ACA Module 9 Challenge Lab: Creating a Scalable and Highly Available Environment for the Cafe

Student name: Duy Hung D Student ID: 104182779

Tutorial session: Monday 1:00PM

1. INTRODUCTION

In the dynamic realm of hospitality, coffee shops serve as lively centers where people come together to enjoy aromatic coffees, indulge in delicious treats, and participate in engaging conversations. Cafe owners understand the importance of using technology to ensure smooth operations, improve customer satisfaction, and foster sustainable growth in order to provide a delightful experience for their customers. Building a scalable and highly reliable environment is crucial to meet the changing demands of the industry, requiring the integration of strong infrastructure, flexible processes, and creative solutions that can address both present and future needs. By combining state-of-the-art technology with hospitality knowledge, coffee shops can offer an exceptional experience where reliability, efficiency, and high standards work together as the foundation of success.

1. Main

**Task 1: Answer the following questions**

Firstly, answer the following questions from details tab. The first question you can go to security group in VPC console, click on CafeSG group and see inbound rules. 2 questions below are in subnets tab or you can answer by yourself easily

A screenshot of a computer

Description automatically generated

*Figure 1 Module 9 Challenge lab questions*

In question 4, you can answer with the same logic in question 2,3. However in next 2 questions, you can find it in EC2 instances and AMI console to get a solution.

A screenshot of a computer

Description automatically generated

*Figure 2 Module 13 Challenge Lab Questions*

**Task 2: Creating a NAT gateway for the second Availability Zone**

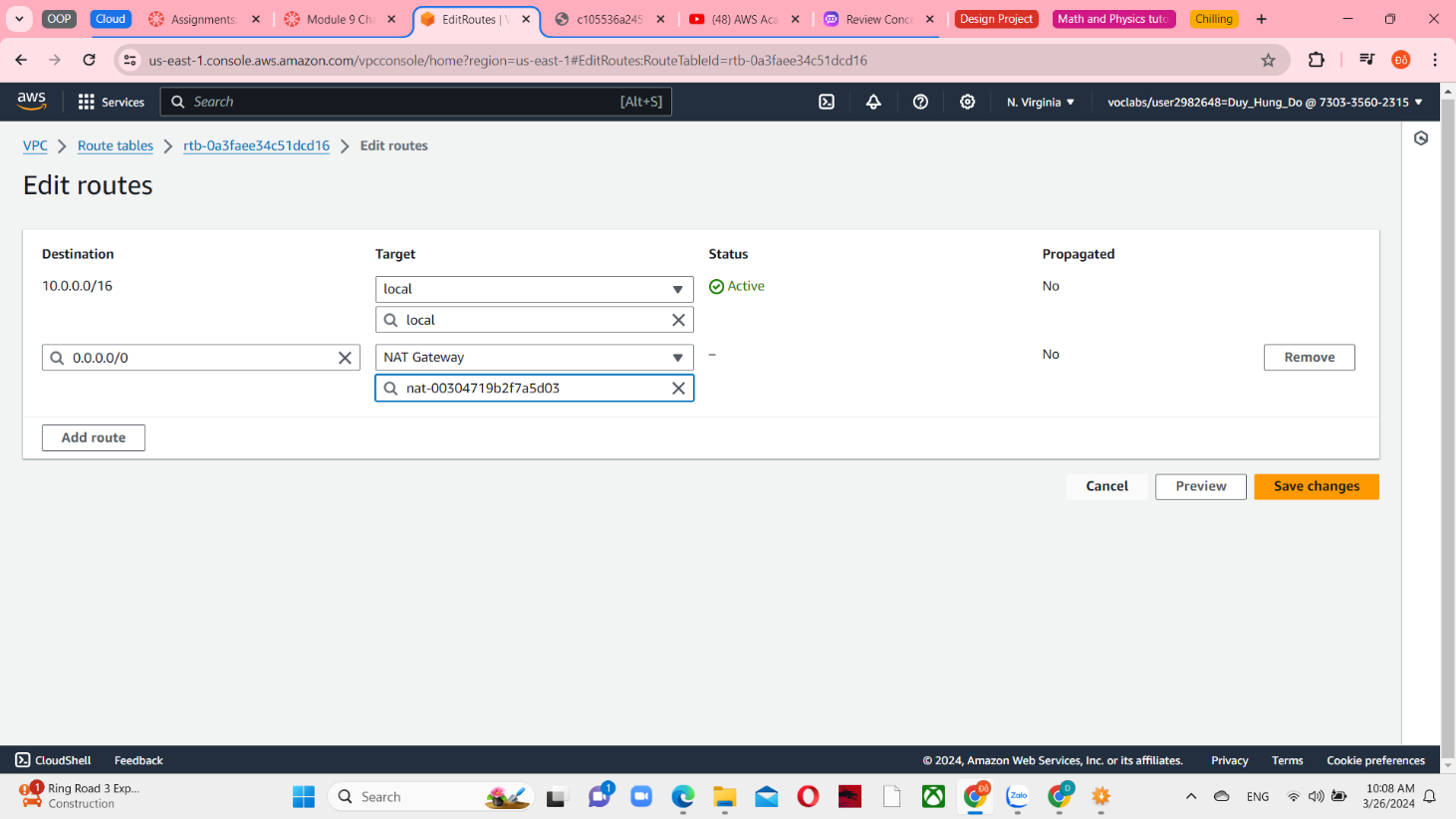
Before launching EC2 instances, you have to create a NAT gateway which allows instances that do not have public IP address to access the internet. Create NAT gateway in the Public subnet 2, which has located in Availably Zone us-east-1b.

A screenshot of a computer

Description automatically generated

*Figure 3 NAT gateway settings*

And then, config NAT gateway to Private Route Table 2 by set the 0.0.0.0/0 source destination and NAT target.

****

*Figure 4 Edit Private Route Table 2*

**Task 3: Creating a bastion host instance in a public subnet**

After NAT gateways, create a bastion host instance with Amazon Linux HVM.

A screenshot of a computer

Description automatically generated

*Figure 5 Name and Application and OS images in EC2 instance*

Next, set t2.micro as a instance type and choose vockey key pair.

A screenshot of a computer

Description automatically generated

*Figure 6 Instance type and key pair in EC2 instance*

Choose LabVPC with public subnet 1. Create new security group that allow SSH from local ip. After that, skip all settings and launch instance.

A screenshot of a computer

Description automatically generated

*Figure 7 Create security group for Bastion host*

**Task 4: Creating a launch template**

Because AMI is the default image by this lab, so when creating launch template, you can select my AMIs and choose Café WebServer image.

A screenshot of a computer

Description automatically generated

*Figure 8 Application and OS images in launch template*

Setting instance type is t2.micro and create new key pair.

A screenshot of a computer

Description automatically generated

*Figure 9 Instance type and key pair in launch template*

Select CafeSG as an existing security group

A screenshot of a computer

Description automatically generated

*Figure 10 Network settings in launch template*

Set a resource tags with webserver as a name and config with CafeRole IAM instance profile

A screenshot of a computer

Description automatically generated

*Figure 11 Resource tags and IAM instance profile in launch template*

**Task 5: Creating an Auto Scaling group**

While launch template is defined, you can create an Auto Scaling group that used the previous launch templateA screenshot of a computer

Description automatically generated

*Figure 12 Choose launch template*

Choose LabVPC and 2 private subnet in 2 availability zones 1a and 1b.

A screenshot of a computer

Description automatically generated

*Figure 13 Choose instance launch options*

Skip the advanced options and config group size that desired and minimum capacity is 2, while maximim is 6. Enables the Target tracking scaling policy and config with Average CPU utilization as a metric type, target value is 25 and instances need 60.

A screenshot of a computer

Description automatically generated

*Figure 14 Configure group size and scaling*

**Task 6: Creating a load balancer.**

Now that your web application server instances are deployed in private subnets, you require a method for external entities to establish a connection with them. Create an HTTP load balancer with LabVPC and 2 public subnet in 2 Availability Zones.

A screenshot of a computer

Description automatically generated

*Figure 15 Network mapping in load balancer*

Create a new security group that allow HTTP traffic from anywhere-ipv4 address.

A screenshot of a computer

Description automatically generated

*Figure 16 Security group settings*

At the same time, create a new target groups and set it to load balancer

A screenshot of a computer

Description automatically generated

*Figure 17 Security groups and Listeners and routing in load balancer*

After that, modify the Auto Scaling group by set Load balancer target groups.

A screenshot of a computer

Description automatically generated

*Figure 18 Edit ASG settings*

**Task 7: Testing the web application**

Copy the DNS name in load balancer and paste in the another web browser, adding /café and you can see café application loading.

A screenshot of a computer

Description automatically generated

*Figure 19 Café application loaded*