

- Create a Virtual machine in AWS Deploy a Web Application

The image displays two screenshots of the AWS Management Console, specifically the 'Launch an instance' page for Amazon EC2.

Top Screenshot: Shows the 'Launch an instance' page. The 'Name and tags' section has 'Name' set to 'Docker'. The 'Application and OS Images (Amazon Machine Image)' section is expanded, showing a search bar and a list of AMIs. The 'Summary' panel on the right shows the configuration: Number of instances: 1, Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI..., Virtual server type (instance type): t2.micro, Firewall (security group): New security group, and Storage (volumes): 1 volume(s) - 30 GiB. The 'Launch instance' button is visible.

Bottom Screenshot: Shows the 'Quick Start' section of the 'Launch an instance' page. It displays various operating system options: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. The 'Amazon Machine Image (AMI)' section is expanded, showing the 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type'. The 'Description' section shows the AMI ID: ami-09538990a0c4fe9be. The 'Architecture' is set to '64-bit (x86)'. The 'Summary' panel on the right shows the same configuration as the top screenshot.

▼ Instance type [Info](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

☐ All generations

[Compare instance types](#)

▼ 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*

Dockerkey

[Create new key pair](#)

▼ Network settings [Info](#)

[Edit](#)

Network [Info](#)

vpc-0d9a66c5cae67d5a0

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

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-09538990a0c4fe9be

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

[Cancel](#)

[Launch instance](#)

[Review commands](#)

▼ Storage (volumes) Info

Simple

EBS Volumes

Hide details

▼ Volume 1 (AMI Root) (Custom)

Storage type Info

EBS

Device name - required Info

/dev/xvda

Snapshot Info

snap-09ae94fb9f215ca46

Size (GiB) Info

30

Volume type Info

gp2

IOPS Info

100 / 3000

Delete on termination Info

Yes

Encrypted Info

Not encrypted

KMS key Info

Select

KMS keys are only applicable when encryption is set on this volume.

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

▼ Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-09538990a0c4fe9be

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

Cancel

Launch instance

Review commands

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-066846ef3023bd006)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Create EBS snapshot policy

Instances (1) Info

Refresh

Connect

Instance state ▼

Actions ▼

Launch instances ▼

Find instance by attribute or tag (case-sensitive)

docker

Clear filters

< 1 >

	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	Docker	i-066846ef3023bd006	Running	t2.micro	Initializing	No alarms +	us-east-1c

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-066846ef3023bd006 (Docker)

Connection Type

☒ Connect using EC2 Instance Connect
 Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

☐ Connect using EC2 Instance Connect Endpoint
 Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address

18.212.38.55

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.

ec2-user

Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

aws

Services

Search

[Alt+S]

```

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

https://aws.amazon.com/amazon-linux-2/
7 package(s) needed for security, out of 8 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-92-247 ~]$ whoami
ec2-user
[ec2-user@ip-172-31-92-247 ~]$

```

It required some update to install the docker in the Instance so used the [“sudo yum update -y”](#) command.

Install a Web Server :

Sudo su

Yum install httpd -y

Cd /var/www/html

Vi index.html – Copy and Paste code in the Editor

Start Server : service httpd start

Once Deployed web application to access a application we have to open a port (Http:80)

Instance ID ---- Security – Security Groups --- Edit Inbound Rules --- Add Rule – Select HTTP Port --- Under source select Anywhere