Lab 2 - Building VPC and Launching a Web Server

Objective: To create VPC and configure subnets

Task 1: Create Your VPC

In this task, you will use the VPC and more option in the VPC console to create multiple resources, including a VPC, an Internet Gateway, a public subnet and a private subnet in a single Availability Zone, two route tables, and a NAT Gateway.

1. In the search box to the right of Services, search for and choose VPC to open the VPC console.
2. Begin creating a VPC.
    a. In the top left of the screen, verify the New VPC Experience is toggled *on*. If it is not, toggle it on now.
    b. Choose the VPC dashboard link which is also towards the top left of the console.
    c. Next, choose Create VPC.
        i. Note: If you do not see a button with that name, choose the Launch VPC Wizard button instead.
3. Configure the VPC details in the VPC settings panel on the left:
    a. Choose VPC and more.
    b. Under Name tag auto-generation, keep Auto-generate selected, however change the value from project to lab.
    c. Keep the IPv4 CIDR block set to 10.0.0.0/16
    d. For Number of Availability Zones, choose 1.
    e. For Number of public subnets, keep the 1 setting.
    f. For Number of private subnets, keep the 1 setting.
    g. Expand the Customize subnets CIDR blocks section
        i. Change Public subnet CIDR block in us-east-1a to 10.0.0.0/24
        ii. Change Private subnet CIDR block in us-east-1a to 10.0.1.0/24

    h. Set NAT gateways to In 1 AZ.

i. Set VPC endpoints to None.
j. Keep both DNS hostnames and DNS resolution enabled.

4. In the Preview panel on the right, confirm the settings you have configured.
    a. VPC**:** Lab-vpc
    b. Subnets:
        i. us-east-1a
            1. Public subnet name**:** lab-subnet-public-us-east-1a
            2. Private subnet name**:** lab-subnet-private-us-east-1a
    c. Route tables
        i. lab-rtb-public
        ii. lab-rtb-private-us-east-1a
    d. Network connections
        i. lab-igw
        ii. lab-nat-public-us-east-1a
5. At the bottom of the screen, choose Create VPC
    a. The VPC resources are created. The NAT Gateway will take a few minutes to activate.
    b. Please wait until all the resources are created before proceeding to the next step.
6. Once it is complete, choose View VPC
    a. The wizard has provisioned a VPC with a public subnet and a private subnet in one Availability Zone with route tables for each subnet. It also created an Internet Gateway and a NAT Gateway.
    b. To view the settings of these resources, browse through the VPC console links that display the resource details. For example, choose Subnets to view the subnet details and choose Route tables to view the route table details. The diagram below summarizes the VPC resources you have just created and how they are configured.

An Internet gateway is a VPC resource that allows communication between EC2 instances in your VPC and the Internet.

The lab-subnet-public-us-east-1a public subnet has a CIDR of 10**.**0.0.0/24, which means that it contains all IP addresses starting with 10.0.0.x. The fact the route table associated with this public subnet routes 0.0.0.0/0 network traffic to the internet gateway is what makes it a public subnet.

A NAT Gateway, is a VPC resource used to provide internet connectivity to any EC2 instances running in private subnets in the VPC without those EC2 instances needing to have a direct connection to the internet gateway.

The lab-subnet-private-us-east-1a private subnet has a CIDR of 10.0.1.0/24, which means that it contains all IP addresses starting with 10.0.1.x.

Task 2: Create Additional Subnets

In this task, you will create two additional subnets for the VPC in a second Availability Zone. Having subnets in multiple Availability Zones within a VPC is useful for deploying solutions that provide High Availability.

After creating a VPC as you have already done, you can still configure it further, for example, by adding more subnets. Each subnet you create resides entirely within one Availability Zone.

1. In the left navigation pane, choose Subnets.
    a. First, you will create a second public subnet.
2. Choose Create Subnet then configure:
    a. VPC ID: lab-vpc (select from the menu).
    b. Subnet name**:** lab-subnet-public2
    c. Availability Zone**:** Select the second Availability Zone (for example, us-east-1b)
    d. IPv4 CIDR block**:** 10.0.2.0/24
    e. The subnet will have all IP addresses starting with 10.0.2.x.
3. Choose Create Subnet
    a. The second public subnet was created. You will now create a second private subnet.
4. Choose Create Subnet then configure:
    a. VPC ID**:** lab-vpc

b. Subnet name**:** lab-subnet-private2
c. Availability Zone**:** Select the second Availability Zone (for example, us-east-1b)
d. IPv4 CIDR block**:** 10.0.3.0/24
e. The subnet will have all IP addresses starting with 10.0.3.x.

5. Choose Create Subnet
    a. The second private subnet was created.
    b. You will now configure this new private subnet to route internet-bound traffic to the NAT Gateway so that resources in the second private subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring a Route Table.
    c. A route table contains a set of rules, called routes, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table controls routing for the subnet.

6. In the left navigation pane, choose Route tables.

7. Select the lab-rtb-private1-us-east-1a route table.

8. In the lower pane, choose the Routes tab.
    a. Note that Destination 0.0.0.0/0 is set to Target nat-xxxxxxxx. This means that traffic destined for the internet (0.0.0.0/0) will be sent to the NAT Gateway. The NAT Gateway will then forward the traffic to the internet.
    b. This route table is therefore being used to route traffic from private subnets.

9. Choose the Subnet associations tab.

a. You created this route table in task 1 when you chose to create a VPC and multiple resources in the VPC. That action also created lab-subnet-private-1 and associated that subnet with this route table.
b. Now that you have created another private subnet, lab-subnet-private-2, you will associate this route table with that subnet as well.

10. Choose Edit Subnet Associations

11. Leave lab-subnet-private1-us-east-1a selected, but also select lab-subnet-private2.
12. Choose Save Associations
13. You will now configure the Route Table that is used by the Public Subnets.
14. Select the lab-rtb-public route table (and deselect any other subnets).
15. In the lower pane, choose the Routes tab.
    a. Note that Destination 0.0.0.0/0 is set to Target igw-xxxxxxxx, which is the Internet Gateway. This means that internet-bound traffic will be sent straight to the internet via the Internet Gateway.
    b. You will now associate this route table to the second public subnet you created.
16. Choose the Subnet associations tab.
17. Choose Edit Subnet associations
18. Leave lab-subnet-public1-us-east-1a selected, but also select lab-subnet-public2.
19. Choose Save Association

Your VPC now has public and private subnets configured in two Availability Zones. The route tables you created in task 1 have also been updated to route network traffic for the two new subnets.

Task 3: Create a VPC Security Group

In this task, you will create a VPC security group, which acts as a virtual firewall. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

1. In the left navigation pane, choose Security groups.

2. Choose Create Security Group and then configure:
    a. Security group name**:** Web Security Group
    b. Description**:** Enable HTTP Access
    c. VPC**:** choose the X to remove the currently selected VPC, then from the drop down list choose lab-vpc

3. In the Inbound rules pane, choose Add Rule
4. Configure the following settings:
    a. Type**:** HTTP
    b. Source: Anywhere-IPv4
    c. Description**:** Permit web request
    d.
5. Scroll to the bottom of the page and choose Create Security Group
    a. You will use this security group in the next task when launching an Amazon EC2 instance.

Task 4: Launch a Web Server Instance

In this task, you will launch an Amazon EC2 instance into the new VPC. You will configure the instance to act as a web server.

1. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.

2. From the Launch instance menu choose Launch instance.

3. Name the instance:
    a. Give it the name Web Server1
        i. When you name your instance, AWS creates a tag and associates it with the instance. A tag is a key value pair. The key for this pair is *****Name*****, and the value is the name you enter for your EC2 instance.

4. Choose an AMI from which to create the instance:
    a. In the list of available Quick Start AMIs, keep the default Amazon Linux AMI selected.
    b. Also keep the default Amazon Linux 2 AMI (HVM**)** selected.
        i. The type of Amazon Machine Image (AMI) you choose determines the Operating System that will run on the EC2 instance that you launch.

5. Choose an Instance type:
    a. In the Instance type panel, keep the default t2**.**micro selected.
        i. The Instance Type defines the hardware resources assigned to the instance.
6. Select the key pair to associate with the instance:
    a. From the Key pair name menu, select vockey.
        i. 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.

7. Configure the Network settings:
    a. Next to Network settings, choose Edit, then configure:
        i. Network**:** lab-vpc
        ii. Subnet**:** lab-subnet-public2 (not Private!)
        iii. Auto-assign public IP**:** Enable
    b. Next, you will configure the instance to use the Web Security Group that you created earlier.
        i. Under Firewall (security groups), choose Select an existing security group.
        ii. For Common security groups, select Web Security Group.
            1. This security group will permit HTTP access to the instance.

8. In the Configure storage section, keep the default settings.
    a. Note: The default settings specify that the root volume of the instance, which will host the Amazon Linux 2 guest operating system that you specified earlier, 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.

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

```
i. 
ii. #!/bin/bash
iii. # Install Apache Web Server and PHP
```

```
yum install -y httpd mysql php
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2-9026/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

xi. This 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. The script installs a web server, a database, and PHP libraries, and then it downloads and installs a PHP web application on the web server.

10. At the bottom of the Summary panel on the right side of the screen choose Lunch Instance
    a. You will see a Success message.
11. Choose View all instances
12. Wait until Web Server 1 shows 2/2 checks passed in the Status check column.
    a. This may take a few minutes. Choose the refresh icon at the top of the page every 30 seconds or so to more quickly become aware of the latest status of the instance.
    b. You will now connect to the web server running on the EC2 instance.
13. Select Web Server 1.
14. Copy the Public IPv4 DNS value shown in the Details tab at the bottom of the page.
15. Open a new web browser tab, paste the Public DNS value and press Enter.

You should see a web page displaying the AWS logo and instance meta-data values.

Conclusion: VPC has been created and it is secured via subnets and NACLs.