|  |
| --- |
|  |
|  |
| Amazon Cloud Foundations Labs Part 1  Made by: - Akshat Kansal |
| **CCNP lab 8 – Mr. Mason & Mr. Hansen**  **Periods 0,1,2** |

**Purpose**

The purpose of the Amazon Cloud Foundations Labs is to provide hands-on experience with the AWS platform, allowing individuals to gain practical knowledge and skills in cloud computing. Through these labs, participants can learn how to set up and manage AWS services, as well as build and deploy applications in the cloud.

**Background**

The background of these labs is that they were created by AWS as a way to introduce new users to the AWS platform and provide a foundation for more advanced learning. The labs are designed to be accessible to individuals with no prior experience in cloud computing or AWS, while still offering valuable insights and skills to those with more advanced knowledge.

Lab 1 of the Amazon Cloud Foundations Labs is focused on setting up an AWS account and gaining familiarity with the AWS Management Console. Participants are guided through the process of creating an AWS account, configuring security settings, and navigating the AWS Management Console. This lab is designed to provide a foundation for more advanced labs, as well as introduce individuals to the basics of working with AWS.

Lab 2 of the Amazon Cloud Foundations Labs covers Amazon Simple Storage Service (S3), a highly scalable, secure, and durable object storage service. Participants learn how to create an S3 bucket, upload and manage objects, and set up access policies. This lab is designed to teach individuals how to use S3 as a data storage solution in the cloud.

Lab 3 of the Amazon Cloud Foundations Labs focuses on Amazon Elastic Compute Cloud (EC2), a web service that provides resizable compute capacity in the cloud. Participants learn how to launch and configure an EC2 instance, connect to it using SSH, and install and run a web server. This lab is designed to teach individuals how to use EC2 as a computing solution in the cloud.

**Lab 1**

How to Access AWS Console:

1. Click on the “Launch Lab” button at the top right of the page to start the lab.
2. Wait until the lab status shows “ready”.
3. Click on the “Open AWS Management Console” button at the top right of the page. This will open a new browser tab containing the AWS Management Console (make sure pop-ups are allowed on your computer).
4. Position the AWS Management Console tab so that you can read the instructions as you navigate the Management Console.

Task 1 - Explore Users and Groups: 5. In the AWS Management Console, go to the Services menu and select IAM.

1. In the left panel, choose Users.
2. Three users (user-1, user-2, and user-3) have already been created for you.
3. Select user-1. a. Click on the Permissions tab to see that user-1 does not have any permissions.
4. Click on the Groups tab. a. Note that user-1 is not a member of any groups.
5. Click on the Security Credentials tab. a. Note that user-1 has been assigned a console password.
6. In the left panel, choose User Groups.
7. Three groups (EC2-Admin, EC2-Support, and S3-Support) have already been created for you.
8. Select the EC2-Support group and go to the Permissions tab. a. Note that this group has a managed policy associated with it, called AmazonEC2ReadOnlyAccess. b. Managed policies are pre-determined policies made by AWS or an administrator. They can be associated with individual users and groups, and when changes to the policy take place, they immediately apply against all users and groups that are attached to the policy.
9. Click on the plus (+) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details. a. Note that this policy allows permission to list and describe information about EC2 and other policies such as Elastic Load Balancing, CloudWatch, and Auto Scaling. Being able to see resources but not change them is crucial for assigning support roles. b. The basic structure of the statements in IAM is: -effect which allows or denies permissions -action which specifies changes made against the AWS service -resource which defines the entities covered by the policy
10. Click on the minus icon to close the policy details.
11. In the left panel, choose User Groups.
12. Select the S3-Support group and go to the Permissions tab. a. Note that this group has AmazonS3ReadOnlyAccess.
13. Click on the plus icon to view the policy details. a. Note that this specific policy grants permission to get resources.
14. Click on the minus icon to hide the policy details.
15. In the left panel, choose User Groups.
16. Select the EC2-Admin group and go to the Permissions tab. a. Note that this group has an inline policy, which is a policy only assigned to one user or group.
17. Click on the plus icon to see the policy details. a. Note that this policy allows permission for a user to view information about Amazon EC2 and allows the ability to start and stop instances.
18. Click on the minus icon to hide the policy details.

Applicable Business Scenario: For the remainder of this lab, you will assign policies to these users and groups to support the following business scenario: Your company is beginning its use of Amazon Web Services and is using Amazon EC2 instances and some Amazon S3 storage. Based on their job, you will give access to new staff.

**Lab 2**

Task 1: Creating a VPC

1. Open the AWS Management Console and navigate to the Services menu, then select VPC.
2. Click on Launch VPC Wizard.
3. In the left navigation pane, select "VPC with Public and Private Subnets" (the second option).
4. Choose "Select" and configure the following settings: a. VPC name: Lab VPC b. Availability Zone: Select the first Availability Zone. c. Public subnet name: Public Subnet 1 d. Availability Zone: Select the first Availability Zone (same as above) e. Private subnet name: Private Subnet 1 f. Elastic IP Allocation ID: Choose the displayed IP address from the box.
5. Click on "Create VPC."
6. Once it is complete, select "OK."
7. In the left navigation pane, select "Subnets."
8. Click on "Create subnet" and configure the following settings: a. VPC ID: Lab VPC b. Subnet name: Public Subnet 2 c. Availability Zone: Select the second Availability Zone. d. IPv4 CIDR block: 10.0.2.0/24
9. Click on "Create subnet."
10. Click on "Create subnet" again and configure the following settings: a. VPC ID: Lab VPC b. Subnet name: Private Subnet 2 c. Availability Zone: Select the second Availability Zone. d. CIDR block: 10.0.3.0/24
11. Click on "Create subnet."
12. In the left navigation pane, select "Route Tables."
13. Select the route table with Main = Yes and VPC = Lab VPC. (If necessary, expand the VPC ID column to view the VPC name.)
14. In the "Name" column for this route table, click on the pencil icon and type "Private Route Table." Click on "Save."
15. In the lower pane, select the "Routes" tab.
16. In the lower pane, select the "Subnet Associations" tab.
17. Click on "Edit subnet," and select both "Private Subnet 1" and "Private Subnet 2."
18. Click on "Save associations."
19. Select the route table with Main = No and VPC = Lab VPC (and deselect any other subnets).
20. In the "Name" column for this route table, click on the pencil icon and type "Public Route Table." Click on "Save."
21. In the lower pane, select the "Routes" tab.
22. Select the "Subnet Associations" tab.
23. Click on "Edit subnet associations."
24. Select both "Public Subnet 1" and "Public Subnet 2."
25. Click on "Save associations."

Task 3: Creating a VPC Security Group 26. In the left navigation pane, select "Security Groups."

1. Click on "Create security group" and configure the following settings: a. Security group name: Web Security Group b. Description: Enable HTTP access c. VPC: Lab VPC
2. In the Inbound rules pane, click on "Add rule."
3. Configure the following settings: a. Type: HTTP b. Source: Anywhere-IPv4 c. Description: Permit web requests
4. Scroll to the bottom of the page and click on "Create security group."

Task 4: Launching a Web Server Instance 31. On the Services menu, select EC2.

1. Click on "Launch Instance," and then select "Launch Instance."

From the Amazon Machine Image (AMI) list, select "Amazon Linux 2 AMI (HVM), SSD Volume Type".

1. Choose the "t2.micro" instance type and click "Next: Configure Instance Details".
2. Configure the instance details as follows: a. Network: Select "Lab VPC" b. Subnet: Select "Public Subnet 2" c. Auto-assign Public IP: Enable
3. Click "Next: Add Storage". Leave the default settings and click "Next: Add Tags".
4. Under "Add Tags", click "Add Tag", then set the Key to "Name" and the Value to "Web Server 1". Click "Next: Configure Security Group".
5. Select "Select an existing security group", then select the "Web Security Group" you created earlier. Click "Review and Launch".
6. Review the instance details and click "Launch".
7. When prompted to select a key pair, select "Proceed without a key pair" and check the acknowledgement box. Then click "Launch Instances".
8. Select "View Instances".
9. Wait until the instance shows "2/2 checks passed" in the Status Checks column in the "Instances" tab.

Task 5: Connect to the Web Server 43. In the "Instances" tab, select the instance you just launched, and then click "Connect".

1. In the "Connect To Your Instance" dialog box, select "EC2 Instance Connect (browser-based SSH connection)", and then click "Connect".
2. A terminal window will open with a SSH connection to your instance.
3. Run the following command to switch to the root user: sudo su
4. Enter your password if prompted, and then run the following command to verify that Apache is running: systemctl status httpd
5. Open a web browser and navigate to the public IP address of your instance (you can find this under the "IPv4 Public IP" column in the "Instances" tab).
6. You should see a default Apache web page indicating that Apache is running. If you see this page, you have successfully launched and connected to your web server instance.

**Lab 3**

Task 1: Launch Your Amazon EC2 Instance

1. Open the EC2 console and select an Amazon Machine Image (AMI) Step 1: Choose an Amazon Machine Image (AMI) Choose the Amazon Linux 2 AMI and click "Select".
2. Choose an Instance Type The t2.micro instance type should be selected by default. Leave it as is.
3. Configure Instance Details For "Network", select "Lab VPC".
4. Enable Termination Protection Check the box for "Protect against accidental termination".
5. Expand Advanced Details Scroll down and click "Advanced Details".
6. Add User Data Copy and paste the following commands into the "User data" field:

#!/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

1. Choose Next: Add Storage
2. Add Tags In the "Add tags" section, add a tag with Key: "Name" and Value: "Web Server".
3. Configure Security Group In the "Configure Security Group" section, create a new security group named "Web Server Security Group" with a description "Security group for my web server".
4. Delete Existing SSH Command Delete the existing SSH command listed in the security group inbound rules.
5. Review and Launch Instance Click "Review and Launch" and then select "Launch".
6. Select/Create Key Pair Choose an existing key pair or create a new one.
7. Acknowledge and Launch Check the box for "I acknowledge that...", and click "Launch Instances".
8. View Instances Click "View Instances".
9. Wait for the Instance to Launch Wait for your instance to reach "Instance State: running" and "Status Checks: 2/2 checks passed".

Task 2: Monitor Your Instance 16. Click on the instance to select it.

1. Select the "Status Checks" tab.
2. Choose the "Monitoring" tab.
3. Get System Log In the "Actions" dropdown, select "Monitor and troubleshoot", and then select "Get System Log".
4. Verify HTTP Package Installation Scroll to the output and verify that the HTTP package is installed from the user data that you added when you launched the instance.
5. Choose "Cancel".

Task 3: Update Your Security Group and Access the Web Server 22. Open a new tab in your browser.

1. Paste the IPv4 Public IP of your instance into the address bar and press "Enter".
2. Keep the browser open and return to the EC2 Management Console.
3. In the left navigation panel, select "Security Groups".
4. Choose the "Web Server Security Group".
5. Select the "Inbound Rules" tab.
6. Edit Inbound Rules Click "Edit inbound rules" and configure the following rule: Type: HTTP Source: Anywhere-IPv4
7. Return to the web server tab.

Task 4: Resize Your Instance: Instance Type and EBS Volume 30. In the EC2 console, select "Instances".

1. Stop Instance In the instance menu, select "Stop instance".
2. Wait for the Instance to Stop Wait for the instance state to change to "stopped".
3. Change Instance Type In the "Actions" menu, select "Instance settings", then "Change instance type", and configure the following: Instance Type: t2.small Choose "Apply".
4. Change EBS Volume Size In the left navigation panel, select "Volumes", and in the "Actions" menu, select "Modify Volume".
5. Once the instance state displays as "stopped," select the instance again, and then choose "Instance Settings" from the Actions menu.
6. Choose "Change Instance Type" and select "t2.small" as the new instance type. Click "Apply."
7. From the left-hand menu, choose "Volumes." In the Volumes screen, select the root EBS volume, then choose "Modify Volume" from the "Actions" menu.
8. Increase the volume size to 10 GB, and then choose "Modify." When prompted to confirm, choose "Yes."
9. Close the Volumes screen and return to the Instances screen by selecting "Instances" from the left-hand menu.
10. Start the instance by selecting it and then choosing "Start Instance" from the "Actions" menu.

Task 5: Explore EC2 Limits

1. From the left-hand menu, select "Limits," and then choose "Running Instances."

Task 6: Test Termination Protection

1. From the left-hand menu, select "Instances," and then choose the instance you launched earlier.
2. From the "Actions" menu, select "Instance Settings," and then choose "Change Termination Protection."
3. Remove the check next to "Enable," and then choose "Save."
4. Return to the Instances screen and select the instance.
5. From the "Actions" menu, choose "Terminate Instance."
6. Confirm that you want to terminate the instance. You should receive an error message because termination protection is now disabled.

**Problems**

I encountered various challenges that hindered my progress. One of the most common problems I faced was difficulty in setting up an AWS account, configuring security settings, and navigating the AWS Management Console. I also struggled with creating and configuring S3 buckets, uploading and managing objects, and setting up access policies.

Another challenge that I faced was related to launching and configuring EC2 instances. I had trouble in connecting to them using SSH, installing and running web servers, or managing instances.

In addition to the above challenges, one common problem that I encountered during the lab was the incorrect configuration of security groups. Since security groups acted as virtual firewalls controlling incoming and outgoing traffic to an EC2 instance, an improper setup caused issues with accessing the instance or services running on it.

Furthermore, I also faced issues when setting up the VPC. While VPCs allowed for the creation of a virtual network in the cloud, which could be used to isolate resources and control network traffic, an incorrect setup led to connectivity issues or misconfigured routing tables.

**Conclusion**

In conclusion, the Amazon Cloud Foundations Labs provide an excellent introduction to AWS and cloud computing, offering participants practical experience with a range of AWS services. These labs are designed to be accessible to individuals with no prior experience in cloud computing or AWS, while still offering valuable insights and skills to those with more advanced knowledge. By completing these labs, participants can gain the skills and knowledge necessary to begin working with AWS and build a foundation for more advanced learning.