



COS20019

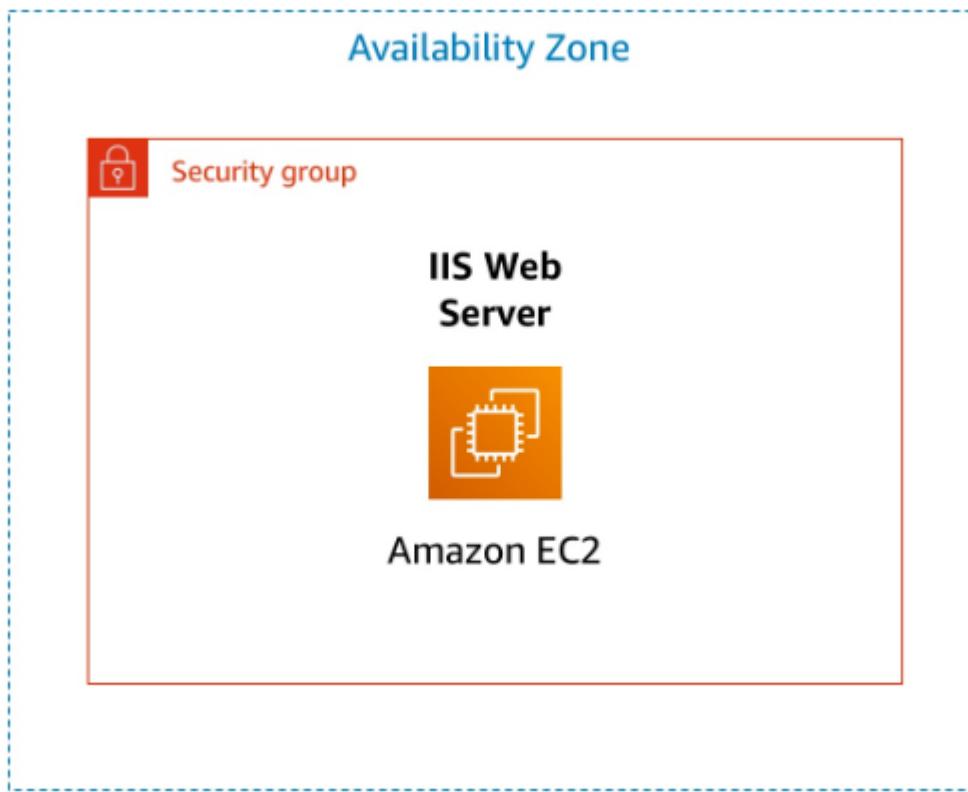
Cloud Computing Architecture

Week 2 – ACF Lab 3 Report
Introduction to EC2

Truong Ngoc Gia Hieu
105565520

Lab 3: Introduction to Amazon EC2

A. Lab overview and objectives



This lab provides you 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 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.

After completing this lab, you should be able to do the following:

- 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 and enable stop protection
- Explore EC2 limits
- Test stop protection
- Stop your EC2 instance

Duration

This lab takes approximately **35 minutes** to complete.

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Accessing the AWS Management Console

1. At the top of these instructions, choose **Start Lab**.
 - The lab session starts.
 - A timer displays at the top of the page and shows the time remaining in the session.
- Tip:** To refresh the session length at any time, choose ▶ **Start Lab** again before the timer reaches 0:00.
- Before you continue, wait until the circle icon to the right of the AWS link in the upper-left corner turns green.

AWS 

Figure 1: Lab Started

2. To connect to the AWS Management Console, choose the AWS link in the upper-left corner.

- A new browser tab opens and connects you to the console.

Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with the message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and then choose **Allow pop-ups**.

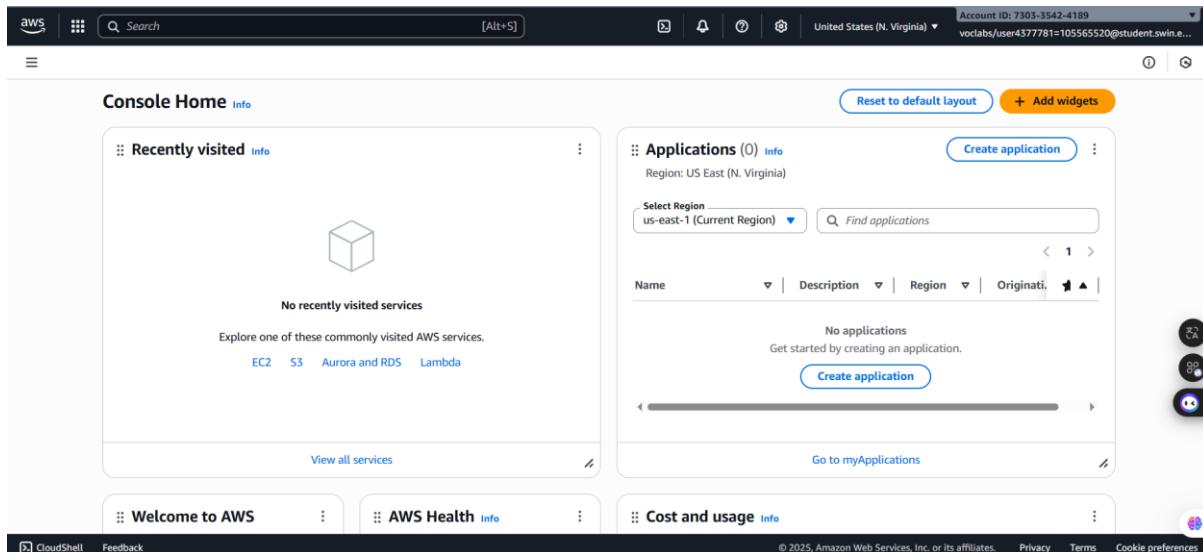


Figure 2: AWS Management Console

3. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you will be able to see both browser tabs at the same time, to make it easier to follow the lab steps.

Getting Credit for your work

At the end of this lab you will be instructed to submit the lab to receive a score based on your progress.

Tip: The script that checks your work may only award points if you name resources and set configurations as specified. In particular, values in these instructions that appear in **This Format** should be entered exactly as documented (case-sensitive).

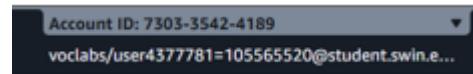
B. Tasks

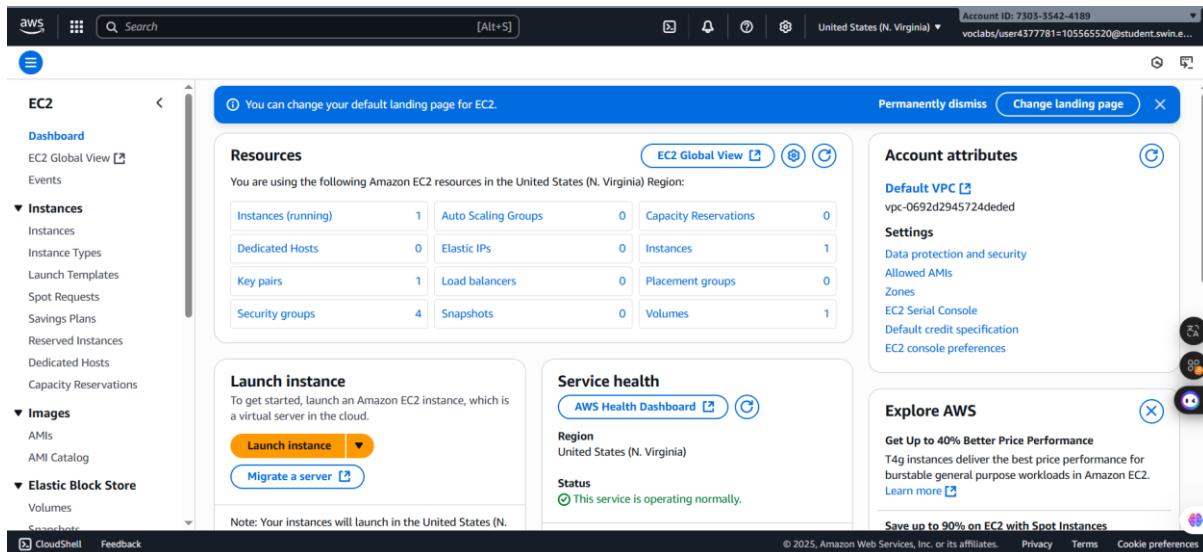
Task 1: Launch Your Amazon EC2 Instance

In this task, you will launch an Amazon EC2 instance with *termination protection* and *stop protection*. Termination protection prevents you from accidentally terminating the EC2 instance and stop protection prevents you from accidentally stopping the EC2 instance. You will also specify a User Data script when you launch the instance that will deploy a simple web server

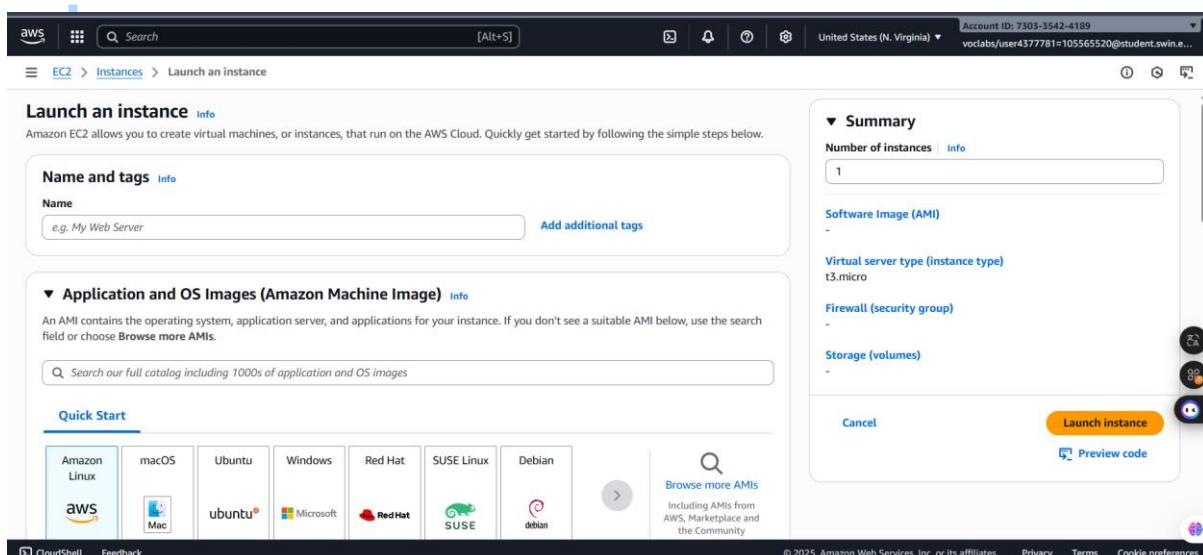
4. In the **AWS Management Console** choose **Services**, choose **Compute** and then choose **EC2**.

Note: Verify that your EC2 console is currently managing resources in the **N. Virginia** (us-east-1) region. You can verify this by looking at the drop down menu at the top of the screen, to the left of your username. If it does not already indicate N. Virginia, choose the N. Virginia region from the region menu before proceeding to the next step.



**Figure 3: EC2 Dashboard**

5. Choose the **Launch instance** menu and select **Launch instance**.

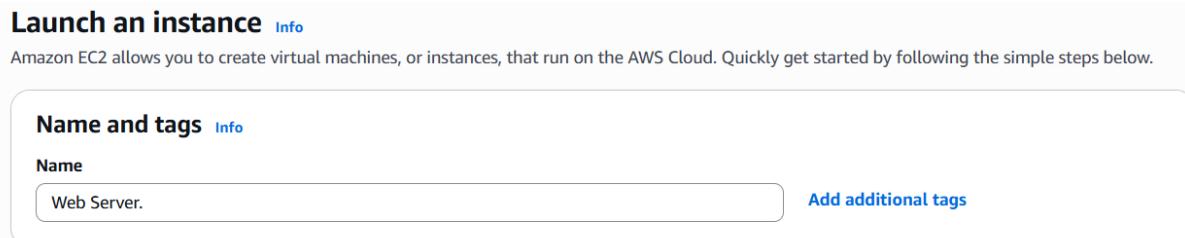
**Figure 4: Launch Instance page**

Step 1: Name and tags

6. Give the instance the name **Web Server**.

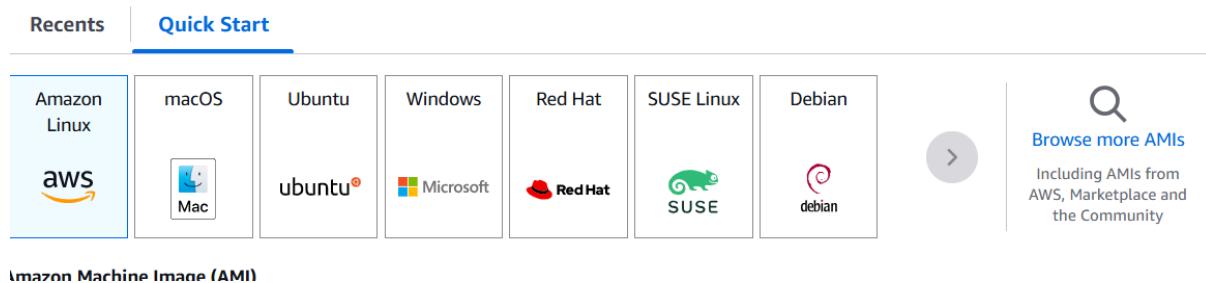
i The Name you give this instance will be stored as a tag. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you have assigned to it. Each tag consists of a Key and a Value, both of which you define. You can define multiple tags to associate with the instance if you want to.

In this case, the tag that will be created will consist of a **key** called **Name** with a **value** of **Web Server**

**Figure 5: Set the instance name**

Step 2: Application and OS Images (Amazon Machine Image)

7. In the list of available Quick Start AMIs, keep the default Amazon Linux AMI selected.

**Figure 6: Quick Start Selection**

8. Also keep the default **Amazon Linux 2023 AMI** selected.

➊ 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. 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.

Amazon Machine Image (AMI)

| | |
|--|--------------------|
| Amazon Linux 2023 kernel-6.1 AMI ami-0b09ffb6d8b58ca91 (64-bit (x86), uefi-preferred) / ami-0b2f2a5d7a4d7f37f (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs | Free tier eligible |
|--|--------------------|

Figure 7: AMI Amazon Linux version

Step 3: Instance type

9. In the *Instance type* panel, keep the default **t2.micro** selected.

Info: 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*, allowing you to scale your resources to the requirements of your target workload.

The t2.micro instance type has 1 virtual CPU and 1 GiB of memory.

Note: You may be restricted from using other instance types in this lab.

Instance type

A screenshot of the AWS CloudFormation instance type selection interface. It shows the t2.micro instance type selected. Below it, detailed information is provided: Family: t2, 1 vCPU, 1 GiB Memory, Current generation: true. Pricing options include On-Demand Windows base pricing: 0.0162 USD per Hour, On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour, On-Demand SUSE base pricing: 0.0116 USD per Hour, On-Demand RHEL base pricing: 0.026 USD per Hour, and On-Demand Linux base pricing: 0.0116 USD per Hour. To the right, there is a toggle switch labeled "All generations" and a blue link "Compare instance types".

[Additional costs apply for AMIs with pre-installed software](#)

Figure 8: instance type selection

Step 4: Key pair (login)

10. For **Key pair name - required**, choose **vockey**.

Info: Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To ensure you will be able to log in to the guest OS of the instance you create, you identify an existing key pair or create a new key pair when launching the instance. Amazon EC2 then installs the key on the guest OS when the instance is launched. That way, when you attempt to login to the instance and you provide the private key, you will be authorized to connect to the instance.

Note: In this lab you will not actually use the key pair you have specified to log into your instance.

▼ 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

vockey

[Create new key pair](#)

Figure 9: Key pair (login) selection

Step 5: Network settings

11. Next to Network settings, choose **Edit**.

12. For **VPC**, select **Lab VPC**.

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

Info: Note: Keep the default subnet **PublicSubnet1**. This is the subnet in which the instance will run. Notice also that by default, the instance will be assigned a public IP address.

VPC - required | [Info](#)

vpc-09844c22f2ff305f4 (Lab VPC)
10.0.0.0/16

Subnet | [Info](#)

subnet-0f76ffbefe22107de **PublicSubnet1**

VPC: vpc-09844c22f2ff305f4 Owner: 730335424189 Availability Zone: us-east-1a (use1-az4) CIDR: 10.0.1.0/28

Zone type: Availability Zone IP addresses available: 1

[Create new subnet](#)

Figure 10: VPC and Subnet selection

13. Under **Firewall (security groups)**, choose **Create security group** and configure:

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

i 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.

- Under **Inbound security group rules**, notice that one rule exists. **Remove** this rule.

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 _-:/()#,@!+=&;!\$*

Description - required | [Info](#)

Security group for my web server

Inbound Security Group Rules

No security group rules are currently included in this template. Add a new rule to include it in the launch template.

[Add security group rule](#)

Figure 11: Firewall configuration

Step 6: Configure storage

14. In the *Configure storage* section, keep the default settings.

i Amazon EC2 stores data on a network-attached virtual disk called *Elastic Block Store*.

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

Step 7: Advanced details

15. Expand ▶ Advanced details.

16. For **Termination protection**, select **Enable**.

- ⓘ When an Amazon EC2 instance is no longer required, it can be *terminated*, which means that the instance is deleted and its resources are released. A terminated instance cannot be accessed again and the data that was on it cannot be recovered. If you want to prevent the instance from being accidentally terminated, you can enable *termination protection* for the instance, which prevents it from being terminated as long as this setting remains enabled.

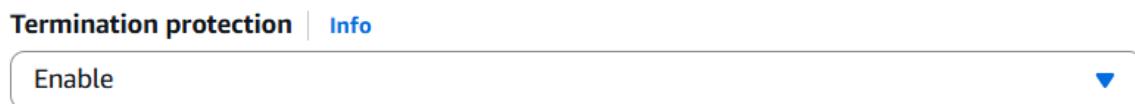


Figure 12: Enable Terminal Protection

17. Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box:

A screenshot of a user interface showing a 'User data - optional' section. It has two tabs: 'User data - optional' (selected) and 'Info'. Below the tabs is a text input field containing a shell script. The script installs Apache (httpd), enables it at boot, starts it, and creates a basic index.html file. The text area has a blue border and a scroll bar on the right side. The script content is:

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

Figure 13: User data configuration

ⓘ When you launch an instance, you can pass user data to the instance that can be used to perform automated installation and configuration tasks after the instance starts.

Your instance is running Amazon Linux 2023. The shell script you have specified will run as the root guest OS user when the instance starts. The script will:

- Install an Apache web server (httpd)
- Configure the web server to automatically start on boot

- Run the Web server once it has finished installing
- Create a simple web page

Step 8: Launch the instance

18. At the bottom of the **Summary** panel choose **Launch instance**

You will see a Success message.

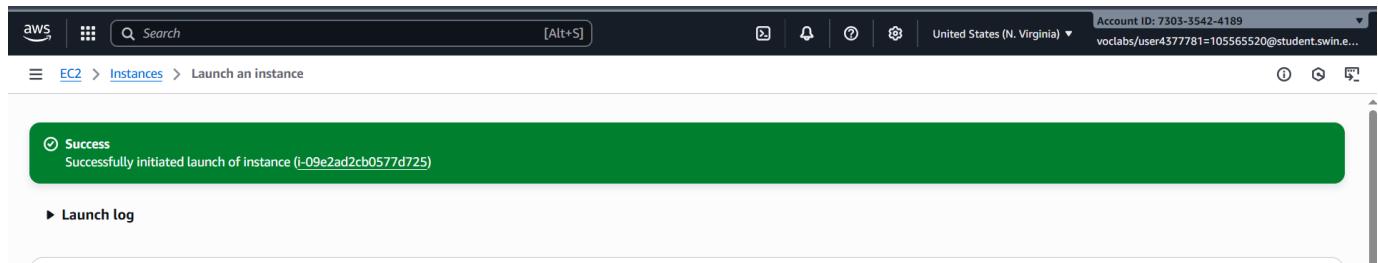


Figure 13: Launch instance successfully

19. Choose **View all instances**

- In the Instances list, select **Web Server**.
- Review the information displayed in the **Details** tab. It includes information about the instance type, security settings and network settings.

The instance is assigned a *Public IPv4 DNS* that you can use to contact the instance from the Internet.

☞ To view more information, drag the window divider upwards.

At first, the instance will appear in a *Pending* state, which means it is being launched. It will then change to *Initializing*, and finally to *Running*.

20. Wait for your instance to display the following:

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

👍 Congratulations! You have successfully launched your first Amazon EC2 instance.

| Instances (2) Info | | Connect | Instance state | Actions | Launch instances |
|------------------------------------|-----------------------------|-------------------------|---|-------------------------|--|
| | | All states | | | |
| <input type="checkbox"/> | Name Filter | Instance ID | Instance state | Instance type | Status check |
| <input type="checkbox"/> | Web Server. | i-09e2ad2cb0577d725 | ✓ Running Details Logs | t2.micro | ✓ 2/2 checks passed View alarms + |
| <input type="checkbox"/> | Bastion Host | i-08da93989df99c9fc | ✓ Running Details Logs | t2.micro | ✓ 2/2 checks passed View alarms + |

Figure 14: Launch the seb server successfully

Task 2: Monitor Your Instance

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

21. Choose the **Status checks** tab.

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

Notice that both the **System reachability** and **Instance reachability** checks have passed.

Status checks Info

Status checks detect problems that may impair i-09e2ad2cb0577d725 (Web Server.) from running your applications.

System status checks

System reachability check passed

Instance status checks

Instance reachability check passed

Figure 15: Status Check

22. Choose 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 the three dots icon in any graph and select **Enlarge** to see an expanded view of the chosen metric.

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

23. In the **Actions ▾** menu towards the top of the console, select **Monitor and troubleshoot > Get system log**.

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 its SSH daemon can be started. If you do not see a system log, wait a few minutes and then try again.

Review system log for instance i-09e2ad2cb0577d725

```
[ 28.455579] cloud-init[2195]: mod_lua-2.4.64-1.amzn2023.0.1.x86_64
[ 28.461762] cloud-init[2195]: complete!
[ 28.598109] cloud-init[2195]: Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ 28.818991] zram_generator::config[3619]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
ci-info: +-----+-----+-----+
ci-info: | Keypair | Fingerprint (sha256) | Options | Comment |
ci-info: +-----+-----+-----+
ci-info: | ssh-rsa | a2:e7:e9:72:66:4d:dc:a9:a1:9a:16:c0:4b:b1:74:f2:3e:06:73:d7:c4:af:0a:c6:6a:2a:82:1a:13:89:f2:6f | - | vockey |
ci-info: +-----+-----+-----+
<14>Sep 12 02:57:57 cloud-init: #####
<14>Sep 12 02:57:57 cloud-init: ----BEGIN SSH HOST KEY FINGERPRINTS----
<14>Sep 12 02:57:57 cloud-init: 256 SHA256:k/OqxpSowE49Mm07gnmLwVF219Lq8Qa08Zxr+lkH/4E root@ip-10-0-1-12.ec2.internal (EDDSA)
<14>Sep 12 02:57:57 cloud-init: 256 SHA256:InfHzl2f8e8HugI+jHYKRaUqyDSnYiVmdgmBdMPJWQ root@ip-10-0-1-12.ec2.internal (ED25519)
<14>Sep 12 02:57:57 cloud-init: ----END SSH HOST KEY FINGERPRINTS----
<14>Sep 12 02:57:57 cloud-init: #####
----BEGIN SSH HOST KEY KEYS----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmzdHAyNTYAAQBBIHLMdg2rlIZXp4oL2wIVHyP5VmTDsseHJXE/iqAcajMps04x5IS6cMbYhOoBpCi4DAv1itItZ2mXN
ssh-ed25519 AAAAC3NzaC1ZD1tNE5AAAIYL64fgZZKPUs7oxF4nEBYrSXFed9ZlVT2zAFI+Bn3J root@ip-10-0-1-12.ec2.internal
----END SSH HOST KEY KEYS----
[ 29.209722] cloud-init[2195]: Cloud-init v. 22.2.2 finished at Fri, 12 Sep 2025 02:57:57 +0000. Datasource DataSourceEc2. Up 29.20 seconds
```

Figure 16: System Console Window

25. Choose **Cancel**.

Task 3: Update Your Security Group and Access the Web Server

28. Ensure **Web Server** is still selected. Choose the **Details** tab

| Instances (1/2) Info | | Connect | Instance state ▼ | Actions ▼ | Launch instances | ▼ | | |
|--|------------------------|--|--|---------------------------------|--|-------------------|-------------------------------------|-------------|
| Find Instance by attribute or tag (case-sensitive) | | All states ▼ | | | | | | |
| <input type="checkbox"/> | Name ▼ | Instance ID | Instance state ▼ | Instance type ▼ | Status check | Alarm status | Availability Zone ▼ | Public IPv4 |
| <input checked="" type="checkbox"/> | Web Server. | i-09e2ad2cb0577d725 | Running Q Q | t2.micro | 2/2 checks passed View alarms + | us-east-1a | ec2-54-226- | |
| <input type="checkbox"/> | Bastion Host | i-08da93989df99c9fc | Running Q Q | t2.micro | 2/2 checks passed View alarms + | us-east-1a | ec2-98-84-1 | |

Figure 17: Web Server Selected

29. Copy the **Public IPv4 address** of your instance to your clipboard.

30. Open a new tab in your web browser, paste the IP address you just copied, then press **Enter**.

Question: Are you able to access your web server? Why not?

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.

From my perspective, I'm currently unable to access the web server because the security group is not permitting inbound traffic on port 80,, which is used for HTTP web requests. As a result, this is demostrate of using a security group as a firewall to restrict the network traffic and allowed in and out of instance

31. Keep the browser tab open, but return to the **EC2 Console** tab.

32. In the left navigation pane, choose **Security Groups**.

| Security Groups (5) Info | | Actions ▼ | Export security groups to CSV ▼ | | Create security group |
|--|------------------------|---|---|---|---------------------------------------|
| Find security groups by attribute or tag | | | | | |
| <input type="checkbox"/> | Name ▼ | Security group ID | Security group name | VPC ID | Description |
| <input type="checkbox"/> | - | sg-0fc71c6c7ebe9fcff | default | vpc-09844c22f2ff305f4 E | default VPC secur |
| <input type="checkbox"/> | - | sg-0bea1cb9f78ade152 | Ec2SecurityGroup | vpc-089fd92667e9234a7 E | VPC Security Gro |
| <input type="checkbox"/> | - | sg-0fc9638515b7f0358 | default | vpc-089fd92667e9234a7 E | default VPC secur |
| <input type="checkbox"/> | - | sg-06f85d8ff852c3326 | Web Server security group | vpc-09844c22f2ff305f4 E | Security group for |
| <input type="checkbox"/> | - | sg-0dff66b527e0714c2 | default | vpc-0692d2945724deded E | default VPC secur |

Figure 18: Security groups

33. Select **Web Server security group**.



Figure 19: Wen Server Security group selected

34. Choose the **Inbound rules** tab.

The security group currently has no inbound rules.

The screenshot shows the AWS Management Console interface for a security group named "sg-06f85d8ff852c3326 - Web Server security group". The "Inbound rules" tab is selected. At the top, there are tabs for "Details", "Inbound rules" (which is active), "Outbound rules", "Sharing - new", "VPC associations - new", and "Tags". Below the tabs is a search bar and filter options for "Name", "Security group rule ID", "IP version", "Type", "Protocol", and "Port range". A message at the bottom states "No security group rules found".

Figure 20: Inbound rules selected

35. Choose **Edit inbound rules**, select **Add rule** and then configure:

- **Type: HTTP**
- **Source: Anywhere-IPv4**
- Choose **Save rules**

The screenshot shows the "Edit inbound rules" configuration page. It includes fields for "Security group rule ID", "Type" (set to "HTTP"), "Protocol" (set to "TCP"), "Port range" (set to "80"), "Source" (set to "Anywh..."), and "Description - optional". There is also a "Delete" button and an "Add rule" link.

Figure 21: Inbound rules configuration

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

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

👍 Congratulations! You have successfully modified your security group to permit HTTP traffic into your Amazon EC2 Instance.

Task 4: 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 t2.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.

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

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

37. On the **EC2 Management Console**, in the left navigation pane, choose **Instances** and then select the **Web Server** instance.

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 |
|---|---------------------|----------------------|---------------|--------------------------------|-----------------------------|-------------------|-------------|
| <input checked="" type="checkbox"/> Web Server. | i-09e2ad2cb0577d725 | Running | t2.micro | 2/2 checks passed | View alarms | us-east-1a | ec2-54-226- |
| <input type="checkbox"/> Bastion Host | i-08da93989df99c9fc | Running | t2.micro | 2/2 checks passed | View alarms | us-east-1a | ec2-98-84-1 |

Figure 22: Web Server Instance selected

38. In the **Instance state ▾** menu, select **Stop instance**.

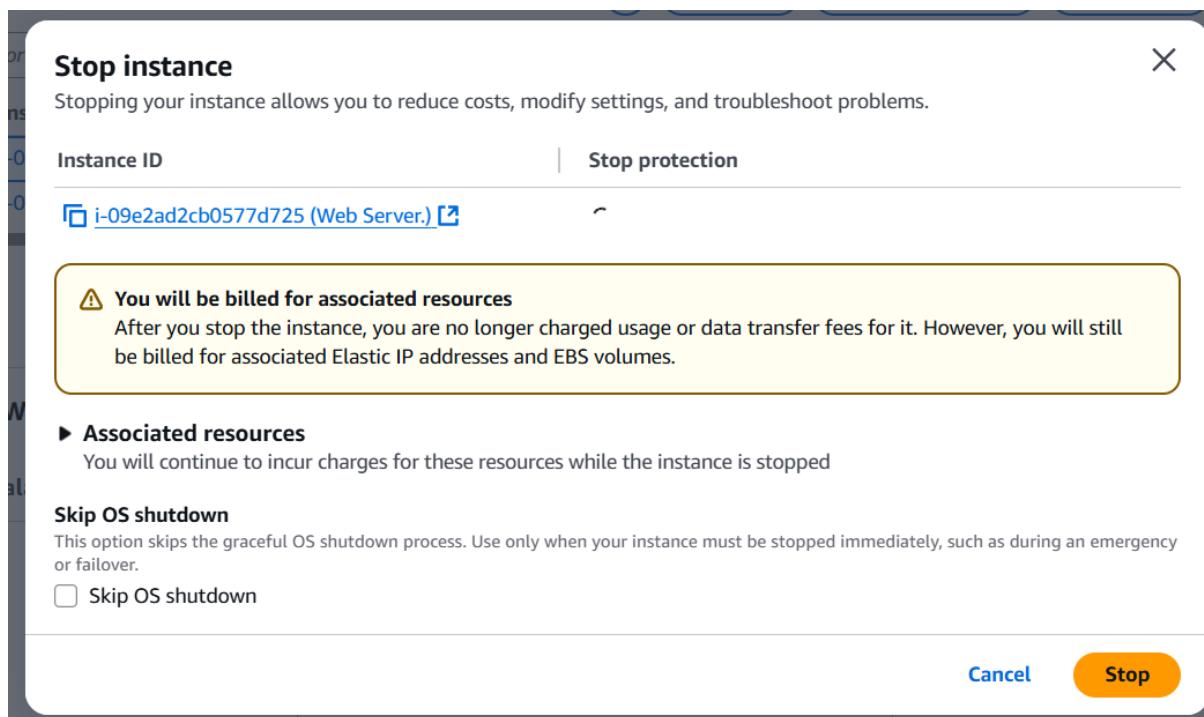


Figure 23: Stop Instance Annoucement

39. Choose **Stop**

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

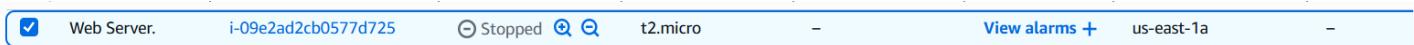
40. Wait for the **Instance state** to display: **Stopped**.

Figure 24: Instance stopped

Change The Instance Type and enable stop protection

41. Select the Web Server instance, then in the **Actions** menu, select **Instance settings** ▶ **Change instance type**, then configure:

- **Instance Type:** *t2.small*
- Choose **Apply**

When the instance is started again it will run as a *t2.small*, which has twice as much memory as a *t2.micro* instance. **NOTE:** You may be restricted from using other instance types in this lab.

Change instance type [Info](#) | [Get advice](#)

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

Instance ID

[i-09e2ad2cb0577d725](#) (Web Server.)

Current instance type

t2.micro

New instance type

Only instance types with x86 (32-bit) / (64-bit) architecture can be chosen.

EBS-optimized

EBS-optimized is not supported for this instance type.

Figure 25: Change Instance type

| <input type="checkbox"/> | Name | ▼ | Instance ID | ▼ | Instance state | ▼ | Instance type | ▼ |
|--------------------------|-------------|---|-------------------------------------|---|----------------|---|---------------|---|
| <input type="checkbox"/> | Web Server. | | i-09e2ad2cb0577d725 | | Stopped | | t2.small | |

Figure 26: Instance changed successfully

42. Select the Web Server instance, then in the **Actions ▾** menu, select **Instance settings ▾ Change stop protection**. Select **Enable** and then **Save** the change.

i When you stop an instance, the instance shuts down. When you later start the instance, it is typically migrated to a new underlying host computer and assigned a new *public* IPv4 address. An instance retains its assigned *private* IPv4 address. When you stop an instance, it is not deleted. Any EBS volumes and the data on those volumes are retained.

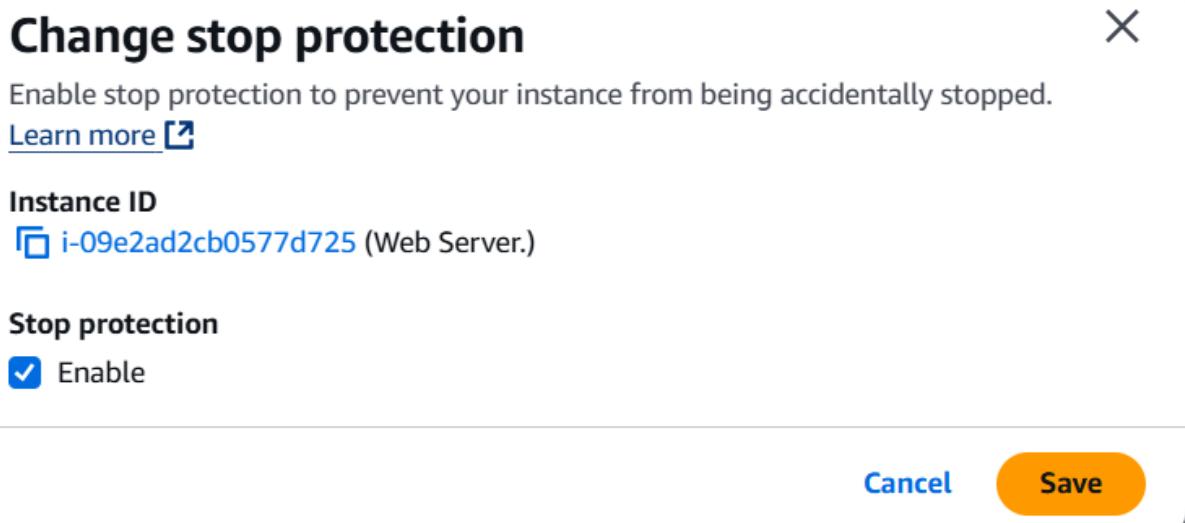


Figure 27: Stop protection configuration

Resize the EBS Volume

43. With the Web Server instance still selected, choose the **Storage** tab, select the name of the Volume ID, then select the checkbox next to the volume that displays.

| Filter block devices | | | | | | |
|-------------------------------------|-----------------------|-------------|-------------------|---------------------|-----------------------|------------------------|
| <input checked="" type="checkbox"/> | Volume ID | Device name | Volume size (GiB) | Volume State | Attachment status | Attachment time |
| <input checked="" type="checkbox"/> | vol-0eb5cda436ca3da44 | /dev/xvda | 8 | In-use | Attached | 2025/09/12 09:57 GMT+7 |

Figure 28: Storage tab

44. In 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.

Modify volume Info

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

Volume details

Volume ID
 vol-0eb5cda436ca3da44

Volume type Info
General Purpose SSD (gp3)

Size (GiB) Info
8
Min: 1 GiB, Max: 16384 GiB.

IOPS Info
3000
Min: 3000 IOPS, Max: 16000 IOPS.

Throughput (MiB/s) Info
125

Figure 29: Modify volume

45. Change the size to: 10 **NOTE:** You may be restricted from creating Amazon EBS volumes larger than 10 GB in this lab.

Size (GiB) Info

Min: 1 GiB, Max: 16384 GiB

Figure 30: Size changed

46. Choose **Modify**

47. Choose **Modify** again to confirm and increase the size of the volume.

Modify vol-0eb5cda436ca3da44?



If you are increasing the size of the volume, you must extend the file system to the new size of the volume. You can only do this when the volume enters the optimizing state. For more information see [Extend the file system after resizing an EBS volume.](#)

The modification might take a few minutes to complete.

You are charged for the new volume configuration after volume modification starts. For pricing information, see [Amazon EBS Pricing](#).

Are you sure that you want to modify vol-0eb5cda436ca3da44?

[Cancel](#)

[Modify](#)

Figure 31: Modify volume size

Start the Resized Instance

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

48. In left navigation pane, choose **Instances**.

49. Select the **Web Server** instance.

| Name | Instance ID | Instance state | Instance type | Status |
|--------------|---------------------|----------------|---------------|--------|
| Web Server. | i-09e2ad2cb0577d725 | Stopped | t2.small | - |
| Bastion Host | i-08da93989df99c9fc | Running | t2.micro | 2/2 |

Figure 31: Start instance

50. In the **Instance state ▾** menu, select **Start instance**.

Congratulations! You have successfully resized your Amazon EC2 Instance. In this task you changed your instance type from *t2.micro* to *t2.small*. You also modified your root disk volume from 8 GiB to 10 GiB.

Task 5: Explore EC2 Limits

Amazon EC2 provides different resources that you can use. These resources include images, instances, volumes, and snapshots. When you create an AWS account, there are default limits on these resources on a per-region basis.

51. In the AWS Management Console, in the search box next to **Services**, search for and choose **Service Quotas**

The screenshot shows the AWS Service Quotas homepage. At the top, there's a navigation bar with the AWS logo, search bar, and account information (Account ID: 7303-3542-4189). The main content area has a dark header 'Management & Governance' and a title 'Service Quotas' with the subtitle 'View and manage AWS quotas'. Below this, a text block explains that Service Quotas helps manage quotas for many AWS services. A large diagram titled 'How it works' illustrates the central role of Service Quotas in managing quotas for both individual accounts and organization-wide accounts. To the right, there are three boxes: 'Manage quotas' (with a dropdown for 'AWS Services' and a 'View quotas' button), 'Pricing' (stating no additional charge), and 'More resources' (links to User Guide, Tutorial, and Quota Request Templates). On the far right, there are several small circular icons.

Figure 32: Service Quotas Homepage

52. Choose **AWS services** from the navigation menu and then in the AWS services Find services search bar, search for ec2 and choose **Amazon Elastic Compute Cloud (Amazon EC2)**.

The screenshot shows the 'Amazon Elastic Compute Cloud (Amazon EC2)' page under the 'Service Quotas' section. The URL in the address bar is 'Service Quotas > AWS services > Amazon Elastic Compute Cloud (Amazon EC2)'. The main content is titled 'Amazon Elastic Compute Cloud (Amazon EC2)' with a sub-section 'Service quotas info'. It describes EC2 as providing resizable compute capacity through virtual machines. Below is a table titled 'Service quotas info' with a search bar at the top. The table columns are: Quota name, Applied account-level quota value, AWS default quota value, Utilization, and Adjustability. The table lists several EC2-specific quotas:

| Quota name | Applied account-level quota value | AWS default quota value | Utilization | Adjustability |
|---|-----------------------------------|-------------------------|-------------|---------------|
| All DL Spot Instance Requests | 96 | 0 | 0 | Account level |
| All F Spot Instance Requests | 64 | 0 | 0 | Account level |
| All G and VT Spot Instance Requests | 0 | 0 | 0 | Account level |
| All Ix Spot Instance Requests | 8 | 0 | 0 | Account level |
| All P4, P3 and P2 Spot Instance Requests | 0 | 0 | 0 | Account level |
| All P5 Spot Instance Requests | 0 | 0 | 0 | Account level |
| All Standard (A, C, D, H, I, M, R, T, Z) Spot Instance Requests | 256 | 5 | 0 | Account level |

Figure 33: Searching result

53. In the *Find quotas* search bar, search for `running on-demand`, but do not make a selection. Instead, observe the filtered list of service quotas that match the criteria.

Notice that there are limits on the number and types of instances that can run in a region. For example, there is a limit on the number of *Running On-Demand Standard...* instances that you can launch in this region. When launching instances, the request must not cause your usage to exceed the instance limits currently defined in that region.

If you are the AWS account owner, you can request an increase for many of these limits.

The screenshot shows the AWS Service Quotas console with a search bar at the top containing 'running on-demand'. Below the search bar is a table titled 'Service quotas info' with 10 matches found. The table has columns: Quota name, Applied account-level quota value, AWS default quota value, Utilization, and Adjustability. The data includes various types of On-Demand instances like DL, F, G, H, P, Standard, and Tn, each with specific quota values.

| Quota name | Applied account-level quota value | AWS default quota value | Utilization | Adjustability |
|--|-----------------------------------|-------------------------|-------------|---------------|
| Running On-Demand DL instances | 96 | 0 | 0 | Account level |
| Running On-Demand F instances | 64 | 0 | 0 | Account level |
| Running On-Demand G and VT instances | 0 | 0 | 0 | Account level |
| Running On-Demand High Memory instances | 0 | 0 | 0 | Account level |
| Running On-Demand HPC instances | 192 | 0 | 0 | Account level |
| Running On-Demand Iinf instances | 8 | 0 | 0 | Account level |
| Running On-Demand P instances | 0 | 0 | 0 | Account level |
| Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances | 256 | 5 | 1 | Account level |
| Running On-Demand Tm instances | 8 | 0 | 0 | Account level |
| Running On-Demand X instances | 0 | 0 | 0 | Account level |

Figure 34: Criteria list

Task 6: Test Stop Protection

You can stop your instance when you do not need to access but you would still like to retain it. In this task, you will learn how to use stop protection.

54. In the AWS Management Console, in the search box next to **Services**, search for and choose **EC2** to return to the EC2 console.

The screenshot shows the AWS EC2 homepage. The left navigation pane is open, showing sections like Instances, Images, and Elastic Block Store. The main content area is titled 'Instances' and displays a summary of resources: 2 running instances, 0 Auto Scaling Groups, 0 Capacity Reservations, 0 Dedicated Hosts, 0 Elastic IPs, 2 instances, 1 key pair, 0 load balancers, 0 placement groups, 5 security groups, 0 snapshots, and 2 volumes. There are also buttons for 'Launch instance' and 'Migrate a server'. To the right, there are sections for 'Account attributes' (Default VPC, Settings), 'Explore AWS' (Optimize EC2 Cost with Spot Instances and EC2 Auto Scaling), and 'Service health' (AWS Health Dashboard).

Figure 35: EC2 Homepage

55. In left navigation pane, choose **Instances**.

56. Select the **Web Server** instance and in the **Instance state ▾** menu, select **Stop instance**.

The screenshot shows the AWS EC2 Instances page. There are two instances listed:

- Web Server:** Instance ID i-09e2ad2cb0577d725, Running, t2.small, 2/2
- Bastion Host:** Instance ID i-08da93989df99c9fc, Running, t2.micro, 2/2

A context menu is open over the "Web Server" instance, with "Stop instance" highlighted. Other options in the menu include "Start instance", "Reboot instance", "Hibernate instance", and "Terminate (delete) instance".

Figure 36: Choose instance to stop

Stop instance

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

| Instance ID | Stop protection |
|--|-----------------------------|
| <input checked="" type="checkbox"/> i-09e2ad2cb0577d725 (Web Server) | ⚠️ On (Can't stop instance) |

You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

Associated resources
You will continue to incur charges for these resources while the instance is stopped

Skip OS shutdown
This option skips the graceful OS shutdown process. Use only when your instance must be stopped immediately, such as during an emergency or failover.
 Skip OS shutdown

Cancel **Stop**

Figure 37: Stop instance announcement

57. Then choose **Stop**

Note that there is a message that says: *Failed to stop the instance i-1234567xxx. The instance 'i-1234567xxx' may not be stopped. Modify its 'disableApiStop' instance attribute and try again.*

This shows that the stop protection that you enabled earlier in this lab is now providing a safeguard to prevent the accidental stopping of an instance. If you really want to stop the instance, you will need to disable the stop protection.

58. In the **Actions ▾** menu, select **Instance settings ▾ Change stop protection**.

59. Remove the check next to **Enable**.

60. Choose **Save**

You can now stop the instance.

61. Select the **Web Server** instance again and in the **Instance state ▾** menu, select **Stop instance**.

62. Choose **Stop**

 **Congratulations!** You have successfully tested stop protection and stopped your instance.

C. Submitting My Work

63. To record your progress, choose **Submit** at the top of these instructions.

64. When prompted, choose **Yes**.

After a couple of minutes, the grades panel appears and shows you how many points you earned for each task. If the results don't display after a couple of minutes, choose **Grades** at the top of these instructions.

 **Important:** Some of the checks made by the submission process in this lab will only give you credit if it has been at least 5 minutes since you completed the action. If you do not receive credit the first time you submit, you may need to wait a couple minutes and submit again to receive credit for these items.

 **Tip:** You can submit your work multiple times. After you change your work, choose **Submit** again. Your last submission is recorded for this lab.

65. To find detailed feedback about your work, choose **Submission Report**.

 **Tip:** For any checks where you did not receive full points, there are sometimes helpful details provided in the submission report.

| | |
|---|-------|
| Total score | 25/25 |
| Task 1 - EC2 instance created correctly | 5/5 |
| Task 2 - get system log requested | 5/5 |
| Task 3 - security group updated | 5/5 |
| Task 4 - EC2 instance updated | 5/5 |
| Task 6 - Instance stopped on second try | 5/5 |

