

2. Introduction to Amazon EC2

Task 1: Launch Your Amazon EC2 Instance

1. In this task, you will launch an Amazon EC2 instance with termination protection. Termination protection prevents you from accidentally terminating an EC2 instance. You will deploy your instance with a User Data script that will allow you to deploy a simple web server.

2. In the **AWS Management Console** in the search box to the right of **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.

3. Choose Launch Instances

Step 1: Name and tags

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

The Name you give this instance will be stored as a tag. Tags enable you to categorise 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**

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

5. In the list of available Quick Start AMIs, keep the default **Amazon Linux** AMI selected.
6. Also keep the default **Amazon Linux 2 AMI (HVM)** selected.

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. A template for the root volume for the instance (for example, an operating system or an application server with applications)
 - b. Launch permissions that control which AWS accounts can use the AMI to launch instances
 - c. A block device mapping that specifies the volumes to attach to the instance when it is launched
7. 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.

Step 3: Instance type

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

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.

 - a.

Step 4: Key pair (login)

9. For **Key pair name - required**, choose **vokey**.

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 authorised 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.

a.

Step 5: Network settings

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

11. 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.

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

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

a. **Security group name:** Web Server security group

b. **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.

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

d.

Step 6: Configure storage

13. In the Configure storage section, keep the default settings.

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).

a.

Step 7: Advanced details

14. Expand **Advanced details**.

15. 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.

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

```
17.#!/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
```

18. 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 2. 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

- d. Create a simple web page

Step 8: Launch the instance

19. At the bottom of the **Summary** panel on the right side of the screen choose Launch Instances
You will see a Success message.
20. Choose View all instances
 - a. Your **Web Server** should be selected.
 - b. Review the information displayed in the **Details** tab. It includes information about the instance type, security settings and network settings.
The instance receives 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
21. Wait for your instance to display the following:
 - a. **Instance State:** Running
 - b. **Status Checks:** 2/2 checks passed
22. **Congratulations!** You have successfully launched your first Amazon EC2 instance.

The screenshot shows the AWS Management Console interface for EC2 instances. On the left is a navigation sidebar with options like EC2 Dashboard, Events, Tags, Limits, and a list of instance types. The main area is titled 'Instances (1/2)' and contains a table with two instances: 'Web Server' (ID: i-0458fc20f4648d227) and 'Bastion Host' (ID: i-0ced84d441bd9836d). Both are in a 'Running' state. Below the table, the details for the 'Web Server' instance are shown in a tabbed view. The 'Details' tab is active, displaying information such as the Instance ID, Public IPv4 address (54.235.24.137), Instance state (Running), Private IP DNS name (ip-10-0-1-77.ec2.internal), and Public IPv4 DNS (ec2-54-235-24-137.compute-1.amazonaws.com).

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Web Server	i-0458fc20f4648d227	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a
Bastion Host	i-0ced84d441bd9836d	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a

Instance: i-0458fc20f4648d227 (Web Server)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary Info

Instance ID i-0458fc20f4648d227 (Web Server)	Public IPv4 address 54.235.24.137 open address	Private IPv4 addresses 10.0.1.77
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-235-24-137.compute-1.amazonaws.com open address
Hostname type IP name: ip-10-0-1-77.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-1-77.ec2.internal	Elastic IP addresses
Answer private resource DNS name	Instance type	

Task 2: Monitor Your Instance

23. 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.

24. 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.

25. 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.

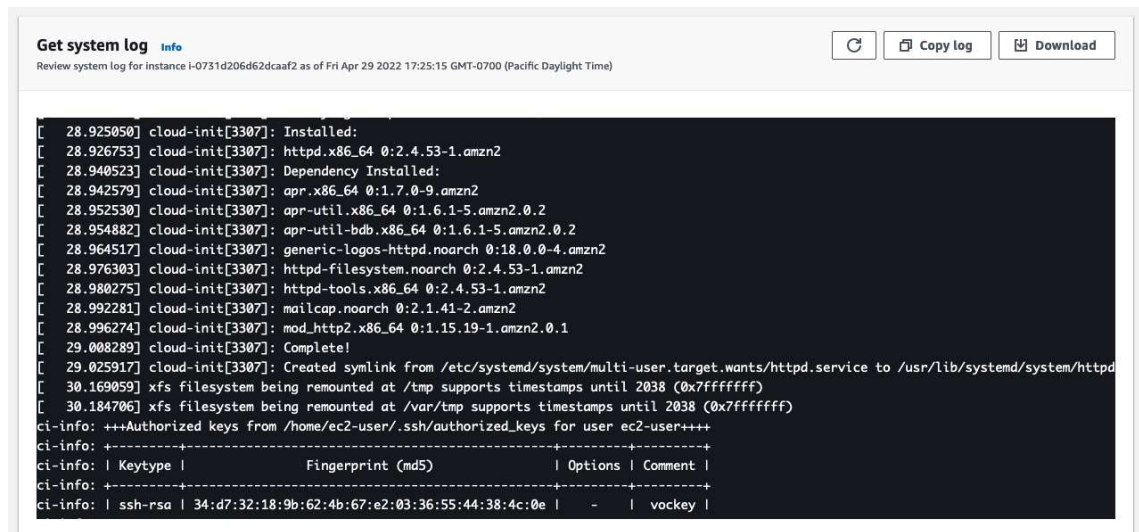
You can choose the three dots icon in any graph and select **Enlarge** to see an expanded view of the chosen metric.

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.

26. 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.

27. Scroll through the output and note that the HTTP package was installed from the **user data** that you added when you created the instance.



Get system log [Info](#) [Copy log](#) [Download](#)

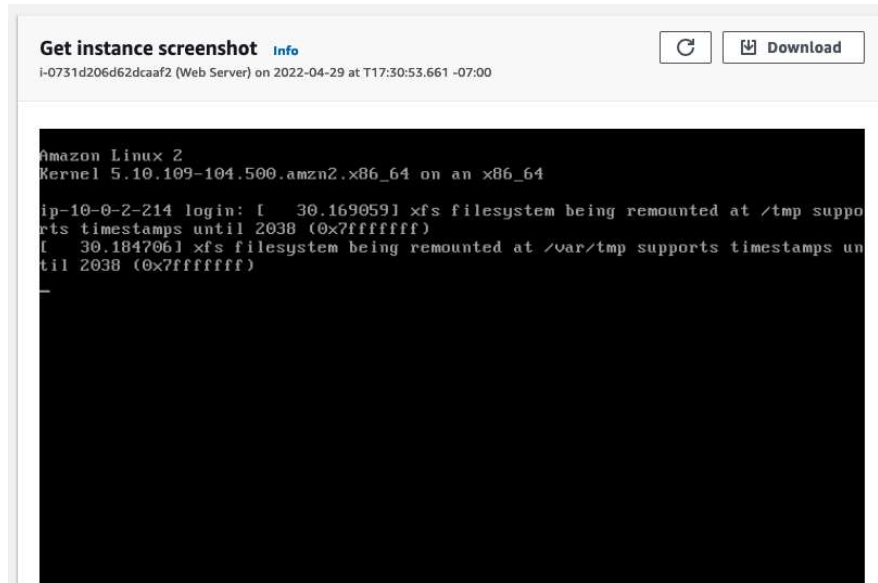
Review system log for instance i-0731d206d62dcaaf2 as of Fri Apr 29 2022 17:25:15 GMT-0700 (Pacific Daylight Time)

```
[ 28.925050] cloud-init[3307]: Installed:
[ 28.926753] cloud-init[3307]: httpd.x86_64 0:2.4.53-1.amzn2
[ 28.940523] cloud-init[3307]: Dependency Installed:
[ 28.942579] cloud-init[3307]: apr.x86_64 0:1.7.0-9.amzn2
[ 28.952530] cloud-init[3307]: apr-util.x86_64 0:1.6.1-5.amzn2.0.2
[ 28.954882] cloud-init[3307]: apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2
[ 28.964517] cloud-init[3307]: generic-logos-httpd.noarch 0:18.0.0-4.amzn2
[ 28.976303] cloud-init[3307]: httpd-filesystem.noarch 0:2.4.53-1.amzn2
[ 28.980275] cloud-init[3307]: httpd-tools.x86_64 0:2.4.53-1.amzn2
[ 28.992281] cloud-init[3307]: mailcap.noarch 0:2.1.41-2.amzn2
[ 28.996274] cloud-init[3307]: mod_http2.x86_64 0:1.15.19-1.amzn2.0.1
[ 29.008289] cloud-init[3307]: Complete!
[ 29.025917] cloud-init[3307]: Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service
[ 30.169059] xfs filesystem being remounted at /tmp supports timestamps until 2038 (0x7fffffff)
[ 30.184706] xfs filesystem being remounted at /var/tmp supports timestamps until 2038 (0x7fffffff)
ci-info: +++Authorized keys from /home/ec2-user/.ssh/authorized_keys for user ec2-user+++
ci-info: +-----+
ci-info: | Keytype |          Fingerprint (md5)          | Options | Comment |
ci-info: +-----+-----+-----+-----+-----+
ci-info: | ssh-rsa | 34:d7:32:18:9b:62:4b:67:e2:03:36:55:44:38:4c:0e | - | vockey |
```

28. Choose **Cancel**.

29. Ensure **Web Server** is still selected. Then, 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.



Get instance screenshot [Info](#) [Download](#)

i-0731d206d62dcaaf2 (Web Server) on 2022-04-29 at T17:30:53.661 -07:00

```
Amazon Linux 2
Kernel 5.10.109-104.500.amzn2.x86_64 on an x86_64

ip-10-0-2-214 login: [ 30.169059] xfs filesystem being remounted at /tmp supports timestamps until 2038 (0x7fffffff)
[ 30.184706] xfs filesystem being remounted at /var/tmp supports timestamps until 2038 (0x7fffffff)
```

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

30. Choose **Cancel**.

Congratulations! You have explored several ways to monitor your instance.

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

31. 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.

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

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

34. 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.

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

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

37. Select **Web Server security group**.

38. Choose the **Inbound rules** tab.

The security group currently has no inbound rules.

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

a. **Type:** HTTP

- b. **Source:** Anywhere-IPv4
 - c. Choose Save rules
40. 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!

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

41. 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.

Stop Your Instance

42. Before you can resize an instance, you must stop it.
43. 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.
44. On the **EC2 Management Console**, in the left navigation pane, choose **Instances**.
- Web Server** should already be selected.

45. In the **Instance State** menu, select **Stop instance**.

46. Choose Stop

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

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

Change The Instance Type

48. In the **Actions** menu, select **Instance settings Change instance type**, then configure:

a. **Instance Type:** t2.small

b. 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.

Resize the EBS Volume

49. Choose the **Storage tab**, select the name of the Volume ID, then select the checkbox next to the volume that displays.

50. 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.

51. Change the size to: **10** **NOTE:** You may be restricted from creating large Amazon EBS volumes in this lab.

52. Choose **Modify**

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

Start the Resized Instance

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

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

56. Select the **Web Server** instance.

57. 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

58. 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.

a.

59. In the left navigation pane, choose **Limits**.

Note: You may see some banner messages indicating that you cannot load some limits. You can safely ignore these messages.

60. From the **All limits** drop down list, choose **Running instances**.

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 Standards... 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.

You can request an increase for many of these limits.

Task 6: Test Termination Protection

61. 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.

62. In left navigation pane, choose Instances.

63. Select the **Web Server** instance and in the **Instance state** menu, select **Terminate instance**.

64. Then choose Terminate

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

This is a safeguard to prevent the accidental termination of an instance. If you really want to terminate the instance, you will need to disable the termination protection.

65. In the **Actions** menu, select **Instance settings Change termination protection**.

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

67. Choose Save

You can now terminate the instance.

68. Select the **Web Server** instance again and in the **Instance state** menu, select **Terminate instance**.

69. Choose Terminate

Congratulations! You have successfully tested termination protection and terminated your instance.

