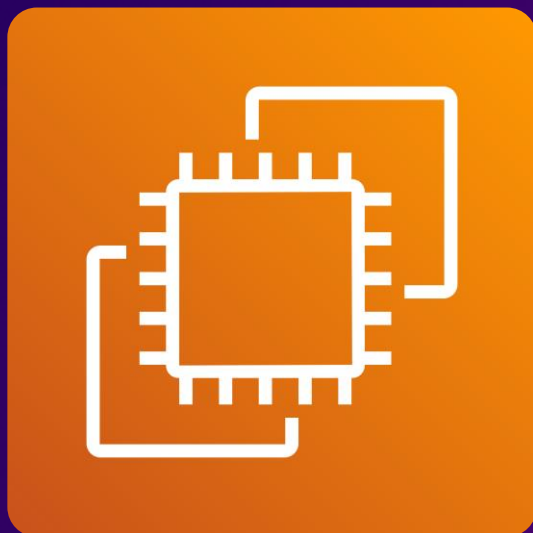


AWS  
re:Start  
LAB

# Introduction to Amazon EC2



**WEEK 1**





# Overview

---

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

Through Amazon EC2, users can deploy and manage virtual machines (VMs) on AWS infrastructure, including support for both Microsoft Windows and Linux environments. These VMs are categorized into various instance types, each offering different combinations of CPU, memory, storage, and networking capacity.

Additionally, Amazon EC2 offers flexible pricing models that allow users to pay only for the compute resources they use, making it an efficient and cost-effective solution for running applications in the cloud.

## Topics covered

- Launch a web server with termination protection enabled
- Monitor Your EC2 instance
- Modify the security group that your web server is using to allow HTTP access
- Resize your Amazon EC2 instance to scale
- Test termination protection
- Terminate your EC2 instance

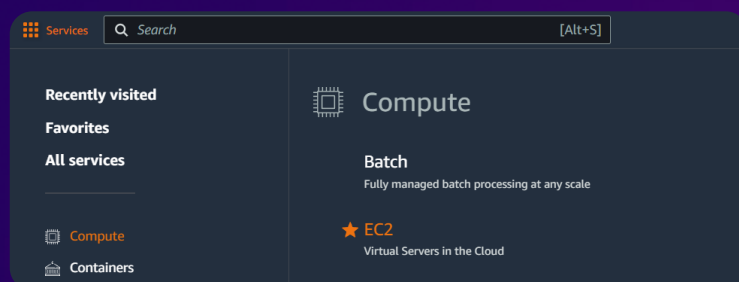


# Task 1

## Launching your EC2 instance

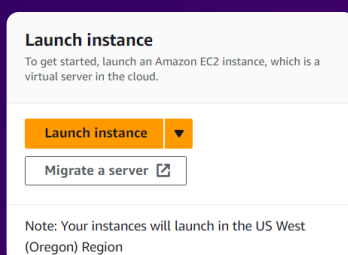
### Step 1: Open the Amazon EC2 console

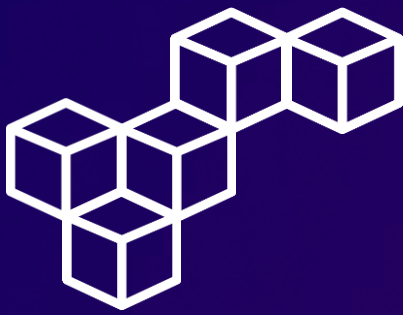
In the AWS Management Console on the **Services** menu, choose [EC2](#).



### Step 2: Launch an instance using the Launch Instance Wizard

In the EC2 Dashboard page select [Launch Instance](#).





# Task 1

## Launching your EC2 instance

### Step 3: Naming your EC2 instance

In the **Name and tags** pane, enter **Web Server** as the instance Name.

**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

Web Server

Add additional tags

### Step 4: Choosing an Amazon Machine Image (AMI)

Under **AMI Machine Image (AMI)**, select the **Amazon Linux 2023 AMI** image, which includes the OS setup configuration.

**Amazon Machine Image (AMI)**

Amazon Linux 2023 AMI

Free tier eligible

ami-0395649fbe870727e (64-bit (x86), uefi-preferred) / ami-01a43c6864f47cef1 (64-bit (Arm), uefi)  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

**Description**

Amazon Linux 2023 AMI 2023.4.20240401.1 x86\_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0395649fbe870727e

Verified provider

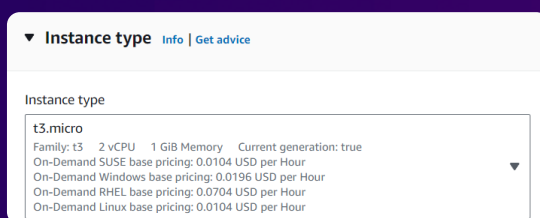


# Task 1

## Launching your EC2 instance

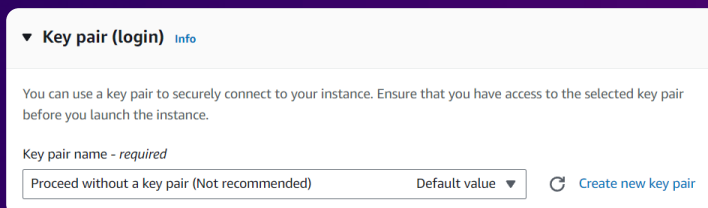
### Step 5: Choosing an instance type

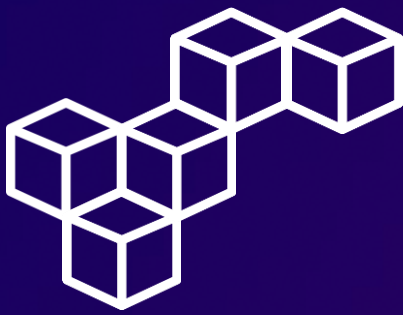
In the **Instance type** pane, select a [t3.micro](#) instance. This instance type has 2 virtual CPU and 1 GiB of memory.



### Step 6: Configuring a key pair

In the **Key pair (login)** pane, select [Proceed without a key pair \(Not recommended\)](#). In this lab, we do not log in to the instance, so we do not require a key pair.





# Task 1

## Launching your EC2 instance

### Step 7: Configuring the network settings

In the **Network settings** pane, for **VPC - required** select **Lab VPC**, configure the **Security Group** **Web Server security group** and **remove** the **Inbound security groups rules**.

▼ Network settings [Info](#)

VPC - required [Info](#)  
vpc-0634a39abe2bc97d8 (Lab VPC)  
10.0.0.0/16

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

Security group name - required  
Web Server security group  
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .-:/()#,@!+=8;~[]\$\*

Description - required [Info](#)  
Security group for my web server

Inbound Security Group Rules

No security group rules are currently included in this template.

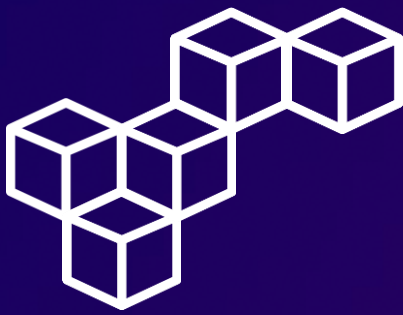
Add security group rule

### Step 8: Adding storage

In the **Configure storage** pane, select a **8 GiB disk volume**.

▼ Configure storage [Info](#)

1x 8 GiB gp3 Root volume (Not encrypted)



# Task 1

## Launching your EC2 instance

### Step 9: Configuring advanced details

In the **Advanced details** pane, **enable** Termination protection and enter a **script** into the **User data** text box **to execute upon instance startup**.

Termination protection [Info](#)

Enable

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' >
/var/www/html/index.html
```

### Step 10: Launching an EC2 instance

The instance is now running and the 2 status checks passed.

Success  
Successfully initiated launch of instance (i-03095c520ff39d2ca)

aws

Services

Search

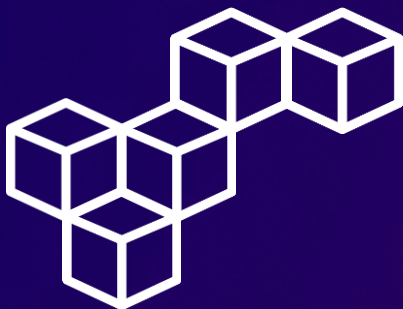
[Alt+S]

Instances (1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

All states

	Name	Instance ID	Instance state	Instance type	Status check
<input type="checkbox"/>	Web Server	i-03095c520ff39d2ca	Running	t3.micro	2/2 checks passed

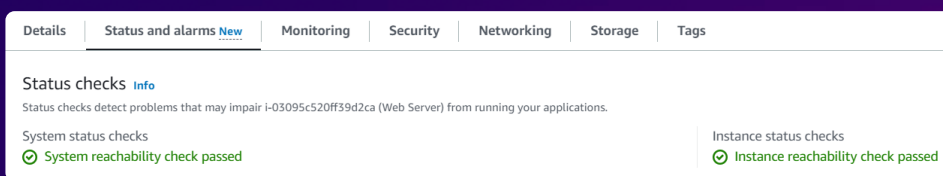


# Task 2

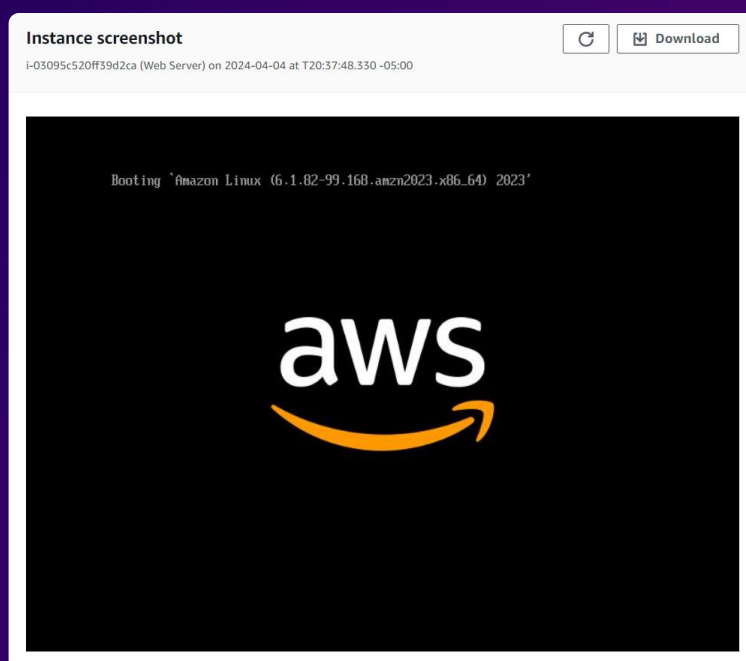
## Monitor Your Instance

With instance status monitoring, you can quickly determine whether Amazon EC2 has detected any problems that might prevent your instances from running applications.

Both the [System reachability](#) and [Instance reachability](#) checks have passed.



Additionally, you can capture a screenshot of your instance and view it as an image. This provides visibility as to the status of the instance, and allows for quicker troubleshooting.







## Task 3

# Update Your Security Group and Access the Web Server

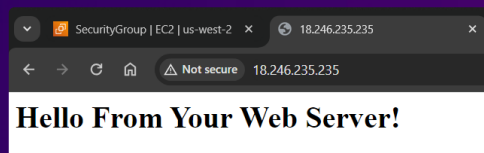
Create an **Inbound rule** for the security group to permit web traffic on port 80 into your Amazon EC2 Instance. Configure the rule with the following settings:

- Type: [HTTP](#).
- Source: [Anywhere-IPv4](#).

The screenshot shows the 'Inbound rules' section of the AWS Management Console. A table lists the inbound rules for a security group. The rule being configured is 'sgr-0952f2e84b6ee62d7'. The configuration fields are as follows:

Security group rule ID	Type	Protocol	Port range	Source
sgr-0952f2e84b6ee62d7	HTTP	TCP	80	Anyw... 0.0.0.0/0

Open a new tab in your web browser, paste the **Public IPv4 address** of your instance, then press Enter. You should see the message [Hello From Your Web Server!](#)





# Task 4

## Resize Your Instance: Instance Type and EBS Volume

### Step 1: Stop Your Instance

Before you can resize an instance, you must [stop it](#).

Instances (1) <a href="#">Info</a>			
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>			
<input type="checkbox"/>	Name <a href="#">↗</a>	Instance ID	Instance state <a href="#">▼</a>
<input type="checkbox"/>	Web Server	<a href="#">i-03095c520ff39d2ca</a>	Stopped <a href="#">🔍</a> <a href="#">🔍</a>

### Step 2: Change The Instance Type

Select a [t3.small](#) instance. This instance type has twice as much memory as a t3.micro instance.

#### Change instance type [Info](#)

You can change the instance type only if the current instance type and the instance type that you want are compatible.

Instance ID

[i-03095c520ff39d2ca](#) (Web Server)

Current instance type

t3.micro

New instance type



# Task 4

## Resize Your Instance: Instance Type and EBS Volume

### Step 3: Resize the EBS Volume

Increase the size of the root disk volume from 8 GiB to **10 GiB**.

### Modify volume Info

Modify the type, size, and performance of an EBS volume.

#### Volume details

Volume ID  
vol-0c9760ab4014142a6

Volume type Info  
General Purpose SSD (gp3)

Size (GiB) Info  
10

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

### Step 4: Start the Resized Instance

Start the instance again. It will now have more memory and more disk space.

Instances (1) <small>Info</small>				
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>				
<input type="checkbox"/>	Name <small>✎</small>	Instance ID	Instance state	Instance type
<input type="checkbox"/>	Web Server	i-03095c520ff39d2ca	Running	t3.small



# Task 5

## Test Termination Protection

If you attempt to terminate the instance, a red error message pops up at the top that says: **Failed to terminate an instance: The instance may not be terminated.** This is because it has **termination protection enabled**.

⊗ Failed to terminate an instance: The instance 'i-03095c520ff39d2ca' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.

Turn off **termination protection** before terminating the instance.

Change termination protection

To prevent your instance from being accidentally terminated, you can enable termination protection for the instance. [Learn more](#)

Instance ID  
i-03095c520ff39d2ca (Web Server)

Termination protection  
☐ Enable

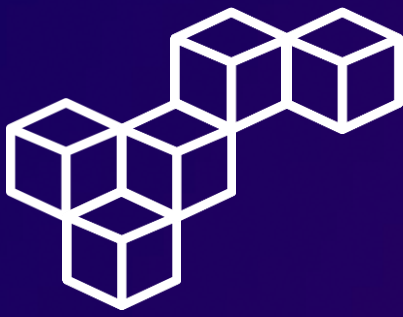
**Termination protection disabled.**  
The instance is no longer protected against accidental termination. If the instance is terminated, data stored on ephemeral storage is lost.

Cancel

Save

Terminate the instance.

Instances (1) <a href="#">Info</a>				
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>				
<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type
<input type="checkbox"/>	Web Server	i-03095c520ff39d2ca	Terminated	t3.small



# Conclusions

---

## Launching your EC2 instance

The launch instance wizard enables you to quickly launch an instance with customizable parameters tailored to various use cases for optimal performance.

## Monitoring your instance

Monitoring instances using AWS's diverse tools is essential to ensure instance reachability and early identification of issues for troubleshooting purposes.

## Security Groups

A security group functions as a firewall, restricting the network traffic allowed in and out of an instance, enhancing security.

## Resizing your Instance

You can modify multiple parameters of your instance, such as instance type, disk space, security groups, network settings, and more, as your computing requirements evolve.

## Terminating your Instance

Termination protection prevents instances from being unintentionally terminated. Terminating an instance causes both the instance itself and its attached storage volume to be shut down, effectively ceasing cost consumption.



**Cristhian Becerra**



[cristhian-becerra-espinoza](#)



+51 951 634 354



[cristhianbecerra99@gmail.com](mailto:cristhianbecerra99@gmail.com)



Lima, Peru

