

# Amazon EC2 Lab

By: Mohamed mourad

[Mohamed MouradPS | LinkedIn](#)

## Basic overview of launching, resizing, managing, and monitoring an Amazon EC2 instance

### What is Amazon EC2 instance?

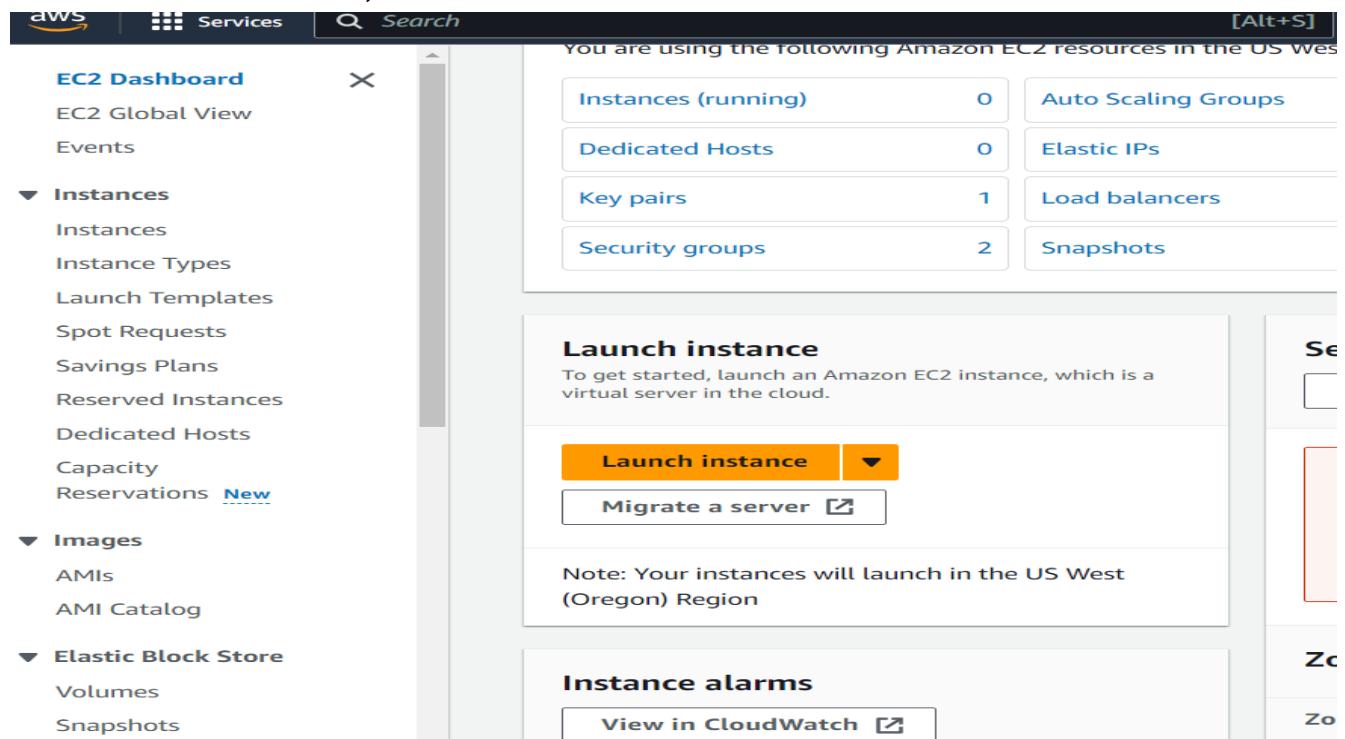
**Amazon EC2** is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.

Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

### Launching your EC2 instance

- In the AWS Management Console on the **Services** menu, choose **EC2**.
- In the left navigation pane, choose **EC2 Dashboard** to ensure that you are on the dashboard page.
- Choose **Launch instance**, and then select **Launch instance**



## Step 1: Naming your EC2 instance

When you name your instance, AWS creates a key value pair. The key for this pair is **Name**, and the value is the name you enter for your EC2 instance.

- In the **Name and tags** pane, in the **Name** text box, enter Web Server.

## Step 2: Choosing an Amazon Machine Image (AMI)

An AMI provides the information required to launch an instance, which is a virtual server in the cloud. An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system or an application server with applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it is launched

The **Quick Start** list contains the most commonly used AMIs. You can also create your own AMI or select an AMI from the AWS Marketplace, an online store where you can sell or buy software that runs on AWS.

- Locate the **Application and OS Images (Amazon Machine Image)** pane.
- Under **AMI Machine Image (AMI)**, notice that the **Amazon Linux 2 AMI** image is selected by default. Keep this setting.

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar, and keyboard shortcuts [Alt+S] and [Esc]. Below the navigation bar, the main content area has a sidebar on the left with a 'Name' input field containing 'My Web Server' and a 'Add additional tags' button. The main content area is titled 'Application and OS Images (Amazon Machine Image)'. It includes a descriptive text about AMIs and a search bar. A red box highlights the 'Quick Start' section, which lists several AMI options: Amazon Linux (selected), macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. A red arrow points from the 'Quick Start' heading to the 'Amazon Linux' option. Another red box highlights the 'Amazon Linux 2023 AMI' card, which displays its AMI ID, virtualization type (hvm), ENA status (true), and root device type (ebs). A 'Free tier eligible' button is also visible.

### Step 3: Choosing an instance type

Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more *instance sizes* so that you can scale your resources to the requirements of your target workload.

Select a **t3.micro** instance. This instance type has 2 virtual CPU and 1 GiB of memory.

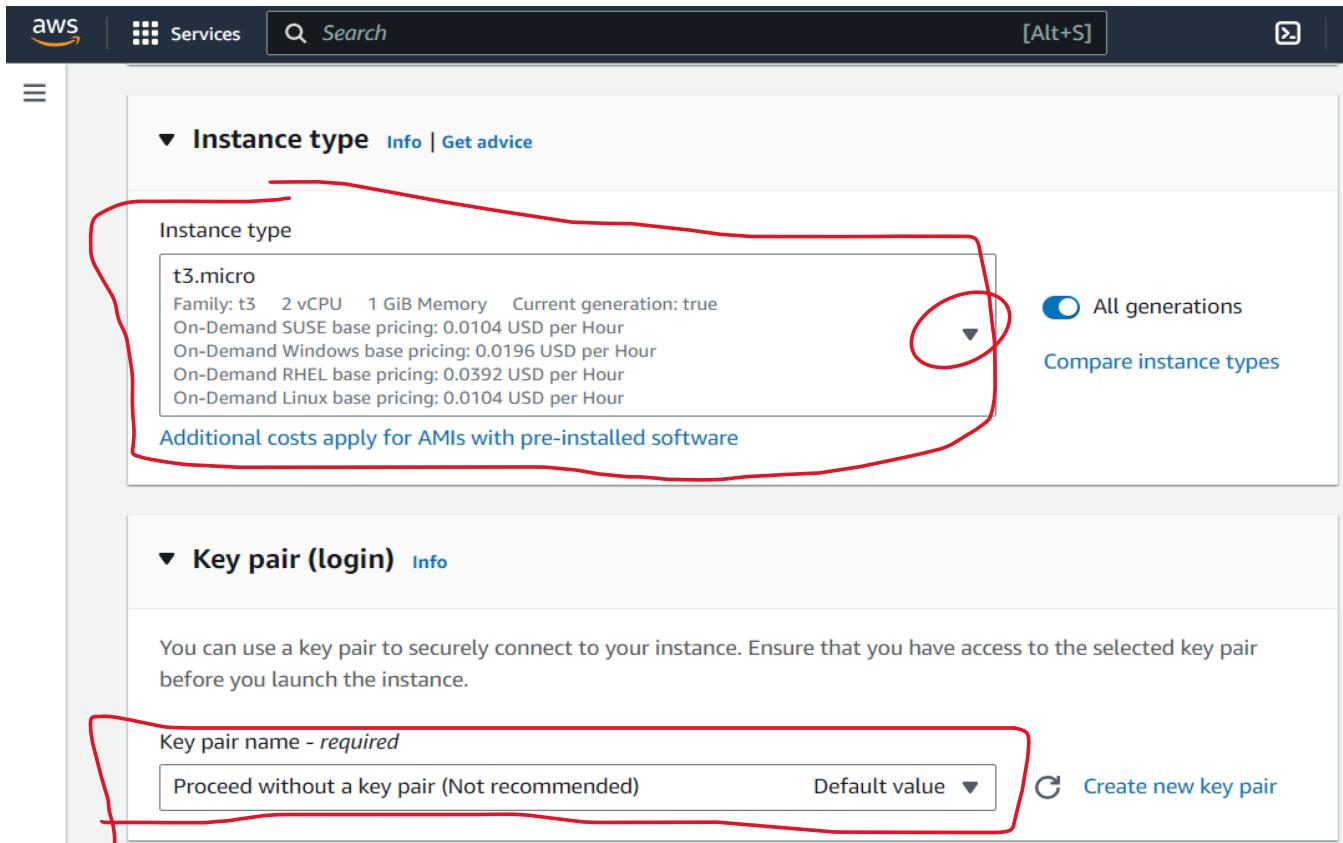
- From the dropdown, select **t3.micro**.

### Step 4: Configuring a key pair

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

In this lab, you do not log in to your instance, so you do not require a key pair.

- In the **Key pair (login)** pane, select **Proceed without a key pair (Not recommended)**.



### Step 5: Configuring the network settings

You use this pane to configure networking settings.

The **VPC** indicates which virtual private cloud (VPC) you want to launch the instance into. You can have multiple VPCs, including different ones for development, testing, and production.

- In the **Network settings** pane, choose **Edit**
- For **VPC - required**, select **Lab VPC( VPC created before)**.
- Still in the **Network settings** pane, configure the Security Group as follows:
  - o **Security group name - required:** Web Server security
  - o **Description:** Security group for my web server

A **security group** acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add *rules* to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

The screenshot shows the AWS Management Console Network settings pane for a new instance. At the top, there's a navigation bar with the AWS logo, Services, a search bar, and a [Alt+S] keyboard shortcut. Below the navigation bar, the 'Network settings' section is open. A large black arrow points to the 'VPC - required' dropdown menu, which contains 'vpc-06e353b922130f758 (Lab VPC)' and '10.0.0.0/16'. Another black arrow points to the 'Create security group' button, which is highlighted with a blue border. A third black arrow points to the 'Security group name - required' input field, which contains 'Web Server security'. A fourth black arrow points to the 'Description' input field, which contains 'Security group for my web server'. The 'Subnet' section shows a subnet named 'subnet-0208d99031572137f' with details: 'Public Subnet 1', 'Owner: 789435219773', 'Availability Zone: us-west-2a', 'Zone type: Availability Zone', and 'IP addresses available: 251 CIDR: 10.0.1.0/24'. There's also a 'Create new subnet' button. The 'Auto-assign public IP' section has 'Enable' selected. A note about additional charges applies when outside of free tier allowance. The 'Firewall (security groups)' section has a note that it's a set of firewall rules controlling traffic to the instance. It includes options to 'Create security group' (selected) or 'Select existing security group'. The 'Security group name - required' field is filled with 'Web Server security'. The 'Description' field is filled with 'Security group for my web server'.

- Under **Inbound security groups rules** select the **Remove**

In this lab, you will not log into your instance using SSH. Removing SSH access will improve the security of the instance.

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type | Info      Protocol | Info      Port range | Info

ssh      TCP      22

Source type | Info      Source | Info      Description - optional | Info

Anywhere      Add CIDR, prefix list or security      e.g. SSH for admin desktop

0.0.0.0/0 X

⚠ 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. X

Add security group rule

► Advanced network configuration

## Step 6: Adding storage

Amazon EC2 stores data on a network-attached virtual disk called Amazon Elastic Block Store (Amazon EBS).

You launch the EC2 instance using a default 8 GiB disk volume. This is your root volume (also known as a boot volume).

- In the **Configure storage** pane, keep the default storage configuration.

Configure storage | Advanced

1x 8 GiB gp3 Type Root volume (Not encrypted)

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

Add new volume

Click refresh to view backup information      Edit

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

## Step 7: Configuring advanced details

- Expand the **Advanced details** pane.
- Select the dropdown for **Termination protection**, then choose **Enable**.

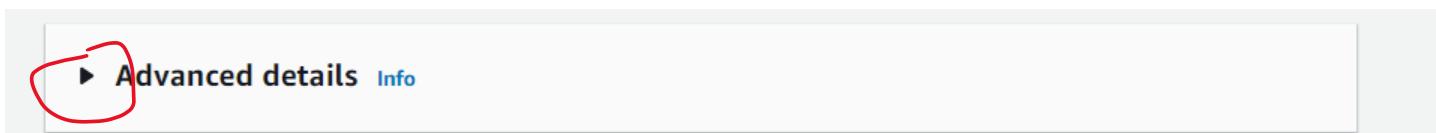
When you launch an instance in Amazon EC2, you have the option of passing user data to the instance. These commands can be used to perform common automated configuration tasks and even run scripts after the instance starts.

- Copy the following commands and paste them into the **User data** text box.

```
#!/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
```

The script does the following:

- o Install an Apache web server (httpd)
- o Configure the web server to automatically start on boot
- o Activate the Web server
- o Create a simple web page



Scroll down to user data



## Step 8: Launching an EC2 instance

Now that you have configured your EC2 instance settings, it is time to launch your instance.

- In the right pane, choose **Launch instance**
- Choose **View all instances**

The instance appears in a **Pending** state, which means it is being launched. It then changes to **Running**, which indicates that the instance has started booting. There will be a short time before you can access the instance.

The instance receives a public DNS name that you can use to contact the instance from the Internet.

- Select the box next to your **Web Server**. The **Details** tab displays detailed information about your instance.

To view more information in the **Details** tab, drag the window divider upward.

Review the information displayed in the **Details**, **Security** and **Networking** tabs.

- Wait for your instance to display the following:

**Note:** Refresh if needed.

- o **Instance State:** Running
- o **Status Checks:** 2/2 checks passed

The screenshot shows the AWS EC2 console interface. On the left, a sidebar navigation bar includes links for EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, and Network & Security. A red arrow points to the 'Instances' link in the sidebar.

The main area is divided into two panes. The top pane is a modal dialog titled 'Summary' containing a 'Cancel' button and an orange 'Launch instance' button, with a red box highlighting the button. Below the modal is a 'Review commands' link. The bottom pane shows the 'Instances (1/1) Info' table. A red box highlights the 'Launch instances' button at the top right of the table header. The table lists one instance: 'My Web Server' (Instance ID: i-02d66bff016414f95), which is currently 'Running'. A red box highlights the 'Running' status. The table also shows the instance type as 't3.micro', status check as '2/2 checks passed', and availability zone as 'us-west-2a'. The public IPv4 DNS is listed as 'ec2-54-212-45-110.us-west-2.compute.amazonaws.com' with a red box highlighting the URL.

The bottom section shows the details for the instance 'i-02d66bff016414f95 (My Web Server)'. The 'Details' tab is selected. The instance summary table includes fields for Instance ID (i-02d66bff016414f95), Public IPv4 address (54.212.45.110), Instance state (Running), Hostname type (IP name: ip-10-0-1-35.us-west-2.compute.internal), Private IP DNS name (ip-10-0-1-35.us-west-2.compute.internal), Instance type (t3.micro), VPC ID (vpc-06e353b922120f758), and AWS Compute Optimizer finding (On-in to AWS Compute Optimizer for recommendations). A red box highlights the Public IPv4 address field.

## Monitor Your Instance

- Select the **Monitoring** tab.

This tab displays Amazon CloudWatch metrics for your instance. Currently, there are not many metrics to display because the instance was recently launched.

You can choose a graph to see an expanded view.

Amazon EC2 sends metrics to Amazon CloudWatch for your EC2 instances. Basic (five-minute) monitoring is enabled by default. You can enable detailed (one-minute) monitoring.

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there's a search bar and filters for 'All states'. Below that, a table lists an instance named 'My Web Server' with details like 'Instance ID: i-02d66bff016414f95', 'Status: Running', 'Type: t3.micro', and 'Last updated: 5 minutes ago'. A red box highlights the 'Monitoring' tab in the navigation bar below the table. The main area displays four metrics: 'CPU utilization (%)', 'Network in (bytes)', 'Network out (bytes)', and 'Network packets in (count)'. Each metric has a time range selector from '1h' to 'Custom' and a 'UTC timezone' dropdown. There are also 'Configure CloudWatch agent' and 'Manage detailed monitoring' buttons.

In the **Actions** menu, select **Monitor and troubleshoot Get Instance Screenshot**.

This shows you what your Amazon EC2 instance console would look like if a screen were attached to it.

The screenshot shows the AWS CloudWatch Metrics interface with the 'Actions' menu open. The 'Actions' menu includes options like 'Connect', 'View details', 'Manage instance state', 'Instance settings', 'Networking', 'Security', 'Image and templates', and 'Monitor and troubleshoot'. A red box highlights the 'Get instance screenshot' option in the 'Actions' menu. The main area shows network metrics for the instance.

Select **Cancel** located at the bottom of the instance screenshot.

## Update Your Security Group and Access the Web Server

When you launched the EC2 instance, you provided a script that installed a web server and created a simple web page. In this task, you will access content from the web server.

- Select the instance by checking the box and select the **Details** tab.
- Copy the **Public IPv4 address** of your instance to your clipboard.
- Open a new tab in your web browser, paste the IP address you just copied, then press **Enter**.
- You are **not** currently able to access your web server because the *security group* is not permitting inbound traffic on port 80, which is used for HTTP web requests. This is a demonstration of using a security group as a firewall to restrict the network traffic that is allowed in and out of an instance.
- To correct this, you will now update the security group to permit web traffic on port 80

The screenshot shows the AWS EC2 Instances page. A single instance is selected, named "my web server" (Instance ID: i-0060a639034f9bb99). The instance is listed as "Running". The "Details" tab is selected, showing the instance summary. The "Public IPv4 address" field is highlighted with a red box, displaying "54.149.235.225 | open address".

- Keep the browser tab open, but return to the **EC2 Management Console** tab.
- In the left navigation pane, select **Security Groups** located under **Network & Security**.
- Select **Web Server security group**.
- Select the **Inbound rules** tab.

The security group currently has no rules.

- Select **Edit inbound rules** then select **Add rule** and configure the rule with the following settings:
  - o **Type:** *HTTP*
  - o **Source:** *Anywhere-IPv4*
  - o Select **Save rules**

Security Groups (1/3) Info

Name	Security group ID	Security group name	VPC ID	Description
-	sg-093347b1e2d2e1800	default	vpc-006f63bb53a0219e4	default VPC security group
-	sg-06ce9d2502a664ee8	default	vpc-01c39a34b521601c2	default VPC security group
<input checked="" type="checkbox"/>	sg-0f4716d660e7837e9	Web Server security group	vpc-006f63bb53a0219e4	Web Server security group

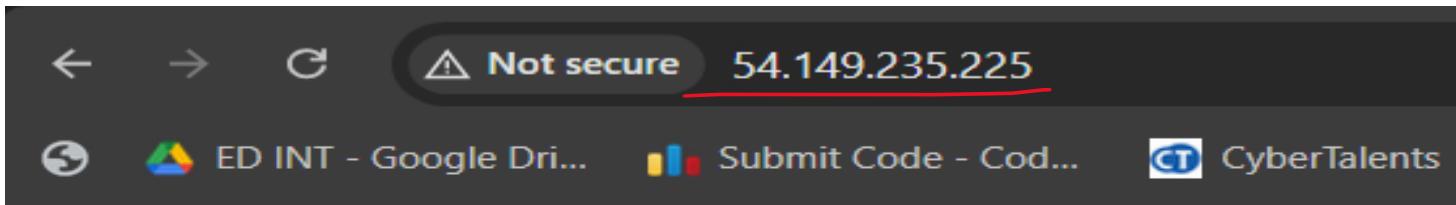
sg-0f4716d660e7837e9 - Web Server security group

Inbound rules (1)

Edit inbound rules

- Return to the web server tab that you previously opened and refresh the page.

You should see the message *Hello From Your Web Server!*



## Hello From Your Web Server!

### Resize Your Instance: Instance Type and EBS Volume

As your needs change, you might find that your instance is over-utilized (too small) or under-utilized (too large). If so, you can change the *instance type*. For example, if a *t3.micro* instance is too small for its workload, you can change it to an *m5.medium* instance. Similarly, you can change the size of a disk.

### Stop Your Instance

Before you can resize an instance, you must *stop* it.

When you stop an instance, it is shut down. There is no charge for a stopped EC2 instance, but the storage charge for attached Amazon EBS volumes remains.

- On the **EC2 Management Console**, in the left navigation pane, select **Instances**.

**My Web Server** should already be selected.

- Select **Instance state > Stop instance**.
- Select **Stop**

Your instance will perform a normal shutdown and then will stop running.

- Wait for the **Instance State** to display: stopped

## Change The Instance Type

- In the **Actions** menu, select **Instance Settings Change Instance Type**, then configure:
  - o **Instance Type: t3.small**
  - o Select **Apply**

When the instance is started again it will be a *t3.small*, which has twice as much memory as a *t3.micro* instance

## Resize the EBS Volume

- In the left navigation menu, select **Volumes** located under **Elastic Block Store**.
- Select the volume by checking the box, and navigate to the **Actions** menu, select **Modify Volume**.

The disk volume currently has a size of 8 GiB. You will now increase the size of this disk.

- Change the size to: 10 **NOTE:** You may be restricted from creating large Amazon EBS volumes in this lab.
- Select **Modify**
- Select **Modify** to confirm and increase the size of the volume.

The screenshot shows the AWS EC2 Volumes page. A modal dialog at the top says "Requested volume modification for volume vol-09be938ada2068dbd. The volume is being modified." Below the dialog, a table lists one volume: "vol-09be938ada2068dbd" (gp3, 8 GiB). The "Actions" menu is open, with "Modify volume" highlighted. The main content area shows the volume details: Volume ID (vol-09be938ada2068dbd), Size (8 GiB), Type (gp3), Volume state (In-use - modifying (0%)), IOPS (3000), Availability Zone (us-west-2a), Created (Thu Sep 12 2024 08:48:50 GMT+0300 (Eastern European Summer Time)), and Volume status (Okay). Throughput is listed as 125. The "Details" tab is selected.

## Start the Resized Instance

You will now start the instance again, which will now have more memory and more disk space.

- In left navigation pane, select **Instances**.
- Select the **Web Server** instance by checking the box, then navigate to **Instance state > Start instance**.

You have successfully resized your Amazon EC2 Instance. In this task you changed your instance type from *t3.micro* to *t3.small*. You also modified your root disk volume from 8 GiB to 10 GiB.

## Test Termination Protection

You can delete your instance when you no longer need it. This is referred to as *terminating* your instance.

You cannot connect to or restart an instance after it has been terminated.

In this task, you will learn how to use *termination protection*.

- In left navigation pane, select **Instances**.
- Select the **Web Server** instance by checking the box and navigate to the top and select **Instance state** menu, select **Terminate instance**.

Note: There is a message that says: *On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.* It will ask if you are sure that you want to terminate the instance. You will be able to select the **Terminate** button.

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
my web server	i-0060a639034f9bb99	Running	t3.small	Initializing	View alarms +	us-west-2a

Note: You will notice that the instance did not terminate and 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.

- In the **Actions** menu, select **Instance settings Change termination protection**.
- Uncheck **Enable** followed by **Save**

You can now terminate the instance.

- In the **Actions** menu, select **Instance State Terminate instance**.
- Select **Terminate**

You have successfully tested termination protection and terminated your instance

Instances (1/1) Info

Last updated 3 minutes ago

Actions ▲

- Connect
- View details
- Manage instance state
- Instance settings ▶
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

Change termination protection

And finally thank you for your time

Mohamed mourad

Mohamed Mouradps | LinkedIn