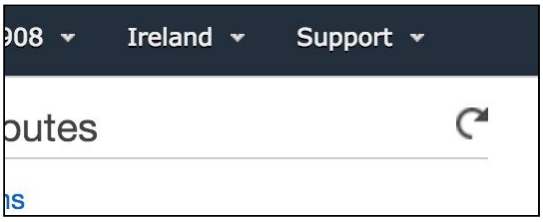
Lab 2: Introduction to Amazon EC2

Task 1: Launch Your Amazon EC2 Instance

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.

For this Lab you can make use of the region 'Ireland' (see right corner of the page)



1) In the **AWS Management Console** on the **Services** menu, click **EC2**.

2) Click **Launch Instance**

Step 1: Choose an Amazon Machine Image (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. 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.

3) Click **Select** next to **Amazon Linux 2 AMI** (at the top of the list).

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your

applications. Each instance type includes one or more *instance sizes*, allowing you to scale your resources to the requirements of your target workload.

You will use a **t2.micro** instance which should be selected by default. This instance type has 1 virtual CPU and 1 GiB of memory. When you are in the free tier of your aws account you can use **t2.micro's** for 750 hours per month for free. Note that any other instance type will be outside the free tier and will incur charges to your credit card.

4) Click **Next: Configure Instance Details**

Step 3: Configure Instance Details

This page is used to configure the instance to suit your requirements. This includes networking and monitoring settings.

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

5) For **Network**, select the **default** VPC.

his VPC includes three public subnets in two different Availability Zones.

6) For **Enable termination protection**, select **Protect against accidental termination**.

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 you want to prevent the instance from being accidentally terminated, you can enable *termination protection* for the instance, which prevents it from being terminated.

7) Scroll down, then expand **Advanced Details**.

A field for **User data** will appear.

When you launch an instance, you 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.

Your instance is running Amazon Linux, so you will provide a *shell script* that will run when the instance starts.

8) Copy the following commands and paste them into the **User data** field:

```
#!/bin/bash
yum -y install httpd
chkconfig httpd on
systemctl start httpd
```

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

The script will:

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

9) Click **Next: Add Storage**

Step 4: Add Storage

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).

10) Click **Next: Add Tags**

Step 5: Add Tags

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.

11) Click **Add Tag** then configure:

- **Key:** Name
- **Value:** Web Server

12) Click **Next: Configure Security Group**

Step 6: Configure Security Group

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.

13) On **Step 6: Configure Security Group**, configure:

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

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

14) Delete the existing SSH rule.

15) Click **Review and Launch**

Step 7: Review Instance Launch

The Review page displays the configuration for the instance you are about to launch.

16) Click **Launch**

A **Select an existing key pair or create a new key pair** window will appear.
Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

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

17) Click the **Create a new keypair** drop-down, fill in a **Key Pair Name**

18) Click on **Download Key Pair**

19) Click **Launch Instances**

Your instance will now be launched.

20) Click **View Instances**

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

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

Your **Web Server** should be selected. The **Description** tab displays detailed information about your instance.

To view more information in the Description tab, drag the window divider upwards.
Review the information displayed in the **Description** tab. It includes information about the instance type, security settings and network settings.

21) 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.

Task 2: Update Your Security Group and Access the Web Server

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

22) Click the **Description** tab.

23) Copy the **IPv4 Public IP** of your instance to your clipboard.

24) 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.

24) Keep the browser tab open, but return to the **EC2 Management Console** tab.

25) In the left navigation pane, click **Security Groups**.

26) Select **Web Server security group**.

27) Click the **Inbound** tab.

The security group currently has no rules.

28) Click **Edit** then configure:

- **Type:** *HTTP*
- **Source:** *Anywhere*
- Click **Save**

29) 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 size of a disk.

Stop Your Instance

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

Resize the EBS Volume

30) In the left navigation menu, click **Volumes**.

31) 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.

32) Change the size to:

33) Click **Modify**

34) Click **Yes** to confirm and increase the size of the volume.

35) Click **Close**

Start the Resized Instance

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

36) In left navigation pane, click **Instances**.

37) In the **Actions** menu, select **Instance State Start**.

38) Click **Yes, Start**

Congratulations! You have successfully 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.

39) In the left navigation pane, click **Limits**.

Note that there is a limit on the number of instances that you can launch in this region. When launching an instance, the request must not cause your usage to exceed the current instance limit in that region.

You can request an increase for many of these limits.

Task 6: Test Termination Protection

You can delete your instance when you no longer need it. This is referred to as *terminating* your instance. You cannot connect to or restart an instance after it has been terminated.
In this task, you will learn how to use *termination protection*.

40) In left navigation pane, click **Instances**.

41) In the **Actions** menu, select **Instance State Terminate**.
Note that there is a message that says: *These instances have Termination Protection and will not be terminated. Use the Change Termination Protection option from the Instances screen Actions menu to allow termination of these instances.*

Also, the **Yes, Terminate** button is dimmed and cannot be clicked.
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.

42) Click **Cancel**.

43) In the **Actions** menu, select **Instance Settings Change Termination Protection**.

44) Click **Yes, Disable**

You can now terminate the instance.

45) In the **Actions** menu, select **Instance State Terminate**.

46) Click **Yes, Terminate**

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