  
[ec2-user@ip-172-31-92-140 ~]$ sudo su  
[root@ip-172-31-92-140 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-m, install-na, install-nevra  
[root@ip-172-31-92-140 ec2-user]# cd /root  
[root@ip-172-31-92-140 ~]# wget https://download.elastic.co/elasticsearch/elast  
icsearch/elasticsearch-1.7.2.noarch.rpm  
--2022-10-09 13:39:01-- 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... c  
onected.  
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  31.8MB/s   in 0.8s  
2022-10-09 13:39:03 (31.8 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [273047  
27/27304727]  
  
[root@ip-172-31-92-140 ~]# 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  
  
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
*** NOT starting on installation, please execute the following statements to con				
figure 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-172-31-92-140 ~]# rm -f elasticsearch-1.7.2.noarch.rpm
```

### Step3: Start the Server

```
root@ip-172-31-92-140:~  
[root@ip-172-31-92-140 ~]# service elasticsearch start  
Starting elasticsearch (via systemctl): [ OK ]  
[root@ip-172-31-92-140 ~]#
```

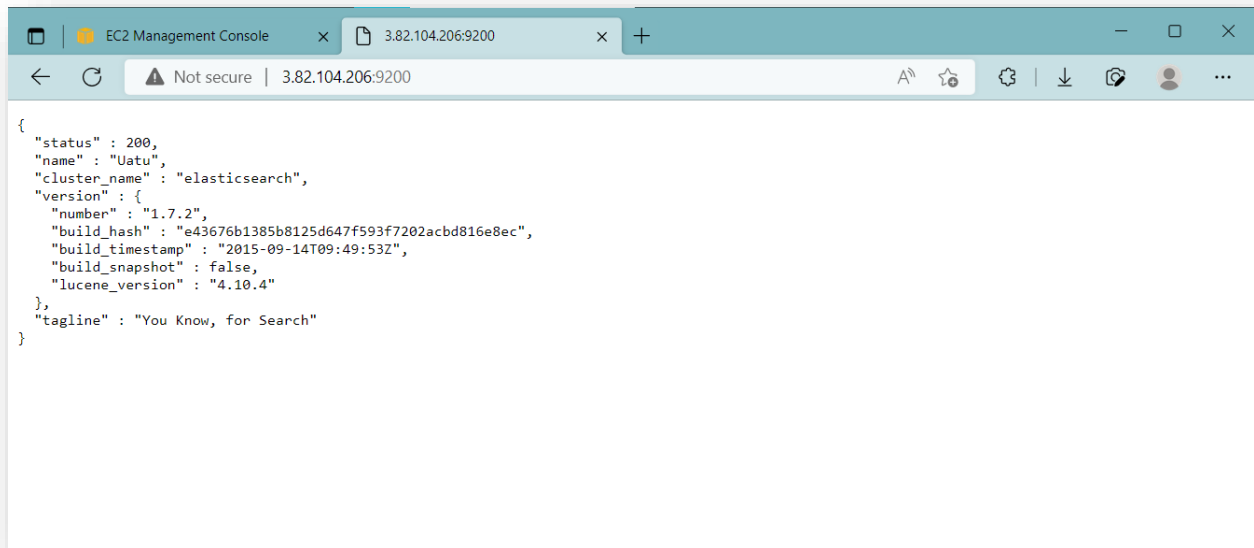
### Step4: Automatically Boot u on start

```
root@ip-172-31-92-140:~  
[root@ip-172-31-92-140 ~]# service elasticsearch start  
Starting elasticsearch (via systemctl): [ OK ]  
[root@ip-172-31-92-140 ~]#  
[root@ip-172-31-92-140 ~]# sudo chkconfig --add elasticsearch  
[root@ip-172-31-92-140 ~]#
```

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

```
root@ip-172-31-92-140:~  
[root@ip-172-31-92-140 ~]# service elasticsearch start  
Starting elasticsearch (via systemctl): [ OK ]  
[root@ip-172-31-92-140 ~]#  
[root@ip-172-31-92-140 ~]# sudo chkconfig --add elasticsearch  
[root@ip-172-31-92-140 ~]#  
[root@ip-172-31-92-140 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml  
[root@ip-172-31-92-140 ~]#
```

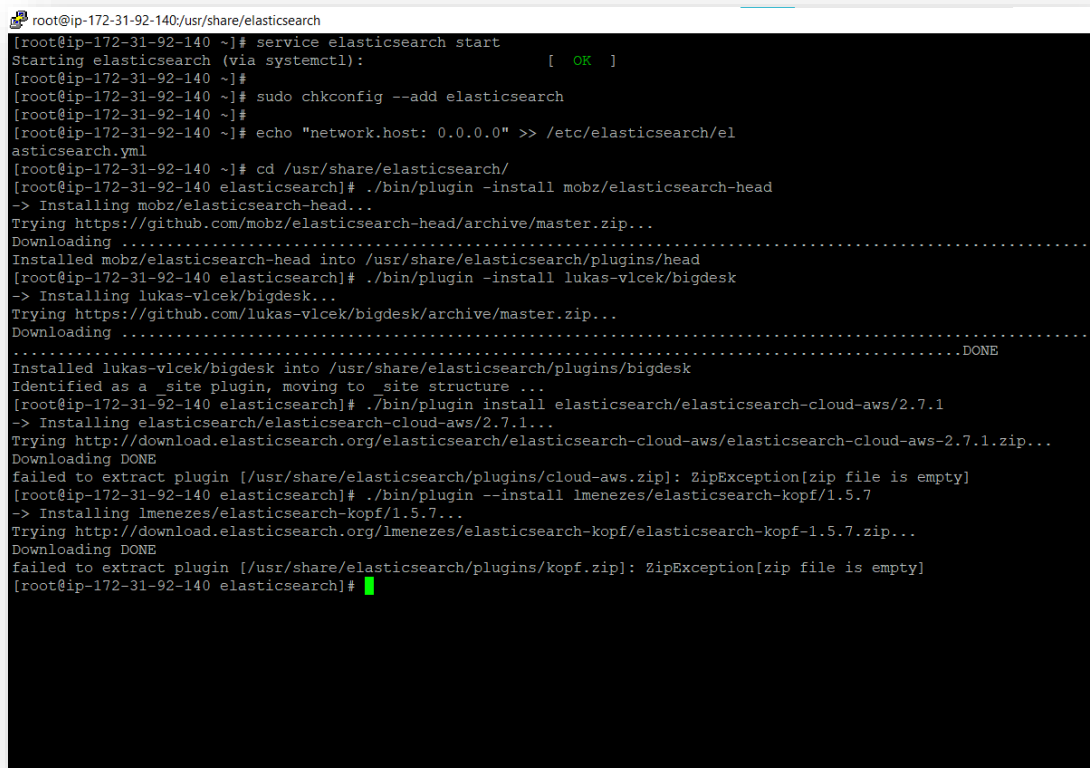
## Checking Elastic Search



The screenshot shows a web browser window with the address bar displaying "3.82.104.206:9200". The page content is a JSON object representing the Elastic Search status:

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

## Step6:Install Plugins



The screenshot shows a terminal window with the following commands and output:

```
root@ip-172-31-92-140:/usr/share/elasticsearch
[root@ip-172-31-92-140 ~]# service elasticsearch start
Starting elasticsearch (via systemctl): [ OK ]
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-92-140 ~]#
[root@ip-172-31-92-140 ~]# echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
[root@ip-172-31-92-140 ~]# cd /usr/share/elasticsearch/
[root@ip-172-31-92-140 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-172-31-92-140 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-172-31-92-140 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-172-31-92-140 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-172-31-92-140 elasticsearch]#
```

## Step 7: Install Kibana

```
root@ip-172-31-92-140:~/kibana-4.1.2-linux-x64
[root@ip-172-31-92-140 elasticsearch]# sudo su
[root@ip-172-31-92-140 elasticsearch]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No packages marked for update
[root@ip-172-31-92-140 elasticsearch]# cd /root
[root@ip-172-31-92-140 ~]# wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
--2022-10-09 14:17:18-- 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  9.50MB/s  in 1.2s

2022-10-09 14:17:19 (9.50 MB/s) - 'kibana-4.1.2-linux-x64.tar.gz' saved [11787239/11787239]

[root@ip-172-31-92-140 ~]# tar xzf kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-92-140 ~]# rm -f kibana-4.1.2-linux-x64.tar.gz
[root@ip-172-31-92-140 ~]# cd kibana-4.1.2-linux-x64
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]# nano config/kibana.yml
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]#
```

```
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]# nohup ./bin/kibana &
[1] 1949
[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]# nohup: ignoring input and appending output to 'nohup.out'

[root@ip-172-31-92-140 kibana-4.1.2-linux-x64]#
```

