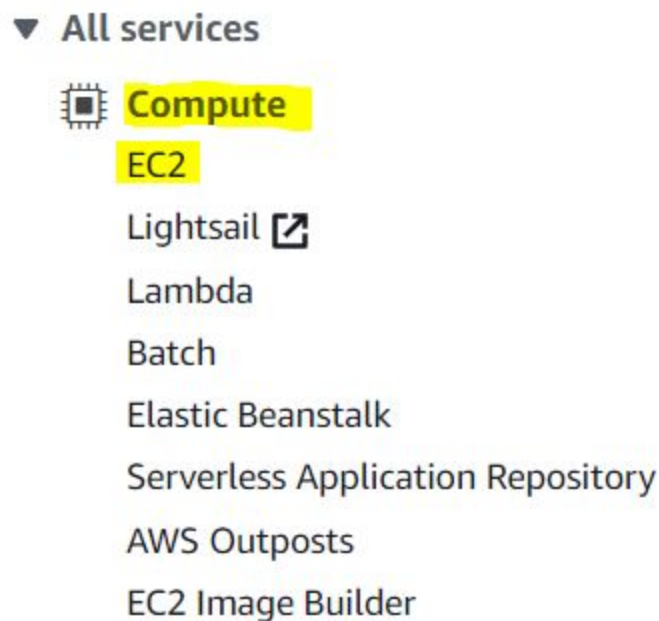


Launching an EC2 Instance in a VPC

Once, you have created a VPC and a subnet within this VPC, you can now launch your EC2 instance within this VPC.

This document will provide you with step by step guide on how to create an EC2 instance within a VPC.

1. On the AWS Management Console, click on the **EC2** service under the **Compute** section as shown below.



2. Once, you do so, you will be redirected to the EC2 management page. On this page, you need to click on the dropdown next to the **Launch instance** button and click on **Launch instance** as shown below.

EC2 Dashboard New

Events

Tags

Limits

▼ Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Scheduled Instances

Capacity Reservations

Elastic IPs 0

Key pairs 4

Placement groups 0

Snapshots 0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Note: Your instances will launch in the US East (N. Virginia) Region

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▲

Launch instance

Launch instance from template

- Now, you will be redirected to a new page. On this page, you will need to select the **Amazon Machine Image** (AMI) for your EC2 instance. For the purpose of this demonstration, you need to select the machine image that is eligible for the

free tier. For this select the check-box next to the Free tier only as shown below. This will show you all the machines images that are eligible for the free tier.

Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter

Quick Start

My AMIs

AWS Marketplace

Community AMIs

☒ Free tier only ⓘ

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0be2609ba883822ec (64-bit x86) / ami-0c582118883b46f4f (64-bit Arm)

Amazon Linux
Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-096fda3c22c1c990a

Red Hat
Free tier eligible

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-0fde50fcbcd46f2f7 (64-bit x86) / ami-05f2f5f76d89313bb (64-bit Arm)

SUSE Linux
Free tier eligible

SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled, Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

4. Next, you need to select the machine image. Select the Amazon Linux 2 AMI. Click on the **Select** button next to this AMI as shown below.

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0be2609ba883822ec (64-bit x86) / ami-0c582118883b46f4f (64-bit Arm)

Amazon Linux
Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-096fda3c22c1c990a

Red Hat
Free tier eligible

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

5. Now, you will be redirected to a new page. On this page, you need to select the **Instance Type**. Select the **t2.micro** instance type as it is eligible for the free tier. This is the instance type that is selected by default.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and network you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: [Show/Hide Columns](#)

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs ⓘ	Memory (GiB)	Instance Storage (GB) ⓘ	EBS-Optimized Available ⓘ	Network Performance ⓘ
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate

- Next, click on the button which says **Next: Configure Instance Details** as shown below.

<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Instance Details](#)

- Now, you will be redirected to a new page. On this page, you will be selecting the **VPC** and the **subnet** that you had created earlier. To select the **VPC** in the **Network** field, click on the dropdown as shown below.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take at

Number of instances ⓘ [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ ⓘ [Create new VPC](#)

Subnet ⓘ ⓘ [Create new subnet](#)

Auto-assign Public IP ⓘ ⓘ

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ ⓘ

- Now from the list that appears select the **upgrad-vpc** as shown in the image below.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-05b8047bfaa5eed52 upgrad-vpc	Create new VPC
Subnet	subnet-037b65eb9e7ffa1b3 upgrad-subnet-a us-e: 251 IP Addresses available	Create new subnet
Auto-assign Public IP	Use subnet setting (Disable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	

9. Next, you need to select the **Subnet**. Since there is only one subnet associated with the VPC, that subnet is selected by default.

10. In the **Auto-assign Public IP** click on the dropdown and select **Enable**.

Network	vpc-05b8047bfaa5eed52 upgrad-vpc	Create new VPC
Subnet	subnet-037b65eb9e7ffa1b3 upgrad-subnet-a us-e: 251 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	

11. Till now, your page should appear as shown below.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-05b8047bfaa5eed52 upgrad-vpc	Create new VPC
Subnet	subnet-037b65eb9e7ffa1b3 upgrad-subnet-a us-e: 251 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	

12. Leave the rest of the settings as default. Next, click on the button **Next: Add Storage**.

Number of instances Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network Create new VPC

Subnet Create new subnet
251 IP Addresses available

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation

Domain join directory Create new directory

IAM role Create new IAM role

CPU options ☐ Specify CPU options

Shutdown behavior

Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Cancel Previous Review and Launch Next: Add Storage

13. Leave the setting as default on this page and click on the **Next: Add Tags** button.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-019159f1e06f32720	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

14. On this page, you can add a tag to your EC2 instance. Click on the text which reads **click to add a Name tag** as shown in the image below.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value	Instances	Volumes				
(128 characters maximum)				(256 characters maximum)			
This resource currently has no tags							
Choose the Add tag button or click to add a Name tag .							
Make sure your IAM policy includes permissions to create tags.							

15. In the value field, you can enter any name of your choice.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
Name	CloudComputing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

16. Now click on the button **Next: Configure Security Group** as shown below.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
Name	CloudComputing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Security Group](#)

17. On this page, you need to use the security group that you have created earlier. To use an existing security group click on the radio button next to the option which reads **Select an existing security group** as shown below.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing

Assign a security group: ☐ Create a new security group

☒ Select an existing security group

18. From the list that appears, select the security group that you had created earlier.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

Security Group ID	Name	Description
<input type="checkbox"/> sg-0aa73b42db6c984ae	default	default VPC security group
<input type="checkbox"/> sg-08d6950a0a5c23930	launch-wizard-7	launch-wizard-7 created 2021-01-14T15:49:27.714+05:30
<input checked="" type="checkbox"/> sg-0b6126887e3c1aa41	UpgradWebServers	Only for Web Servers

Inbound rules for sg-0b6126887e3c1aa41 (Selected security groups: sg-0b6126887e3c1aa41)

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	106.207.9.161/32
SSH	TCP	22	106.207.9.161/32

19. Next click on the **Review and Launch** button.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-0aa73b42db6c984ae	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-08d6950a0a5c23930	launch-wizard-7	launch-wizard-7 created 2021-01-14T15:49:27.714+05:30	Copy to new
<input checked="" type="checkbox"/> sg-0b6126887e3c1aa41	UpgradWebServers	Only for Web Servers	Copy to new

Inbound rules for sg-0b6126887e3c1aa41 (Selected security groups: sg-0b6126887e3c1aa41)

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
HTTP	TCP	80	106.207.9.161/32	
SSH	TCP	22	106.207.9.161/32	

[Cancel](#) [Previous](#) [Review and Launch](#)

20. On this page, you can review the settings for the EC2 instance that you are about to launch. Now, to launch this instance, you need to click on the **Launch** button as shown below.

AMI Details

Free tier eligible

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0be2699ba883822ec

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a ...

Root Device Type: ebs Virtualization type: hvm

Edit AMI

Instance Type

Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups

Edit security groups

Security Group ID	Name	Description
sg-0b6126887e3c1aa41	UpgradWebServers	Only for Web Servers

All selected security groups inbound rules

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
--------	------------	--------------	----------	---------------

Cancel

Previous

Launch

21. Once, you click on this button, it will prompt you to select a key pair for this EC2 instance.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

Assignment_key_pair

☐ I acknowledge that I have access to the selected private key file (Assignment_key_pair.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

22. If this is the first time you are launching an EC2 instance, you need to generate a new key pair. Click on the dropdown and select **Create a new key pair** as shown below.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair



Select a key pair

Assignment_key_pair



☐ I acknowledge that I have access to the selected private key file (Assignment_key_pair.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

23. You also need to specify a name for the key pair. You can name it anything as per your convenience. After you have named it, click on the **Download Key Pair** button as shown below.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair



Key pair name

sd-cloud

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

A **.pem** file will be downloaded. If you are using a Linux or Mac operating system, you will need this **.pem** file to login to your EC2 instance. If you are a Windows user, you will need to convert this file to a **.ppk** to login to your EC2 instance.

Irrespective of the operating system, it is very important to keep this .pem file safe. Under no circumstances, you should lose this file.

24. If you already have one key pair, you can use the same file to login to this EC2 instance. Select the option that says **Choose an existing key pair** and from the next dropdown select the existing key pair. You would also need to check the box as shown below.

Follow this step if and only if you have downloaded a key pair for this AWS account.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

upgrad-siben

☒ I acknowledge that I have access to the selected private key file (upgrad-siben.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

25. Once you have either downloaded the key pair or selected the option to use an existing pair, then you can launch the EC2 instance. To launch the EC2 instance, click on the **Launch Instances** button as shown below.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

upgrad-siben

☒ I acknowledge that I have access to the selected private key file (upgrad-siben.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

26. A new page will appear which says **Your instances are now launching**. Scroll down to the bottom and click on the **View Instances** button as shown below.

Launch Status

 **Your instances are now launching**
The following instance launches have been initiated: [i-0e49785211a8f451f](#) [View launch log](#)

 **Get notified of estimated charges**
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out how to connect to your instances.](#)

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2: User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances

27. On this page, you can see the instance that you have just launched.

Instances (1) Info									
<input type="text" value="Filter instances"/>				<input type="button" value="Refresh"/>	<input type="button" value="Connect"/>	Instance state ▾	Actions ▾	<input type="button" value="Launch instances"/> ▾	
<input type="text" value="search: CloudCom"/> <input type="button" value="Clear filters"/>									
<input type="checkbox"/>	Name ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Public IP	
<input type="checkbox"/>	CloudComputing	i-0e49785211a8f451f	Running	t2.micro	⌚ Initializing	No alarms +	us-east-1c		-

You can see that the name is CloudComputing and the instance type is **t2.micro**.

With this, you have successfully launched a new EC2 instance within a VPC that you had created earlier.