Lab 2: Creating an EC2 Instance

Overview

The objective of this lab is to use the AWS Management Console to launch an EC2 instance that hosts a simple website.

Objective

- Create an EC2 instance that hosts a simple website.

Lab instructions

Access the AWS Management Console

1. To start the lab session, choose **Start Lab** in the upper-right corner of the page.
    - The lab session starts.
    - A timer displays in the upper-right corner 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 continuing, wait until the lab environment is ready. The environment is ready when the lab details appear on the right side of the page and the circle icon next to the **AWS** link in the upper-left corner turns green.

2. To return to these instructions, choose the **Readme** link in the upper-right corner.
3. To connect to the AWS Management Console, choose the **AWS** link in the upper-left corner, above the terminal window.

   A new browser tab opens and connects you to the AWS Management 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**.

Task 1. Start creating the instance and assign a name

4. Choose the **Services** menu, locate the **Compute** services, and select **EC2**.
5. Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.
6. Name the instance:
    - Give it the name `Web Server 1`

    Tags help you 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*, which you define.

    Note: *Name* is simply another tag. The *key* for this tag is `Name`, and the *value* is `Web Server 1`.

Task 2. Application and OS Images

7. Choose an AMI from which to create the instance:
    - In the list of available *Quick Start* AMIs, keep the default **Amazon Linux** AMI selected.
    - Also keep the default **Amazon Linux 2 AMI (HVM)** selected.

      The type of *Amazon Machine Image (AMI)* you choose determines the Operating System (OS) that will run on the EC2 instance that you launch. In the case, you have chosen Amazon Linux 2 as the guest OS.

Task 3. Choose an instance type

8. Specify an Instance type:
    - In the *Instance type* panel, keep the default **t2.micro** selected.

      The *Instance Type* defines the hardware resources assigned to the instance. This instance type has 1 virtual central processing unit (CPU) and 1 GiB of memory.

Task 4. Choose a key pair

9. Select the key pair to associate with the instance:
    - From the **Key pair name** menu, select **vockey**.

      The *vockey* key pair you selected will allow you to connect to this instance via SSH after it has launched. Although you will not need to do that in this lab, it is still required to identify an existing key pair, or create a new one, when you launch an instance.

Task 5. Network settings

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

11. Keep the default *VPC* and *subnet* settings. Also keep the **Auto-assign public IP** setting set to **Enable**.

    The Network indicates the virtual private cloud (VPC) you want to launch the instance into. You can have multiple networks; for example, one for *development*, a second for *testing*, and a third for *production.*

12. Under *Firewall (security groups)*, keep the default **Create security group** option chosen.

13. Configure a new security group:
    - Keep the default selection **Create a new security group**.
    - **Security group name:** Clear the text and enter `Web Server`
    - **Description:** Clear the text and enter `Security group for my web server`
    - Choose **Remove** to remove the default SSH inbound rule.

      Note: You will configure a different inbound rule later in this lab.

      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.

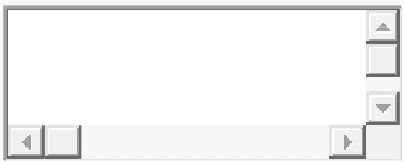
Task 6. Configure storage

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

    You will launch the Amazon EC2 instance using a default Elastic Block Store (EBS) disk volume. This will be your root volume (also known as a *boot volume*) which will host the Amazon Linux 2 guest operating system that you specified earlier. It will run on a general purpose SSD (*gp2*) hard drive that is 8 GiB in size. You could alternatively add more storage volumes, however that is not needed in this lab.

Task 7. Advanced details

15. Configure a script to run on the instance when it launches:
    - Expand the **Advanced details** panel.
    - Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box:



```
#!/bin/bash
yum update -y
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello World!</h1></html>' > /var/www/html/index.html
```

    This bash script will run with root user permissions on the guest OS of the instance. It will run automatically when the instance launches for the first time. This script does the following:

    - Updates the server
    - Installs an Apache web server (httpd)
    - Configures the web server to automatically start on boot
    - Activates the web server
    - Creates a simple webpage

Task 8. Review the instance and launch

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 instances**

    The instance will first appear in the *Pending* state, which means it is being launched. The state will then change to *Running*, which indicates that the instance has started booting. It takes a few minutes for the instance to boot.

18. Select the **Web Server 1** instance and review the information in the **Details** tab that displays in the lower pane.

    Notice that the instance has a **Public IPv4 address**. You can use this IP address to communicate with the instance from the internet.

19. Before you continue, wait for your instance to display the following:
    - **Instance state:** *Running*
    - **Status check:** *2/2 checks passed*

      This may take a few minutes. Choose the refresh icon at the top of the page every 30 seconds or so to become more quickly aware of the latest status of the instance.

Task 9. Access your EC2 instance

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

20. From the **Details** tab, copy the **Public IPv4 address** value of your instance to your clipboard.

    Note: A *public* address means that the instance can be reached from the internet. Each instance that receives a public IP address is also given an external DNS hostname; for example, ec2-xxx-xxx-xxx-xxx.compute-1.amazonaws.com. AWS resolves an external DNS hostname to the *public* IP address of the instance when communicate comes from outside its VPC.

When communicate comes from inside its VPC, the DNS hostname is resolved to the *private* IPv4 address.

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

    The webpage does not load. You must update the security group to be able to access the page.

Task 10. Update the security group

You are not 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. In this task, you update the security group.

22. Return to the **EC2 Management Console** browser tab.
23. In the left navigation pane, under **Network & Security**, choose **Security Groups**.
24. Select the **Web Server** security group, which you created when launching your EC2 instance.
25. In the lower pane, choose the **Inbound rules** tab.

Task 11. Create an inbound rule

26. Choose **Edit inbound rules**, and then choose **Add rule**.
27. Configure the following:
    - **Type:** HTTP
    - **Source:** Anywhere-IPv4
    - Choose **Save rules**

    The new inbound HTTP rule creates an entry for IPv4 IP (0.0.0.0/0) and IPv6 IP addresses (::/0).

Task 12. Test the rule

28. Return to the tab that you used to try to connect to the web server.
29. Refresh the page.

    The page should display the message *Hello World!*

Lab complete

Congratulations! You have completed the lab.

30. Log out of the AWS Management Console.
    - In the upper-right corner of the page, choose your user name. Your user name begins with **voclabs/user**.
    - Choose **Sign out**.
31. Choose **End Lab** at the top of this page, and then select **Yes** to confirm that you want to end the lab.