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

**Purpose**

The purpose of Amazon Cloud Foundations Labs 4-6 is to provide hands-on experience with Amazon Elastic Compute Cloud (EC2) instances, storage volumes, and the Elastic Block Store (EBS). This lab aims to help learners understand how to launch and manage EC2 instances, attach and detach EBS volumes, create snapshots, and troubleshoot common EC2 issues.

**Background**

Amazon EC2 is a widely used cloud computing service that provides scalable computing capacity in the Amazon Web Services (AWS) cloud. EC2 instances can be launched with a variety of hardware and software configurations, and users can choose from a range of instance types to suit their specific workload requirements. The Elastic Block Store (EBS) is a block-level storage service that provides persistent storage for EC2 instances. EBS volumes can be attached to and detached from instances as needed, and they can also be backed up using snapshots.

**Lab Summary**

The Amazon Cloud Foundations Labs 4-6 is divided into three parts, each focusing on a specific aspect of Amazon EC2 and EBS:

Part 1: Launching an Amazon EC2 Instance In this section, learners will launch an EC2 instance using the AWS Management Console, configure its network settings and security group, and install a web server on the instance. Learners will also learn how to monitor their instance using the console and access the web server from a web browser.

Part 2: Attaching and Detaching an EBS Volume In this section, learners will learn how to attach and detach an EBS volume from an EC2 instance using the AWS Management Console. Learners will also learn how to create a snapshot of an EBS volume and restore it as a new volume.

Part 3: Troubleshooting an EC2 Instance In this section, learners will learn how to troubleshoot common issues with EC2 instances using the AWS Management Console. Learners will explore how to check the system log, view instance screenshots, and use Amazon CloudWatch to monitor and troubleshoot their instances.

**Lab 4**

How to access the AWS Management Console:

1. Launch your lab by clicking the "Start Lab" button at the top of the instructions. A "Start Lab" panel will appear, showing the status of the lab.
2. Wait until the lab status is "ready", then close the "Start Lab" panel by clicking the "X" button.
3. Click "AWS" at the top of the instructions to open the AWS Management Console in a new browser tab. You will be automatically logged in. If a new tab does not open, your browser may be blocking pop-ups. Check for a banner or icon at the top of your browser and allow pop-ups if necessary.
4. Resize the AWS Management Console tab so that it can be displayed alongside these instructions. Ideally, both tabs should be visible at the same time for easier navigation.

Task 1: Creating a New EBS Volume

In this task, you will create a new Amazon EBS volume and attach it to an Amazon EC2 instance.

1. From the AWS Management Console, click "EC2" on the Services menu.
2. In the left navigation pane, select "Instances". An EC2 instance named "Lab" has already been launched for your lab.
3. Take note of the Availability Zone of the instance, which will be displayed similar to "us-east-1a".
4. In the left navigation pane, select "Volumes". You will see an existing volume being used by the EC2 instance, which has a size of 8 GiB. The new volume you will create next will be 1 GiB in size and can be easily distinguished from the existing volume.
5. Click "Create Volume", then configure the following settings:

* Volume Type: General Purpose SSD (gp2)
* Size (GiB): 1. Note that there may be restrictions on the maximum size you can create.
* Availability Zone: Select the same zone as your EC2 instance.
* Add a tag by selecting "Add Tag" and entering the following in the Tag Editor:
  + Key: Name
  + Value: My Volume

1. Click "Create Volume". Your new volume will appear in the list and move from the "Creating" state to the "Available" state. You may need to click "Refresh" to see the new volume.

Task 2: Attaching the Volume to an Instance

You can now attach the new volume to the Amazon EC2 instance.

1. Select "My Volume".
2. From the "Actions" menu, choose "Attach Volume".
3. Choose the instance from the "Instance" field that appears (Lab). Note that the device identifier is set to "/dev/sdf", which you will use in a later task.
4. Click "Attach Volume". The volume state will now be "In-use".

Task 3: Connecting to Your Amazon EC2 Instance

For Windows users only: using SSH to connect.

1. Before starting, read through the three bullet points in this step since these instructions will not be visible when the "Details" panel is open. Click the "Details" drop-down menu above these instructions and select "Show". A "Credentials" window will open.
2. Click "Download PPK" and save the "labsuser.ppk" file. Your browser will typically save it to the "Downloads" directory.
3. Close the "Details" panel by clicking the "X" button.
4. Download PuTTY if you have not already.
5. Open "putty.exe".
6. Configure PuTTY to not timeout by selecting "Connection" and setting "Seconds between keepalives" to 30. This will allow you to keep the PuTTY session open for a longer period of time.
7. When prompted to login as, enter: **ec2-user**. This will connect you to the EC2 instance.

Task 4: Mount and Format the Attached Volume

In this task, you will mount and format the EBS volume you attached to the instance in Task 2.

1. In the PuTTY session, enter the following command to list the available block devices:

lsblk

The command output should display a block device named **/dev/xvdf** which represents the attached volume.

1. Enter the following command to create a file system on the attached volume:

sudo mkfs -t ext4 /dev/xvdf

This command creates an ext4 file system on the **/dev/xvdf** block device.

1. Enter the following command to create a new directory for mounting the volume:

sudo mkdir /data

1. Enter the following command to mount the volume to the newly created directory:

sudo mount /dev/xvdf /data

This command mounts the **/dev/xvdf** block device to the **/data** directory.

1. Verify that the volume is mounted correctly by entering the following command:

df -h

The command output should show a new entry for the **/data** directory that displays the size and available space of the attached volume.

Task 5: Create an Amazon EBS Snapshot

In this task, you will create a snapshot of your EBS volume.

You can create any number of point-in-time, consistent snapshots from Amazon EBS volumes at any time. Amazon EBS snapshots are stored in Amazon S3 with high durability. New Amazon EBS volumes can be created out of snapshots for cloning or restoring backups. Amazon EBS snapshots can also be easily shared among AWS users or copied over AWS regions.

1. In the AWS Management Console, on the Services menu, click EC2.
2. In the left navigation pane, click Volumes.
3. Select My Volume from the list of volumes.
4. In the Actions menu, click Create snapshot.
5. In the Create snapshot dialog box, enter My Snapshot as the value for the Name tag.
6. Click Create snapshot.

The snapshot is created and will be in a pending state at first. It may take several minutes for the snapshot to be created.

1. In the left navigation pane, click Snapshots.

The snapshot will be displayed in the list. Wait until the Status changes to completed before continuing with the lab.

**Lab 5**

How to access the AWS Management Console

1. To begin with, click on the Start Lab button located at the top of these instructions to initiate your lab. A panel will open showing the lab status.
2. Wait for the message "Lab status: ready" to appear, then click on the X to close the Start Lab panel.
3. Now, select AWS located at the top of these instructions. This will launch the AWS Management Console in a new tab on your browser. The system will log you in automatically. Tip: If a new tab doesn't open, there will usually be a banner or icon at the top of your browser that indicates your browser is blocking pop-up windows. Click on the banner or icon and select "Allow pop-ups".
4. Arrange the AWS Management Console tab such that it is displayed alongside these instructions. Ideally, you should be able to view both browser tabs simultaneously for easy following of the lab steps.

Task 1: Creating a Security Group for the RDS DB Instance In this task, you will develop a security group that will enable your web server to access the RDS DB instance. This security group will be utilized during the launch of the database instance.

1. Open the AWS Management Console, and click on the Services menu, then choose VPC.
2. On the left navigation pane, select Security Groups.
3. Click on Create security group and fill in the following: o Security group name: DB Security Group o Description: Permit access from Web Security Group o VPC: Lab VPC Now, add a rule to the security group to allow inbound database requests.
4. On the Inbound rules pane, select Add rule. Currently, the security group has no rules. Add a rule to allow access from the Web Security Group.
5. Configure the following settings: o Type: MySQL/Aurora (3306) o CIDR, IP, Security Group or Prefix List: Type sg and select Web Security Group. This configuration sets the Database security group to allow inbound traffic on port 3306 from any EC2 instance that is connected to the Web Security Group.
6. Click on Create security group. This security group will be used when launching the Amazon RDS database.

Task 2: Creating a DB Subnet Group In this task, you will set up a DB subnet group to specify to RDS which subnets can be utilized for the database. Each DB subnet group must have subnets in at least two Availability Zones.

1. Click on RDS on the Services menu.
2. On the left navigation pane, click on Subnet groups. If the navigation pane is not visible, click on the menu icon located in the top-left corner.
3. Click on Create DB Subnet Group and fill in the following: o Name: DB-Subnet-Group o Description: DB Subnet Group o VPC: Lab VPC
4. Scroll down to the Add Subnets section.
5. Expand the list of values under Availability Zones and select the first two zones: us-east-1a and us-east-1b.
6. Expand the list of values under Subnets and select the subnets linked with the CIDR ranges 10.0.1.0/24 and 10.0.3.0/24. These subnets will now be displayed in the Subnets selected table.
7. Click on Create. This DB subnet group will be utilized when creating the database in the following task.

Task 3: Create an Amazon RDS DB Instance In this task, you will configure and launch a Multi-AZ Amazon RDS for MySQL database instance. Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB instance, Amazon RDS automatically creates a primary DB instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).

1. In the AWS Management Console, navigate to the Databases page.
2. Choose the Create database button to start creating a new database instance.
3. Under Engine options, select MySQL as the database engine.
4. Under Templates, choose the Dev/Test option.
5. Under Availability and durability, select the Multi-AZ DB instance option.
6. Under Settings, enter the following configurations:

* DB instance identifier: lab-db
* Master username: main
* Master password: lab-password
* Confirm password: lab-password

1. Under DB instance class, select Burstable classes (includes t classes) and choose db.t3.micro as the instance type.
2. Under Storage, select General Purpose (SSD) as the storage type and allocate 20 GB of storage.
3. Under Connectivity, select the Lab VPC as the virtual private cloud (VPC) for the database.
4. Under Existing VPC security groups, choose the DB Security Group from the dropdown list and deselect the default security group.
5. Expand Additional configuration, then enter the following configurations:

* Initial database name: lab
* Uncheck Enable automatic backups.
* Uncheck Enable encryption.
* Uncheck Enable Enhanced monitoring.

This will turn off backups, which is not normally recommended, but will make the database deploy faster for this lab. 29. Choose Create database to launch the database instance. If you receive an error that mentions "not authorized to perform: iam:CreateRole", make sure you unchecked Enable Enhanced monitoring in the previous step.

1. Choose the lab-db link to navigate to the database details page. You will need to wait approximately 4 minutes for the database to be available. The deployment status will change from creating to available once the database is ready.

**Lab 6**

Task 1: AMI Creation for Auto Scaling For this task, your objective is to generate an Amazon Machine Image (AMI) for Auto Scaling by using the current Web Server 1. This will ensure that new instances can be launched with identical contents since it stores the contents of the boot disk.

To get started, access the AWS Management Console and click on EC2 from the Services menu. Next, navigate to Instances on the left-hand side of the screen.

Your first step will be to confirm that the instance is up and running. You can do this by waiting until the Status Checks for Web Server 1 displays 2/2 checks passed. Don't forget to click refresh to update the information.

Now that you've verified the instance is running, it's time to create an AMI based on this instance. To do this, select Web Server 1 and go to the Actions menu. From there, click on Image and templates > Create image, and then configure the following settings:

* Image name: WebServerAMI
* Image description: Lab AMI for Web Server

Once you have configured these settings, click on Create image. A confirmation banner will display the AMI ID for your newly created AMI. You'll use this AMI when launching the Auto Scaling group in the next lab session.

Task 2: Load Balancer Creation In this task, you will create a load balancer that can distribute traffic across multiple EC2 instances and Availability Zones.

Start by navigating to Target Groups on the left-hand side of the screen. Target Groups define where to send traffic that comes into the Load Balancer. For this web application, you will use only one Target Group. Click on Create target group and configure the following settings:

* Target type: Instances
* Target group name: LabGroup
* VPC: Select Lab VPC from the drop-down menu

Click Next to move on to the Register targets screen. Since you do not have any web application instances yet, you can skip this step. Review the settings and click on Create target group.

Now, go to Load Balancers on the left-hand side of the screen and click on Create Load Balancer at the top of the screen. You will be using an Application Load Balancer that operates at the request level (layer 7) and can route traffic to EC2 instances, containers, IP addresses, and Lambda functions based on the content of the request. Under Application Load Balancer, click on Create and configure the following settings:

* Load balancer name: LabELB
* VPC: Select Lab VPC from the drop-down menu
* Subnets: Select both Public Subnet 1 and Public Subnet 2
* Security groups: Choose Web Security Group from the drop-down menu and remove the default security group

Next, go to the Listener HTTP:80 row and set the Default action to forward to LabGroup. Scroll down to the bottom of the page and click on Create load balancer. The load balancer will show a state of provisioning, but there's no need to wait until it's ready. You can move on to the next task.

Task 3: Generate a Launch Configuration and an Auto Scaling Group In this task, you will produce a template for launching EC2 instances called a launch configuration, and create an Auto Scaling group that utilizes it. When creating a launch configuration, you will need to specify details such as the AMI, instance type, security group, key pair, and disks.

1. Navigate to Launch Configurations on the left-hand menu.
2. Click on the Create launch configuration button.
3. Configure the following settings: o Launch configuration name: LabConfig o Amazon Machine Image (AMI): Choose the Web Server AMI o Instance type: ♣ Choose Choose instance type ♣ Select t3.micro ♣ Choose Choose Note: If you launched the lab in the us-east-1 Region, choose the t2.micro instance type. You can find the Region in the top right-hand corner of the Amazon EC2 console. Note: In case you receive an error message "Something went wrong. Please refresh and try again.", you can disregard it and proceed with the exercise. o Additional configuration ♣ Monitoring: Select Enable EC2 instance detailed monitoring within CloudWatch This permits Auto Scaling to rapidly respond to any fluctuations in usage.
4. Under Security groups, configure the launch configuration to use the pre-existing Web Security Group. o Choose Select an existing security group o Select Web Security Group
5. Under Key pair configure: o Key pair options: Choose an existing key pair o Existing key pair: vockey o Select I acknowledge... o Click Create launch configuration You will now build an Auto Scaling group that incorporates this Launch Configuration.
6. Check the checkbox for the LabConfig Launch Configuration.
7. From the Actions menu, select Create Auto Scaling group
8. Enter the Auto Scaling group name: o Name: Lab Auto Scaling Group
9. Choose Next
10. On the Network page configure o Network: Lab VPC You can disregard the message about "No public IP address." o Subnet: Select Private Subnet 1 (10.0.1.0/24) and Private Subnet 2 (10.0.3.0/24) This will launch EC2 instances in private subnets across both Availability Zones.
11. Choose Next
12. In the Load balancing - optional pane, select Attach to an existing load balancer
13. In the Attach to an existing load balancer pane, use the dropdown list to select LabGroup.
14. In the Additional settings - optional pane, choose Enable group metrics collection within CloudWatch This will capture metrics at 1-minute intervals, which allows Auto Scaling to react quickly to changing usage patterns.
15. Choose Next
16. Under Group size, configure: o Desired capacity: 2 o Minimum capacity: 2 o Maximum capacity: 6 This will enable Auto Scaling to add or remove instances automatically, always maintaining a count between 2 and 6.
17. Under Scaling policies, choose Target tracking scaling policy and configure: o Lab policy name: LabScalingPolicy o Metric type: Average CPU Utilization o Target value: 60 This instructs Auto Scaling to maintain an average CPU utilization across all instances at 60%. Auto Scaling will automatically add or remove capacity as required to keep the metric at, or close to, the specified target value. It adjusts to fluctuations in the metric due to a fluctuating load pattern.
18. Choose Next Auto Scaling can send a notification when a scaling event takes place. You will use the default settings.

Task 4: Verify Load Balancer Functionality

For this task, you need to confirm that the Load Balancing feature is functioning properly.

1. Navigate to the Instances tab on the left-hand side of the screen.

You should see two freshly launched instances with the name "Lab Instance." These instances were created by the Auto Scaling tool.

If the instances are not visible, wait for 30 seconds and refresh the page by clicking on the Refresh button located in the top-right corner.

Now, your first objective is to validate that the new instances have successfully passed their Health Check.

1. On the left-hand side of the screen, click on Target Groups located under the Load Balancing section.
2. Select "LabGroup."
3. Click on the Targets tab.

The target group should have two listed targets, which are the "Lab Instance" instances.

1. Wait for the Status of both instances to transition to "healthy." Use the Refresh button in the upper-right corner to check for updates.

If an instance is deemed "healthy," it implies that it has passed the Load Balancer's health check. Consequently, the Load Balancer will route traffic to the instance.

You can now access the Auto Scaling group through the Load Balancer.

1. In the left navigation pane, click Load Balancers.
2. In the lower pane, copy the DNS name of the load balancer, ensuring that you exclude "(A Record)."

It should appear similar to this: LabELB-1998580470.us-west-2.elb.amazonaws.com

1. Open a new tab in your web browser, paste the DNS Name copied in the previous step, and hit Enter.

The application should display on your screen, indicating that the Load Balancer has received the request, sent it to one of the EC2 instances, and then transmitted back the outcome.

Task 5: Testing Auto Scaling An Auto Scaling group was set up with a minimum of two instances and a maximum of six instances. Currently, there are two instances running because the minimum size is two and the group is not under any load. The aim is to increase the load to trigger Auto Scaling to add additional instances.

1. Go back to the AWS management console, but do not close the application tab as it will be used later.
2. Click on CloudWatch under the Services menu.
3. In the left navigation pane, select All alarms.

Two alarms will be displayed. These alarms were automatically created by the Auto Scaling group. They ensure that the average CPU load remains close to 60% while also staying within the range of two to six instances.

Note: Follow these steps only if the alarms are not visible after 60 seconds.

* Click on EC2 under the Services menu.
* In the left navigation pane, select Auto Scaling Groups.
* Choose the Lab Auto Scaling Group.
* In the bottom half of the page, select the Automatic Scaling tab.
* Choose LabScalingPolicy.
* Click on Actions and Edit.
* Change the Target Value to 50.
* Click Update.
* Click on CloudWatch under the Services menu.
* In the left navigation pane, select All alarms and check that two alarms are visible.

1. Click on the OK alarm, which has AlarmHigh in its name.

If no alarm is showing OK, wait for a minute and then click refresh in the top-right corner until the alarm status changes. The OK status means that the alarm has not been triggered. It is the alarm for CPU Utilization > 60, which will add instances when the average CPU load is high. At the moment, the chart should show very low levels of CPU.

The next step is to instruct the application to perform calculations that will increase the CPU level.

1. Return to the browser tab with the web application.
2. Click on Load Test beside the AWS logo.

This will cause the application to generate high loads, and the browser page will automatically refresh so that all instances in the Auto Scaling group will generate load. Do not close this tab.

1. Return to the browser tab with the CloudWatch console.

In less than 5 minutes, the AlarmLow alarm should change to OK, and the AlarmHigh alarm status should change to In alarm.

You can click Refresh in the top-right corner every 60 seconds to update the display. The AlarmHigh chart should indicate an increasing CPU percentage. Once it crosses the 60% line for more than 3 minutes, Auto Scaling will add additional instances.

1. Wait until the AlarmHigh alarm enters the In alarm state.

You can now view the additional instance(s) that were launched.

1. Click on EC2 under the Services menu.

In the left navigation pane, select Instances.

There should be more than two instances labeled Lab Instance running. The new instance(s) were created by Auto Scaling in response to the Alarm.

**Problems**

I encountered various challenges that hindered my progress. Some of the most common problems that I faced included issues with setting up the AWS CLI, incorrect or missing IAM permissions, and errors in setting up the CloudFormation stack. To avoid these issues, I carefully followed the instructions and double-checked all inputs.

In case any errors occurred, I troubleshooted them by checking the CloudFormation stack events and reviewing the AWS CLI output for any error messages. By addressing these common problems, I successfully completed the lab and gained valuable experience in using AWS services.

**Conclusion**

The Amazon Cloud Foundations Labs 4-6 provides learners with valuable experience in launching and managing Amazon EC2 instances, attaching and detaching EBS volumes, and troubleshooting common issues. By completing this lab, learners will gain a deeper understanding of how to configure and manage EC2 instances and EBS volumes, as well as how to use the AWS Management Console to monitor and troubleshoot their cloud resources.