**Objective and Learning Experience**:

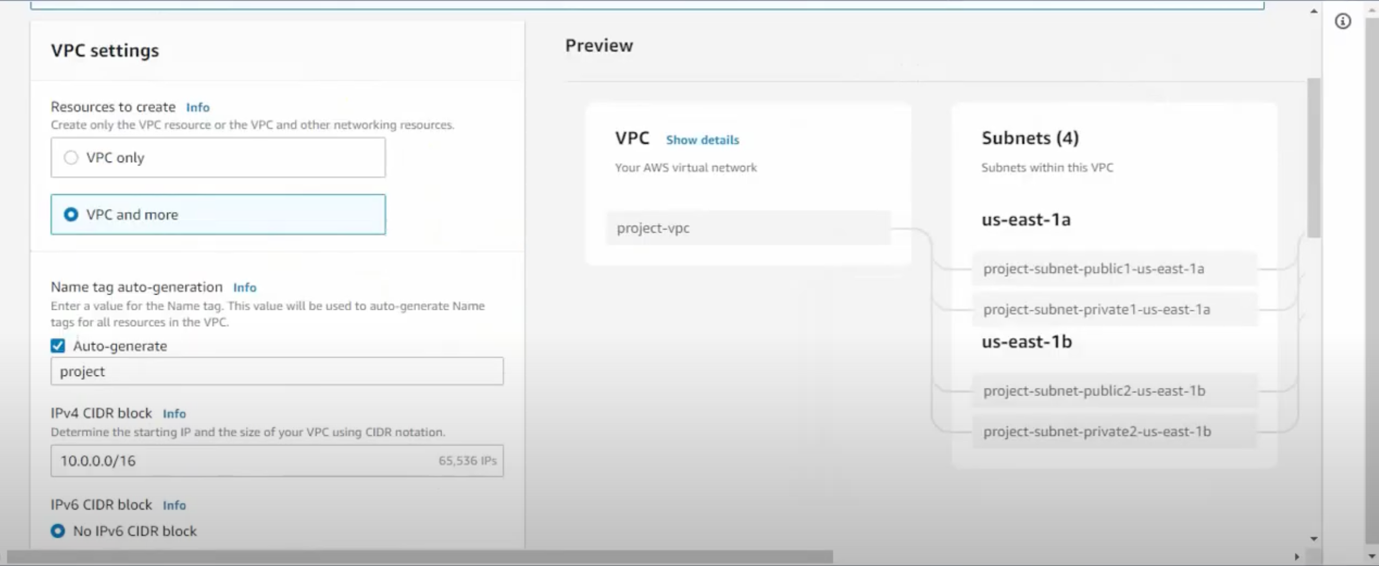
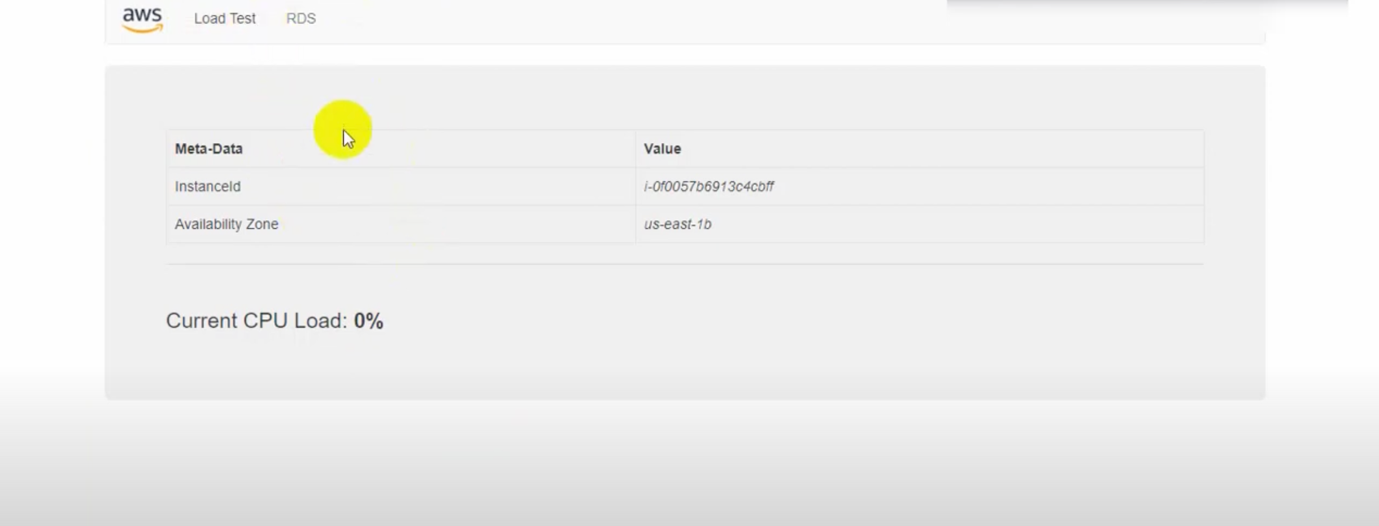
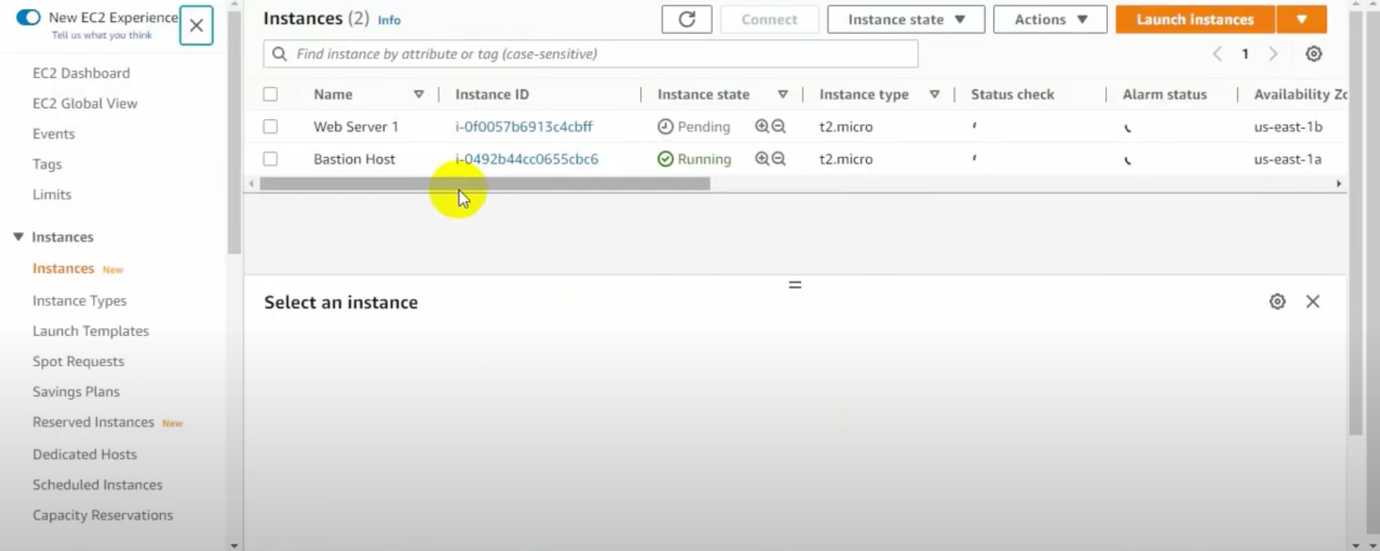
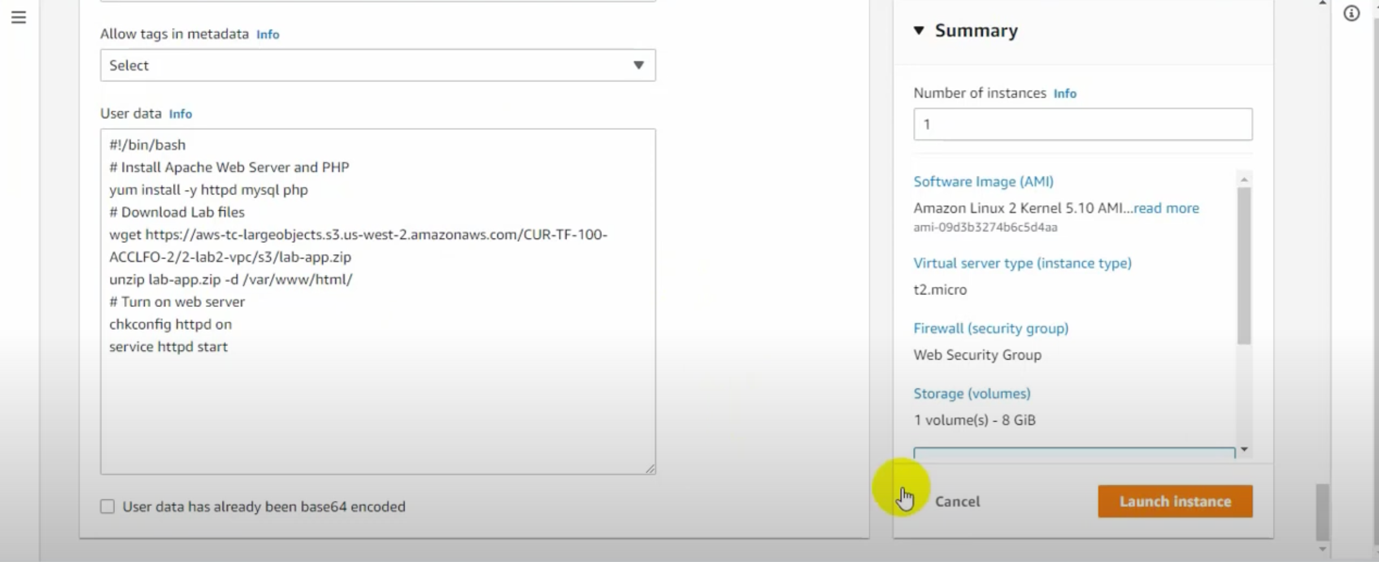
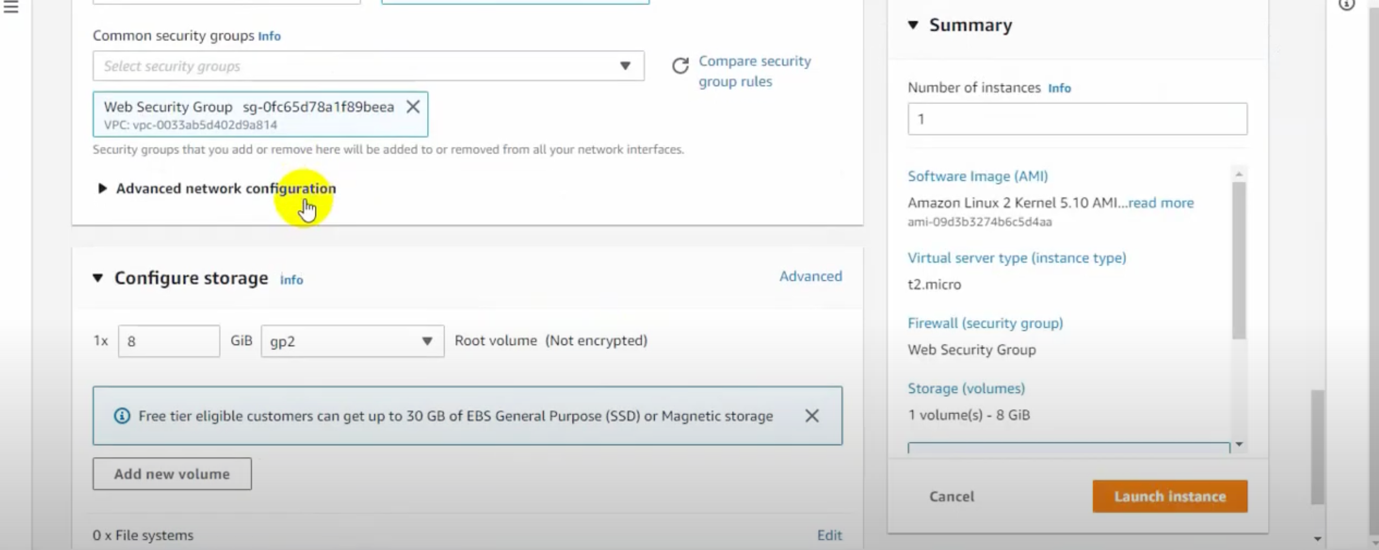
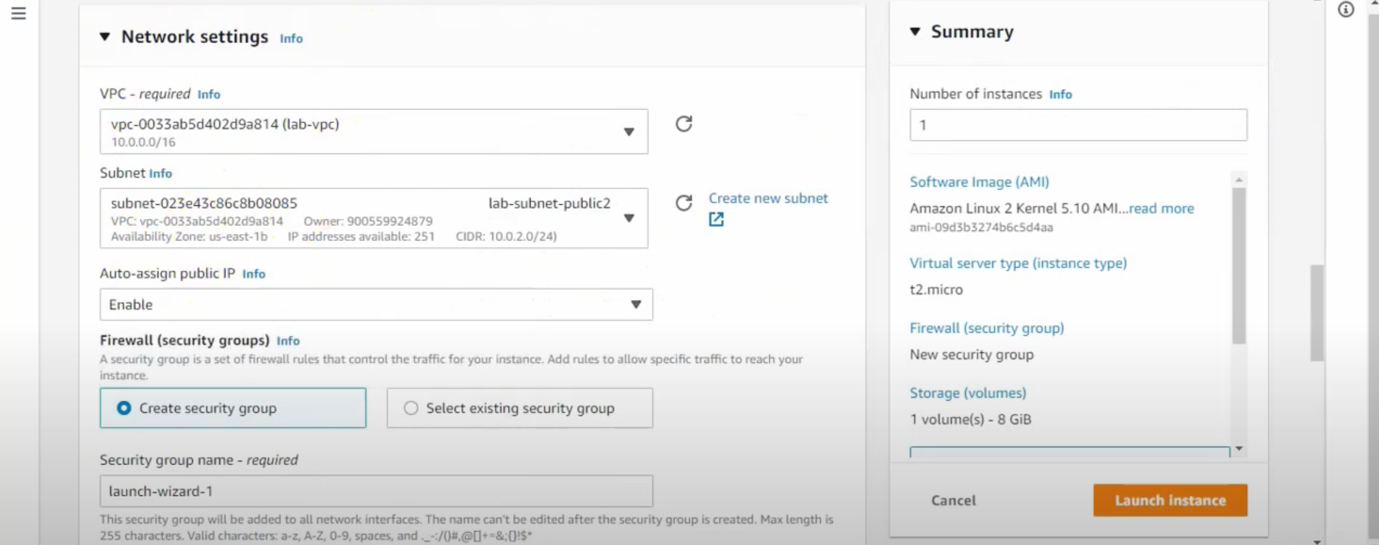
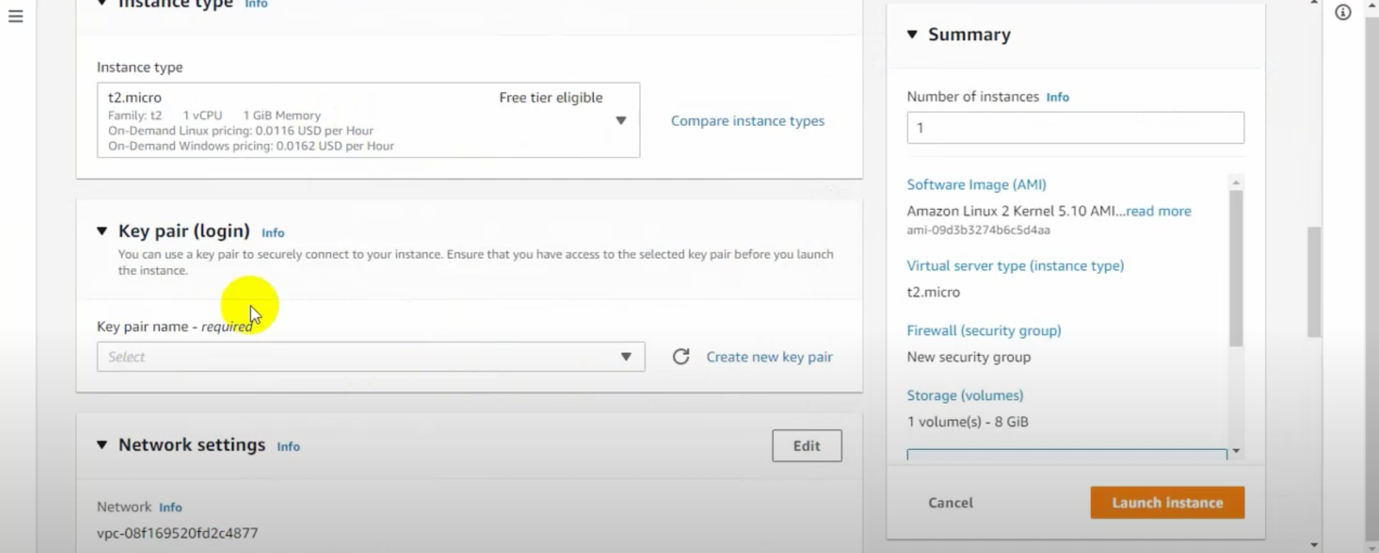
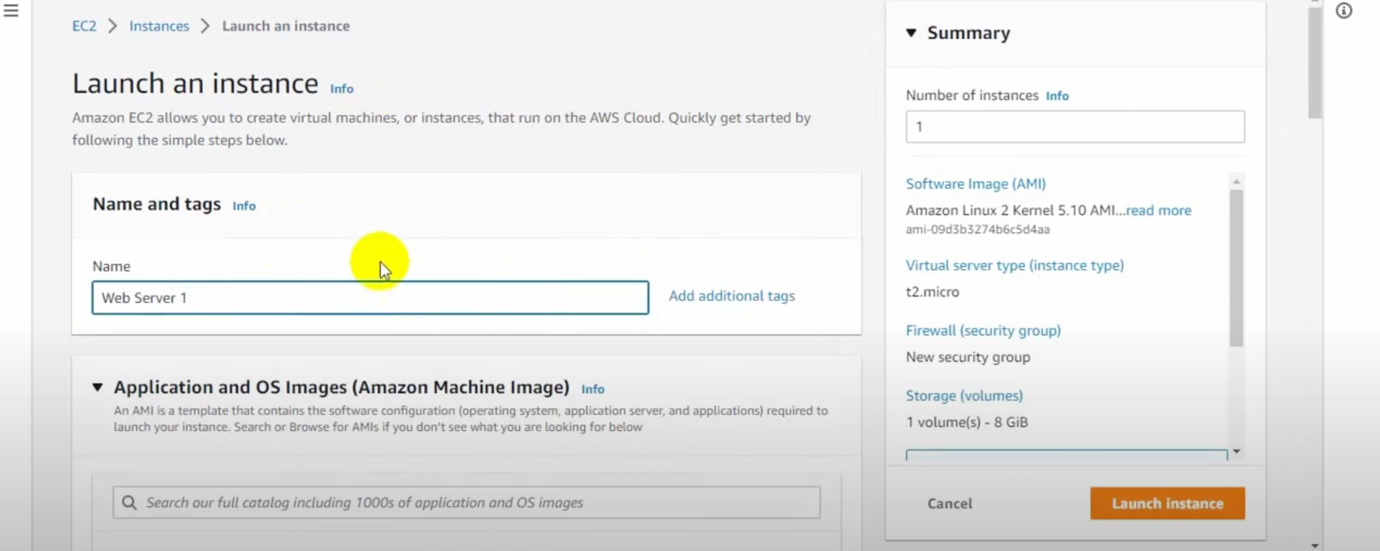
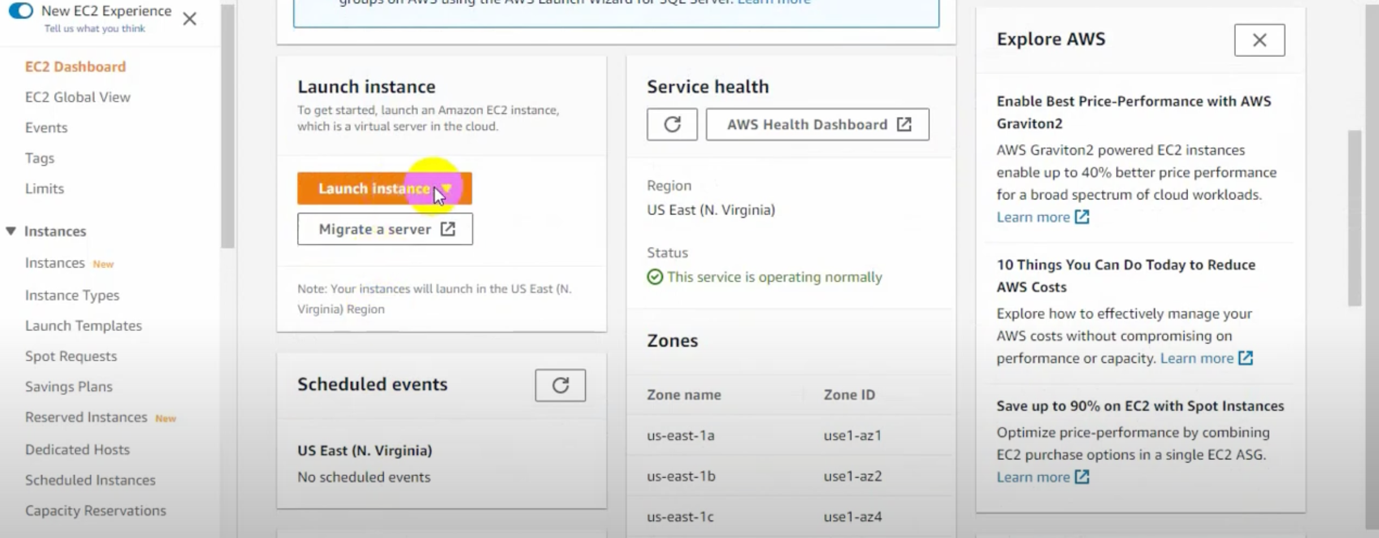
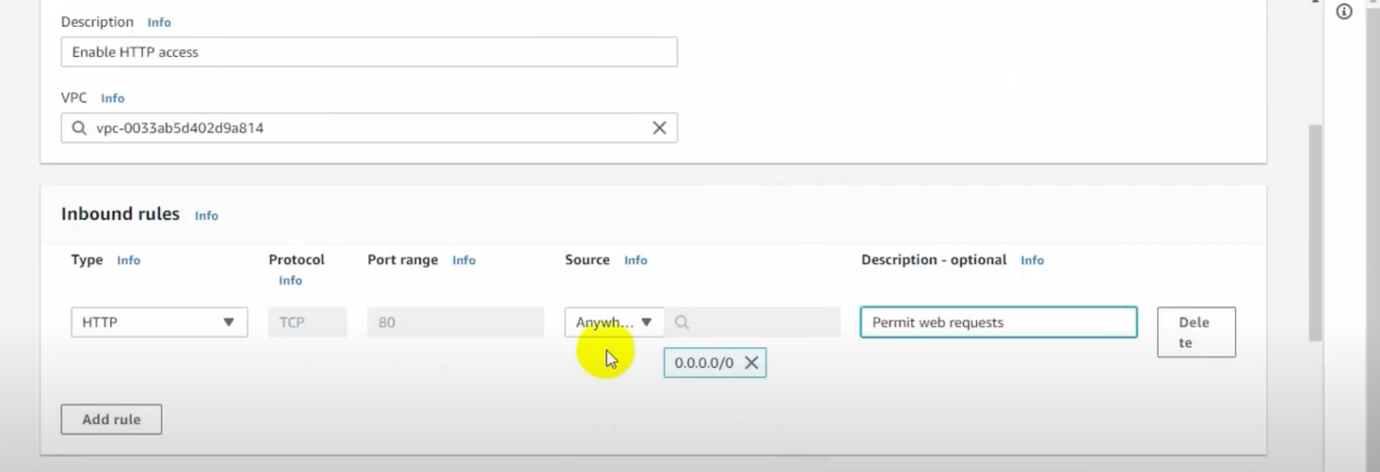
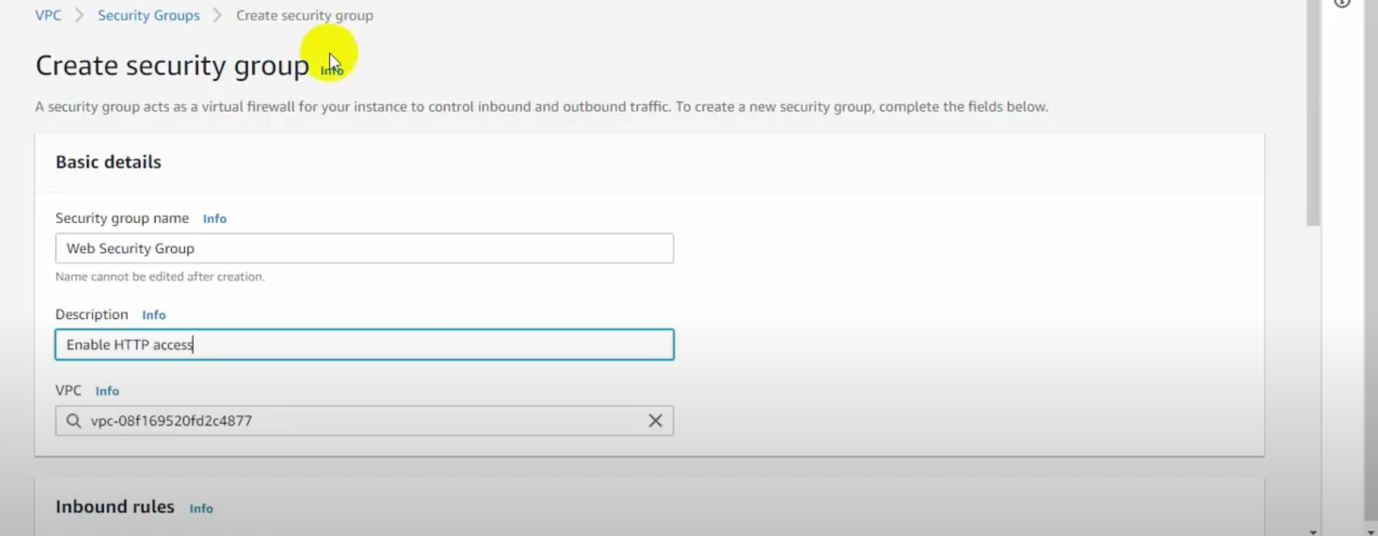
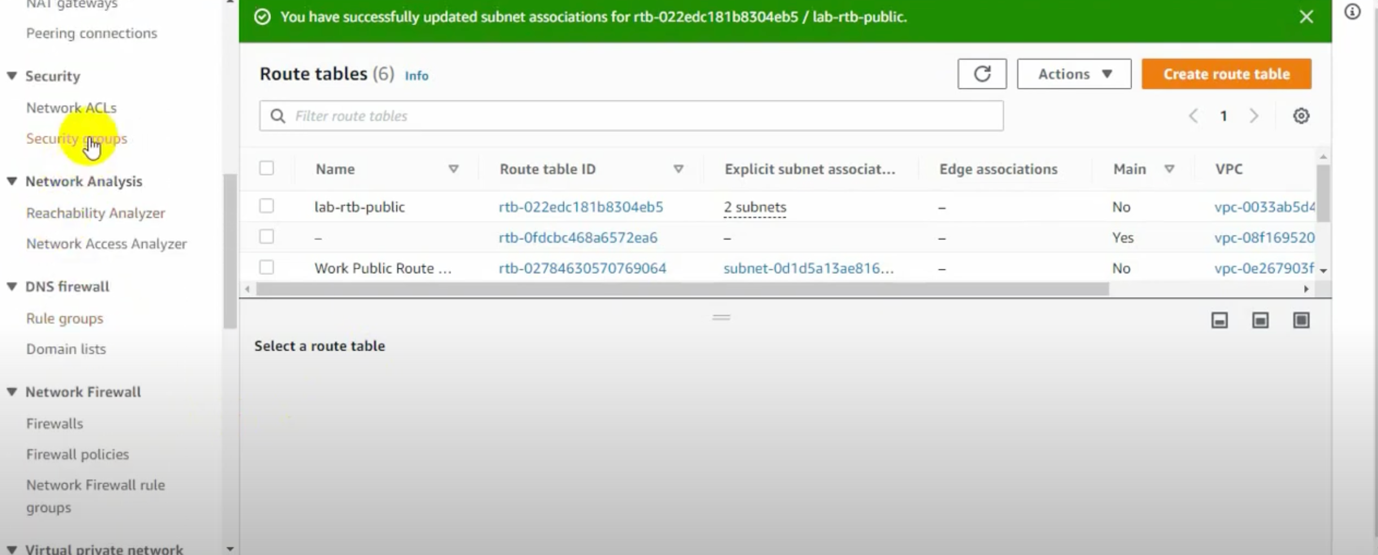
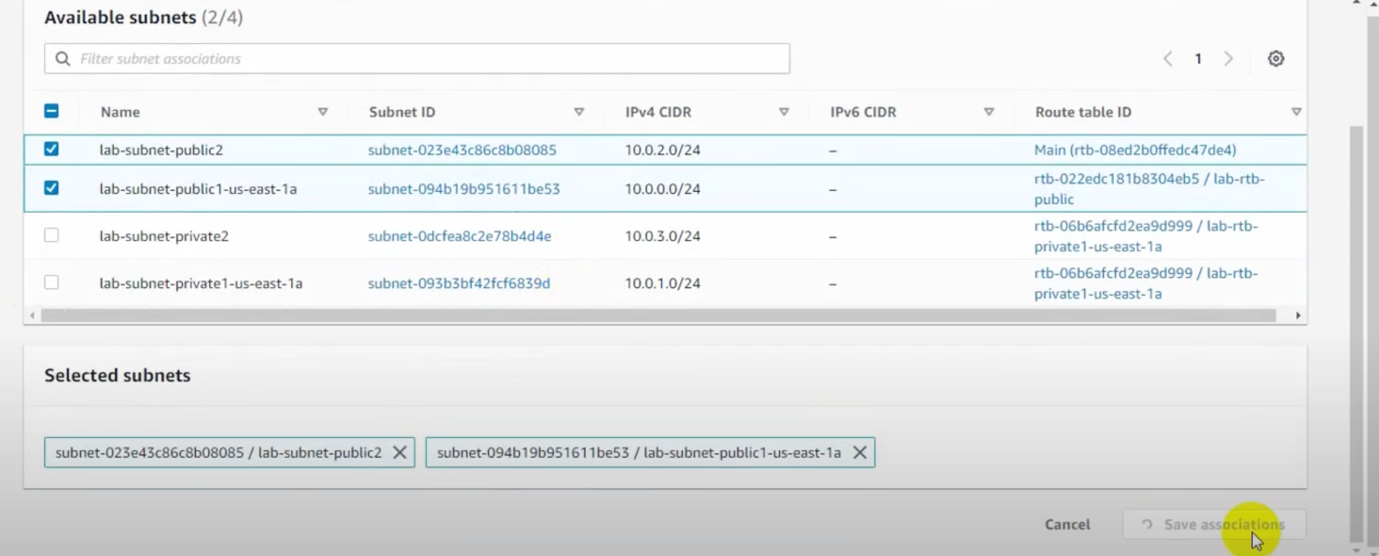
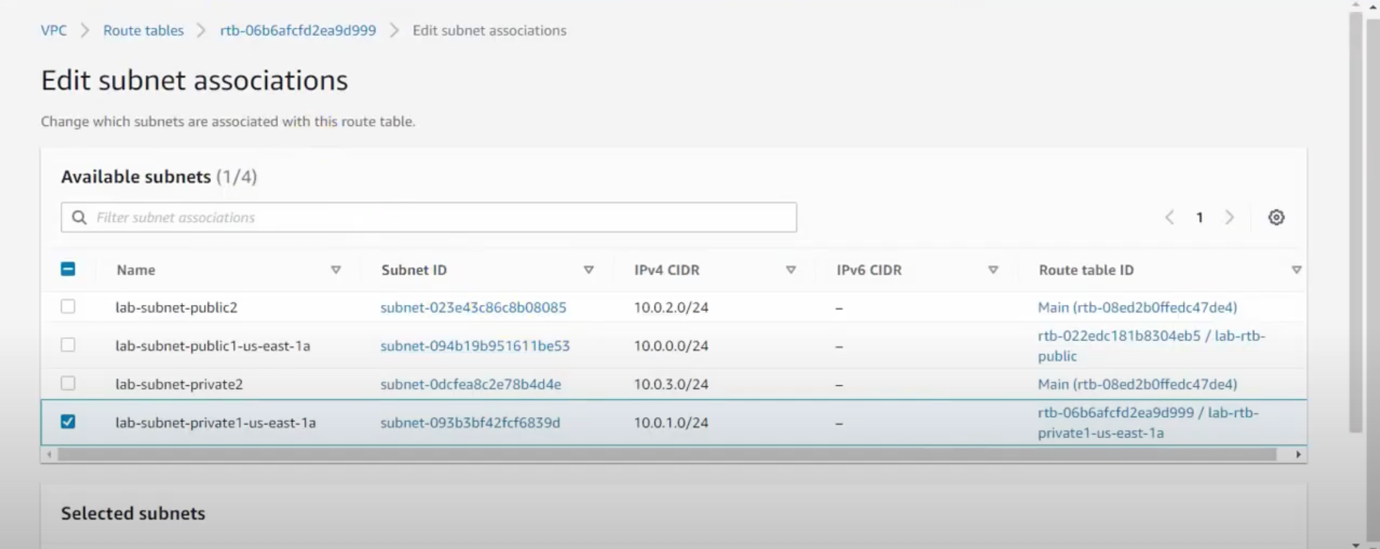
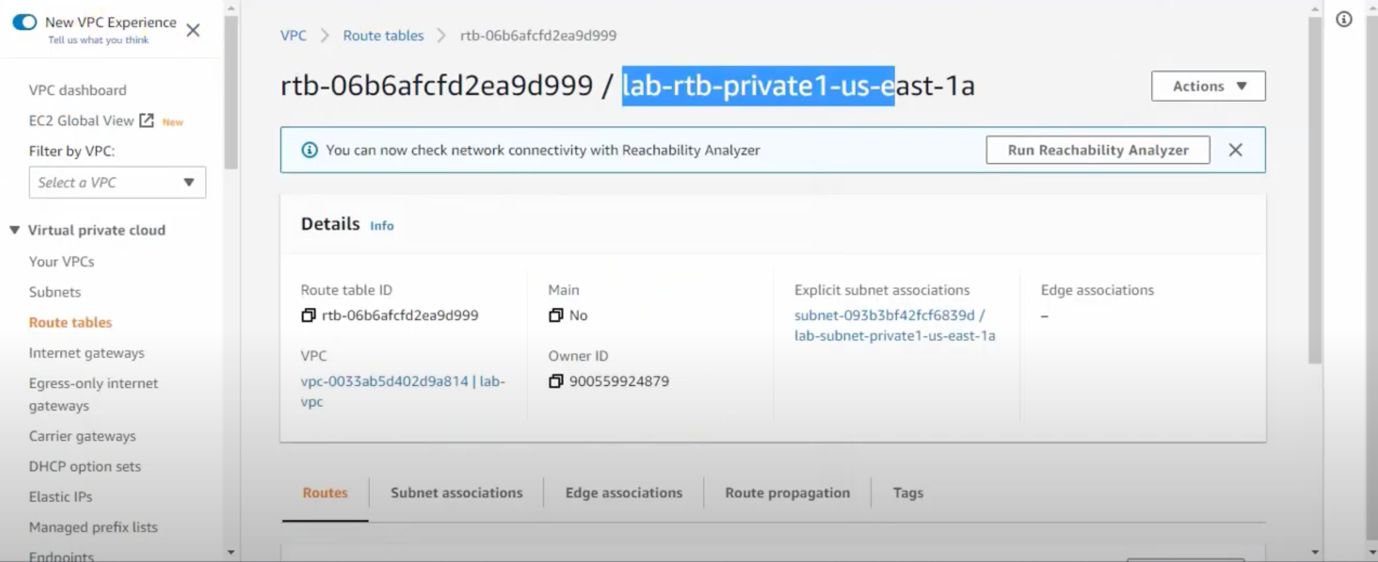
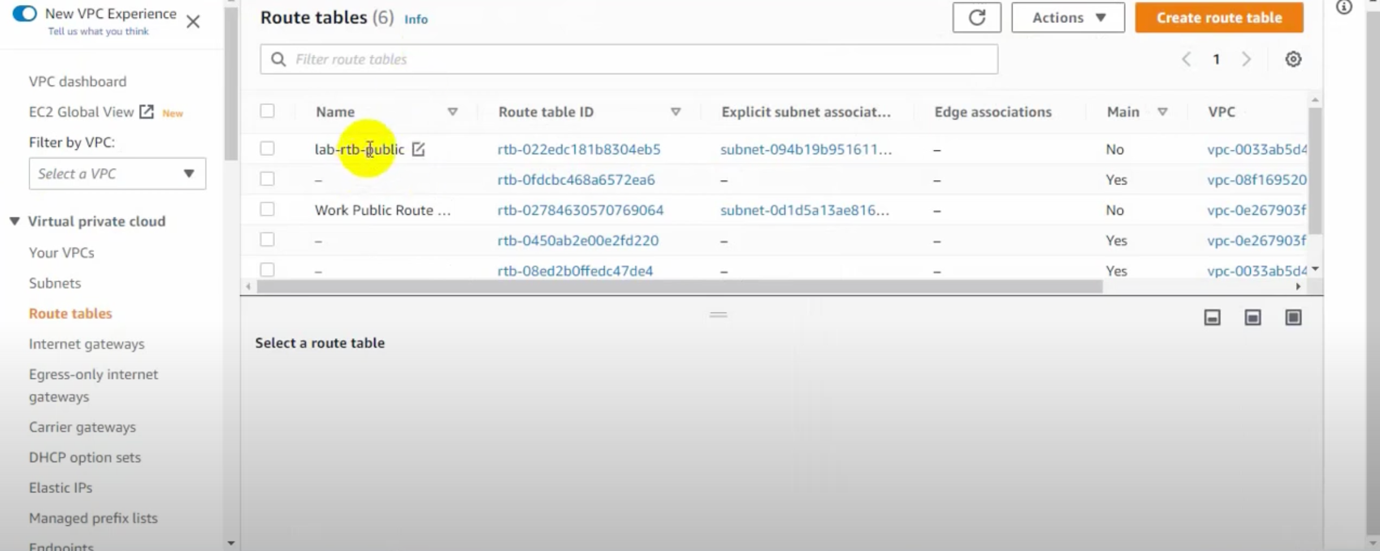
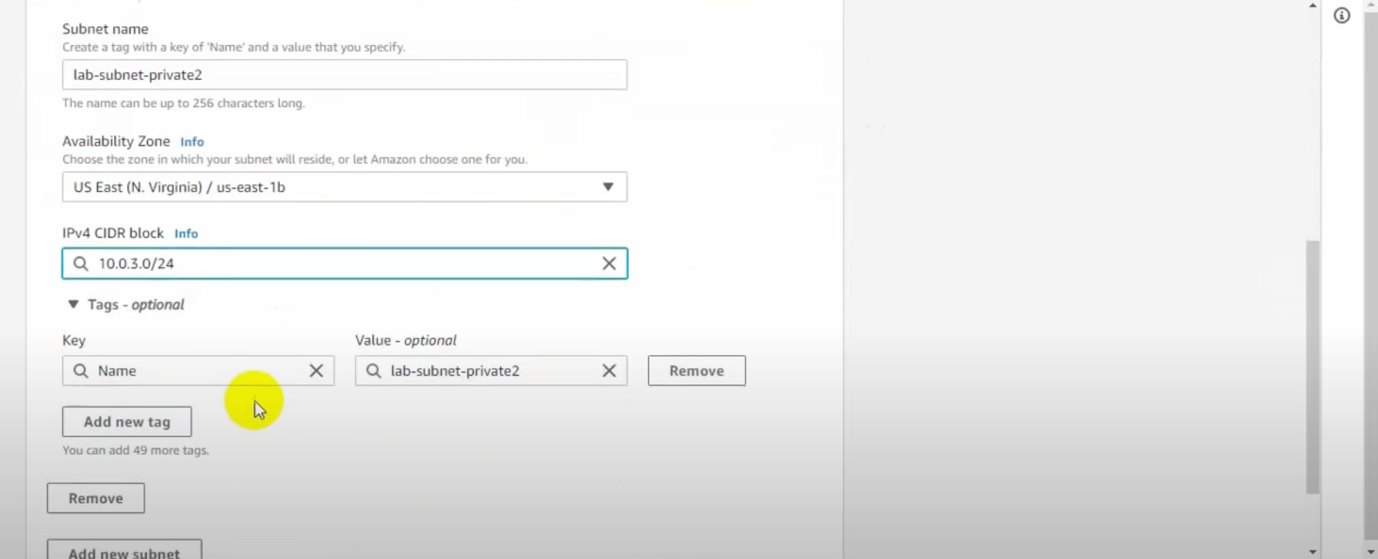
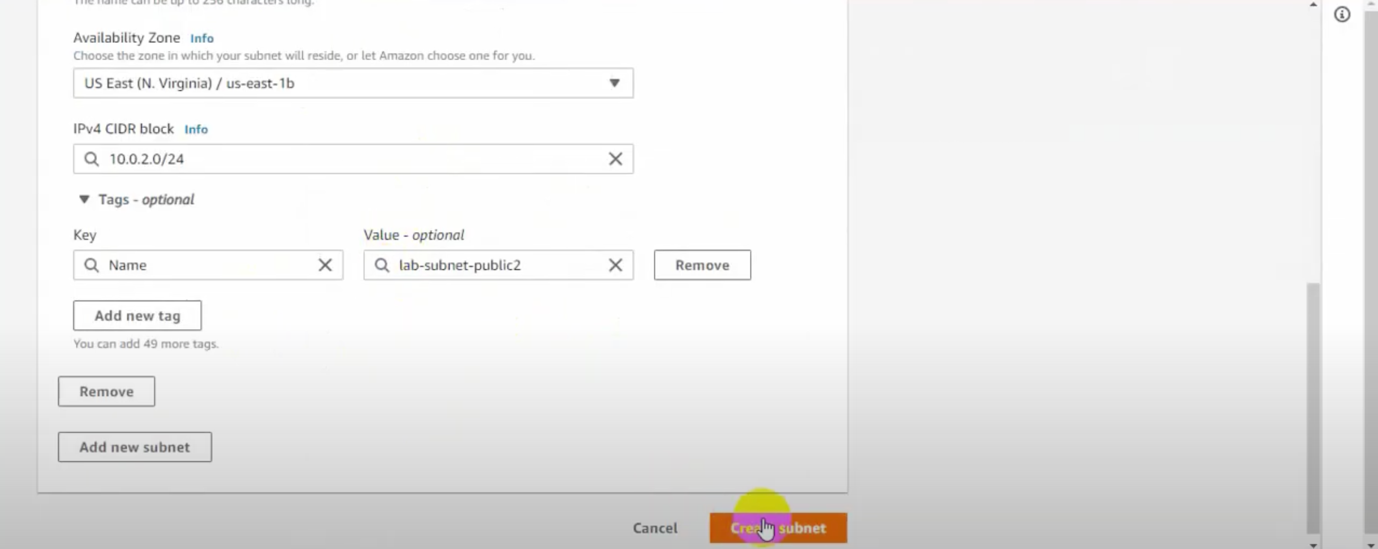
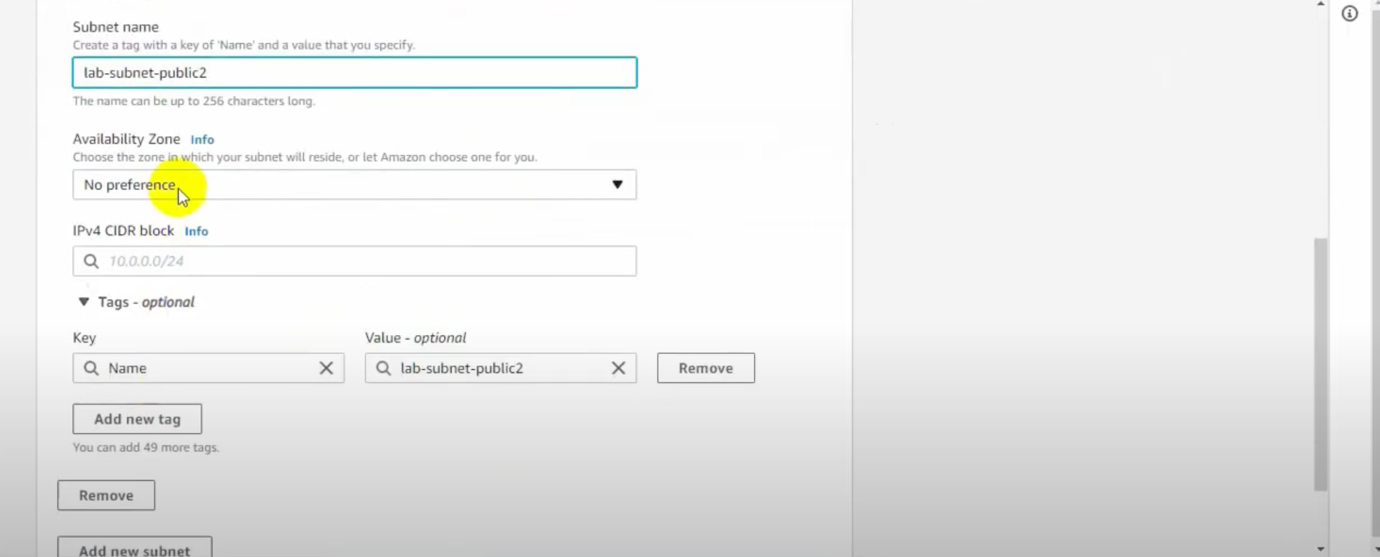
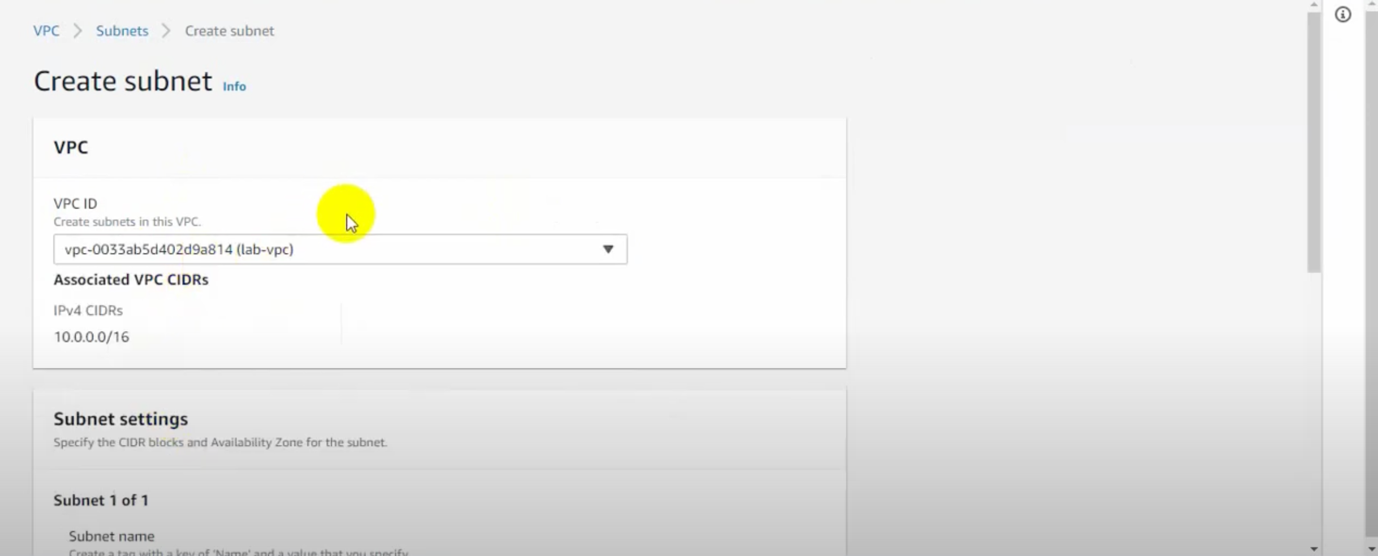
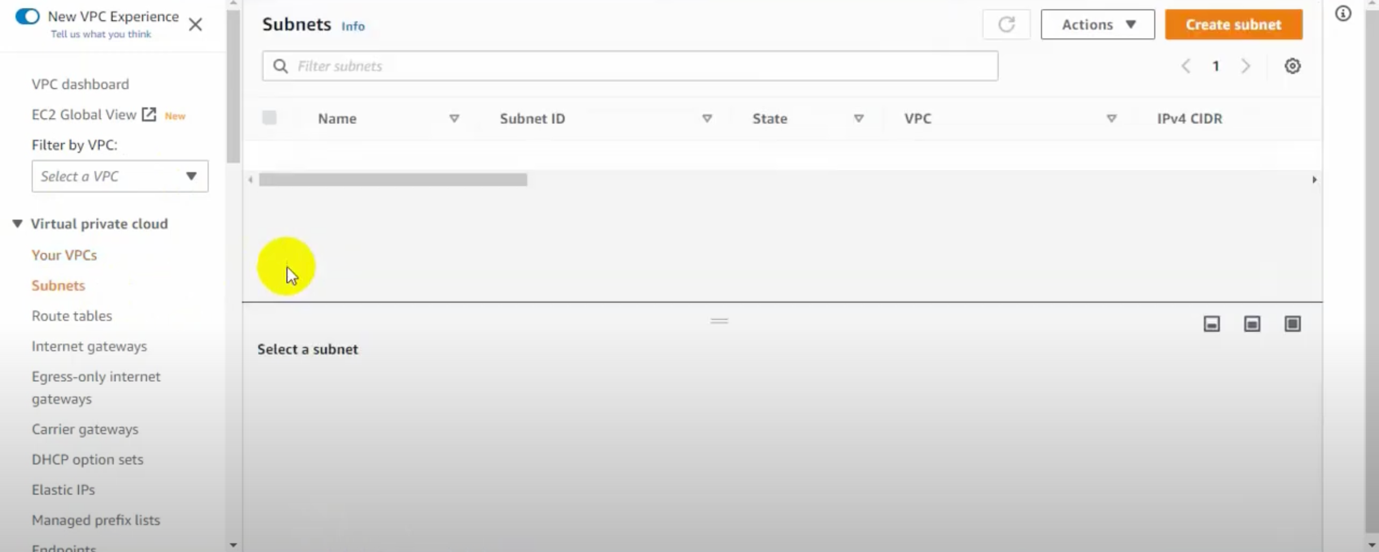
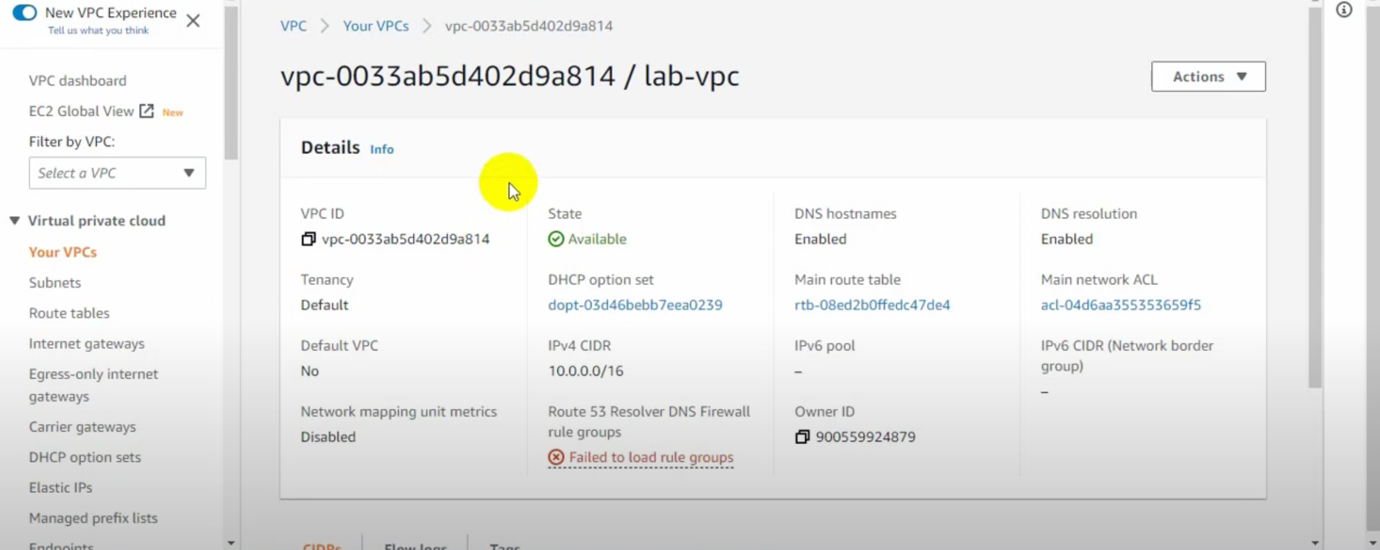
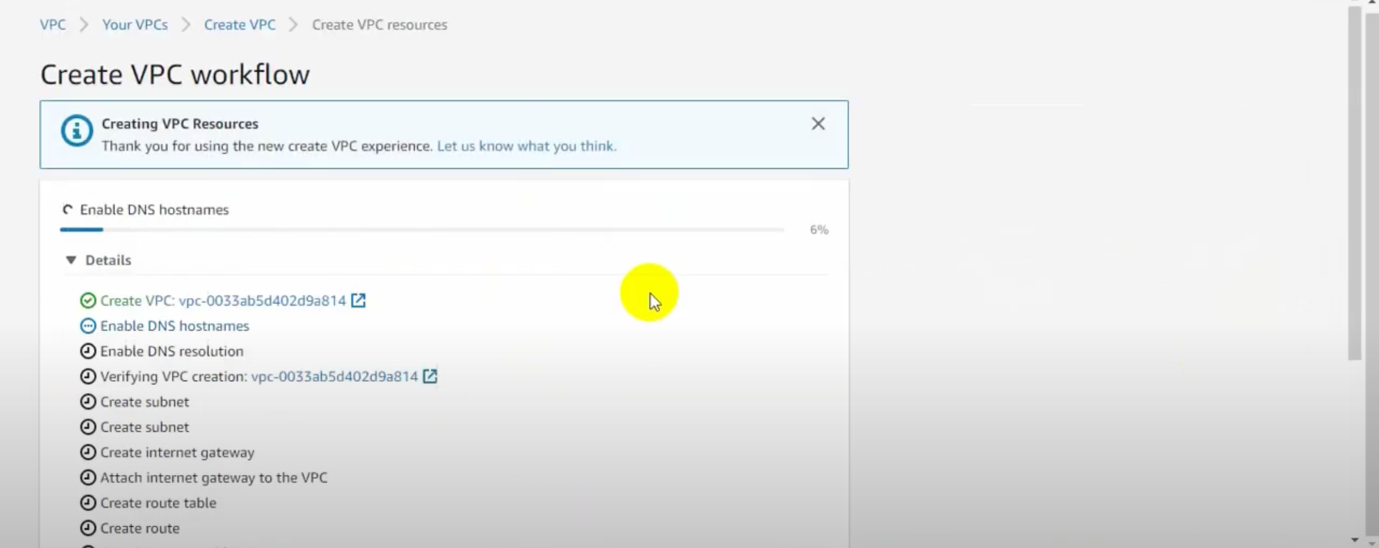
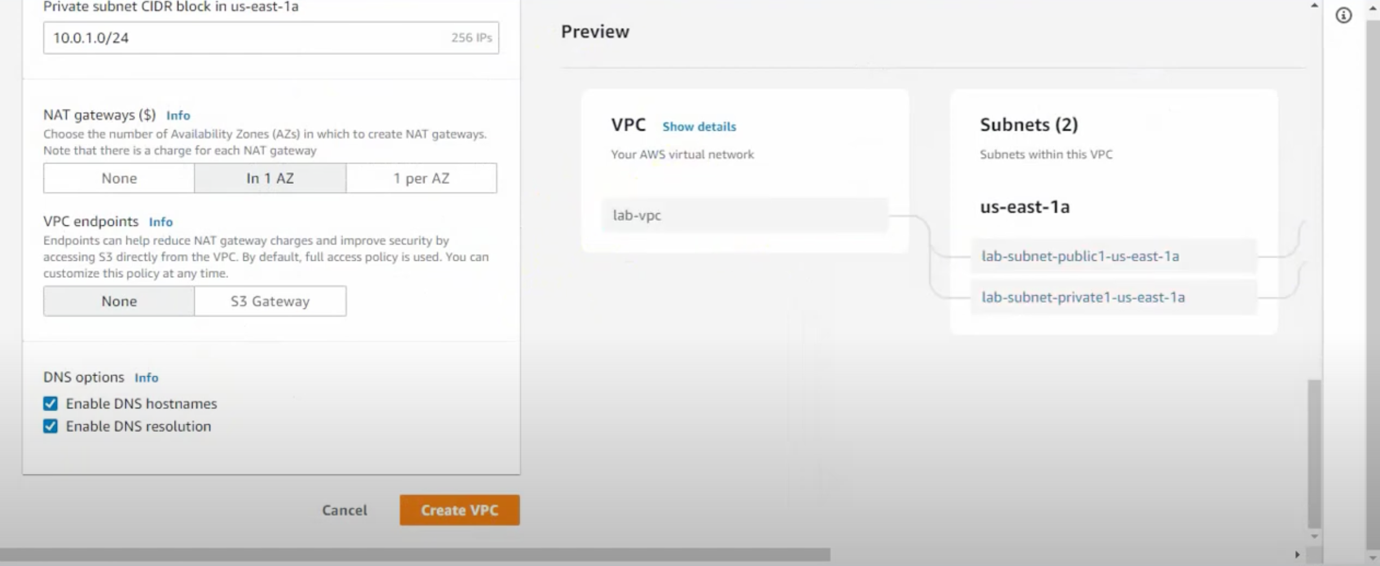
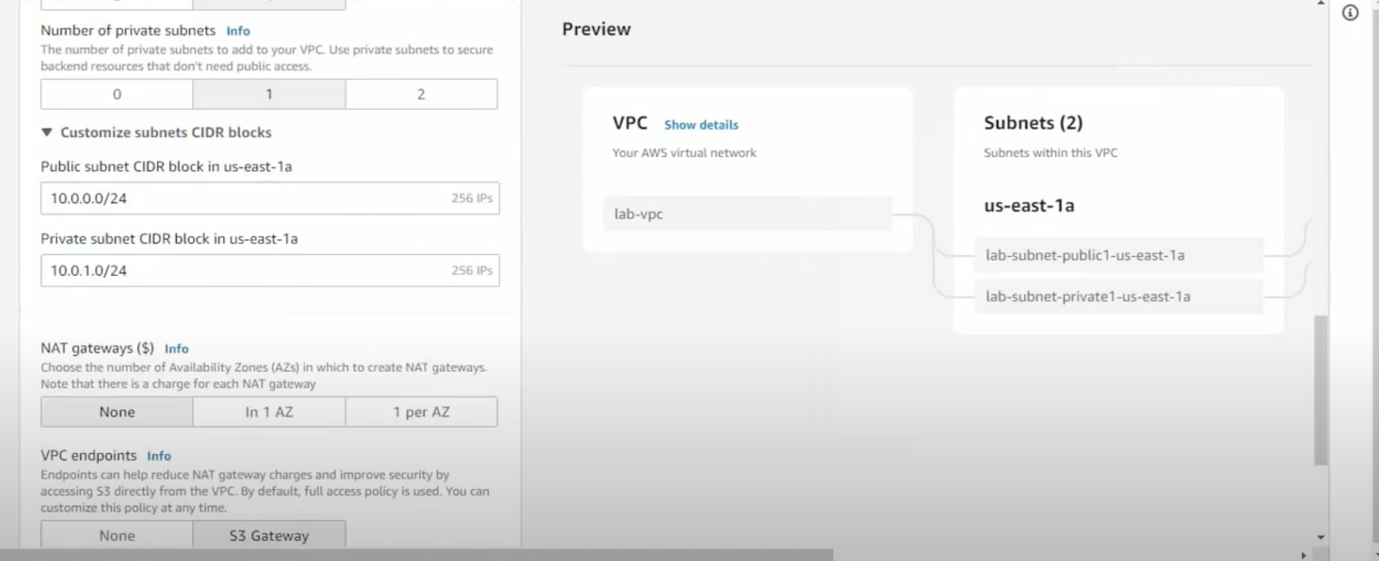
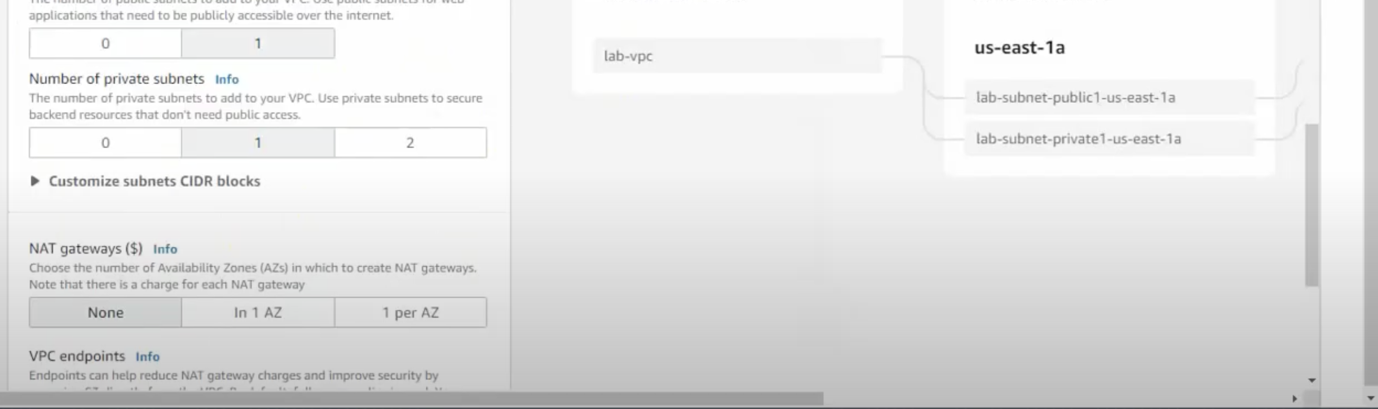
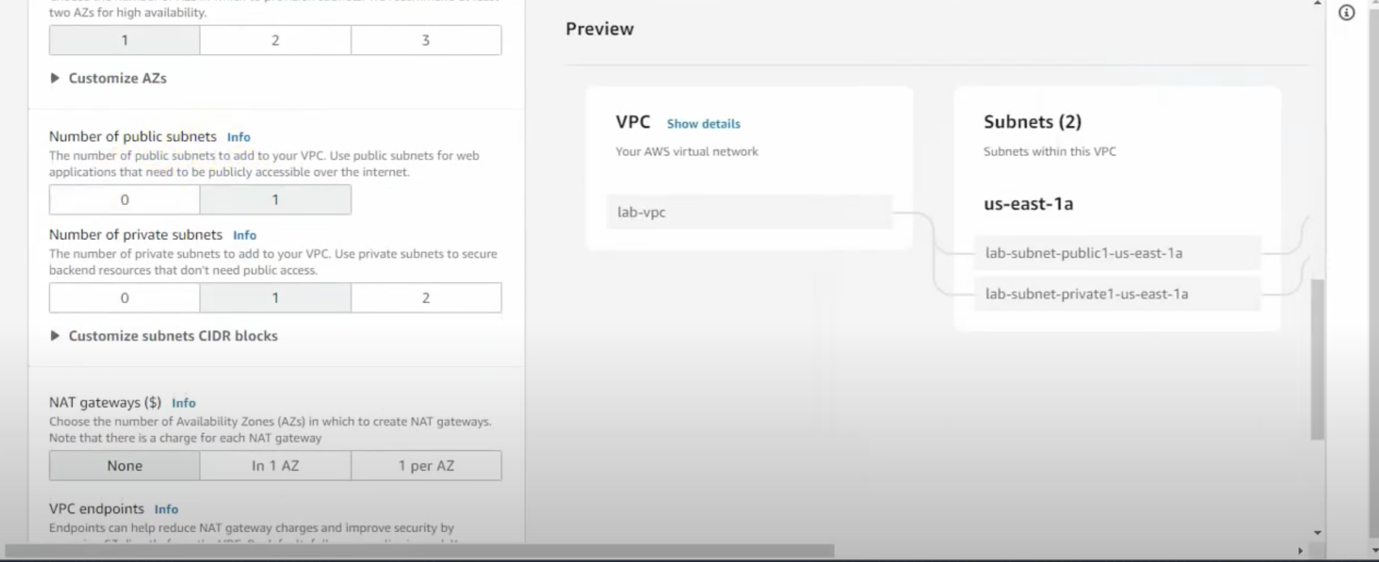
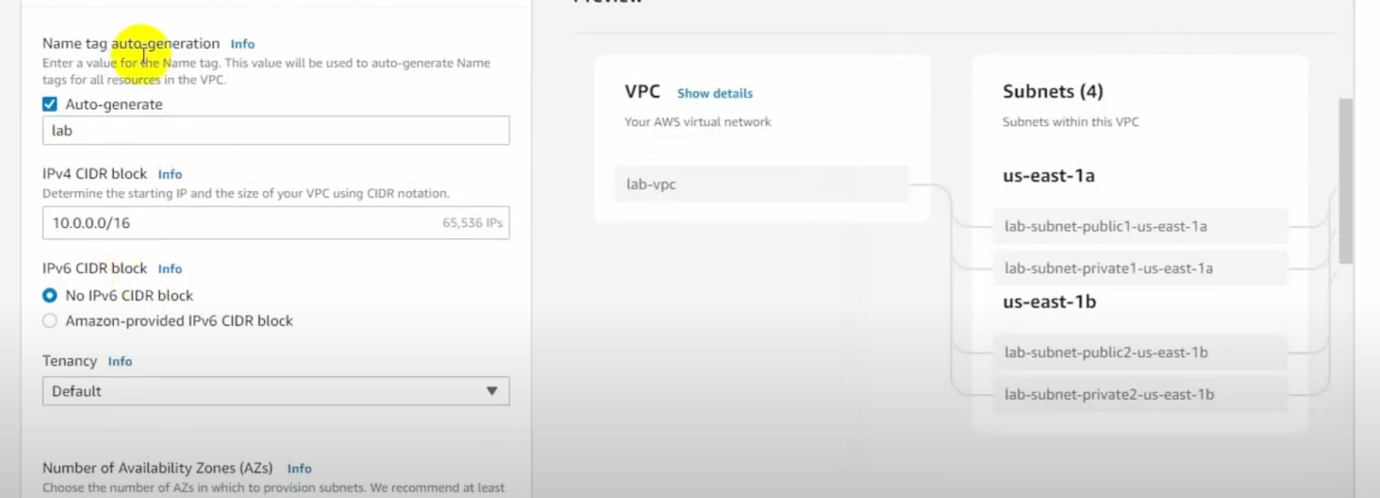
The objective of the lab experiment was to introduce the user to Virtual Private Cloud (VPC) in AWS and teach them how to create a custom VPC, subnet, internet gateway, security group, and launch a web server in the VPC. To accomplish this goal, I first learned the basics of VPC concepts such as CIDR blocks, routing tables, and network access control lists (NACLs). After grasping the fundamentals, I was then able to create the necessary VPC components, such as the custom VPC, subnet, internet gateway, and security group. I also learned how to configure the security group rules in order to enable the desired level of access to the web server. The final step of the lab was to launch a web server in the VPC, which I was able to successfully do.

Overall, this lab experience enabled me to become familiar with the fundamentals of AWS VPC, as well as gain experience with the process of creating and configuring the necessary components. By completing this lab, I now have the skills and knowledge necessary to create, configure, and maintain VPCs in AWS.

**Procedure:**

The lab began by creating a new VPC with a CIDR block range, and then dividing it into two subnets. Each subnet was assigned a different CIDR block range. The next step was to create an internet gateway and attach it to the VPC in order to enable internet access. This was a vital step in the process, as it allowed the VPC to communicate with other networks and the Internet. All these steps were necessary in order to complete the lab and ensure a properly configured network.

In the next step of the lab, the attendees were shown how to create a security group and configure the inbound and outbound rules to allow access to the web server. The instructor demonstrated how to create an Amazon Elastic Compute Cloud (EC2) instance and launch it in one of the subnets, as well as how to assign a public IP address to the instance for external access. This was done in order to allow for secure remote access to the web server. After the security group was created and configured, the instructor proceeded to show how to connect to the EC2 instance using the PuTTY SSH client. Finally, the instructor tested the connection to the web server by accessing a web page hosted in the EC2 instance.



**Developing Knowledge:**

Learning how to create and configure the VPC resources was the most beneficial part of the activity for me. I was able to understand the importance of creating a secure network environment in order to protect my AWS resources. The process of configuring subnets, an internet gateway, and security groups gave me a better comprehension of how to make sure my resources were secure and functioning properly. Through this activity, I was able to develop a more comprehensive understanding of how to create a secure environment using VPCs.

**Difficulties and Incompleteness:**

I found the lab to be quite straightforward overall, but there were a few sections that were a bit challenging. Configuring NACLs and troubleshooting connectivity issues were two sections I found to be a bit tricky. However, the instructions provided were a great help in overcoming these issues. I was able to work through each of the sections without any problems, and I am confident that I have completed all the tasks set out in the lab. All in all, I was able to complete the lab without too much difficulty.