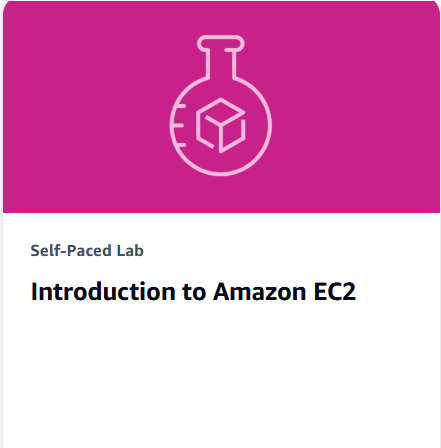
**Introduction to Amazon EC2**

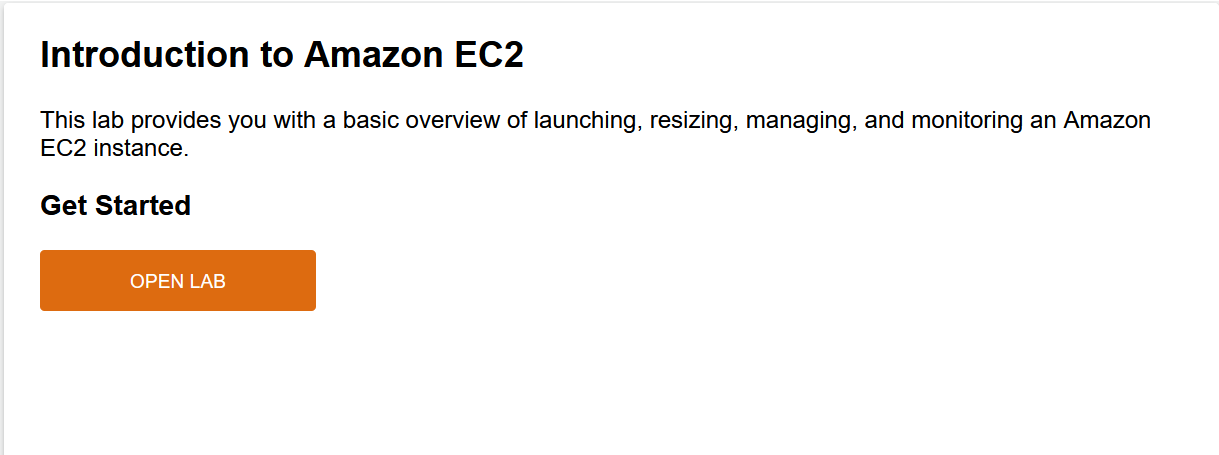
**Lab Topics**

* [Lab overview](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#lab-overview)
* [Start lab](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#start-lab)
* [Task 1: Launch Our Amazon EC2 Instance](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#task-1-launch-your-amazon-ec2-instance)
* [Task 2: Monitor Our Instance](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#task-2-monitor-your-instance)
* [Task 3: Update Our Security Group and Access the Web Server](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#task-3-update-your-security-group-and-access-the-web-server)
* [Task 4: Resize Our Instance: Instance Type and EBS Volume](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#task-4-resize-your-instance-instance-type-and-ebs-volume)
* [Task 5: Test Termination Protection](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#task-5-test-termination-protection)
* [Conclusion](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#conclusion)
* [End lab](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-200%3A1.3.14-416f4f80/en-US#end-lab)

**Lab overview**

This lab provides us with a basic overview of launching, resizing, managing, and monitoring an Amazon EC2 instance. **Amazon Elastic Compute Cloud (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 us to obtain and configure capacity with minimal friction. It provides us with complete control of our computing resources and lets we run on Amazon’s proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing us to quickly scale capacity, both up and down, as our computing requirements change.

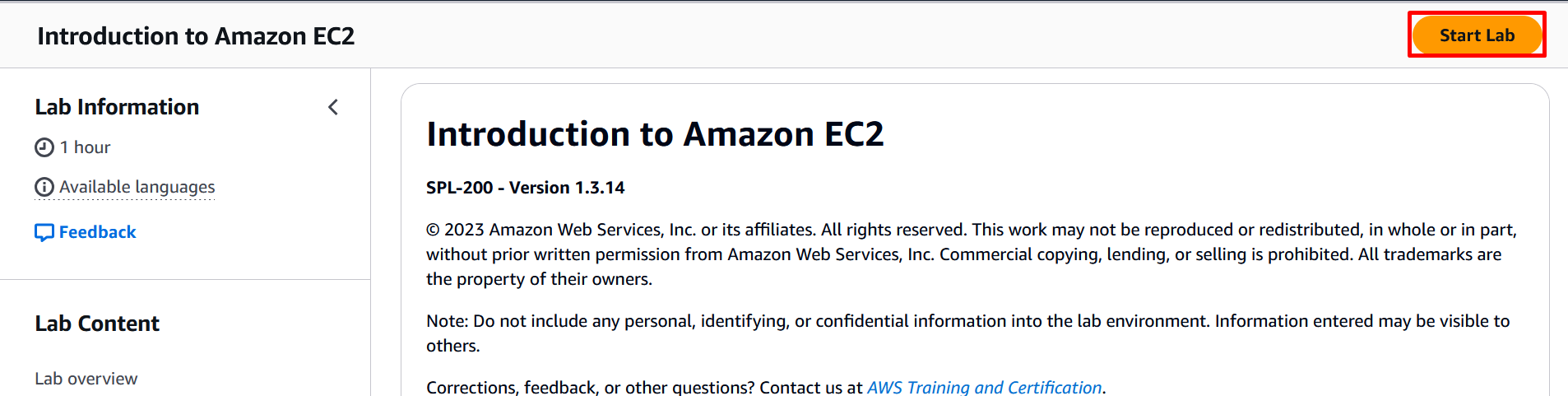
**Objectives**

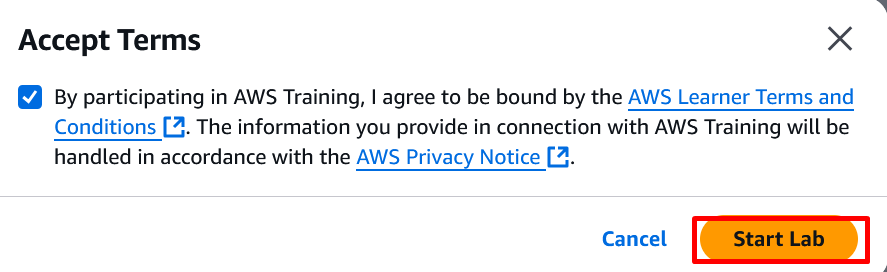
By this lab, we will be able to do the following:

* Launch a web server with termination protection enabled.
* Monitor Our EC2 instance.
* Modify the security group that our web server is using to allow HTTP access.
* Resize our Amazon EC2 instance to scale.
* Test termination protection.
* Terminate our EC2 instance.

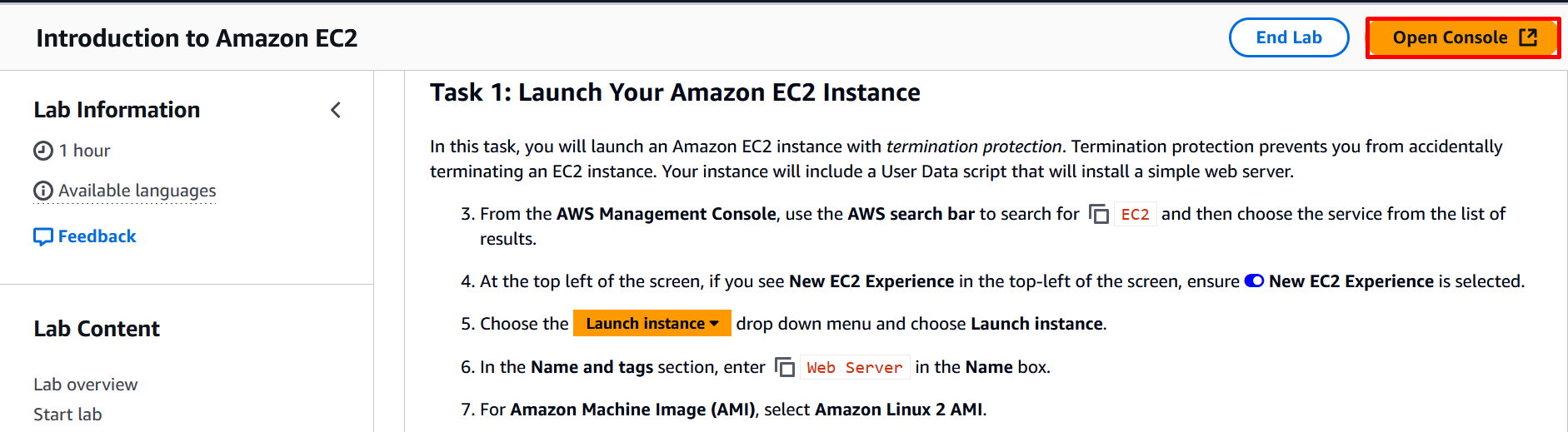
**Start lab**

1. To launch the lab, at the top of the page, click **Start lab**. We must wait for the provisioned AWS services to be ready before we can continue.

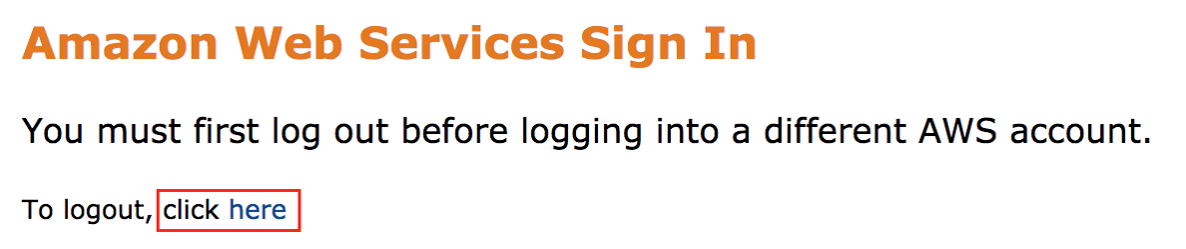




1. To open the lab, click **Open Console**. We are automatically signed in to the AWS Management Console in a new web browser tab.



If we see the message, **we must first log out before logging into a different AWS account:**

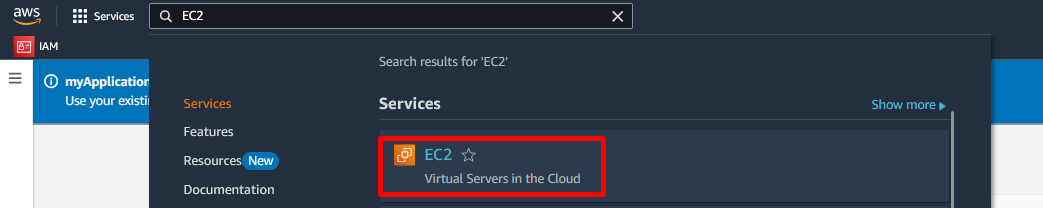


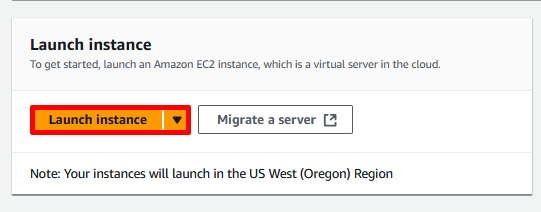
* Choose the **click here** link.
* Close our **Amazon Web Services Sign In** web browser tab and return to the initial lab page.
* Choose and click **Open Console** again.

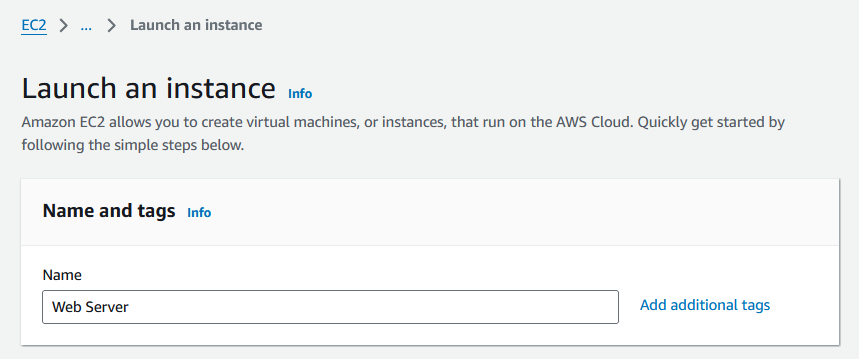
**Task 1: Launch Our Amazon EC2 Instance**

In this task, we will launch an Amazon EC2 instance with *termination protection*. Termination protection prevents us from accidentally terminating an EC2 instance. We instance will include a User Data script that will install a simple web server.

* 1. From the **AWS Management Console**, use the **AWS search bar** to search for **EC2** and then choose the service from the list of results.



1. At the top left of the screen, if we see **New EC2 Experience** in the top-left of the screen, ensure **New EC2 Experience** is selected.
2. Choose the **Launch instance** dropdown menu and click **Launch instance**.  
     
    
3. In the **Name and tags** section, enter **Web Server** in the **Name** box.

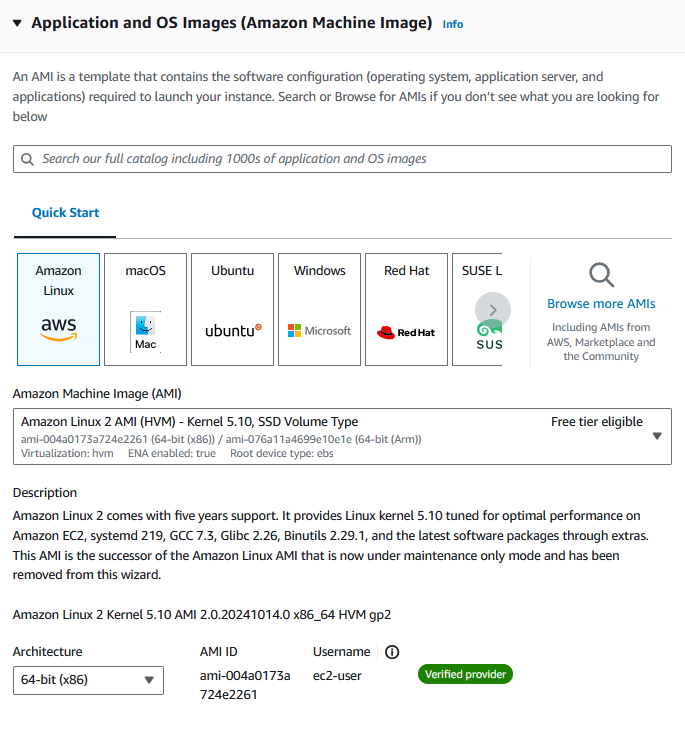


1. For **Amazon Machine Image (AMI)**, select **Amazon Linux 2 AMI**.

This lab will only work with an Amazon Linux 2 AMI. An **Amazon Machine Image (AMI)** provides the information required to launch an instance, which is a virtual server in the cloud. An AMI includes:

* 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. We can also create our own AMI or select an AMI from the AWS Marketplace, an online store where we can sell or buy software that runs on AWS.



1. In the **Instance Type** section, choose the **Instance type** dropdown menu and click **t3.micro**.

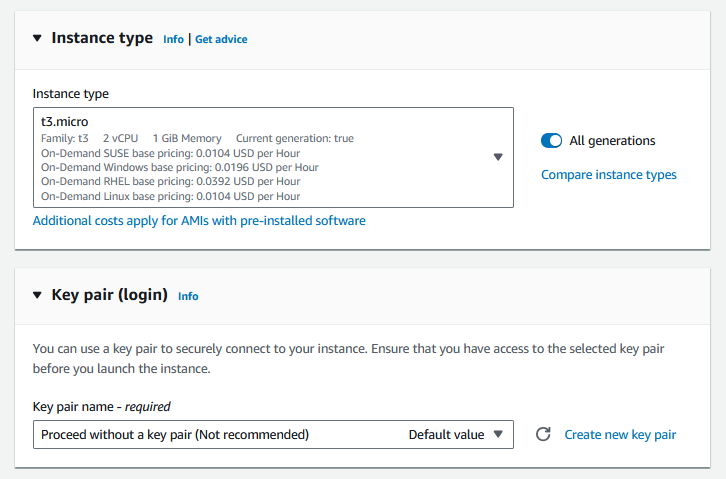
Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give us the flexibility to choose the appropriate mix of resources for our applications. Each instance type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

A **t3.micro** instance type has 2 virtual CPUs and 1 GiB of memory.

1. In the **Key pair (login)** section, locate the **Key pair name** dropdown menu and click **Proceed without a key pair (Not recommended)**.

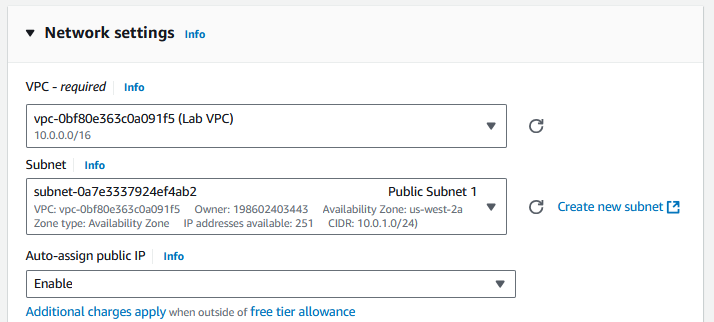
Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. To log in to our instance, we must create a key pair, specify the name of the key pair when we launch the instance, and provide the private key when we connect to the instance.

In this lab we will not log into our instance, so we do not require a key pair.



1. In the **Network settings** section, click the **Edit** button. Make the following selections:

* VPC: Choose the VPC with the name that contains **Lab VPC**
* Subnet: Choose the Subnet with the name that contains **Public Subnet 1**



The **Network** indicates which Virtual Private Cloud (VPC) we wish to launch the instance into. We can have multiple networks, such as different ones for development, testing and production.

The Lab VPC was created using a CloudFormation template during the setup process of our lab. This VPC includes two public subnets in two different Availability Zones.

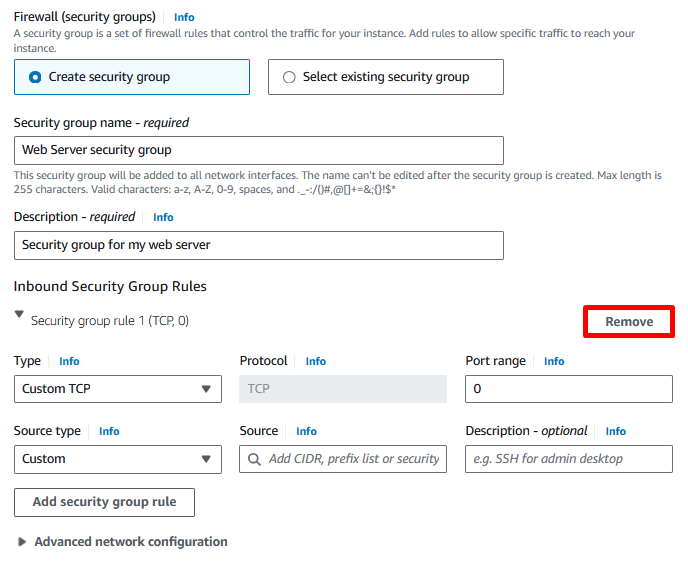
1. In the **Firewall (security groups)** section, click **Create security group**

* Security group name = **Web Server security group**
* Description = **Security group for my web server**

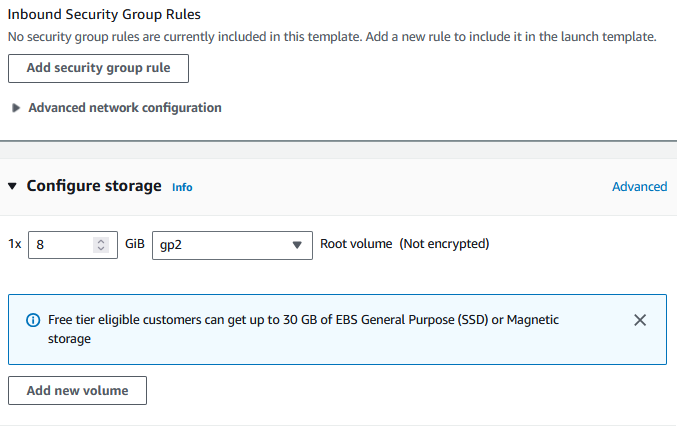
A **security group** acts as a virtual firewall that controls the traffic for one or more instances. When we launch an instance, we associate one or more security groups with the instance. We add *rules* to each security group that allow traffic to or from its associated instances. We can modify the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

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

1. Choose and click the **Remove** button to remove the existing SSH rule. We should have no security group rules.

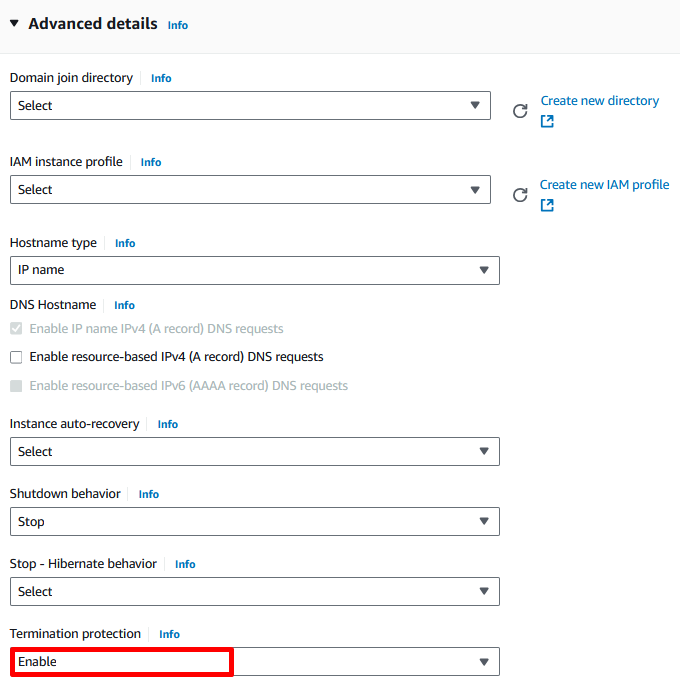


1. The **Configure storage** section default choices can be left alone.



Amazon EC2 stores data on a network-attached virtual disk called *Elastic Block Store*. We will launch the Amazon EC2 instance using a default 8 GiB disk volume. This will be our root volume (also known as a ‘boot’ volume).

1. Expand the **Advanced details** section. Scroll down to the **Termination protection** dropdown menu and set to **Enable**.



When an Amazon EC2 instance is no longer required, it can be *terminated*, which means that the instance is stopped and its resources are released. A terminated instance cannot be started again. If we want to prevent the instance from being accidentally terminated, we can enable *termination protection* for the instance, which prevents it from being terminated.

1. Scroll all the way to the bottom until we see a field for **User data**.

When we launch an instance, we can pass *user data* to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. Our instance is running Amazon Linux, so we will provide a *shell script* that will run when the instance starts.

Copy the following text and paste it into the **User data** field:

#!/bin/bash

yum -y install httpd

systemctl enable httpd

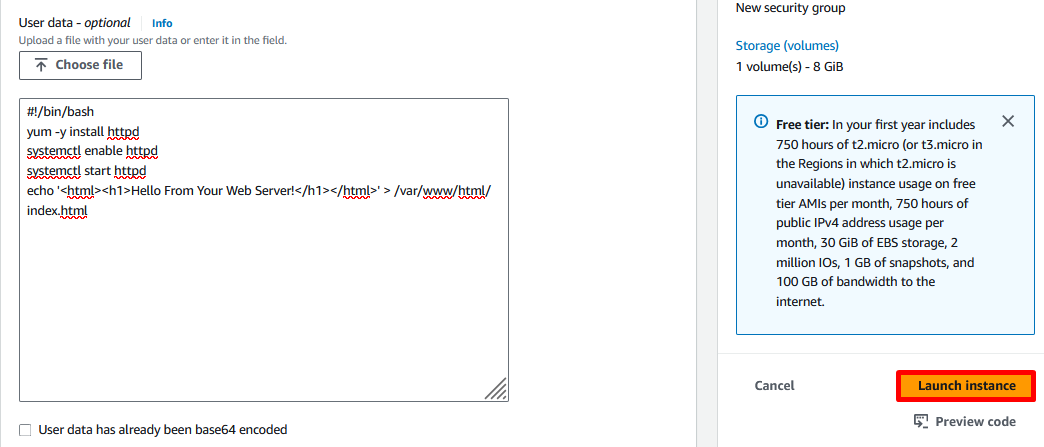
systemctl start httpd

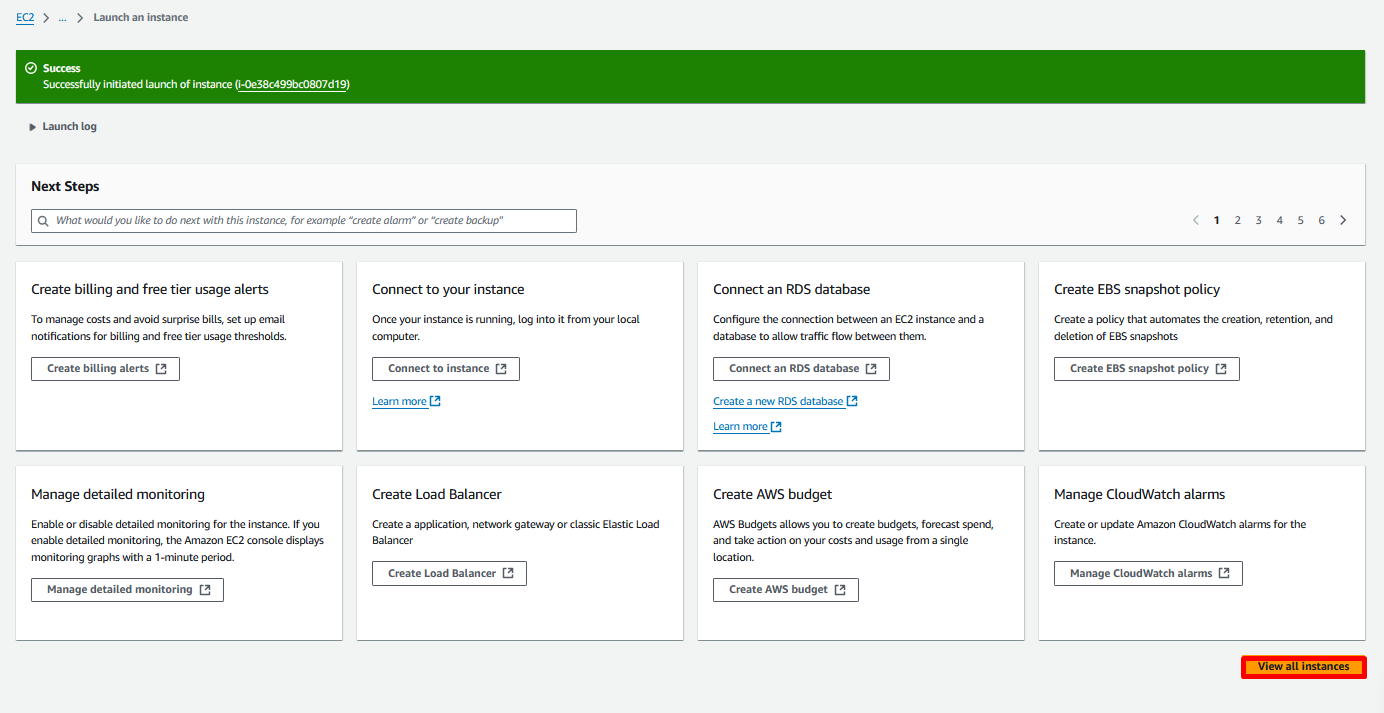
echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html

The script will:

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

1. Choose and click **Launch instance**.



After successful launch instance, we see the following message:  
  


1. Choose and click **View All Instances**. The instance might appear in a **pending** state, which means it is being launched. Then, it will change to **running**, which indicates that the instance has started booting. When creating a new instance, there will usually be a short time before we can access the instance.
2. Wait for our instance to display the following:

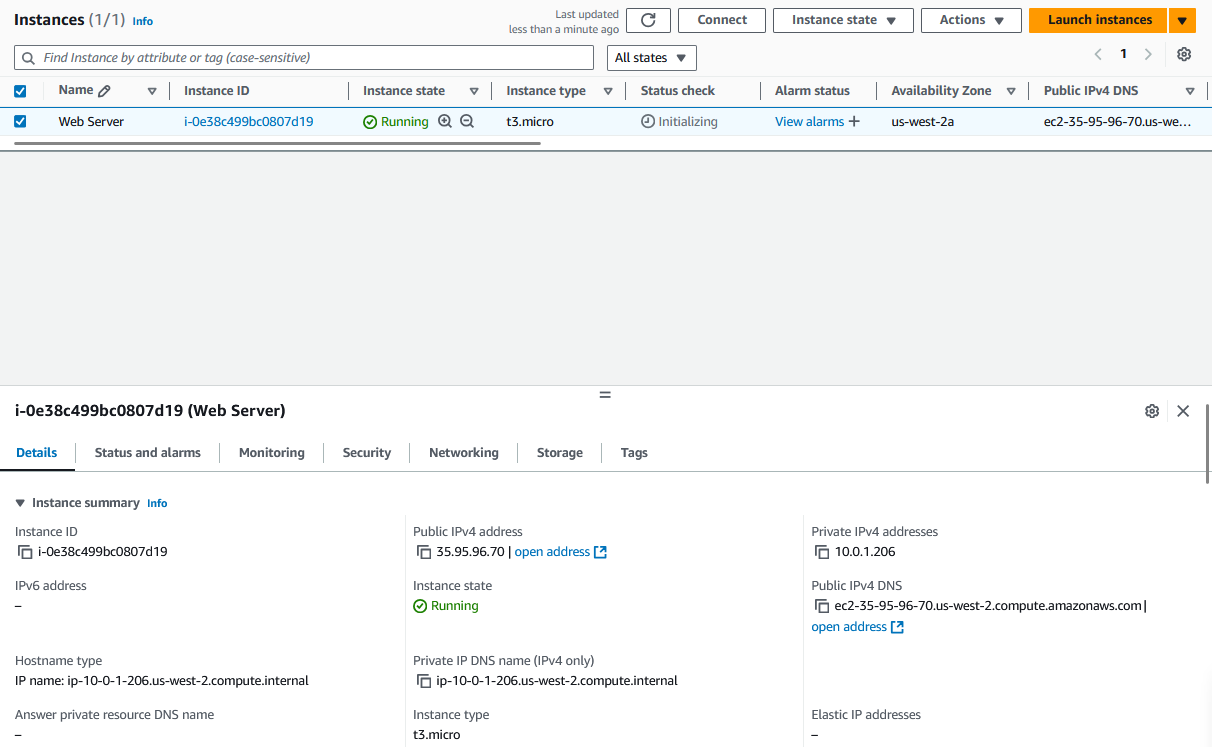
* **Instance state:** Running .
* **Status check:** 2/2 checks passed .

Periodically refresh the page if we don’t see a change in the Instance state or Status check values.

Select our newly-created **Web Server** and the **Details** tab displays detailed information about our instance.

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

Review the information displayed in the **Details** tab. It includes information about the instance type, security settings, network settings, and more. The instance receives a *Public IPv4 DNS* name that we can use to communicate with the instance from the Internet.  
  
**Congratulations!** We have successfully launched our first Amazon EC2 instance.



**Task 2: Monitor Our Instance**

Monitoring is an important part of maintaining the reliability, availability, and performance of our Amazon Elastic Compute Cloud (Amazon EC2) instances and our AWS solutions.

* 1. Select the **Status checks** tab.

With instance status monitoring, we can quickly determine whether Amazon EC2 has detected any problems that might prevent our instances from running applications. Amazon EC2 performs automated checks on every running EC2 instance to identify hardware and software issues.

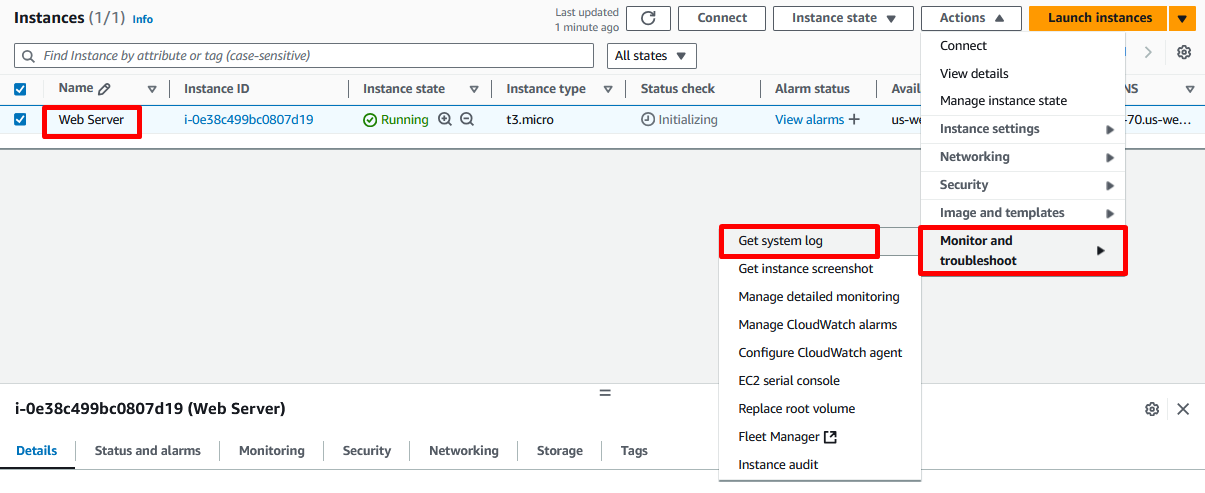
**Noted** both the **System reachability** and **Instance reachability** checks have passed.

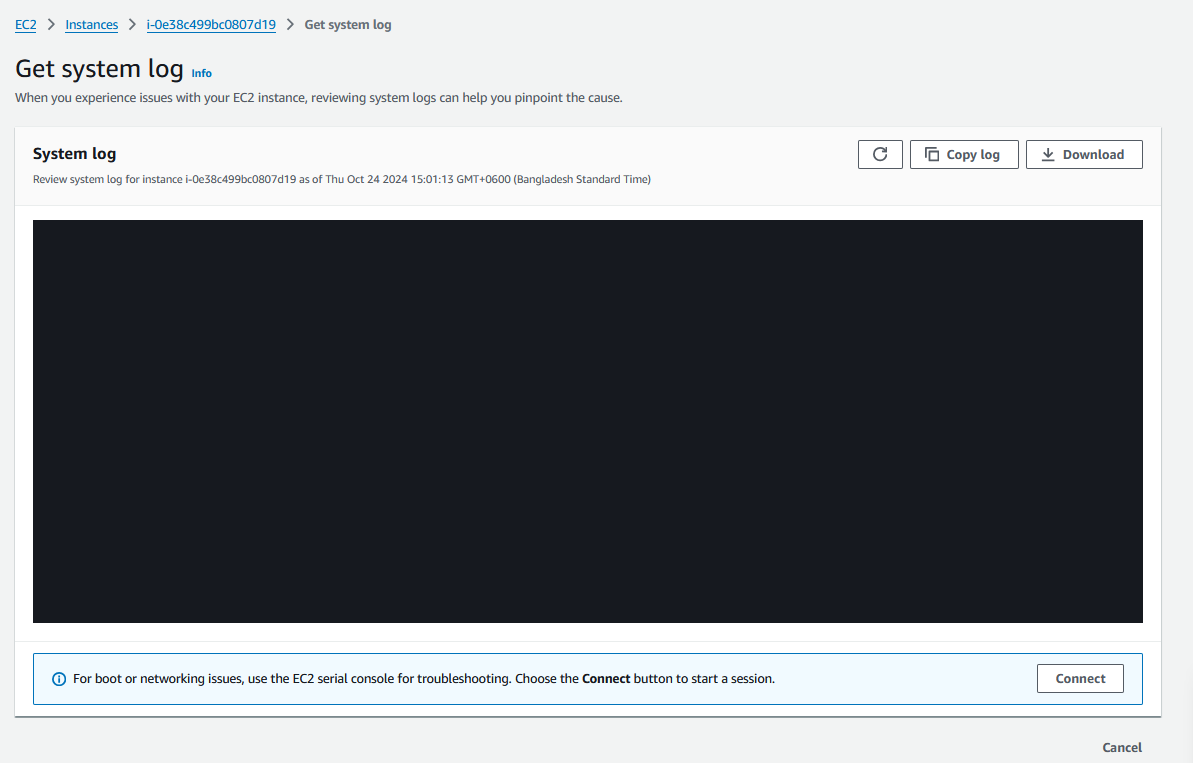
* 1. Select the **Monitoring** tab.

This tab displays CloudWatch metrics for our instance. Currently, there are not many metrics to display because the instance was recently launched. We can choose a graph to see an expanded view.

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

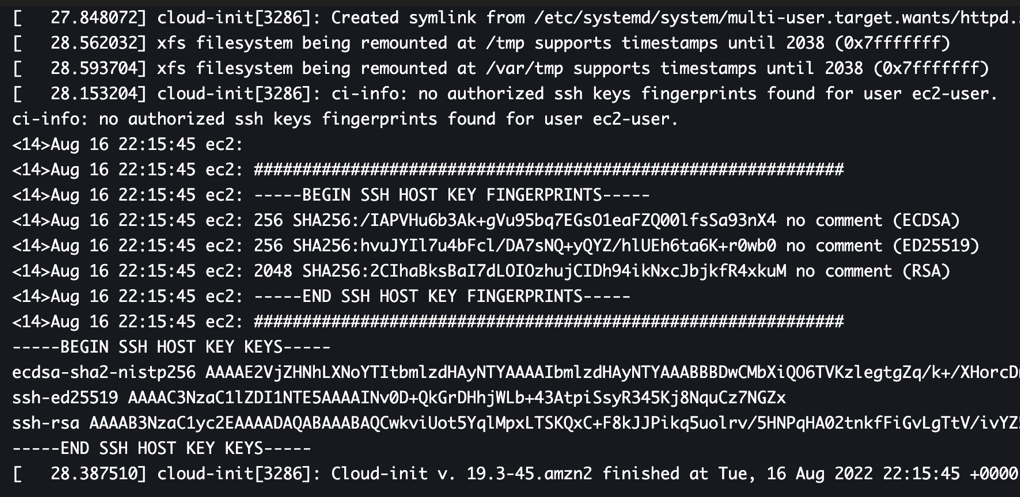
* 1. Select the **Actions** menu (in the upper right of the console), select **Monitor and troubleshoot** and then select **Get system log**.



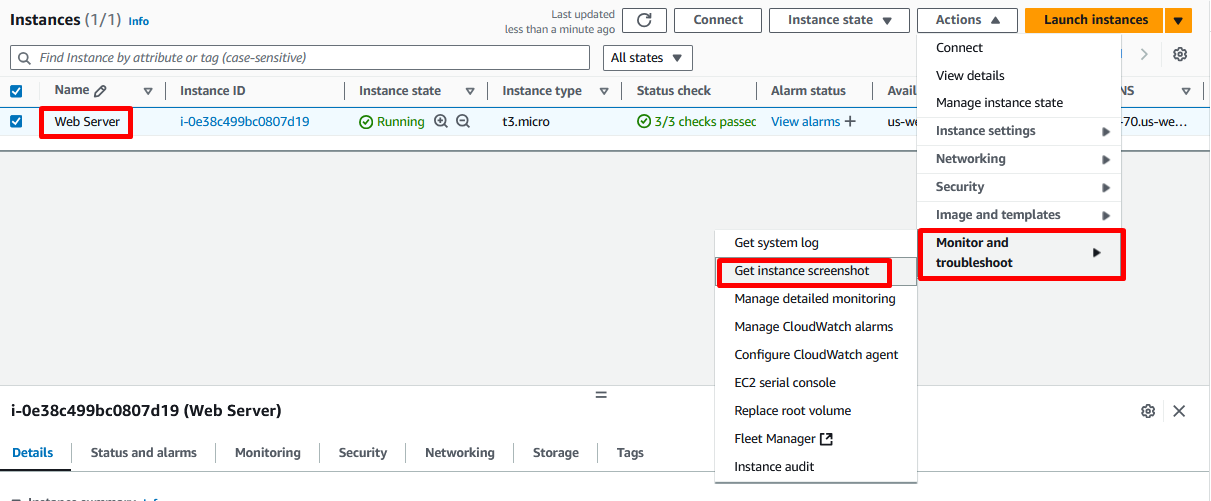
  
  
**Noted** If we do not see a system log, wait a couple of minutes and refresh the log screen until it appears.

The System Log displays the console output of the instance, which is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before it’s SSH daemon can be started.

**System log output example:**

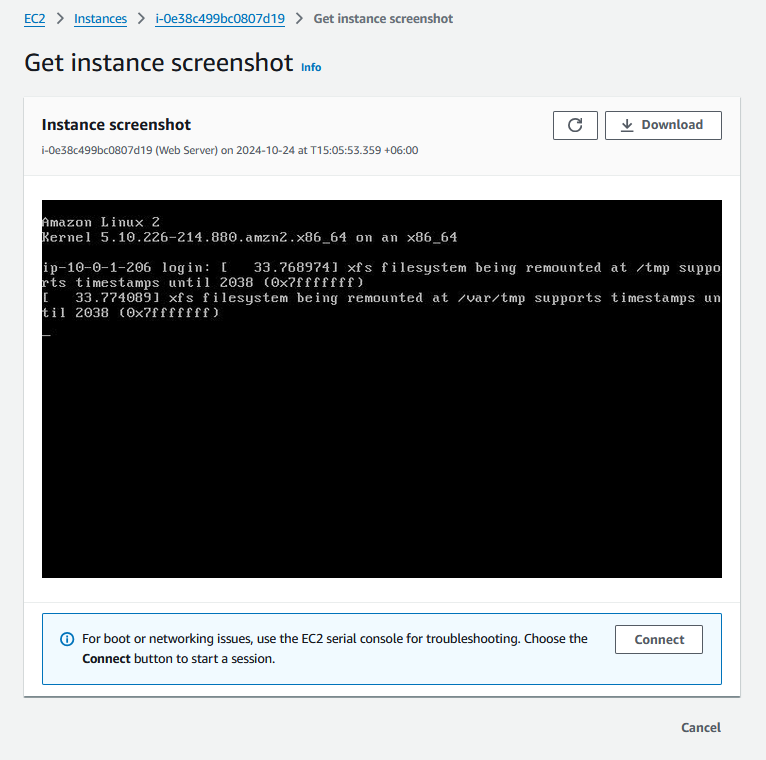


* 1. Scroll through the output and see that the httpd package was installed from the **user data** that we added when we created the instance.
  2. Scroll down to the bottom of the browser window and select **Cancel**.
  3. Select the **Web Server**, then select the **Actions** menu, select **Monitor and troubleshoot** and then select **Get instance screenshot**.



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

If we are unable to reach our instance via SSH or RDP, we can capture a screenshot of our instance and view it as an image. This provides visibility as to the status of the instance, and allows for quicker troubleshooting.



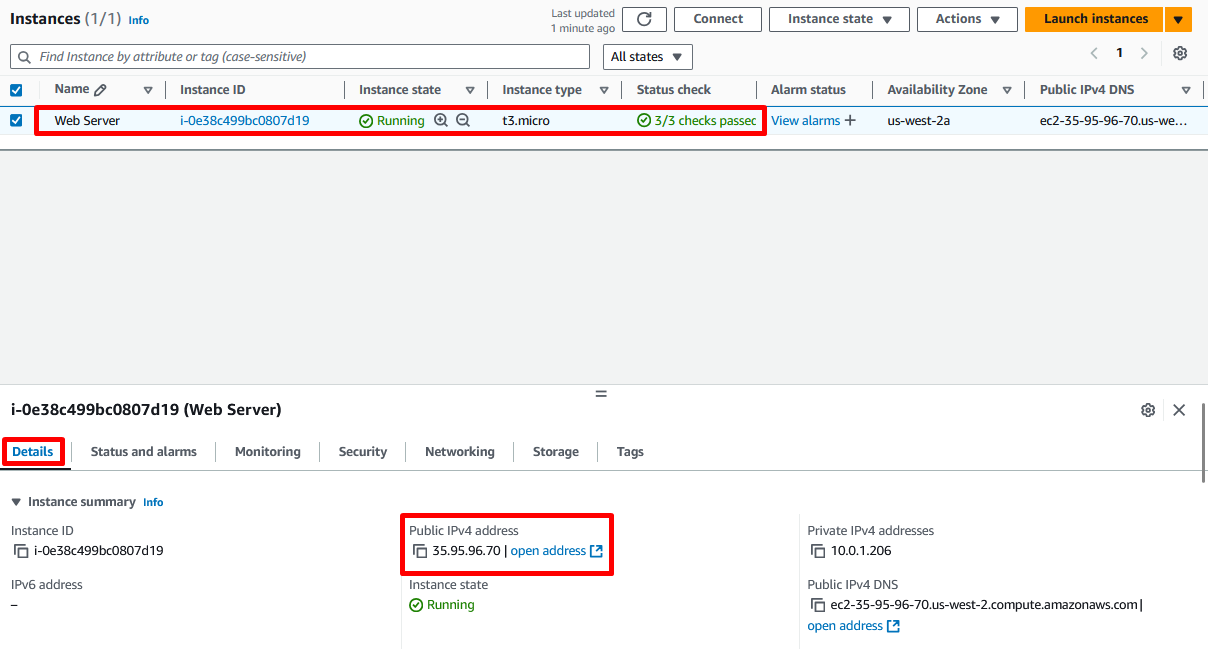
* 1. Scroll down to the bottom of the browser window and select **Cancel**.

**Congratulations!** We have explored several ways to monitor our instance.

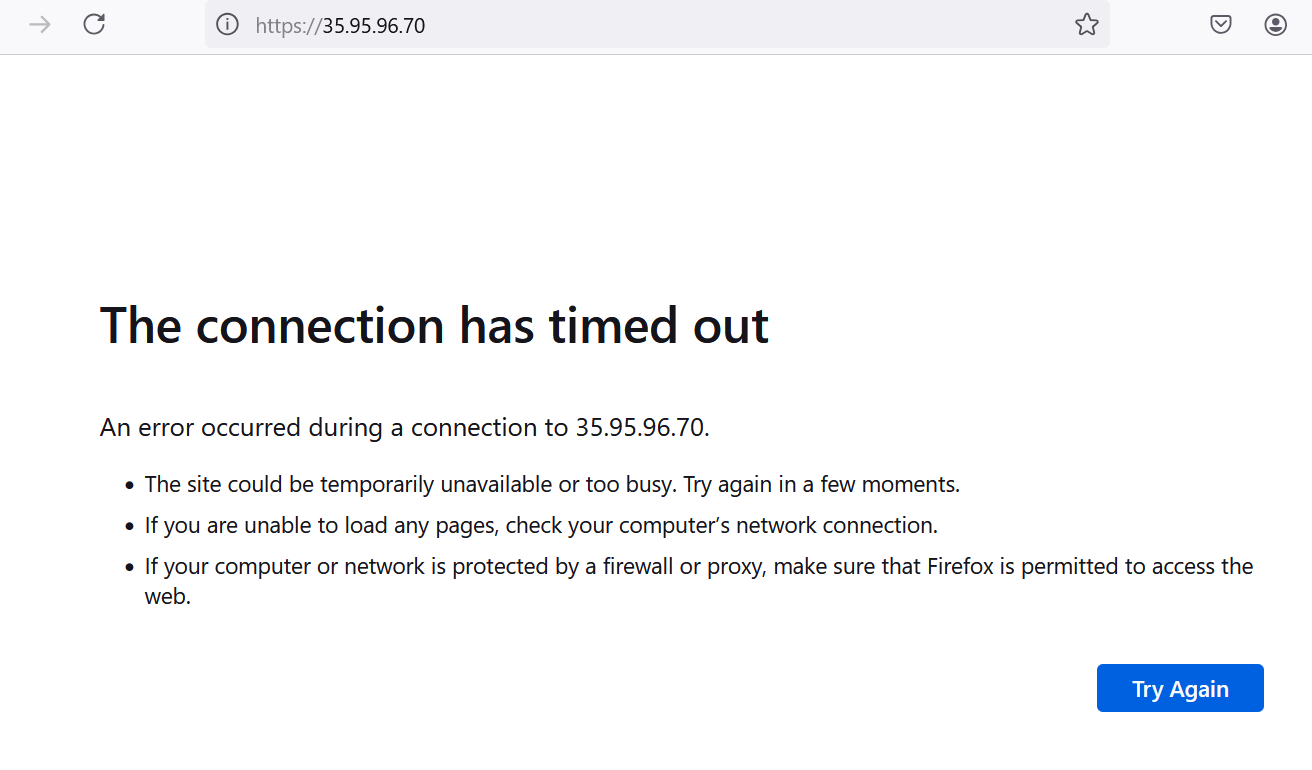
**Task 3: Update Our Security Group and Access the Web Server**

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

1. Select the **Web Server**, then choose the **Details** tab.

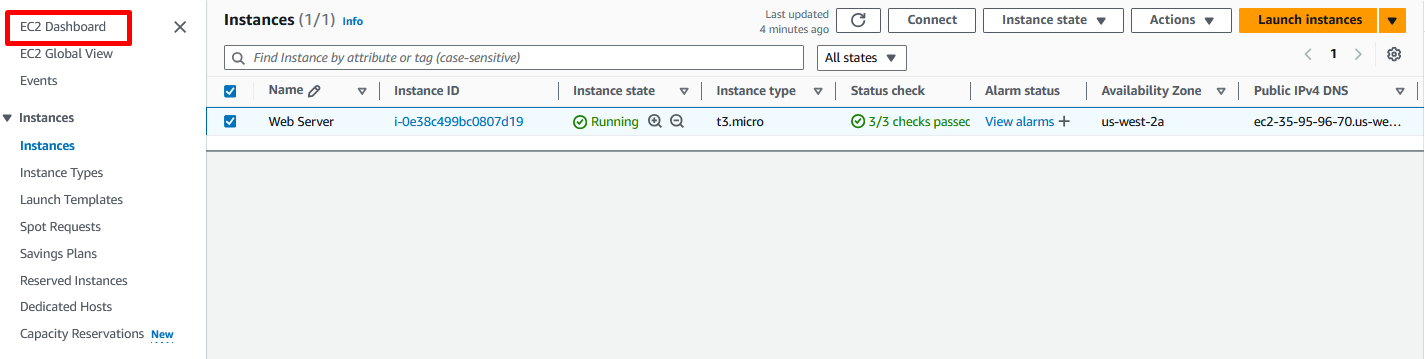


1. Copy the **Public IPv4 address** of our instance to our clipboard.
2. Open a new tab in our web browser, type **http://** in the browser and paste the IP address we just copied, then press **Enter**.

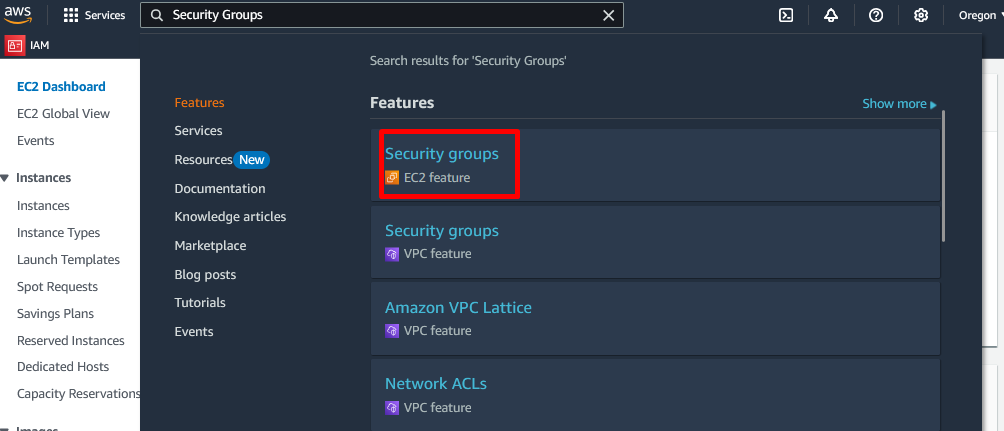


Now we see that, we are **not** currently able to access our web server because the **security group** is not permitting inbound traffic on port 80, which is used for HTTP web requests. This is a demonstration of using a security group as a firewall to restrict the network traffic that is allowed in and out of an instance. To correct this, now we will update the security group to permit web traffic on port 80.

1. Now we go to the **EC2 Dashboard** menu.



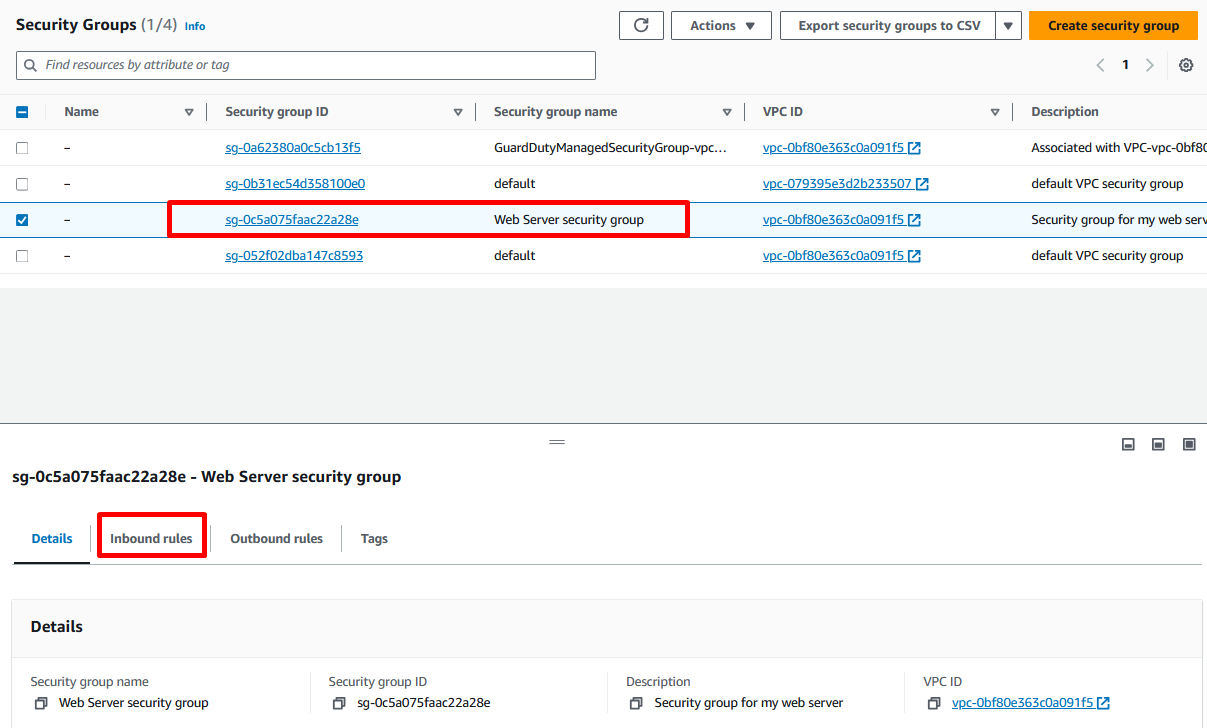
1. In the left navigation pane, select **Security Groups**.



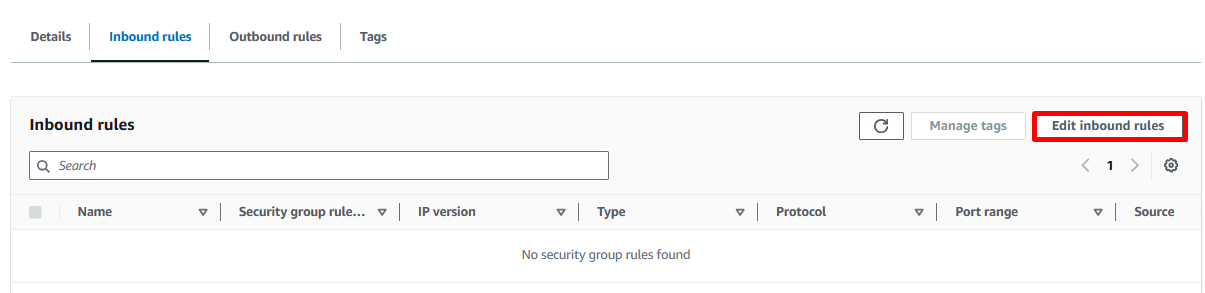
1. Select the **Security group ID** with the Security group name **Web Server security group**.

The security group currently has no rules.

1. Choose the **Inbound rules** tab.



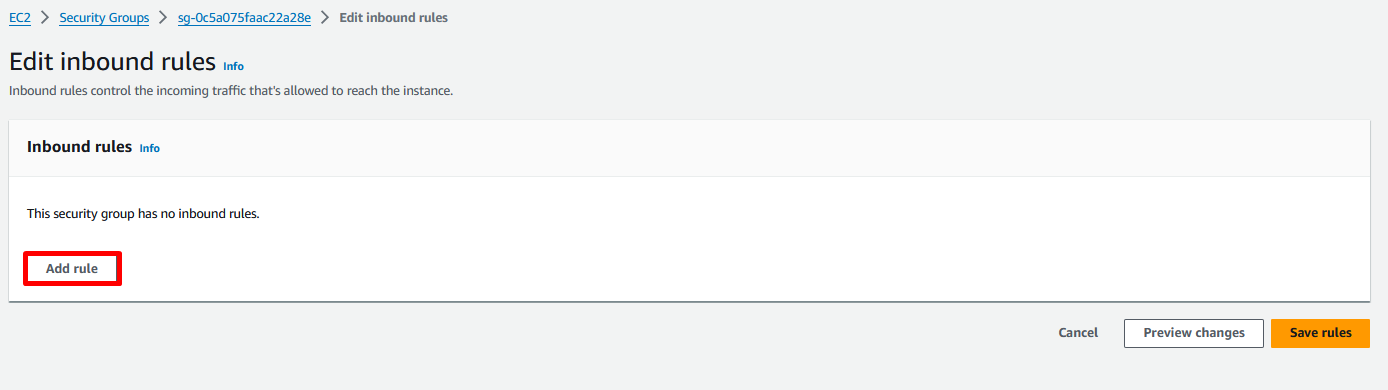
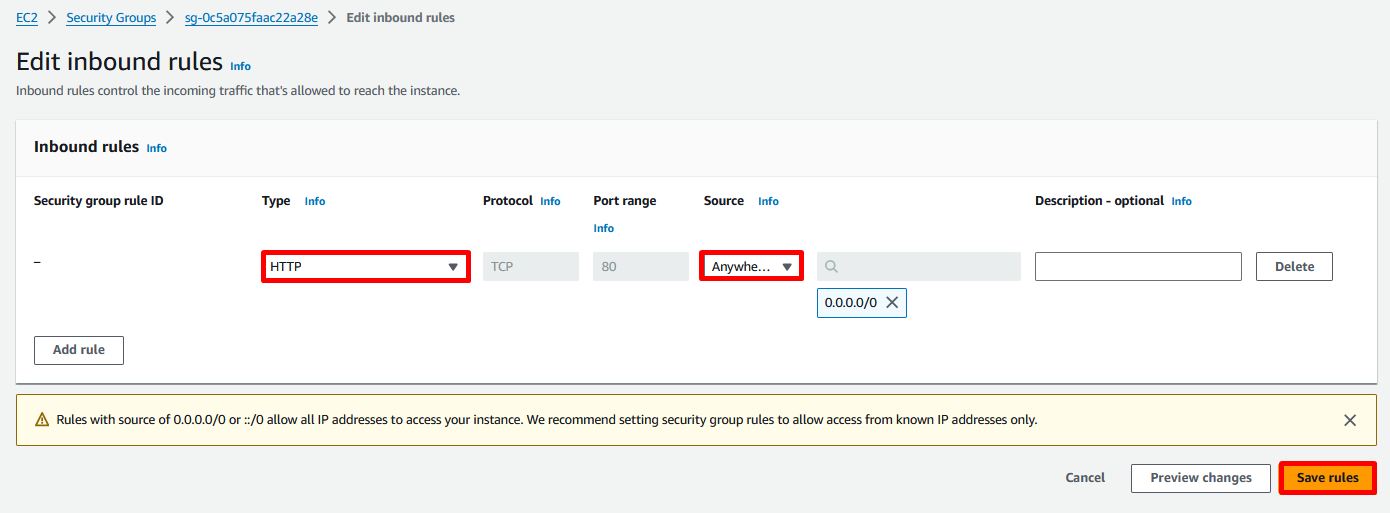
1. Choose and click **Edit inbound rules**.



1. Choose **Add rule** then configure:

* **Type:** HTTP
* **Source:** Anywhere-IPv4

1. Choose and click **Save rules**.

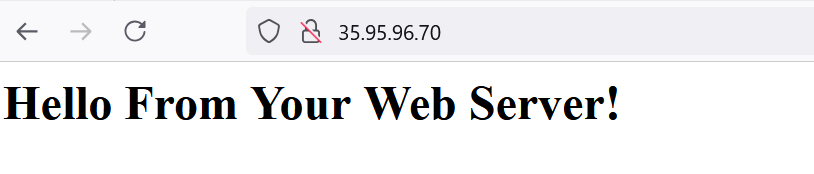
  
  


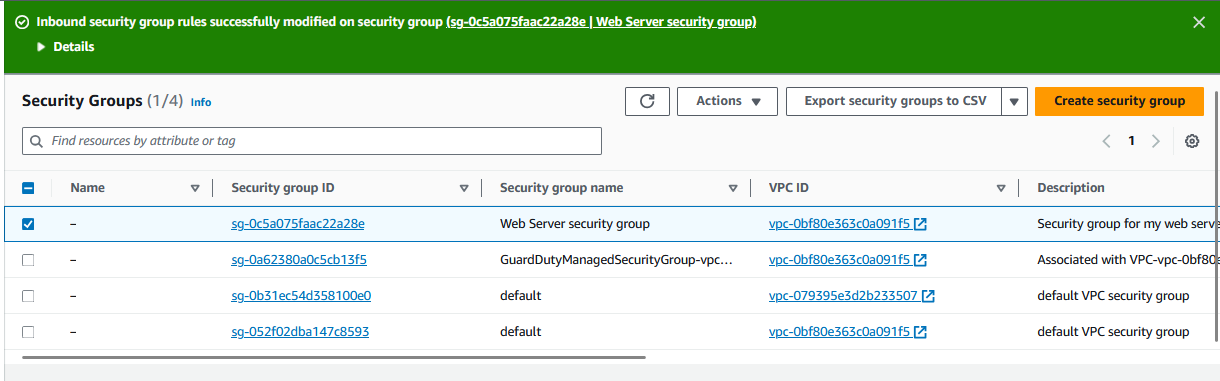
The new Inbound HTTP rule will create an entry for both IPV4 IP address (0.0.0.0/0) as well as IPV6 IP address (::/0).

**Noted** using “Anywhere”, or more specifically, using 0.0.0.0/0 or ::/0 is not a recommended best practice for production workloads.

1. Return to the web server tab that we previously opened and refresh the page.

**Expected output:**





Inbound security group rules successfully modified on security group message is displayed on top of the screen.

**Congratulations!** We have successfully modified our security group to permit HTTP traffic into our Amazon EC2 Instance.

**Task 4: Resize Our Instance: Instance Type and EBS Volume**

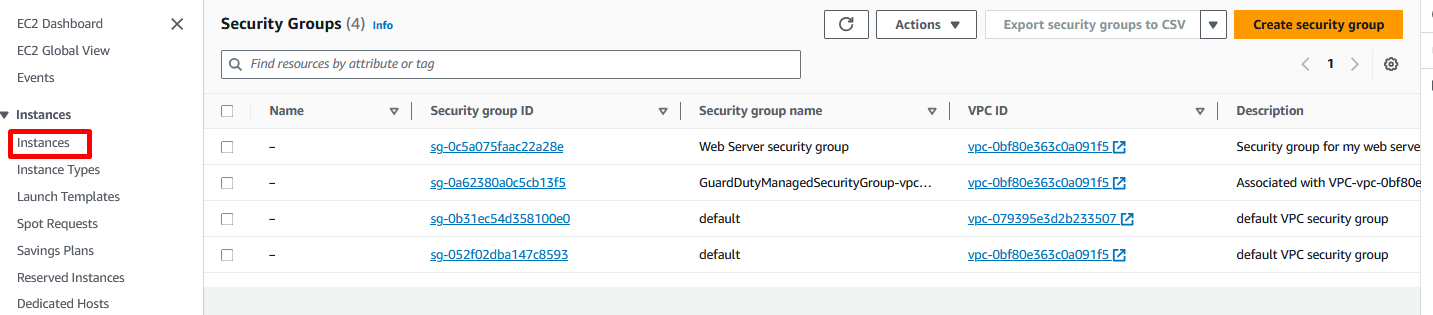
As our needs change, we might find that our instance is over-utilized (too small) or under-utilized (too large). If so, we can change the *instance type*. For example, if a *t3.micro* instance is too small for its workload, we can change it to a *t3.small* instance. Similarly, we can change the size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

**Stop Our Instance**

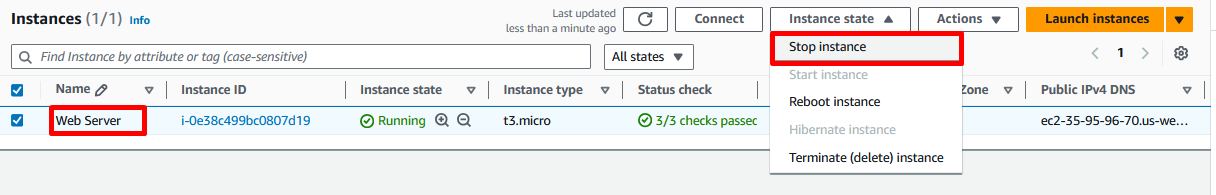
Before we can resize an instance, we must **stop** it.

When we **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.

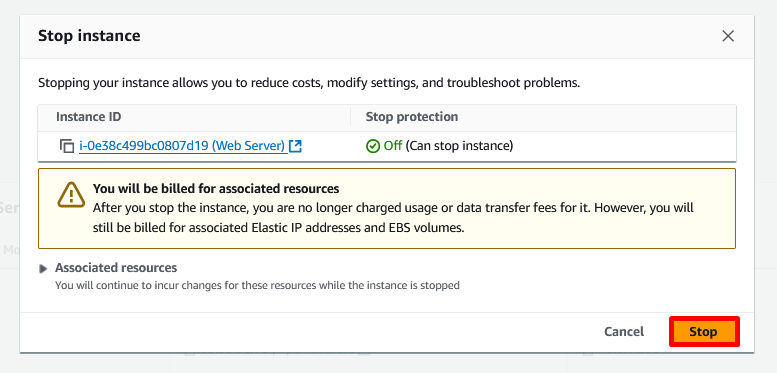
1. On the **EC2 Management Console**, in the left navigation pane, choose **Instances**.



1. If it is not already selected, select the **Web Server**.
2. Select **Instance state** menu, then **Stop instance**.

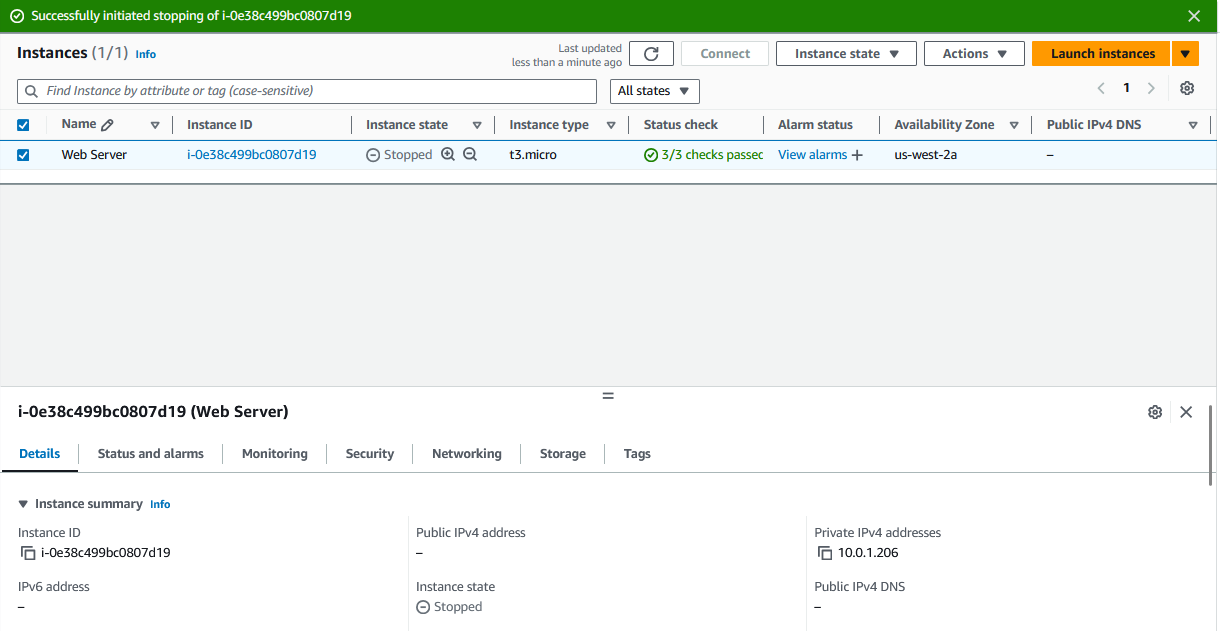


1. On the **Stop instance?** Pop-up window, click **Stop**.



Now, instance will perform a normal shutdown and then it will stop running. This may take a few minutes.

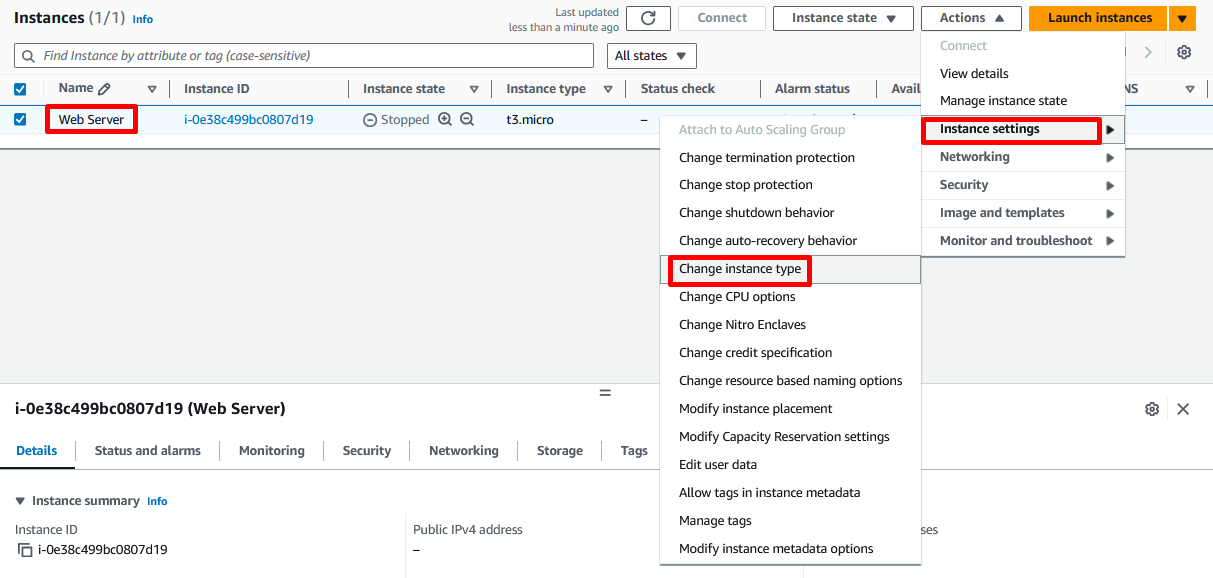
1. Wait for the **Instance State** to display: **Stopped**.



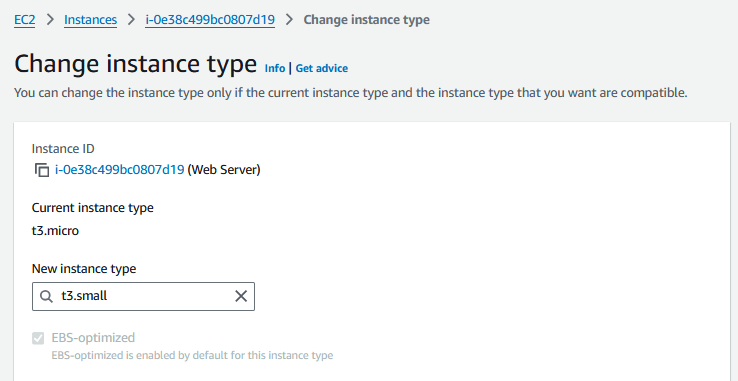
Successfully initiated stopping message is displayed on top of the screen.

**Change the Instance Type**

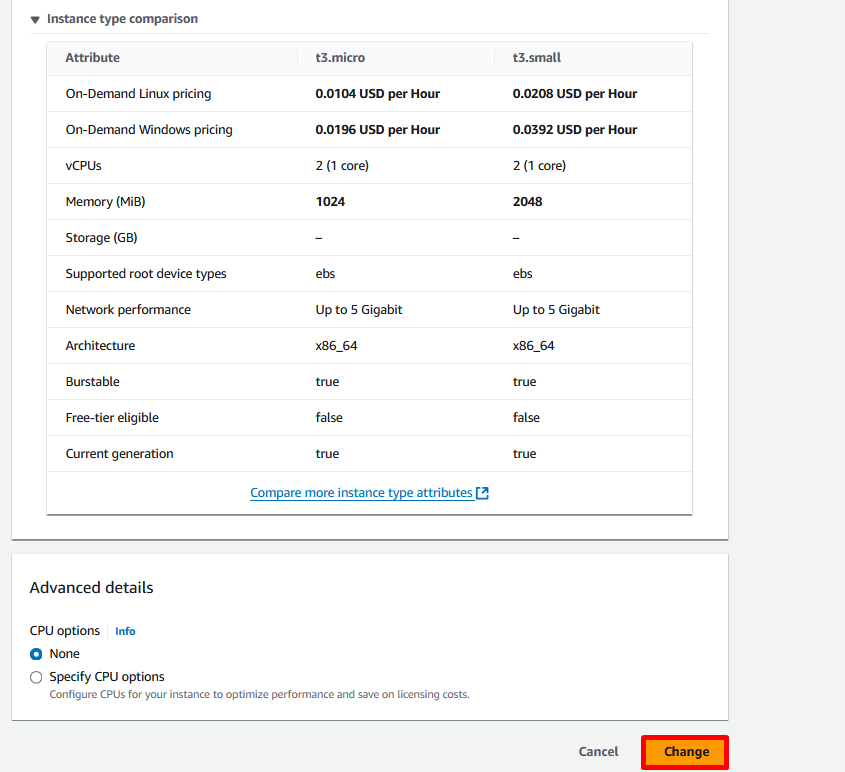
1. If it is not already selected, select the **Web Server**.
2. Select the **Actions** menu, select **Instance settings** and **Change instance type**, then configure:



* **Instance type:** *t3.small*



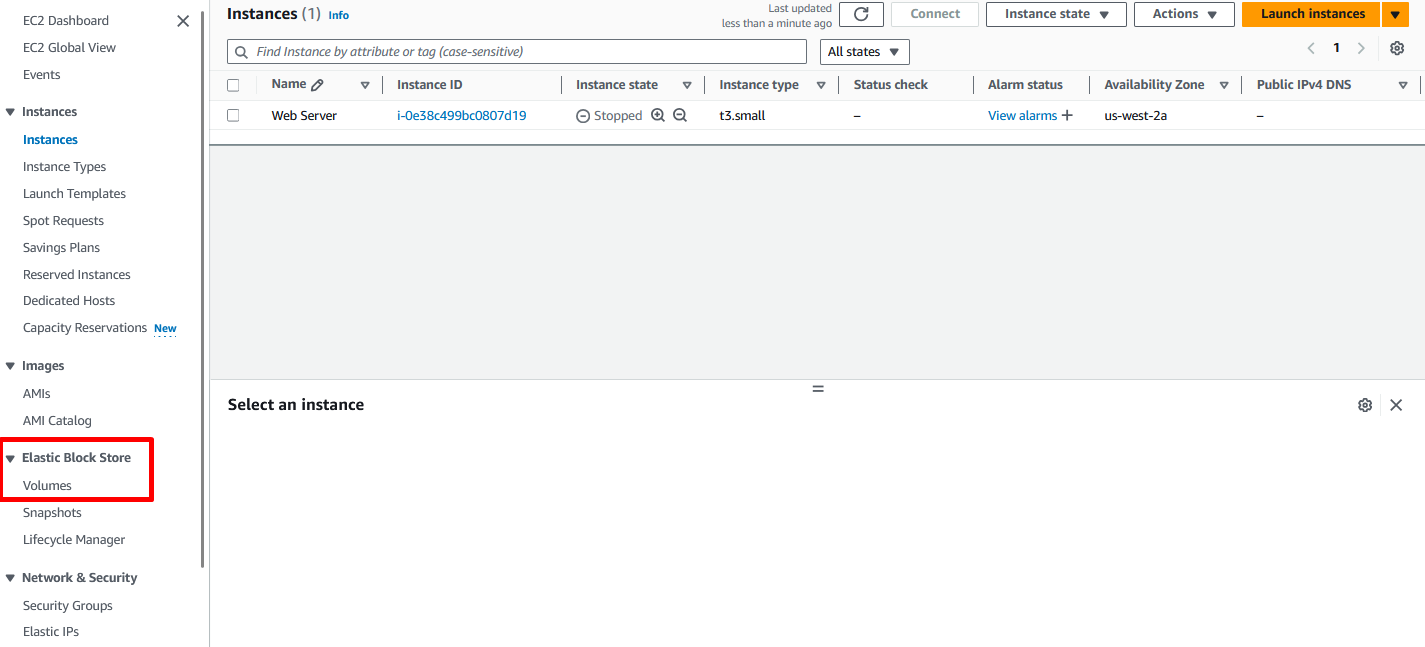
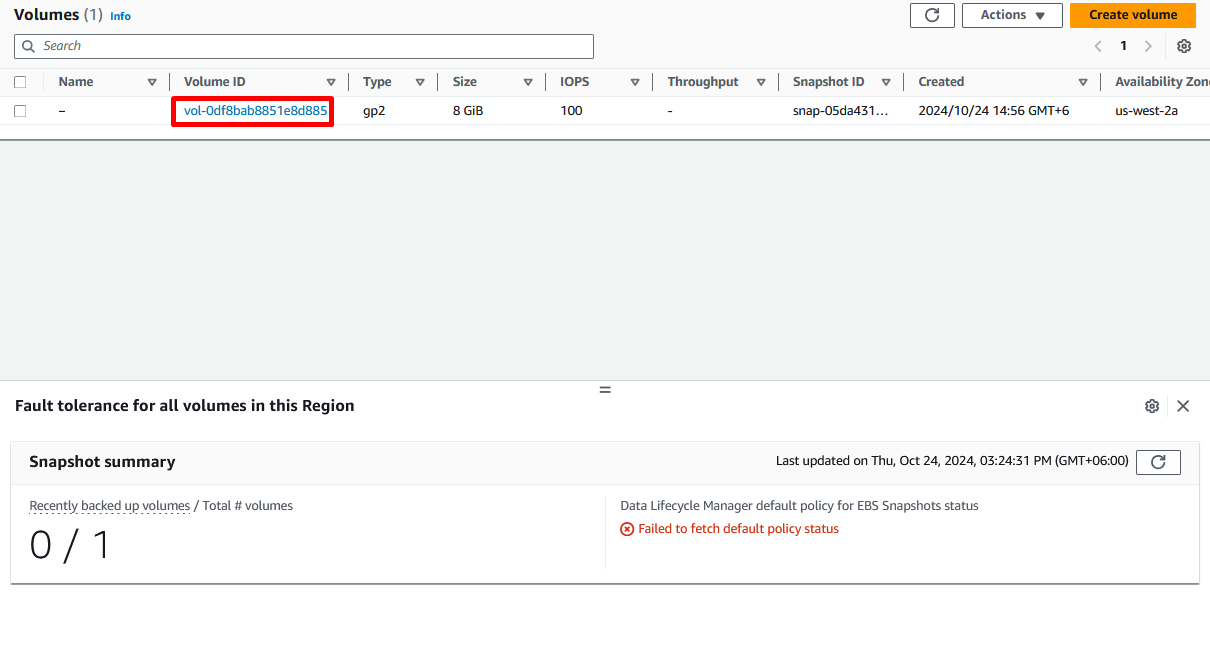
1. Choose and click **Change** button.



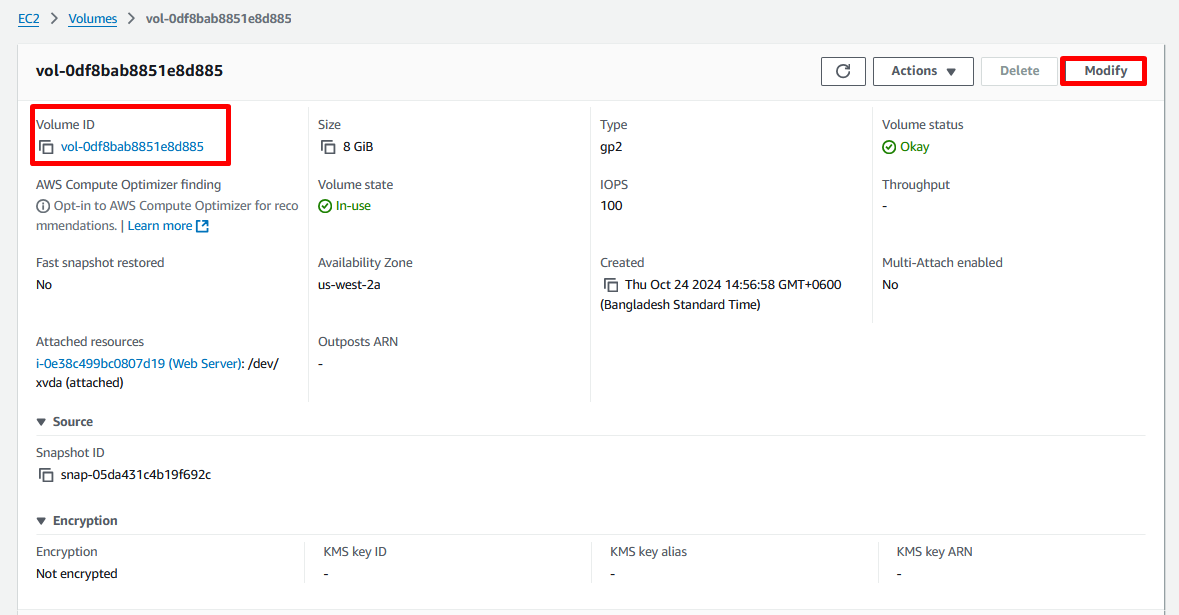
When the instance is started again it will be a *t3.small*, which has twice as much memory as a *t3.micro* instance.

**Resize the EBS Volume**

* 1. In the left navigation pane, select **Volumes** from the **Elastic Block Store** section.
  2. Select the **volumes** there.

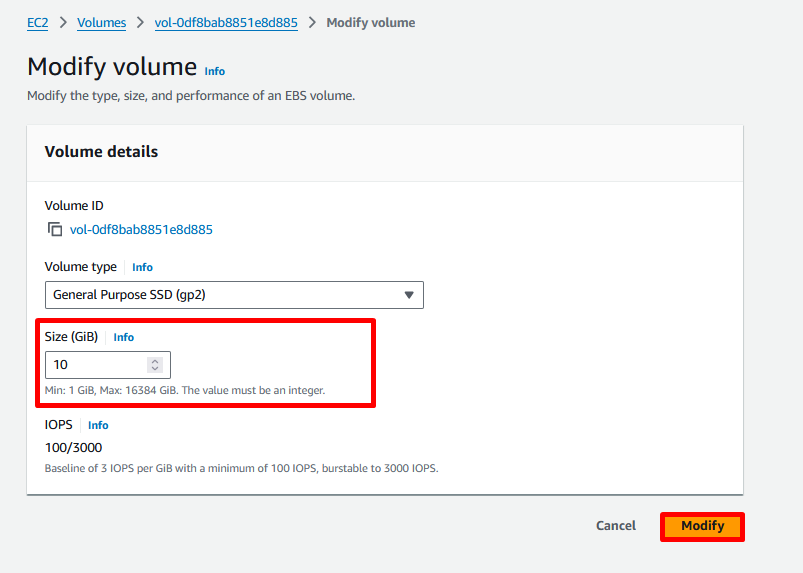
  
  
  


* 1. For Modifying, select **Volume ID** and then Click **Modify** button.

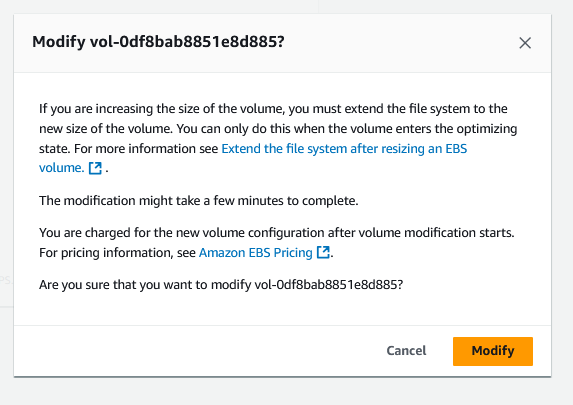


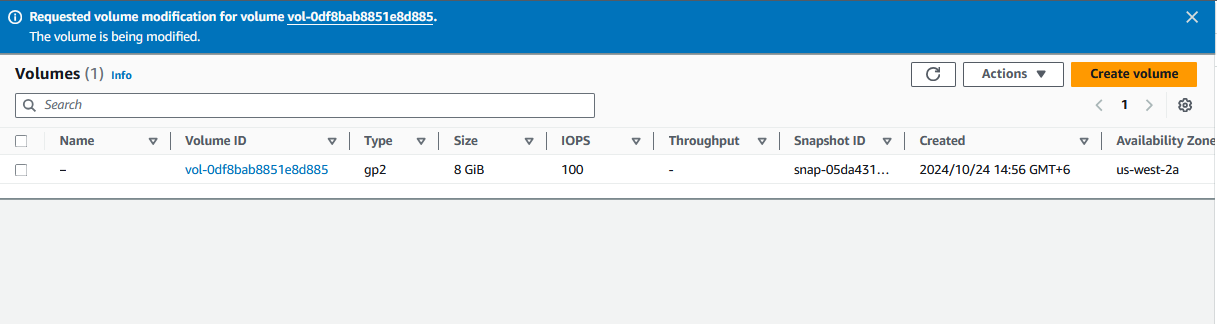
The disk volume currently has a size of 8 GiB. We will now increase the size of this disk.

* 1. Change the **volume size (GiB)** to: **10** GiB
  2. Choose and click **Modify**.



* On the **Modify volume?** Pop-up window, click **Modify** to confirm and increase the size of the volume.



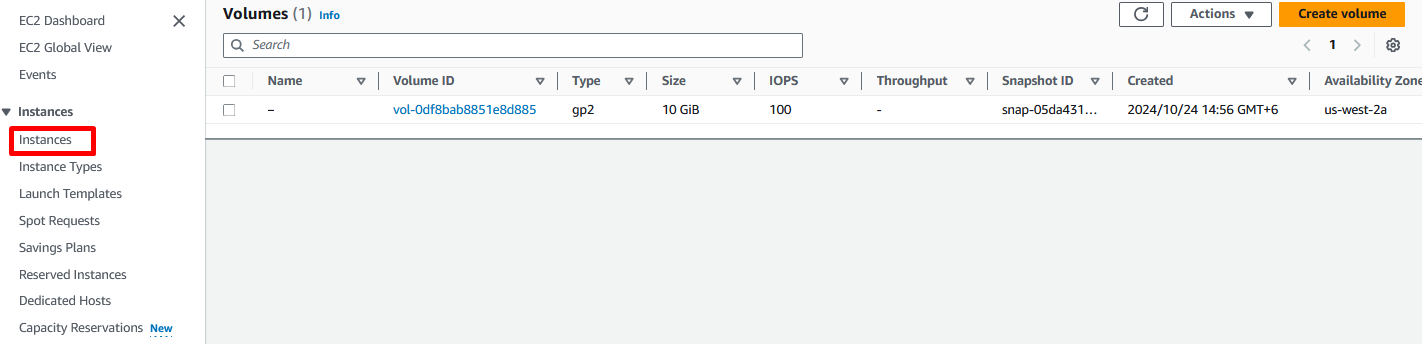


A Requested volume modification for volume message is displayed on top of the screen.

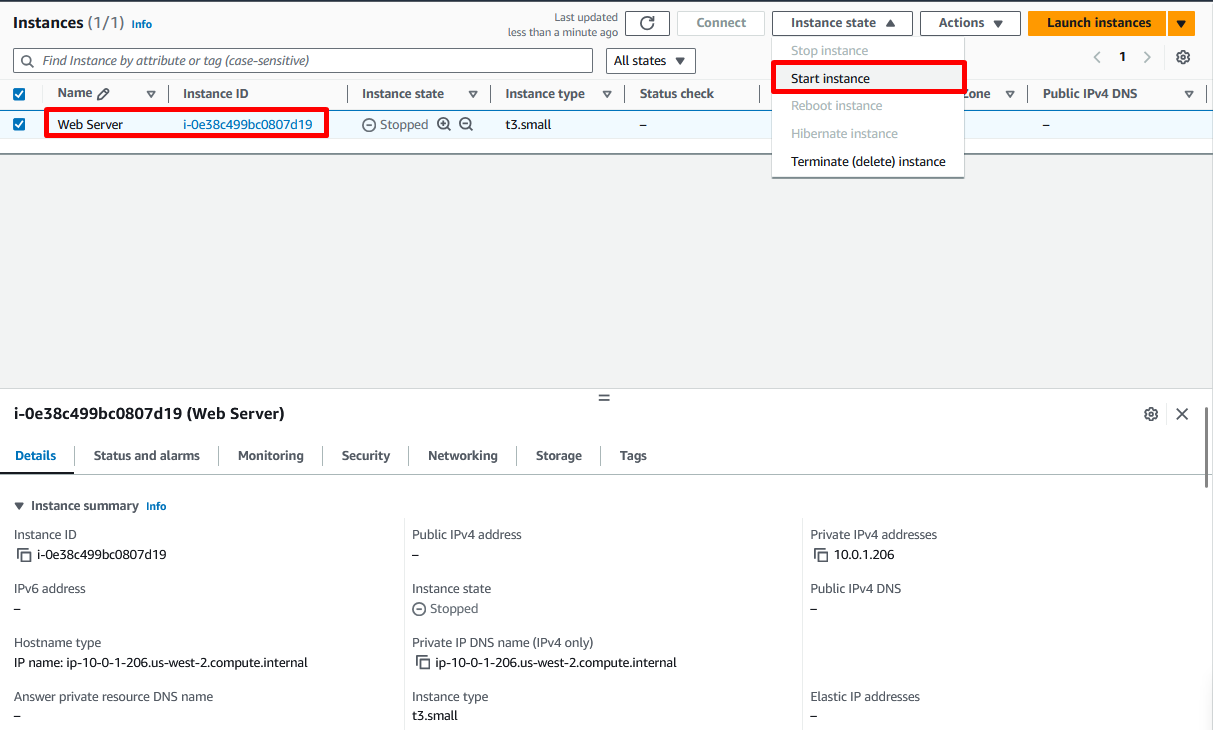
**Start the Resized Instance**

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

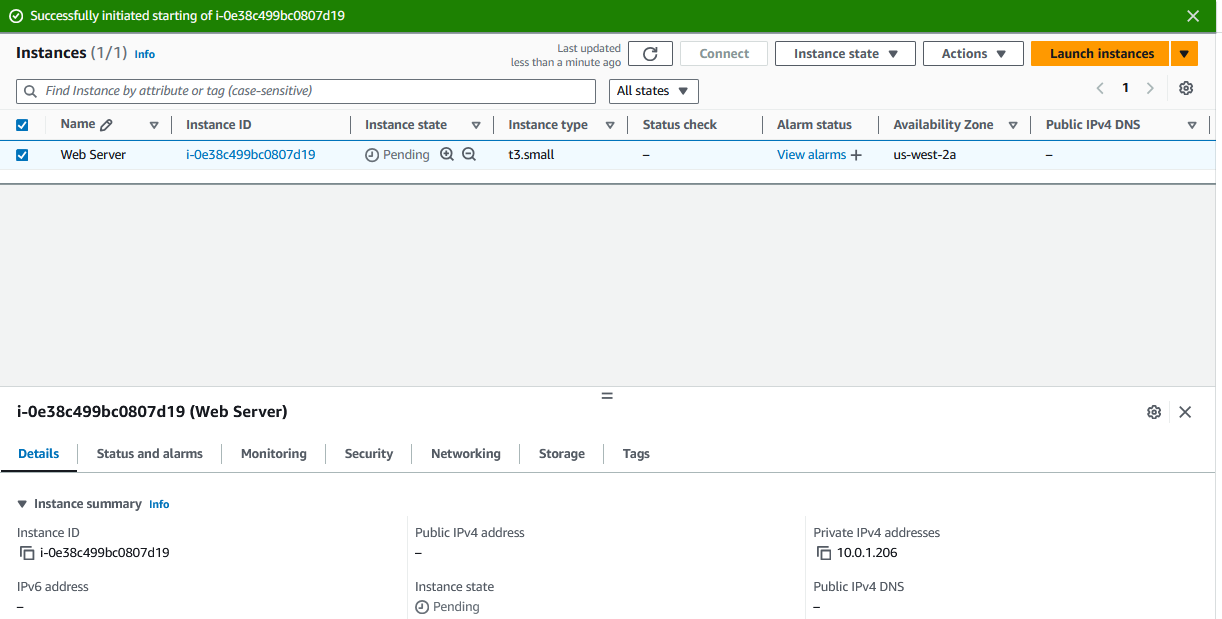
* 1. In left navigation pane, select **Instances**.



* 1. Select the **Web Server**.
  2. Select **Instance state** and then **start instance**.



An EBS volume being modified goes through a sequence of states: Modifying, Optimizing, and finally complete.



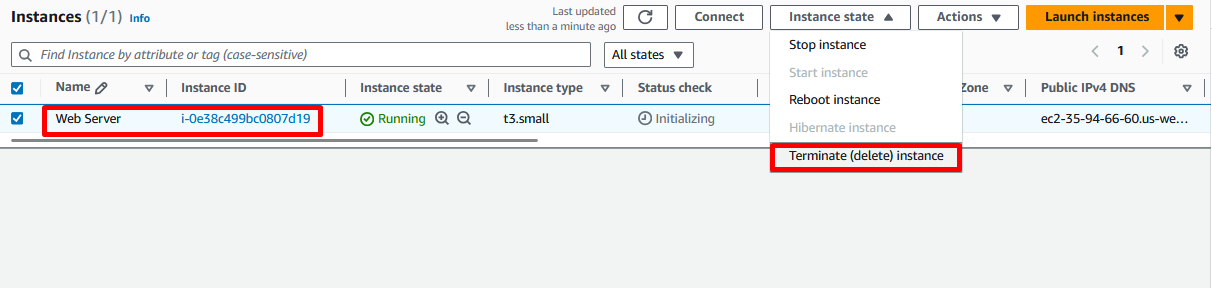
A Successfully initiated starting message is displayed on top of the screen.  
  
**Congratulations!** We have successfully resized our Amazon EC2 Instance. In this task, we changed our instance type from *t3.micro* to a *t3.small*. We also modified our root disk volume from 8 GiB to 10 GiB.

**Task 5: Test Termination Protection**

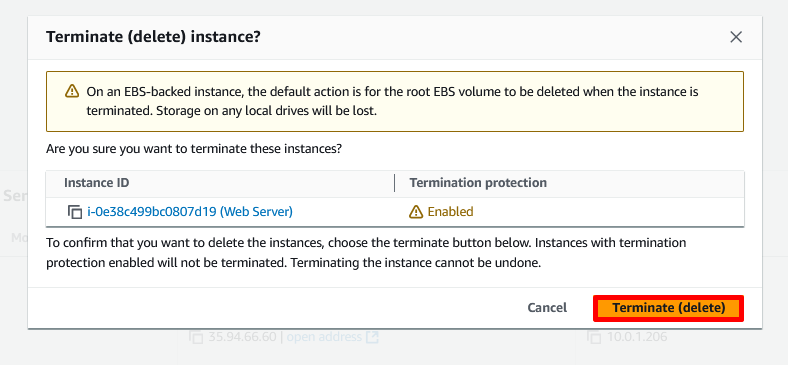
We can delete our instance when we no longer need it. This is referred to as **terminating** our instance. We cannot connect to or restart an instance after it has been terminated.

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

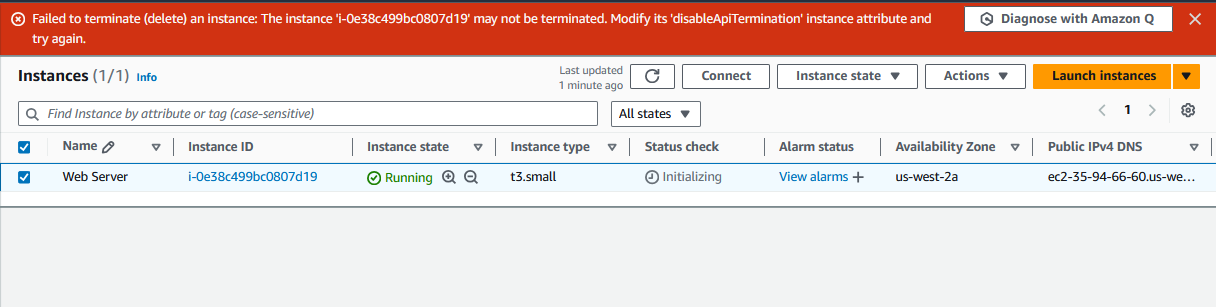
1. In left navigation pane, select **Instances**.
2. Select the **Web Server**.
3. Select **Instance state** and then **terminate instance**.



1. On the **Terminate (delete) instance?** Pop-up window, click **Terminate (delete)**.



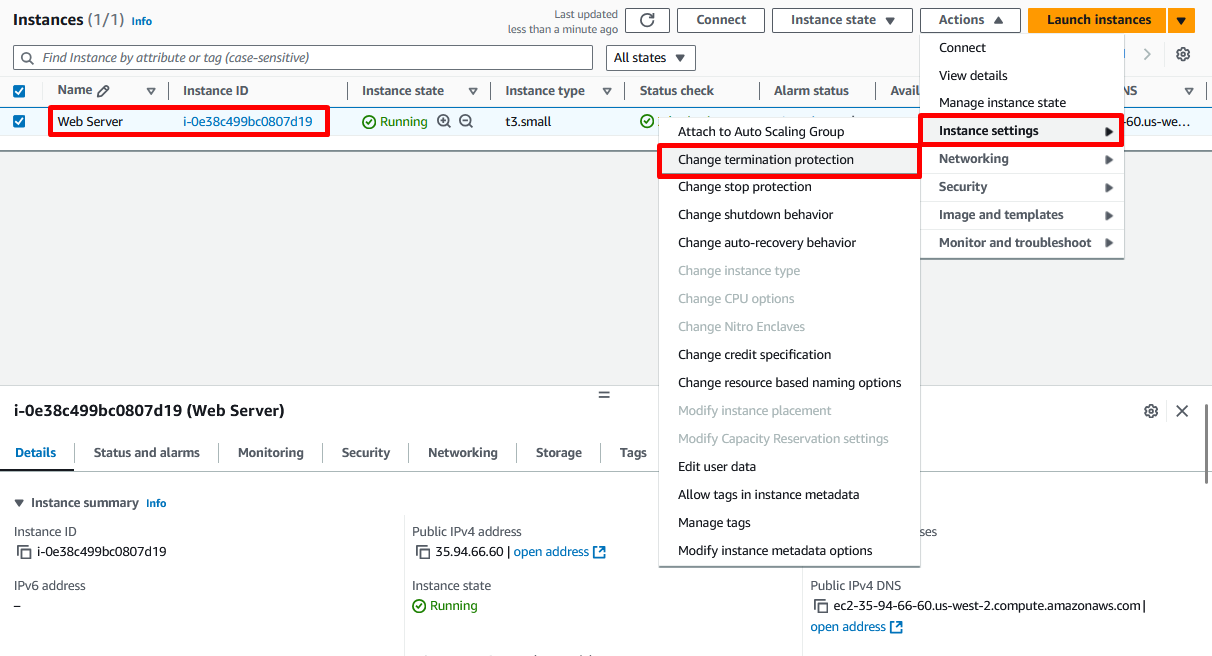
At this point we see the following error message on top of the page:



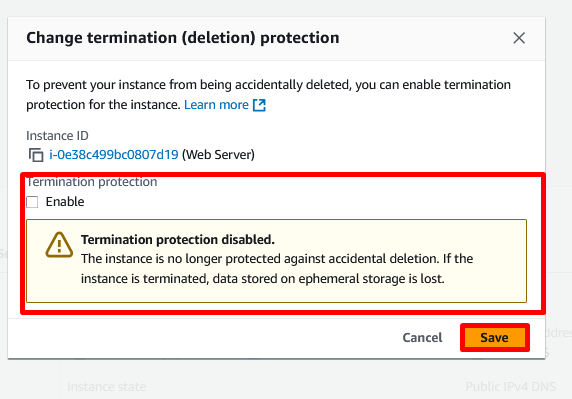
A Failed to terminate (delete) an instance. The instance may not be terminated. Modify its “disabledApiTerminator” instance attribute and try again. message is displayed on top of the screen.

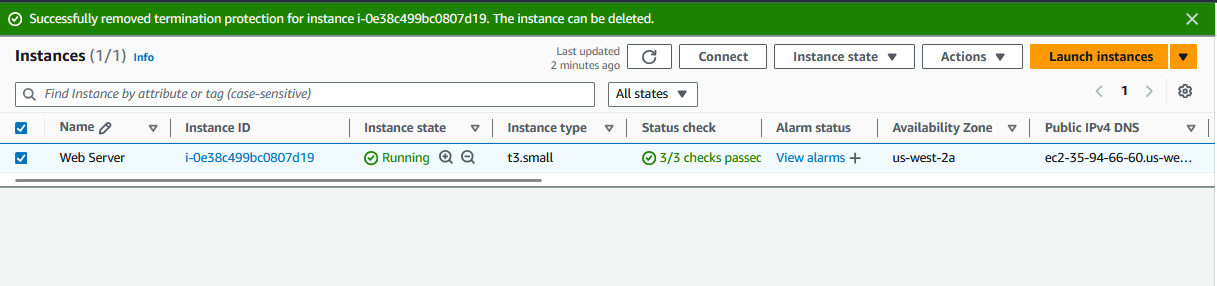
The above error is expected, and this is a safeguard to prevent the accidental termination of an instance. If we really want to terminate the instance, we will need to disable the termination protection.

1. Select **Actions**, choose **Instance settings**, and then click **Change termination protection**.



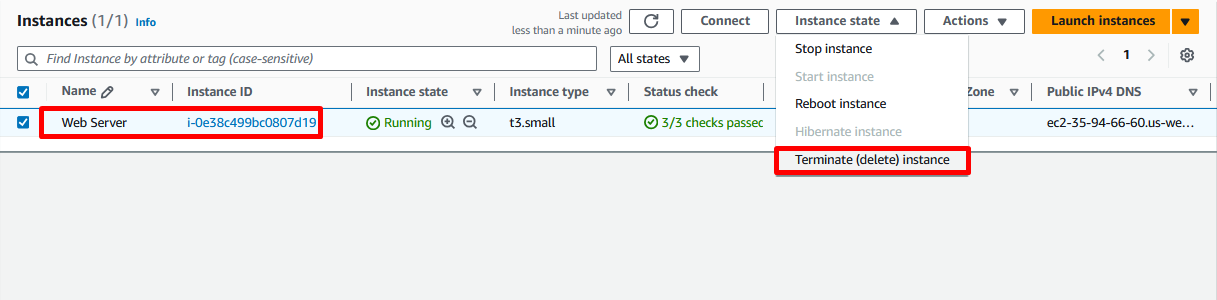
1. On the **Change Termination (deletion) protection?** Pop-up window, click **Save**.
2. Unselect **Enable** (Termination protection).



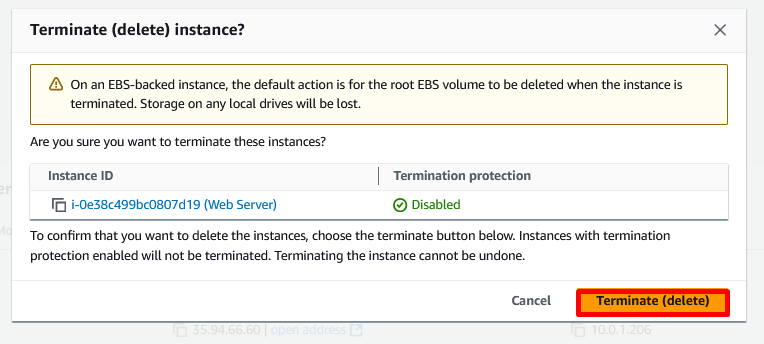


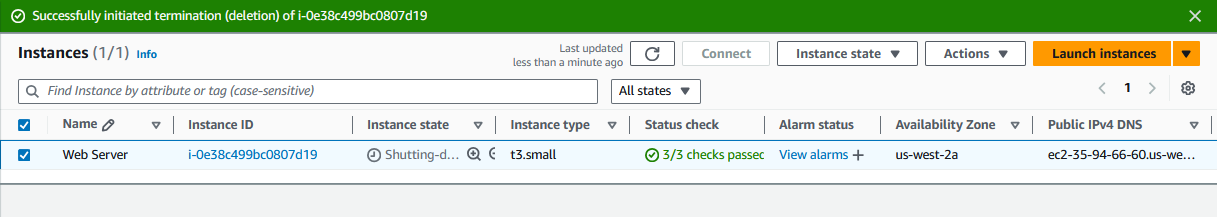
A Successfully removed termination protection for instance message is displayed on top of the screen. Now, we can terminate the instance.

1. Refresh the instance console screen.
2. Select the **Web Server**, Choose **Instance state**, and then click **Terminate (delete) instance**.



1. On the **Terminate (delete) instance?** Pop-up window, click **Terminate (delete)**.





A Successfully initiated termination (deletion) message is displayed on top of the screen.

**Congratulations!** We have successfully tested termination protection and terminated our instance.

**End lab**

Follow these steps to close the console and end our lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then click **Sign out**.
3. Choose and click **End lab** and then confirm that we want to end our lab.