

Deploying ELK Stack screenshots

The screenshot shows the AWS Management Console 'Instances' page. The instance 'ELK' (i-0f0278272f257c1cc) is in a 'Running' state. The instance details show it is an Amazon Linux 2 instance with a public IP address of 34.230.70.89.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
ELK	i-0f0278272f257c1cc	Running	t2.micro	-	No alarms	us-east-1c

Instance: i-0f0278272f257c1cc (ELK)

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
Instance summary Instance ID: i-0f0278272f257c1cc (ELK) IPv6 address: -	Public IPv4 address: 34.230.70.89 open address	Private IPv4 addresses: 172.31.30.211 Public IPv4 DNS: ec2-34-230-70-89.compute-1.amazonaws.com open address	Instance state: Running			

The screenshot shows the AWS Management Console 'Launch an instance' page. The 'Name and tags' section shows the instance name 'DemoELK'. The 'Application and OS Images (Amazon Machine Image)' section shows the selected AMI 'Amazon Linux 2 Kernel 5.10 AMI'. The 'Summary' section shows the instance type 't2.micro' and the storage configuration '1 volume(s) - 8 GiB'.

Launch an instance

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

Name: DemoELK

Application and OS Images (Amazon Machine Image)

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

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...
ami-026b57f3c383c2e0c

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750

Cancel Launch Instance

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

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

N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

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

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220912.1 x86_64 HVM gp2

Architecture

AMI ID

64-bit (x86) ami-026b57f3c383c2eec **Verified provider**

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) - 8 GiB

Free tier: In your first year includes 750 X

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

27°C Cloudy 08:48 PM 10-10-2022

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

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

N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249

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 (login) **Info**

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

keyELK [Create new key pair](#)

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) - 8 GiB

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

keyELK.pem [Show all](#)

27°C Cloudy 08:49 PM 10-10-2022

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]

N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249

Network vpc-0cfe83917d27e618a

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 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.

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) - 8 GiB

Free tier: In your first year includes 750

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

27°C Cloudy 08:49 PM 10-10-2022

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]

N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249

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 (Not encrypted)

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

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

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

27°C Cloudy 08:50 PM 10-10-2022

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

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

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances New

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	DemoELK	i-0991eb55687bbe151	Running	t2.micro	-	No alarms	us-east-1b

Instance: i-0991eb55687bbe151 (DemoELK)

Details Security Networking Storage Status checks Monitoring Tags

▼ Instance summary Info

Instance ID i-0991eb55687bbe151 (DemoELK)	Public IPv4 address 34.205.30.30 open address	Private IPv4 addresses 172.31.92.160
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-34-205-30-30.compute-1.amazonaws.com open address
Hostname type IP name: ip-172-31-92-160.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-92-160.ec2.internal	

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

27°C Cloudy 08:51 PM 10-10-2022

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ConnectToInstance:instanceId=i-0991eb55687bbe151

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

EC2 > Instances > i-0991eb55687bbe151 > Connect to instance

Connect to instance Info

Connect to your instance i-0991eb55687bbe151 (DemoELK) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID
i-0991eb55687bbe151 (DemoELK)

Public IP address
34.205.30.30

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

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

27°C Cloudy 08:51 PM 10-10-2022

```
(15534) Orange: x Unified Access x Mail - Ayya Prakash - x Practice Labs x Connect to instance | x EC2 Instance Connect x + - v x x
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0991eb55687bbe151&osUser=ec2-user&region=us-east-1...
AWS Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-92-160 ~]$ java -version
-bash: java: command not found
[ec2-user@ip-172-31-92-160 ~]$ sudo yum -y install java-1.8.0-openjdk
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
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
Feedback Looking for language selection? Find it in the new Unified Settings [?] © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
26°C Cloudy ENG 08:57 PM 10-10-2022
```

```
(15534) A Vachi B x Unified Access x Mail - Ayya Prakash - x Practice Labs x Connect to instance | x EC2 Instance Connect x + - v x x
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0991eb55687bbe151&osUser=ec2-user&region=us-east-1...
AWS Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249
xorg-x11-fonts-Type1.noarch 0:7.5-9.amzn2
Complete!
[ec2-user@ip-172-31-92-160 ~]$ 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-172-31-92-160 ~]$ sudo su
[root@ip-172-31-92-160 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-172-31-92-160 ec2-user]# cd /root
[root@ip-172-31-92-160 ~]# wget https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.2.noarch.rpm
--2022-10-10 15:30:51-- 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 14.8MB/s in 1.8s

2022-10-10 15:30:53 (14.8 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]

[root@ip-172-31-92-160 ~]#
Feedback Looking for language selection? Find it in the new Unified Settings [?] © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
26°C Cloudy ENG 09:01 PM 10-10-2022
```

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0991eb55687bbe151&osUser=ec2-user®ion=us-east-1...

Search for services, features, blogs, docs, and more [Alt+S] N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249

```
100%[=====>] 27,304,727 14.8MB/s in 1.8s
2022-10-10 15:30:53 (14.8 MB/s) - 'elasticsearch-1.7.2.noarch.rpm' saved [27304727/27304727]

[root@ip-172-31-92-160 ~]# 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
```

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

26°C Cloudy ENG IN 09:03 PM 10-10-2022

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0991eb55687bbe151&osUser=ec2-user®ion=us-east-1...

Search for services, features, blogs, docs, and more [Alt+S] N. Virginia Corestack_Role/ayya.prakash_mphasis @ 0830-2657-2249

```
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-172-31-92-160 ~]# rm -f elasticsearch-1.7.2.noarch.rpm
[root@ip-172-31-92-160 ~]# service elasticsearch start
Starting elasticsearch (via systemctl): [ OK ]
[root@ip-172-31-92-160 ~]# sudo chkconfig --add elasticsearch
[root@ip-172-31-92-160 ~]#
```

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

26°C Cloudy ENG IN 09:04 PM 10-10-2022

