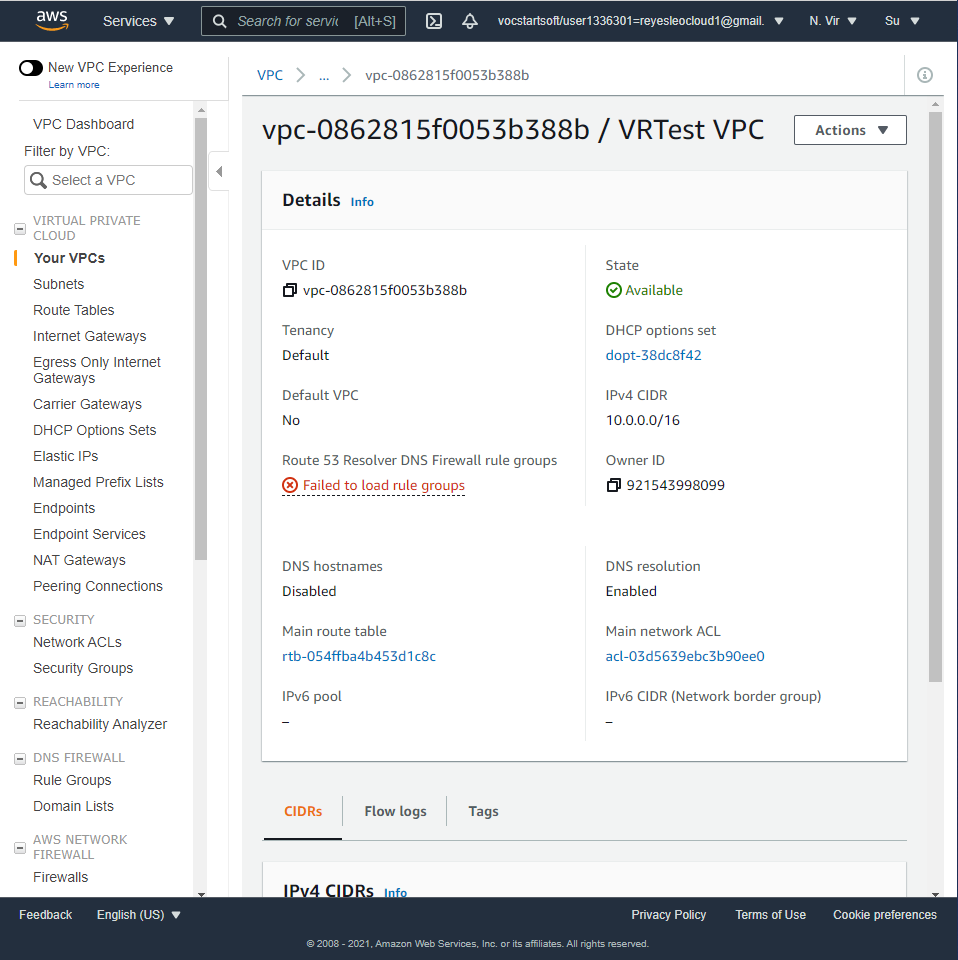
**AWS Lab 6: Launch Amazon EC2 in a non-default virtual private cloud**

Leo Reyes

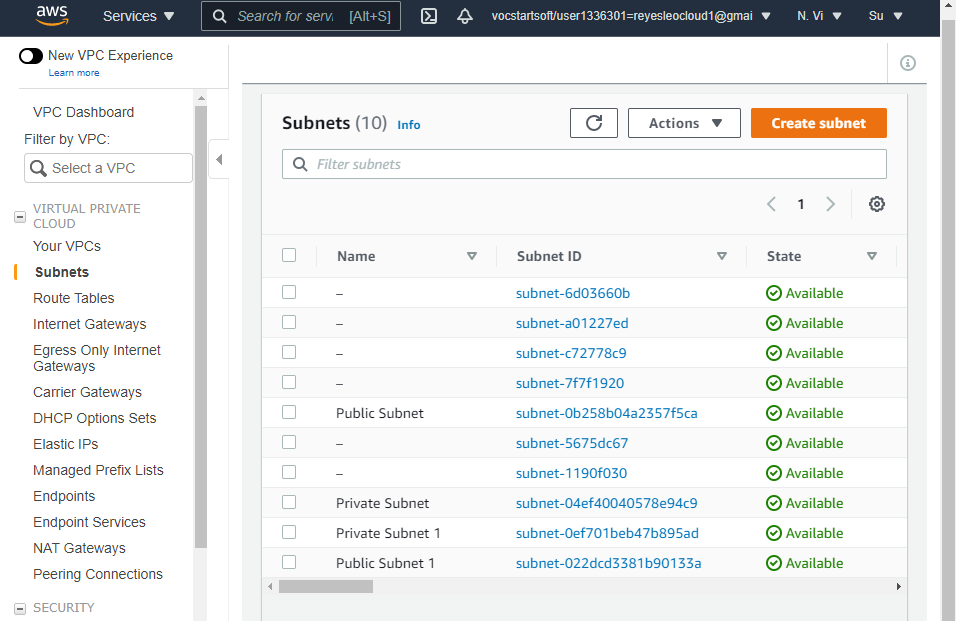
**Purpose**

The purpose of this lab is to create a Virtual Private Cloud (VPC) and use an Amazon EC2 instance in the networks created in the VPC. This lab is also meant to learn and practice setting up a VPC manually and set up a web server with the EC2 t-2 micro instance. This will help review how to set up networks in the VPC as well as set up subnets, Internet Gateways (IGWs) and route tables in the VPC.

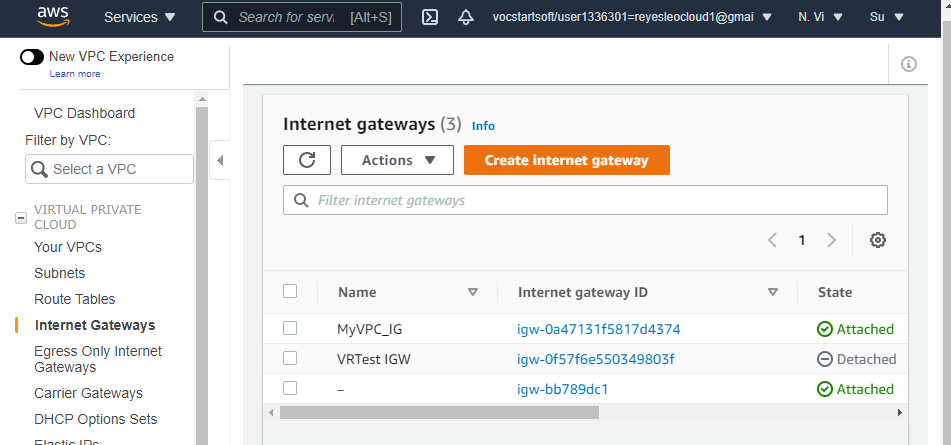
**Process**

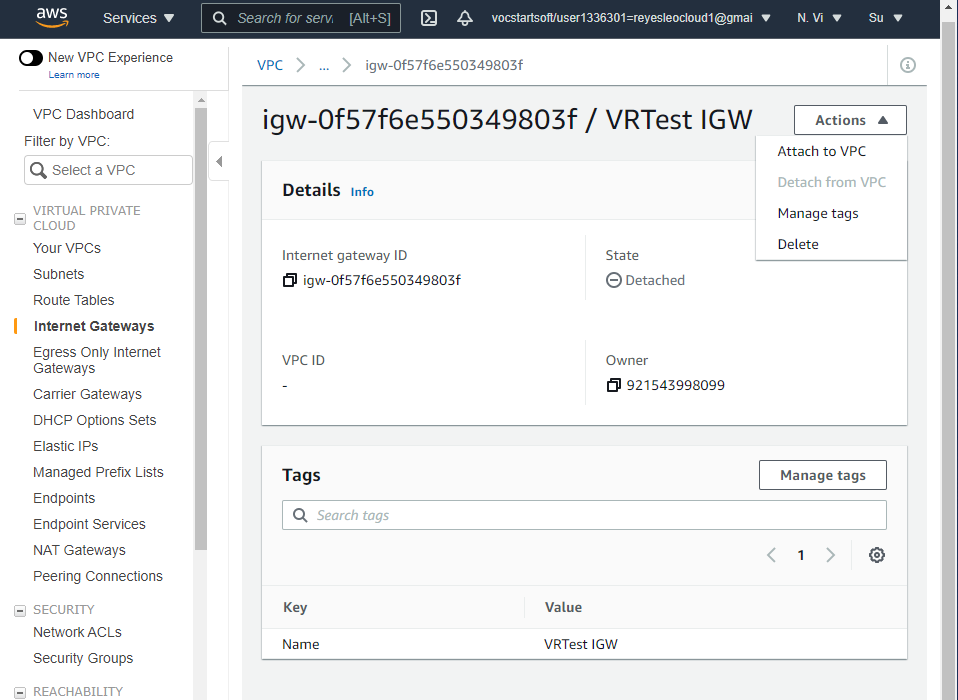


When the VPC is created, the subnets also need to be created. During this, the IPv4 block used also needs to be set up along with the other settings of the VPC.

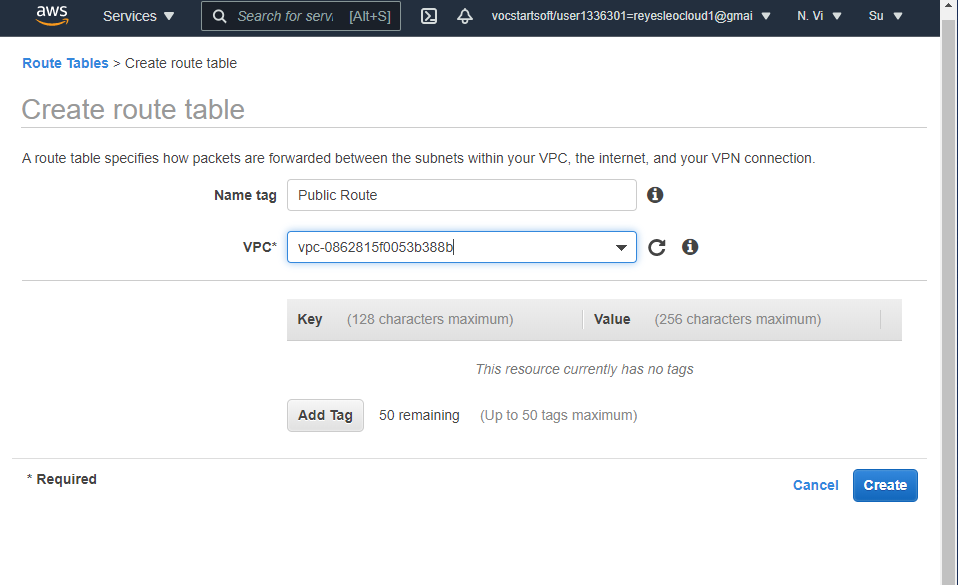


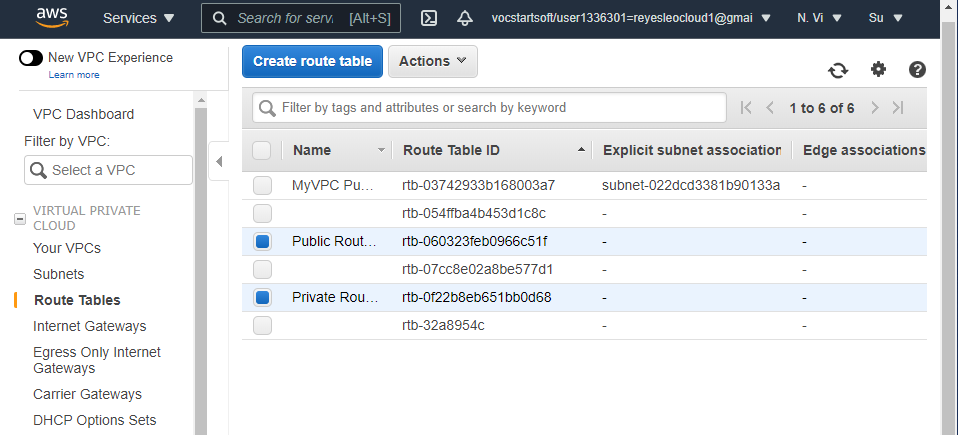
After the subnets and the VPC are created, they will be available to be seen on the left of the VPC dashboard in the subnets tab. The private and public subnets here will be available to be seen and they can be identified from other subnets by the id.



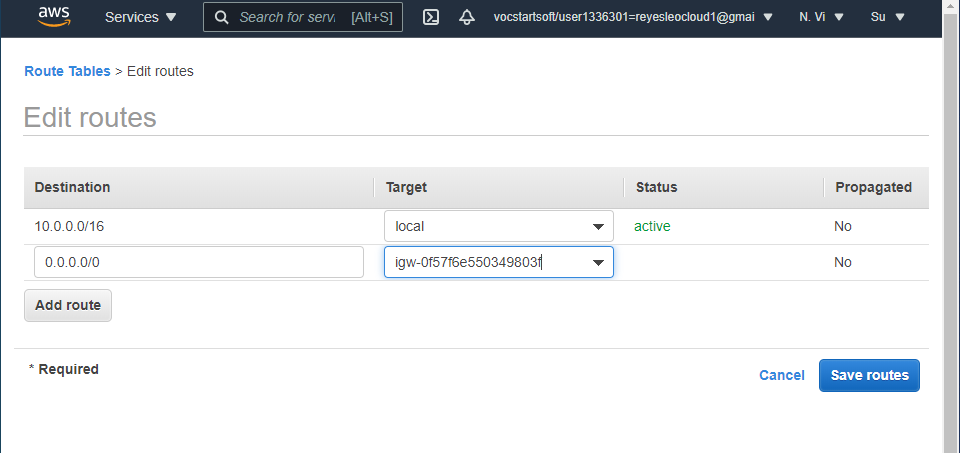


After creating the Internet Gateway (IGW), it has to be attached to the VPC for it to work with the subnets. This can be done from going to the Internet Gateways option in the VPC dashboard. From here, the IGW that was previously created will be available and by clicking on the actions, it can be attached to the VPC.

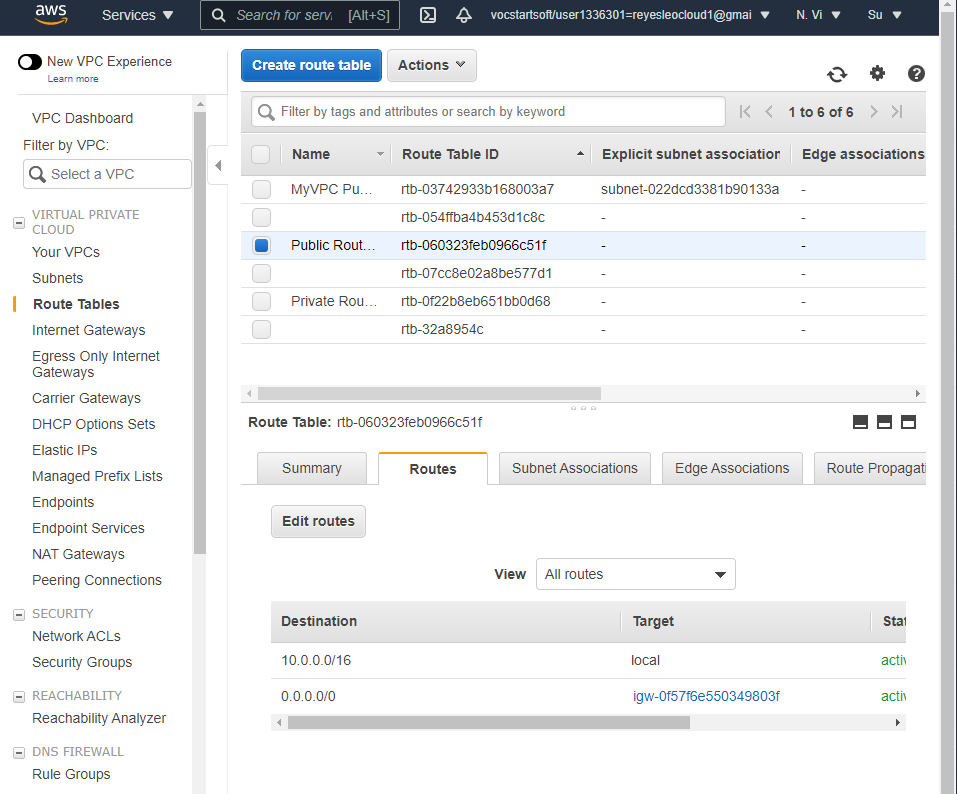




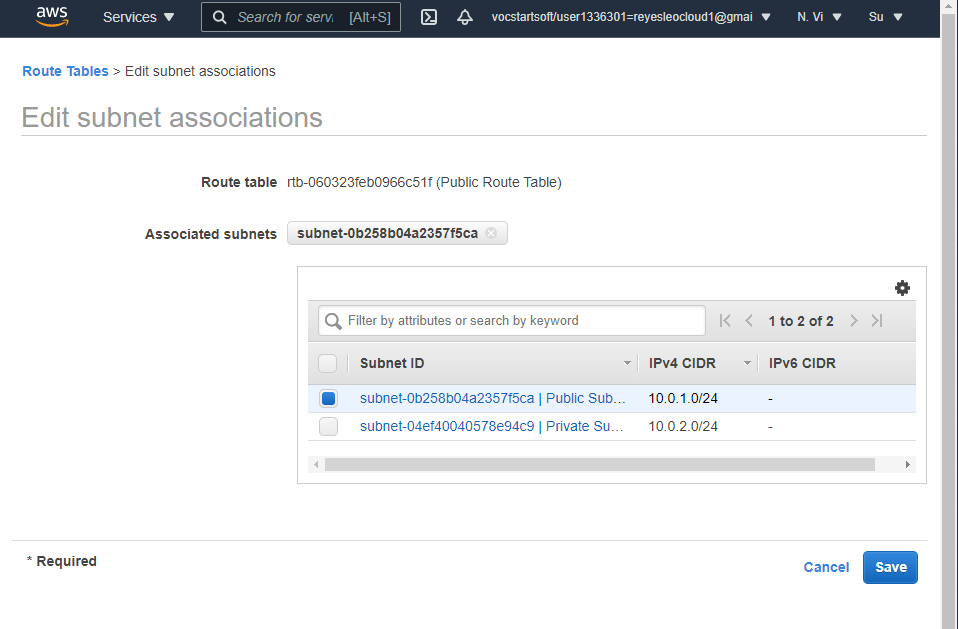
A route table must also be created to keep track of the IP addresses in the network for both he private and the public subnets. While creating the route table, it must be assigned immediately to a VPC.

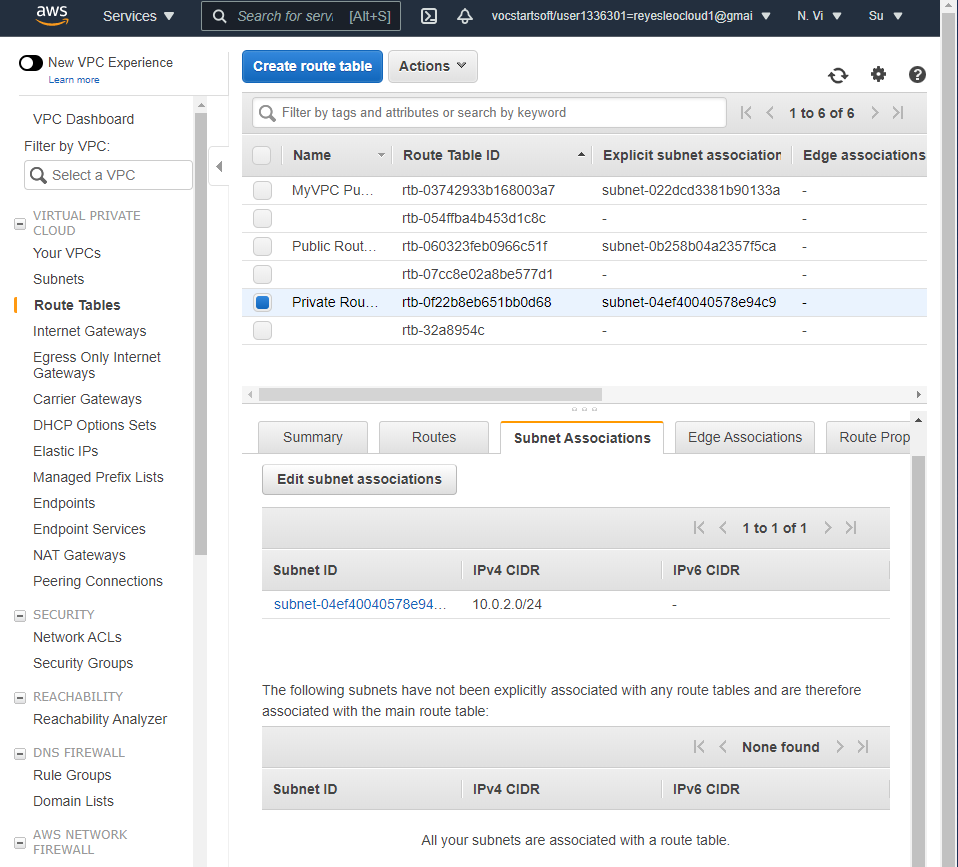


When editing the routes in the route table, any number of routes can be created. These routes need to have a target destination, such as the IGW previously created.

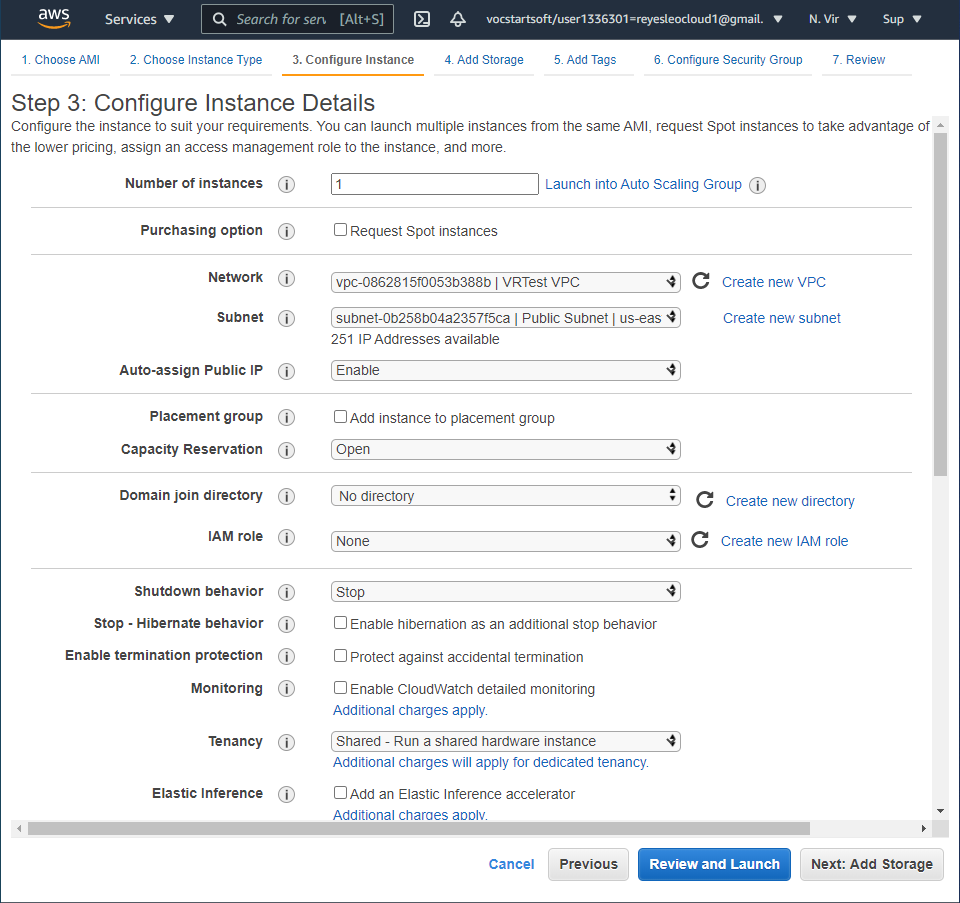


After creating the route tables, you can select a route table to see the routes for the public and private subnets, but no routes will appear until the routes are associated with the route table.

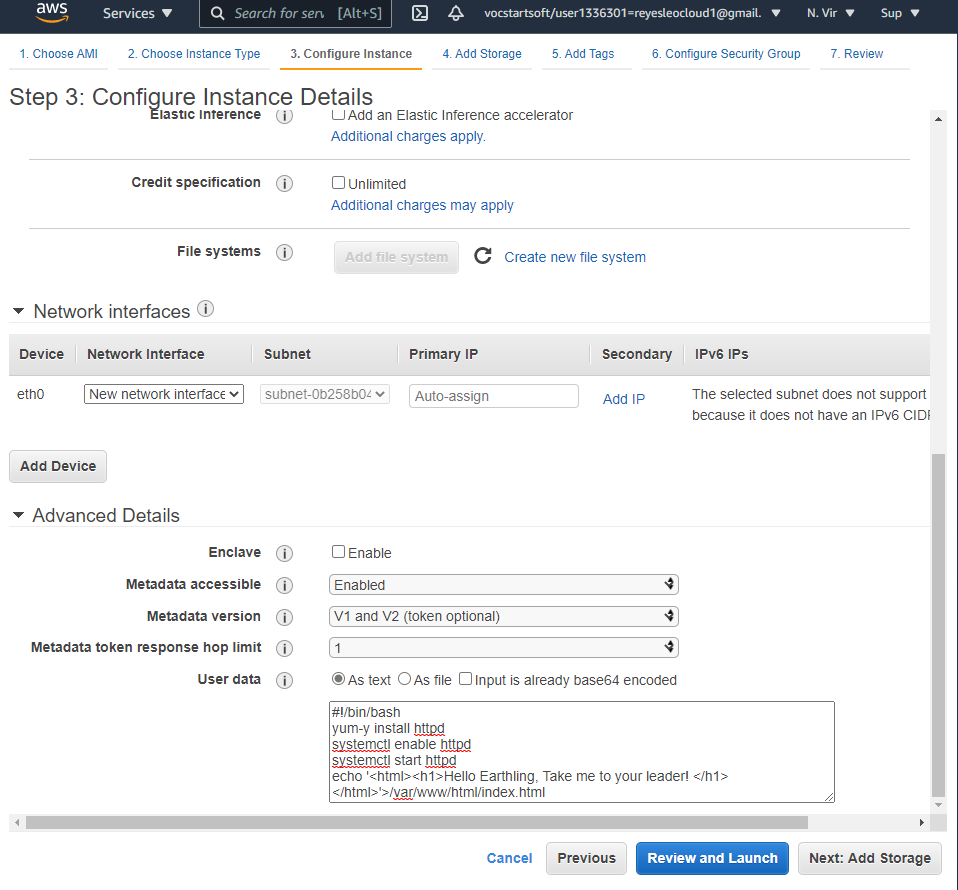




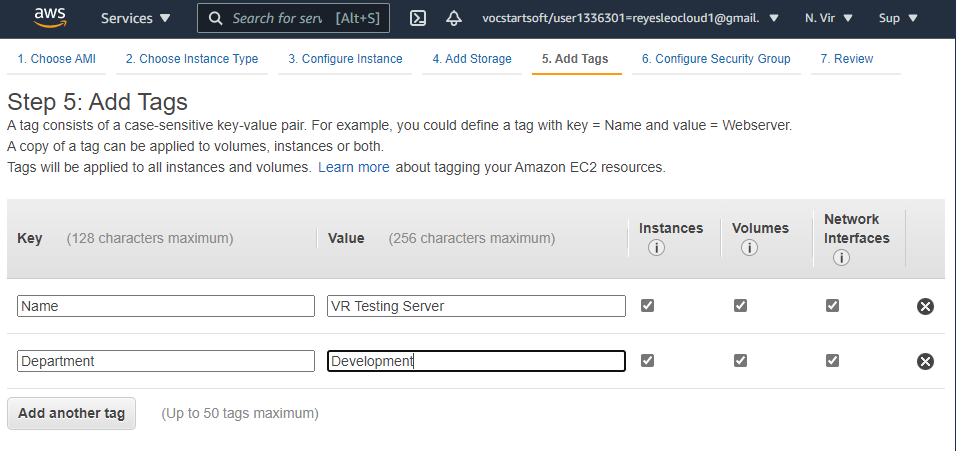
The routes will be shown in the same bottom part of the selected route table for both the private and public route tables.



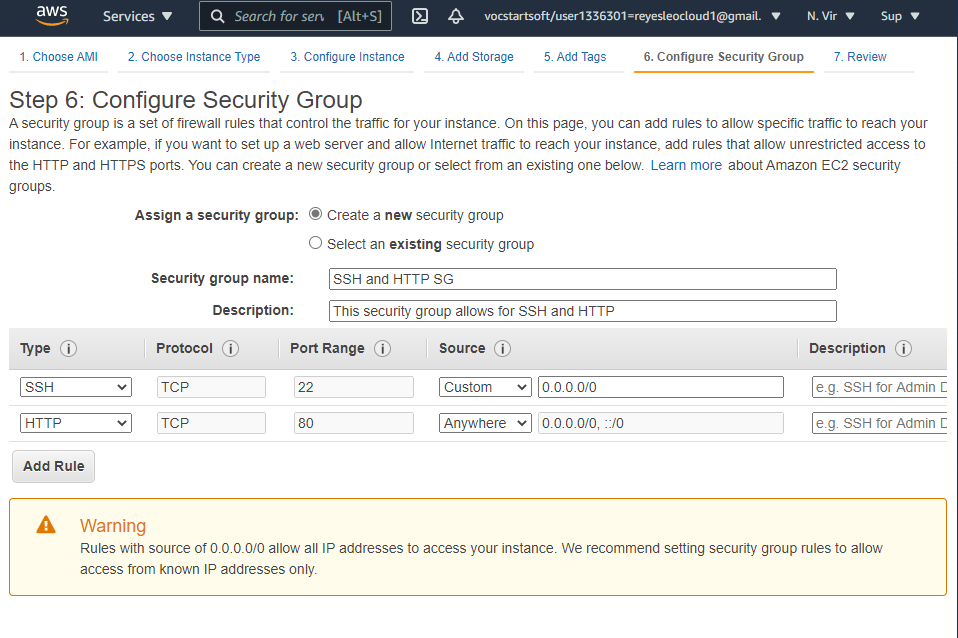
After creating the route tables, the subnets and the VPC, it is time for the EC2 instance to be created. The first 2 steps will be kept as default, but on the third step, the instance must be assigned to the subnet and the VPC.



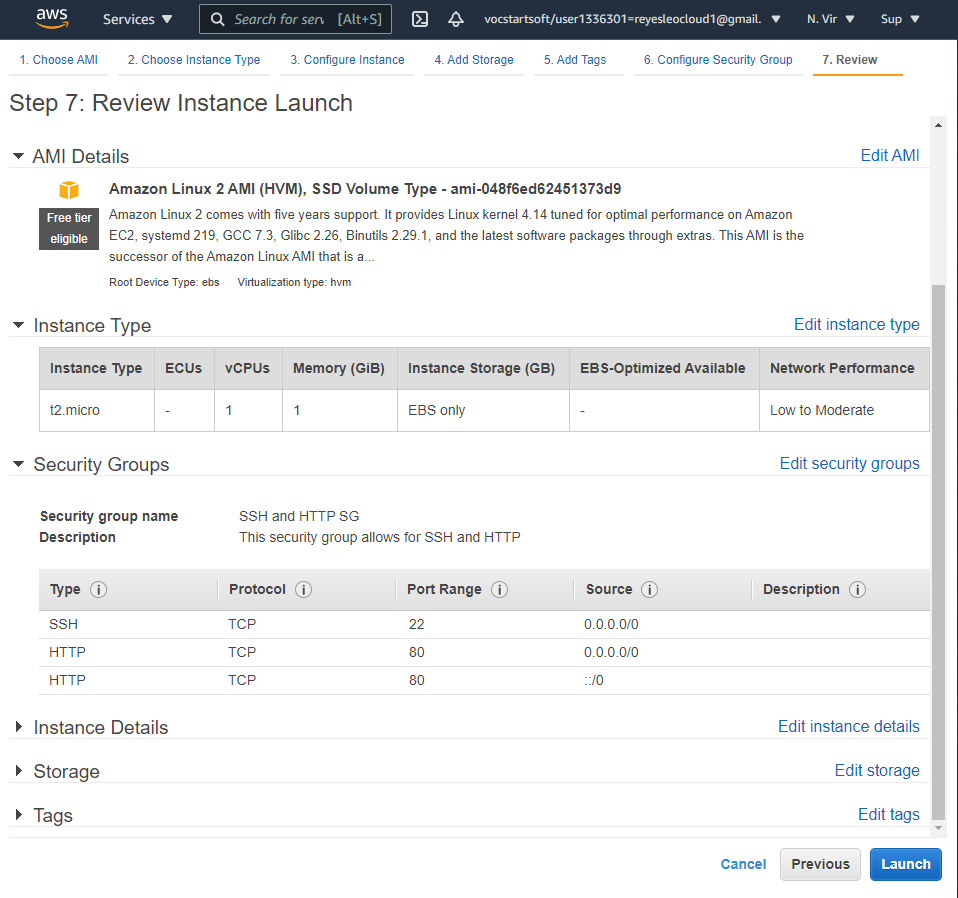
The network interfaces must have the following data in order to set up the instance correctly.



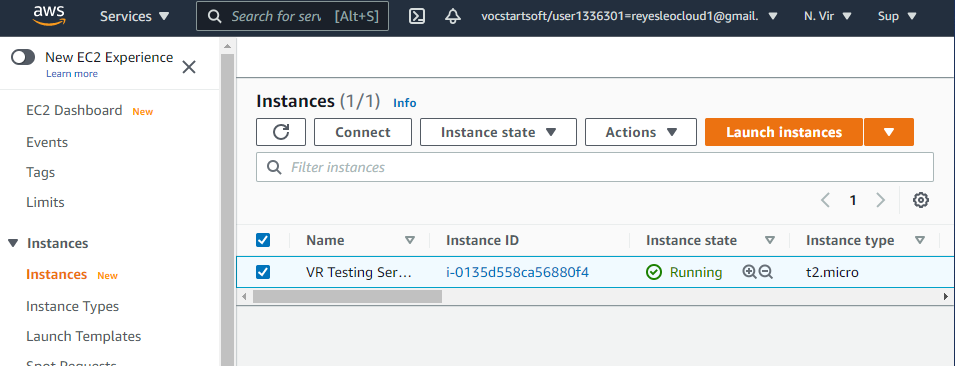
No extra storage is needed for this lab, but some tags will be added. These tags will be used to set up security groups.



These security groups will be used to manage the networks and the subnets and protect the web server from unauthorized users.

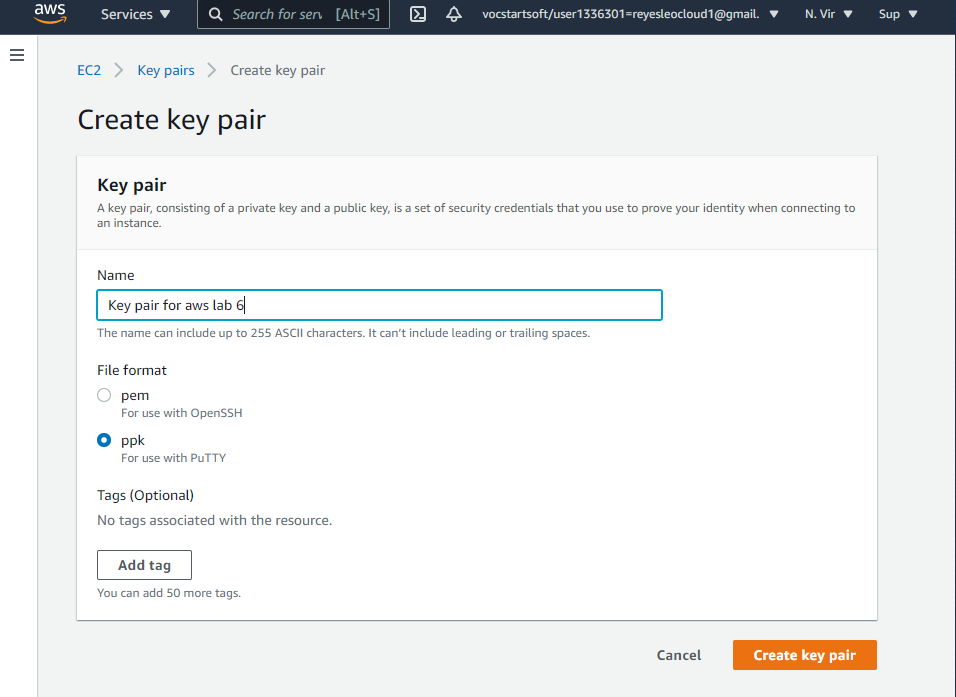


The final step of setting up the instance is checking the settings are correct on everything.

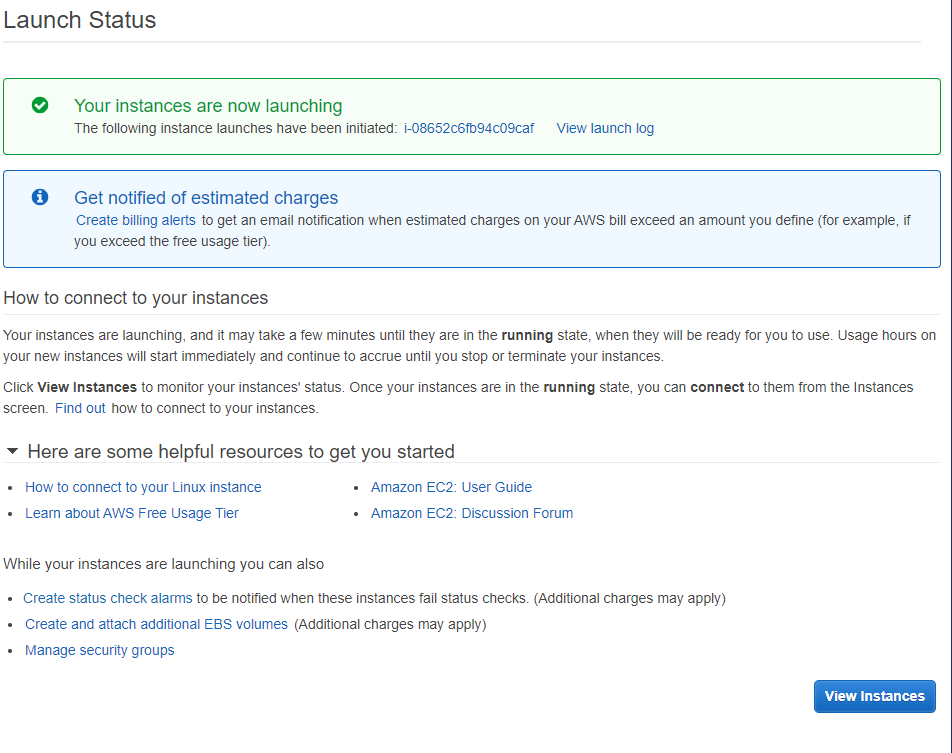


Finally, the instance will be able to be seen from the EC2 dashboard under instances. With this, the web server will be up and running.

**Process (for Key Pairs)**

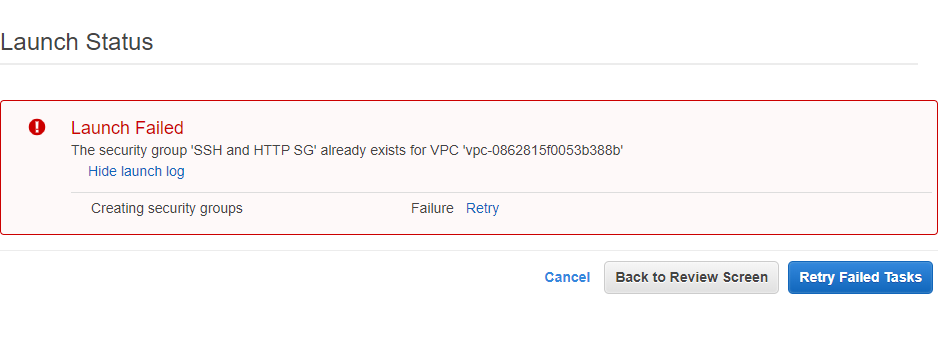


To create a key pair, the option is available under the EC2 dashboard. From here, creating the key pair is simple where you click on “Create key pair” change the settings and finally create it.



This message will be shown which will tell you the pair was successfully created.

**Problems**

****

There was a slight problem when creating the EC2 instance. The instance could not be created without a key pair. The problem with the Key pair was that the name was duplicated and after changing the name of it, the instance was able to be created.

**Conclusion**

In conclusion, this lab helped me explore how to create and EC2 instance and how to manually create a VPC with a public and private subnets along with their own route tables and security groups for them in the EC2 instance. This all helped creating a web server with resources which are all protected due to the private and public subnets as well as the security groups.

**Questions**

1. A default VPC is a virtual private cloud which is used to access websites with objects stored in the VPC.
2. Attach the internet gateway (IGW) so that the public subject has access to the internet
3. The route table organizes what resources can be accessed from each subnet and who can access them. Only people with a key pair can access the VPC’s settings on the EC2 service
4. It will use the default settings in the VPC but the instance will not work as it needs a specific availability zone (AZ)
5. It assigns IP addresses to the users who are trying to access the website. This is done through the IGW that is attached to the VPC
6. The VPC and the IGW won’t be able to connect to the internet and it won’t assign users with ip addresses to access the website
7. A security group determines what protocols for security are used and which ones are allowed into the website and servers. They are important because they protect the servers as well as block users using certain protocols to access the website.
8. The private subnet would be used for the users with a key pair to access it. It would be used when wanting to access private parts of the website.
9. The internet gateway helps direct users to the website. It also ensures that they run through the Route Table and that will check if they are allowed in by the security groups created in the instances.