Lab 1 - Introduction to Amazon EC2

Objective: To create and Lunch Amazon EC2 instance

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.

1. In the AWS Management Console in the search box to the right of Services, choose Compute and then choose EC2.
    a. 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.
2. Choose Lunch Instance

    Step 1: Name and tags

3. Give the instance the name Web Server.
    a. 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.
    b. 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)

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

5. Also keep the default Amazon Linux 2 AMI (HVM**)** selected.
    a. An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. An AMI includes:
    b. A template for the root volume for the instance (for example, an operating system or an application server with applications)
    c. Launch permissions that control which AWS accounts can use the AMI to launch instances
    d. A block device mapping that specifies the volumes to attach to the instance when it is launched
    e. 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

6. In the Instance type panel, keep the default t2.micro selected.
    a. 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.
    b. The t2.micro instance type has 1 virtual CPU and 1 GiB of memory.
    c. **Note**: You may be restricted from using other instance types in this lab.

Step 4: Key pair (login)

7. For Key pair name - required, choose vockey.
    a. 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.

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

Step 5: Network settings

8. Next to Network settings, choose Edit.
9. For VPC, select Lab VPC.
    a. 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.
    b. 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.
10. 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
        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.
    c. Under Inbound security group rules, notice that one rule exists. Remove this rule.

Step 6: Configure storage

11. In the Configure storage section, keep the default settings.
    a. Amazon EC2 stores data on a network-attached virtual disk called Elastic Block Store.

b. 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

12. Expand Advanced details.
13. For Termination protection, select Enable.
    a. 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.
14. Scroll to the bottom of the page and then copy and paste the code shown below into the User data box:

a. 

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

g. 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.
h. 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:
i. Install an Apache web server (httpd)
j. Configure the web server to automatically start on boot
k. Run the Web server once it has finished installing

l. Create a simple web page

15. Step 8: Launch the instance
16. At the bottom of the Summary panel on the right side of the screen choose Launch instance You will see a Success message.
17. Choose View all instance
    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.
        i. The instance receives a Public IPv4 DNS that you can use to contact the instance from the Internet.
        ii. To view more information, drag the window divider upwards.
        iii. 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
18. Wait for your instance to display the following:
    a. Instance State**:** Running
    b. Status Checks**:** 2/2 checks passed

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.

1. Choose the Status Checks tab.
    a. 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.
    b. Notice that both the System reachability and Instance reachability checks have passed
2. Choose the Monitoring tab.
    a. This tab displays Amazon CloudWatch metrics for your instance. Currently, there are not many metrics to display because the instance was recently launched.

    b. You can choose the three dots icon in any graph and select Enlarge to see an expanded view of the chosen metric.
    c. 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.
3. In the Action menu towards the top of the console, select Monitor and troubleshoot Get system log.
    a. 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.
4. Scroll through the output and note that the HTTP package was installed from the user data that you added when you created the instance.
5. Choose Cancel.
6. Ensure Web Server is still selected. Then, in the Action menu, select Monitor and troubleshoot Get instance screenshot.
    a. This shows you what your Amazon EC2 instance console would look like if a screen were attached to it.
    b. 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.
7. Choose Cancel.

Task 3: 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.

1. Ensure Web Server is still selected. Choose the Details tab.
2. Copy the Public IPv4 address of your instance to your clipboard.
3. Open a new tab in your web browser, paste the IP address you just copied, then press Enter.

a. Question**:** Are you able to access your web server? Why not?
b. 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.
c. To correct this, you will now update the security group to permit web traffic on port 80.

4. Keep the browser tab open, but return to the EC2 Console tab.
5. In the left navigation pane, choose Security Groups.
6. Select Web Server security group.
7. Choose the Inbound rules tab.
    a. The security group currently has no inbound rules.
8. Choose Edit inbound rule, select Add rules and then configure:
    a. Type**:** HTTP
    b. Source**:** Anywhere-IPv4
    c. Choose Save Rules
9. Return to the web server tab that you previously opened and refresh the page.
    a. You should see the message Hello From Your Web Server!

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.

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 runtime 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.
    a. Web Server should already be selected.
2. In the Instance State menu, select Stop instance.
3. Choose Stop
    a. Your instance will perform a normal shutdown and then will stop running.
4. Wait for the Instance State to display: Stopped.

Change The Instance Type

1. In the Actions menu, select Instance settings Change instance type, then configure:
    a. Instance Type**:** t2.small
    b. Choose Apply
        i. 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.
2. Resize the EBS Volume
3. Choose the Storage tab, select the name of the Volume ID, then select the checkbox next to the volume that displays.
4. In the Actions menu, select Modify volume.
    a. The disk volume currently has a size of 8 GiB. You will now increase the size of this disk.
5. Change the size to:10
6. Choose Modify
7. Choose Modify again to confirm and increase the size of the volume.
8. Start the Resized Instance
9. You will now start the instance again, which will now have more memory and more disk space.
10. In left navigation pane, choose Instances.
11. Select the Web Server instance.
12. In the Instance State menu, select Start instance.

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.

1. In the left navigation pane, choose Limits.
    a. Note: You may seem some banner messages indicating that you cannot load some limits. You can safely ignore these messages.

2. From the All limits drop down list, choose Running instances.
    a. 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.
    b. 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.

1. In left navigation pane, choose Instances.
2. Select the Web Server instance and in the Instance State menu, select Terminate instance.
3. Then choose Terminate
4. In the Actions menu, select Instance settings Change termination protection.
5. Remove the check next to Enable.
6. Choose Save

    a. You can now terminate the instance.
7. Select the Web Server instance again and in the Instance State menu, select Terminate instance.
8. Choose Terminate

Conclusion: EC2 instance has been created, stopped and terminated in sandbox environment.