

Deploying ELK Stack on Docker Container (Source Code)

Install java and its Dependencies:

```
java -version
```

```
sudo yum -y install java-1.8.0-openjdk
```

```
sudo yum -y remove java-1.7.0-openjdk
```

```
java -version
```

Install java and its Dependencies:

```
sudo su
```

```
yum install -y
```

```
cd /root
```

```
wget https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
```

```
yum install elasticsearch-1.7.2.noarch.rpm -y
```

```
rm -f elasticsearch-1.7.2.noarch.rpm
```

start the server:

```
service elasticsearch start
```

Automatically Boot u on start:

```
sudo chkconfig --add elasticsearch
```

Configuration AWS IP so you can access using public IP:

```
echo "network.host: 0.0.0.0" >> /etc/elasticsearch/elasticsearch.yml
```

Deploying ELK Stack on Docker Container (Source Code)

```
Practice Labs x Connect to instance | EC2 Manag x EC2 Instance Connect x 3.94.203.150:9200 x +
Not secure | 3.94.203.150:9200
{
  "status": 200,
  "name": "Sunnyre",
  "cluster_name": "elasticsearch",
  "version": {
    "number": "1.7.2",
    "build_hash": "a43676b1385b8125d647f93f7202acbd816e8ec",
    "build_timestamp": "2015-09-14T09:49:53Z",
    "build_snapshot": false,
    "lucene_version": "4.10.4"
  },
  "tagline": "You Know, for Search"
}
```

```
ELKProject.pem Show all x
```

Install plugins:

```
cd /usr/share/elasticsearch/
```

```
./bin/plugin -install mobz/elasticsearch-head
```

```
./bin/plugin -install lukas-vlcek/bigdesk
```

```
./bin/plugin install elasticsearch/elasticsearch-cloud-aws/2.7.1
```

```
./bin/plugin --install lmenezes/elasticsearch-kopf/1.5.7
```

```
Practice Labs x Connect to instance | EC2 M... x EC2 Instance Connect x 3.94.203.150:9200 x Bigdesk x +
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 ~]# 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 .....
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 .....
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-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-172-31-88-11 elasticsearch]#
[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.
```

Deploying ELK Stack on Docker Container (Source Code)

Install Kibana:

```
sudo su
```

```
yum update -y
```

```
cd /root
```

```
wget https://download.elastic.co/kibana/kibana/kibana-4.1.2-linux-x64.tar.gz
```

```
tar xzf kibana-4.1.2-linux-x64.tar.gz
```

```
rm -f kibana-4.1.2-linux-x64.tar.gz
```

```
cd kibana-4.1.2-linux-x64
```

```
nano config/kibana.yml
```

```
nohup ./bin/kibana &
```

```
Practice Labs | Connect to EC2 Instance Connect | 3.94.201.150:2000 | BigDesk
```

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-084c16ada9f3bddf&osUser=ec2-user®ion=us-east-1&...
AWS Services Search [Alt+5] N. Virginia Corestack_RoleInBoobalan_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'