

Output:

Deploying ELK Stack on Docker Container

First we need to create an EC2- instance.

EC2 > Instances > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name: DemoELK [Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat S

▼ Summary

Number of instances [Info](#): 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-026b57f3c383c2eec

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 16 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 1 million IOPS of provisioned IOPS.

[Cancel](#) [Launch Instance](#)

Activate Windows
Go to Settings to activate Windows.

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-026b57f3c383c2eec (64-bit (x86)) / ami-0636eac5d73e0e5d7 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs [Free tier eligible](#)

Description: Amazon Linux 2 Kernel 5.10 AMI 2.0.20220912.1 x86_64 HVM gp2

Architecture: 64-bit (x86) AMI ID: ami-026b57f3c383c2eec [Verified provider](#)

▼ Instance type [Info](#)

Instance type: t2.micro [Free tier eligible](#) [Compare instance types](#)

Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

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 [Info](#)

☐ 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

Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-026b57f3c383c2eec

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 16 GiB

[Free tier](#): In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 3 million IOPS, 1 TB of cross-region and

[Cancel](#) [Launch Instance](#)

Feedback Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

☐ 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 GiB 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](#)

Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-026b57f3c383c2eec

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 16 GiB

[Free tier](#): In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 3 million IOPS, 1 TB of cross-region and

[Cancel](#) [Launch Instance](#)

Activate Windows
Go to Settings to activate Windows

Now connect to the instance using putty

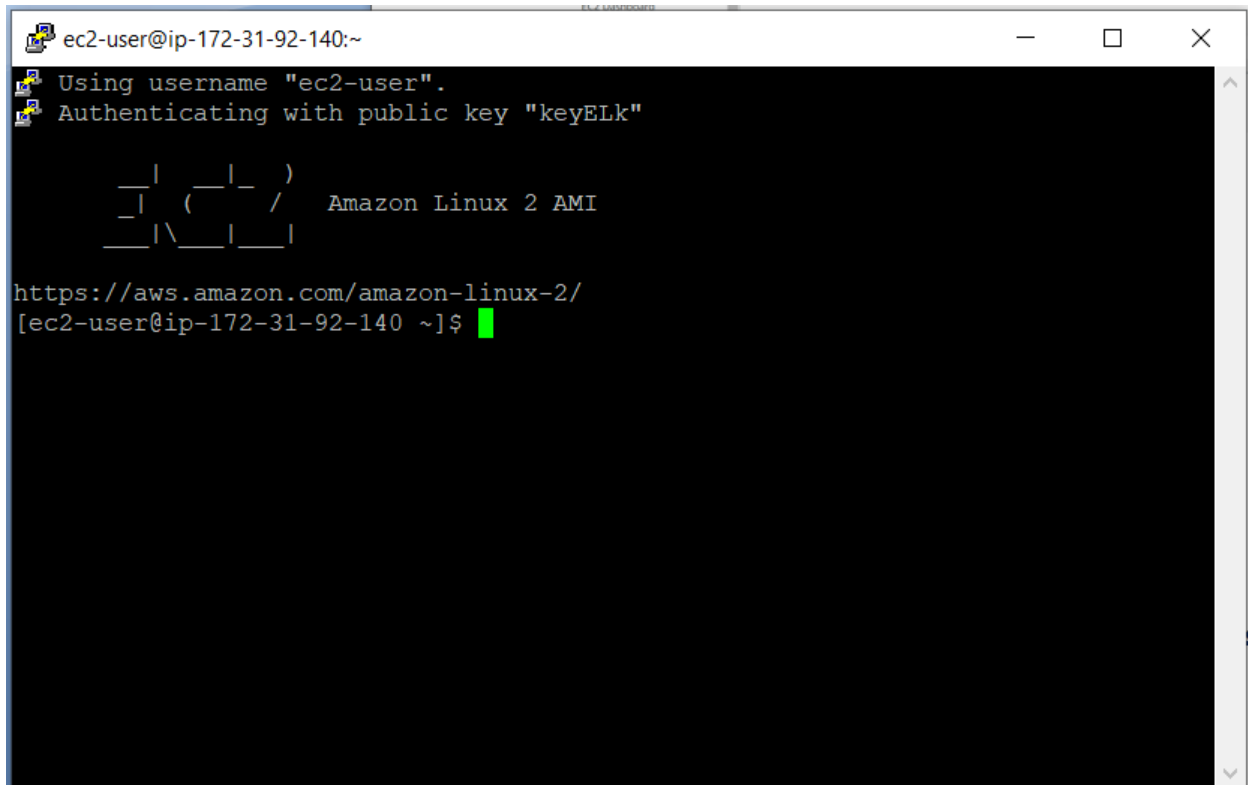
New EC2 Experience [Tell us what you think](#)

EC2 Dashboard
EC2 Global View
Events
Tags
Limits

Instances (1) [Info](#) [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
<input type="checkbox"/>	DemoELK	i-074867d378e731590	Running	t2.micro	-	No alarms	us-east-1d	ec2-3-82-104-

▼ Instances

A terminal window titled "ec2-user@ip-172-31-92-140:~" with standard window controls. It displays the login process for an Amazon Linux 2 instance, including the username "ec2-user", the public key "keyELk", and the ASCII art logo for Amazon Linux 2. The terminal also shows the URL "https://aws.amazon.com/amazon-linux-2/" and the command prompt "[ec2-user@ip-172-31-92-140 ~]\$" with a green cursor.

```
ec2-user@ip-172-31-92-140:~  
Using username "ec2-user".  
Authenticating with public key "keyELk"  
  
  _ | _ | _ )  
 _ | ( _ | /  Amazon Linux 2 AMI  
 _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-92-140 ~]$
```

Now follow the following step

Step1: Install java and its Dependencies

ec2-user@ip-172-31-92-140:~

Using username "ec2-user".

Authenticating with public key "keyELk"

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

<https://aws.amazon.com/amazon-linux-2/>

[ec2-user@ip-172-31-92-140 ~]\$ java -version

-bash: java: command not found

[ec2-user@ip-172-31-92-140 ~]\$ sudo yum -y install java-1.8.0-openjdk

Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.7 kB 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

```
libxshmfence.x86_64 0:1.2-1.amzn2.0.2  
libxslt.x86_64 0:1.1.28-6.amzn2  
lksctp-tools.x86_64 0:1.0.17-2.amzn2.0.2  
log4j-cve-2021-44228-hotpatch.noarch 0:1.3-7.amzn2  
mesa-libEGL.x86_64 0:18.3.4-5.amzn2.0.1  
mesa-libGL.x86_64 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 0:1.8.8-7.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  
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-172-31-92-140 ~]\$

ec2-user@ip-172-31-92-140:~

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

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-n, 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
onnection established.
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
```

root@ip-172-31-92-140:~

2022-10-09 13:39:03 (31.8 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]

[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 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-172-31-92-140 ~]# 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 ~]#
```

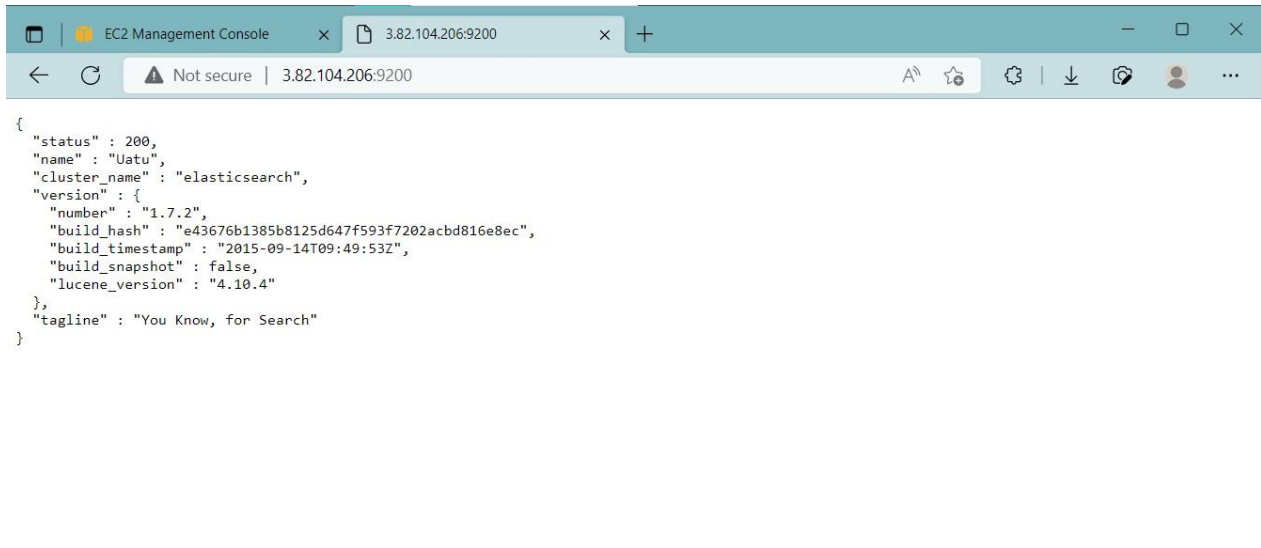
Step4: Automatically Boot u on start

```
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



Step6:Install Plugins

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]#

```

The screenshot displays the Kibana web interface in a browser window. The address bar shows the URL `http://3.82.104.206:9200/_plugin/head/`. The page header includes the 'Elasticsearch' logo and a status bar indicating 'cluster health: green (0 of 0)'. Below the header, there are navigation tabs for 'Overview', 'Indices', 'Browser', 'Structured Query [+]', and 'Any Request [+]'. The 'Cluster Overview' section is currently active, showing a star icon and the name 'Uatu'. The interface is clean and modern, with a light blue and white color scheme.

EC2 Management Console x Bigdesk x +

Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes

ES node REST endpoint Refresh every 2 sec Keep 5 min history Disconnect

[nodes](#) [cluster](#)

Cluster: elasticsearch
Number of nodes: 1
Status: green

Uatu

EC2 Management Console x Bigdesk x +

Not secure | 3.82.104.206:9200/_plugin/bigdesk/#nodes/I3KMFR7ITRWX6lpCsLfNsw

ES node REST endpoint 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: I3KMFR7ITRWX6lpCsLfNsw
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: 247.6mb
Used: 51.6mb

Non-Heap Mem

Committed: 42.5mb
Used: 41.8mb

Threads

Peak: 26
Count: 26

GC (Δ)

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 Windows

