Lab Report - Lab 1

Name: Tyler Burleson Date: 1/24/2024

Summary

In this lab we focused on creating and configuring VPC with our desired settings to be used when accessing our instances on EC2. We started by creating a new named “FluxVPC” and setting the IPv4 CIDR then configuring the subnet to access the us-east-1e availability zone. Next, we created an internet gateway using these configurations and attached it to our VPC. Once this was linked, we edited the routes to allow our gateway to speak to “anywhere.” We then added this association to our Flux subnet.

After we created our VPC we entered EC2 to test the connection and our key pairs. We started by downloading the private keys shared to us on D2L then importing them into the network settings on EC2. Once this was linked, we were able to create our first instance. In this example we used an Amazon Linux image with minimal storage and processing resources. We then told the instance to be accessible through the Key pair “FluxKey” and created its security group in the firewall.

Once this was complete, we were able to test our connection using PuTTY. When we opened PuTTY we started by configuring our SSH to allow public key authentication. We took the .ppk file and added it as our private key file for authentication. Once this was set up we were then able to to connect to our session.

When connecting to our session we have to use the instance’s public IP address. In my case this was 50.90.39.5. I then started my connection and was able to connect to my instance/ server. Once connected I logged in using the ec2-user profile. Once I was connected to my server I tested the access my instance had by pinging the google DNS server using “ping -c4 google.com.” Once I was knew I was able to access outside resources I ran another command to update it. I updated and upgraded yum by

using “sudo yum update && sudo yum upgrade -y” once this was complete I closed my instance and “completed the lab.”

Screen Shots

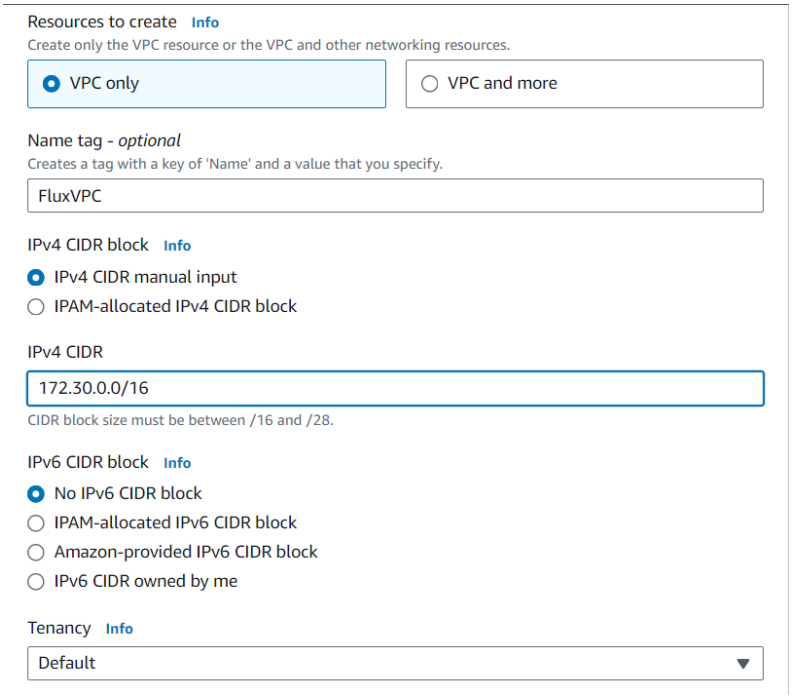

Figure 1

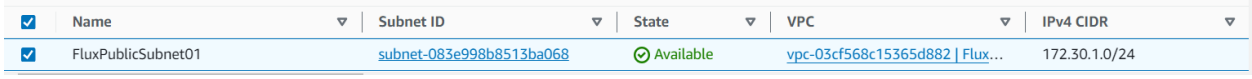

Figure 2

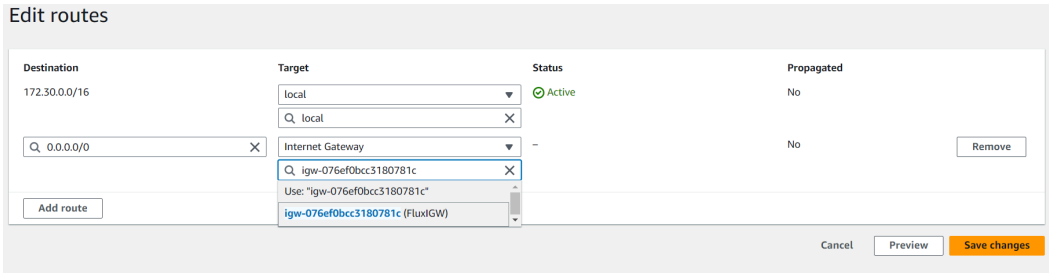

Figure 3

Figure 4

Research Questions

1. What's a CIO and why is knowing that important to you, the lead sysadmin?

CIO – Chief Information Officer. The CIO is important to be able to achieve the organizations mission through Information Technology.

2. What IP class is this - 10.0.0.0/8 (i.e. A, B, C?)

This is an example of a type A IP class.

3. How many potential addresses will be available to #23's network (ignoring the fact that a few are reserved for
DHCP, gateway, etc.)? Hint: There are 32 bits in an IPv4 address and we're using 8 of them for the netmask.

2^8 = 256. This means there are a total of 256 available hosts for 172.30.1.0/24.

4. So the potential addresses in this CIDR block go from 172.30.1.0 to -what?

The range is "172.30.1.0" to "172.30.1.255"

5. What protocol uses port 443?

HTTP**S** is the protocol that uses 443 and secures the network packets before they're transmitted.

6. If we create another subnet with 172.30.2.0/23 as the CIDR block, how many hosts can it handle?

By creating another subnet we are adding another 256 hosts to the original set, this allows us to handle 512 total hosts.

7. What is the subnet range for #15?

The subnet range is 255.255.0.0

8. What is the base CIDR class for #15 (i.e., A, B, C, D, or E)?

172.30.0.0 is a class B.

9. What is `sudo` and what does it mean?

Sudo stands for super user and is a method for the user to run a command as a root user.

10. What is a Route Table? What does it do?

A route table is used to determine where the network traffic from your subnet is directed to.