Metropolitan State University
ICS 432 - 01: Distributed and Cloud Computing
Fall 2021

Lab 05: Networking and Load Balancing in AWS
Total points: 25
Out: Saturday, October 2, 2021
Due: 11:59 PM on Friday, October 8, 2021

What to submit?

The objective of this lab is to learn about Networking and Load Balancing in the AWS cloud. To complete this lab:

- Read this lab assignment carefully.
- At various parts of the lab, you are asked to take screen shots of your work. Open a word document and paste the screen shots in this document in the same order as mentioned in the lab. Make sure to highlight the screen shot number.
- After you complete all the lab exercises, upload the word document to the designated D2l folder by 11:59 PM on Friday, October 8, 2021.

NOTE: On Windows machines, you may consider using Snip & Sketch for screenshot handling.

Exercise 1: Virtual Private Network (VPC) on AWS

In this exercise, you will complete Lab 2: Build your VPC and Launch a Web Server from Module 5 of the AWS Academy Cloud Foundations course. In this lab, you will use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to produce a customized network. You will also create security groups for your EC2 instance. You will then configure and customize an EC2 instance to run a web server and launch it into the VPC.

> DO NOT END LAB after you complete all the steps because you are going to do you Exercise 2 using the same lab environment.

1- Log in to your AWS Academy account and go to Module 5 and click on Lab2: Build your VPC and Launch a Web server.
2- Start the lab and follow the lab instructions. Take screenshots as explained in the following steps.
3- **Task 1: Create Your VPC**
   a. In step 8, use last name in the VPC name, for example, my VPC name is set to Ghanem Lab VPC.

b. After step 10, after you see the message 'Your VPC has been successfully created', click on Your VPCs from the left navigation pane and **Lab screenshot #1** to show the details of the VPC. Make sure the VPC name clearly appears in the screenshot.

4- Task 2: Create Additional Subnets

a. After step 15, click on Subnets from the left navigation menu, take **Lab screenshot #2** to show the list of subnets including the the recently created subnets.
b. In step 19, add your last name to the route table. For example, my route table is named Ghanem Private Route table.
c. In step 25, add your last name to the route table. For example, my route table is named Ghanem Public Route table.
d. After step 30, take **Lab screenshot #3** to show the list of route tables. The list should show two route tables with your last name and each one of these two route table is shown to be associated to 2 subnets.

5- Task 3: Create a VPC Security Group

a. In step 32, put your last name in the security group name. For example, my security group is called Ghanem Web Security Group. Make sure to choose your recently created VPC in the VPC box.
b. After step 35, take **Lab screenshot #4** to show the details of the security group. Make sure the security group name appears clearly in the screenshot.

6- Task 4: Launch a Web Server Instance

a. In step 49, add your last name to the tag, for example, the value in my case is Ghanem Web Server 1.
b. After step 58, take **Lab screenshot #5** to show the list of instances including your recently created instance with status Running. Note that this may take a while for the instance to be completely up and running. Wait until the instance status check is 2/2 before trying to access the instance from the browser.

c. After step 60, take **Lab screenshot #6** to show the information displayed in the web page. Make sure the URL bar is shown in the screenshot with the IP address of your instance.

Exercise 2: Connecting to instances in public and private subnets

The goal of this exercise is to do hands-on exercises to connect to instances in the public and private subnets created in Exercise 1. Note that, AWS Educate accounts has limited resources and you cannot create a VPC using your AWS Educate Account.

1- Change the security group you created in Exercise 1 by adding the following inbound rules:
   a. A rule to allow ping to connect to the instance
      i. Type: Custom ICMP – Ipv4
      ii. Protocol: Echo Request
      iii. Source: Anywhere IPv4

b. A rule to allow SSH:
    i. Type: SSH
    ii. Protocol: TCP
    iii. Source: Anywhere

Lab screenshot #7: take a screenshot of all the three inbound rules in your security group.

2- Create an EC2 instance called <your-last-name> public instance with the following parameters:
    a. Network: the VPC network you created in Exercise 1.
    b. Subnet: public subnet 1
    c. **Auto-assign Public IP:** *Enable*
    d. Security group: the security group you created in exercise 1.
    e. Create and download a new key pair called 'lab5keypair'.

Lab screenshot #8: take a screenshot of the instance details to show the private and public IPv4 addresses of the instance.

3- Create an EC2 instance called <your-last-name> private instance with the following parameters:
    a. Network: Lab 5 VPC (the network you created in Exercise 1).
    b. Subnet: private subnet 1
    c. **Auto-assign Public IP:** *Enable*
    d. Security group: the security group you created in exercise 1.
    e. Use the 'lab5keypair' you created in step 2 above.

Lab screenshot #9: take a screenshot of the instance details to show the private and public IPv4 addresses of the instance.

4- From your local computer, open a terminal window and execute

```
ping -c <public IPv4>
```

two times, once using the public IPv4 of the public instance and once using the publiv IPv4 of the private instance.

Lab screenshot #10: take a screenshot to show the output of the two `ping` command.

5- Try to establish an SSH connection to your private instance. This should not succeed because private subnets do not allow any inbound traffic.

6- Establish an SSH connection to the public instance. Once connected, execute `ping` using using the private instance's private IPv4 from inside the public instance.

Lab screenshot #11: take a screenshot to show the ping output when trying to ping the private instance from inside the public instance.

7- From inside the public instance, establish an SSH connection to the private instance.

8- From inside the private instance's command window, ping the public instance using the instance's private IPv4 address.

Lab screenshot #12: take a screenshot to show the output of ping from inside the private instance.

9- From inside the private instance, perform `curl <any url>` to make sure that the private instance can access the internet.

Lab screenshot #13: take a screenshot to show the output of curl.

10- Run the following `curl` command FIVE times on each instance to retrieve the following instance details: `ami-id`, `local-ipv4`, `hostname`, `public-ipv4`, and `public-keys`

```
curl -w "\n"  http://169.254.169.254/latest/meta-data/<meta-data-item>
```

For example, the following command prints the local-ipv4

```
curl -w "\n" http://169.254.169.254/latest/meta-data/local-ipv4
```

Lab screenshot #14(a) and #14(b): take a screenshot to show the meta data of both instances.

Exercise 3: Scaling and Load Balancing

In this exercise, you will complete Lab 6: Scale & Load Balance your Architecture from Module 10 of the AWS Academy Cloud Foundations course. This lab walks you through using the Elastic Load Balancing (ELB) and Auto Scaling services to load balance and automatically scale your infrastructure.

1- Log in to your AWS Academy account and go to Module 10 and click on Lab6: Scale & Load balance your Architecture.
2- Start the lab and follow the lab instructions. Take screenshots as explained in the following steps.
3- **Task 1: Create an AMI for Auto Scaling**
   a. In step 9, add your last name to the image name. For example, my image name is called GhanemWebServerAMI.
   b. After step 10, click on Images→ AMIs from the left navigation pane. Take **Lab screenshot #15** of the list of images showing your recently created image.
4- **Task 2: Create a Load Balancer:**
   a. In step 13, add your last name to the name of ELB. For example, my ELB is called GhanemLabELB.

b. In step 18, add your last name to the target group name. For example, my group is called GhanemLabGroup.
c. After step 21, take **Lab screenshot #16** to show the list of load balancers including the recently created ELB.

5- **Task 3: Create a Launch Configuration and an Auto Scaling Group**
   a. In step 24, add your name to the launch configuration name. For example, my launch configurations is called GhanemLabConfig. Then, choose the AMI that you created in Task 1.
   b. After step 26, take **Lab screenshot #17** to show the list of launch configurations including your recently created configuration.
   c. In step 29, add your last name to the auto scaling group name. For example, my group is called Ghanem Lab Auto Scaling Group.
   d. In step 34, choose group that you recently created (e.g., GhanemLabGroup).
   e. In step 38, add your last name to the policy name. For example, my policy name is GhanemLabScalingPolicy.
   f. In step 41, add you last name to the tag value, for example, my value is Ghanem Lab Instance.
   g. After step 34, wait until the number of instances in your group is 2 then take **Lab screenshot #18** to show the list of Auto scaling group including your group. Note that you can refresh the browser to update the list.

6- **Task 4: Verify load balancing is working**
   a. After step 44, take **Lab screenshot #19** to show the list of instances.
   b. After step 48, take **Lab screenshot #20** to show the list of targets in the group.
   c. After step 51, take **Lab screenshot #21** of the browser window showing the meta data and take note of `InstanceId`. If you get an error from message from the browser that the page cannot be opened, try to use another browser. Refresh the browser window several times until the `InstanceId` value is changed which means the load balancer forwarded the request to the other instance. Take **Lab screenshot #22** of the browser with the other `InstanceId`.

7- **Task 5: Test Auto Scaling**
   a. After step 54, take **Lab screenshot #23** to show the two alarms in CloudWatch.
   b. After step 55, take **Lab screenshot #24** to show the CPUUtilization graph.
   c. After step 58, and after you refresh the page until both Alarms are showing OK status.
   d. Go to the browser page that show the application and it should be displaying the current CPU load. Take **Lab screenshot #25** of this reading.
   e. After step 62, take **Lab screenshot #26** to show the list of EC2 instances with more than two instances labeled with your last name.