Department of Computer Engineering

Academic Term: JAN-MAY 2022

Class: ***BE COMPUTERS***

Subject Name: ***CLOUD COMPUTING LABORATORY***

Subject Code: CSL803

Practical No:	**07**
Title:	**AWS VPC**
Date of Performance:	**02/02/22**
Date of Submission:	**14/02/2022**
Roll No:	**8626**
Name of the Student:	**Divita Phadakale**

Evaluation:

Sr. No	Rubric	Grade
1	On time submission(2)	
2	Preparedness(2)	
3	Output(2)	
4	Post Lab Questions (4)	
	TOTAL	

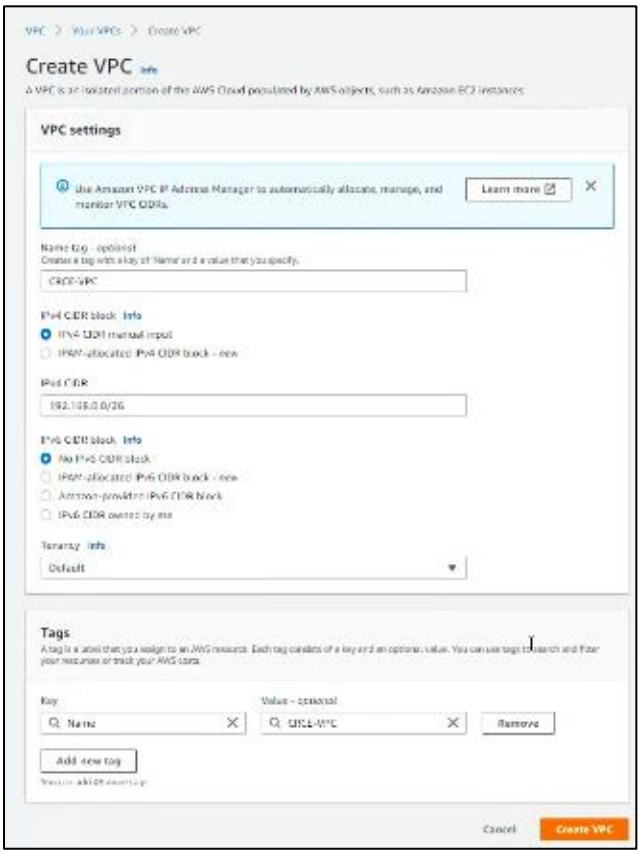
Signature of the Teacher:

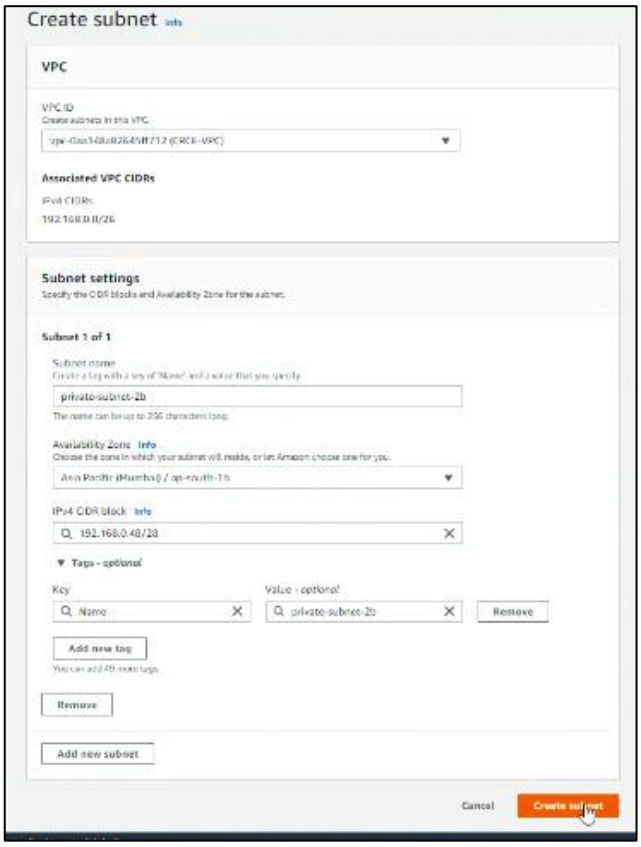
AWS VPC Configuration

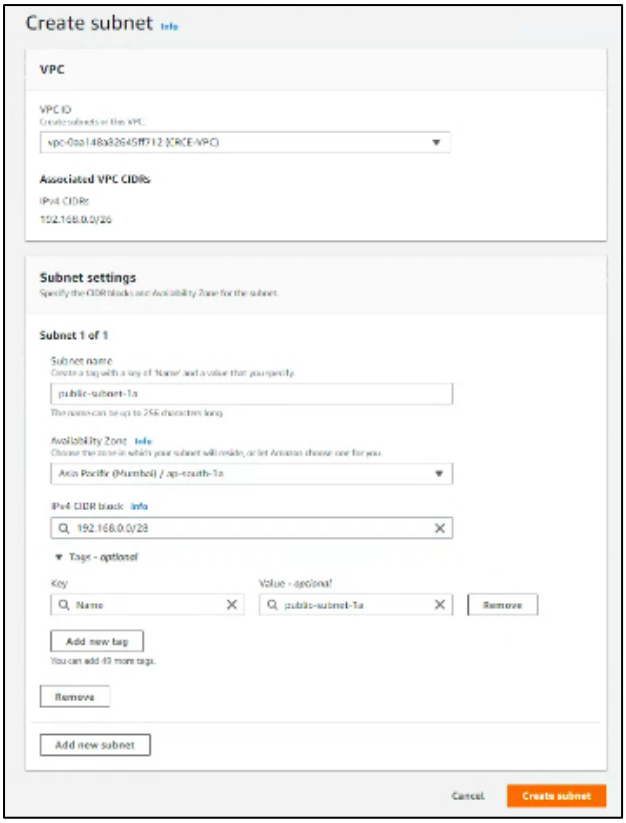
Steps to create a VPC

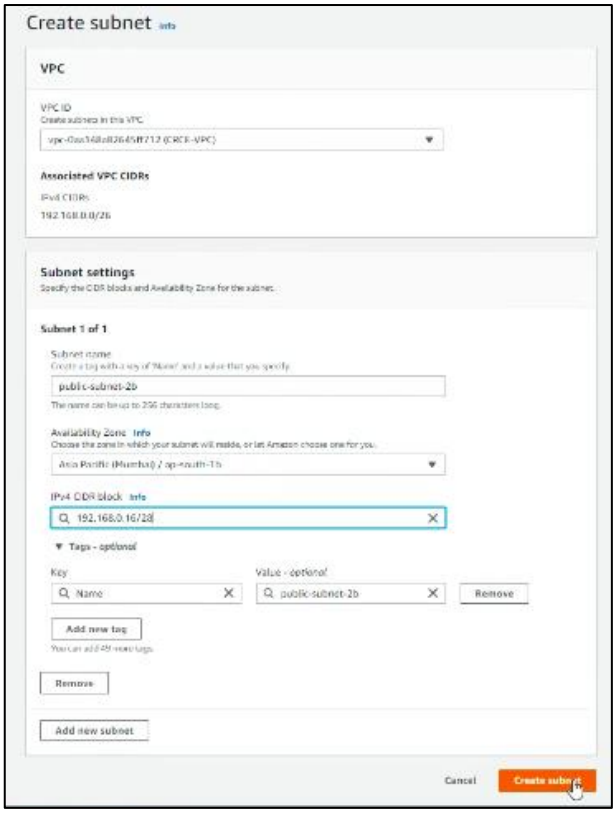
- Create VPC and public and private subnets
- Create Internet Gateway and attach to VPC
- Create public and private routing tables
- Set public routing table for IG
- Add subnet association (public subnet) in public routing table
- Create NAT Gateway in public subnet
- Set private routing table for NAT
- Add subnet association (private subnet) in private routing table
- Create EC2 instances for public and private subnets

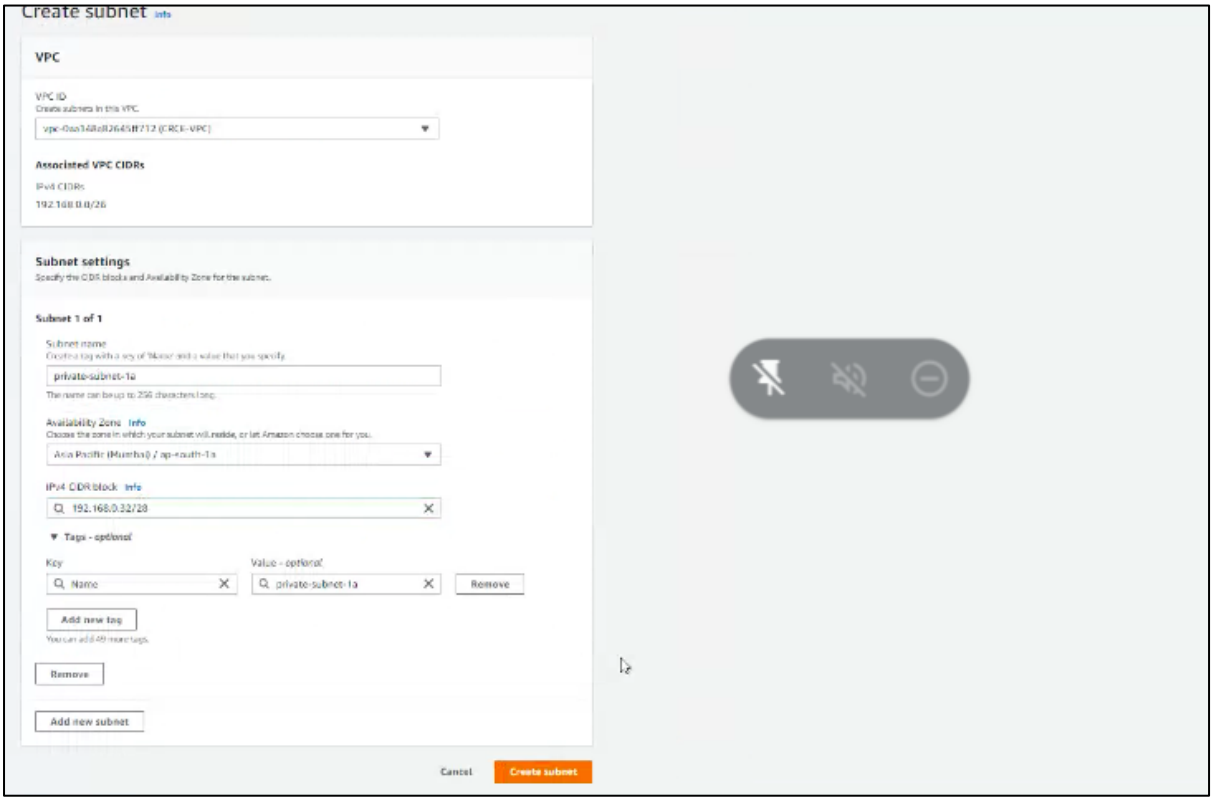
1. Create VPC and 4 subnets (2 public and 2 private)



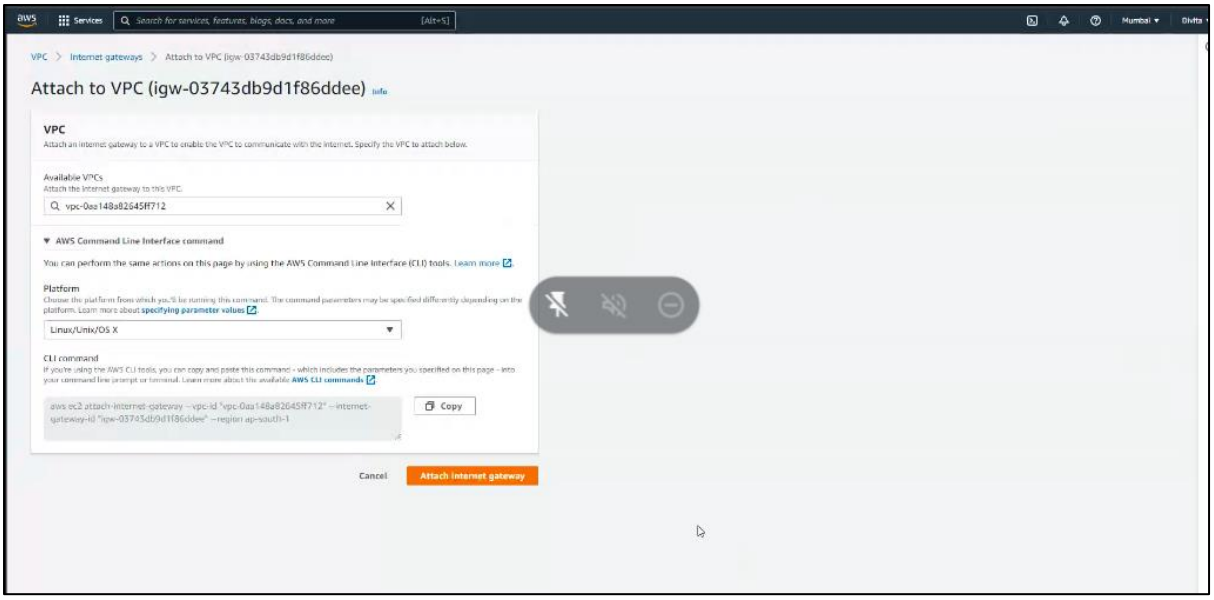




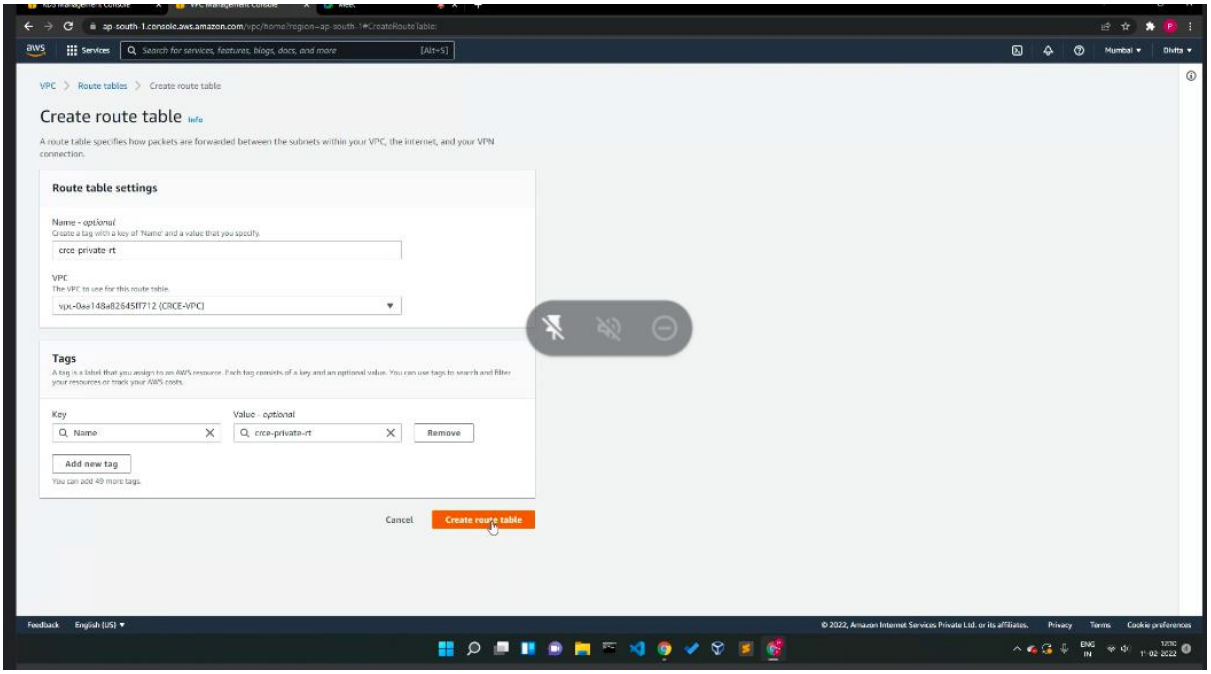




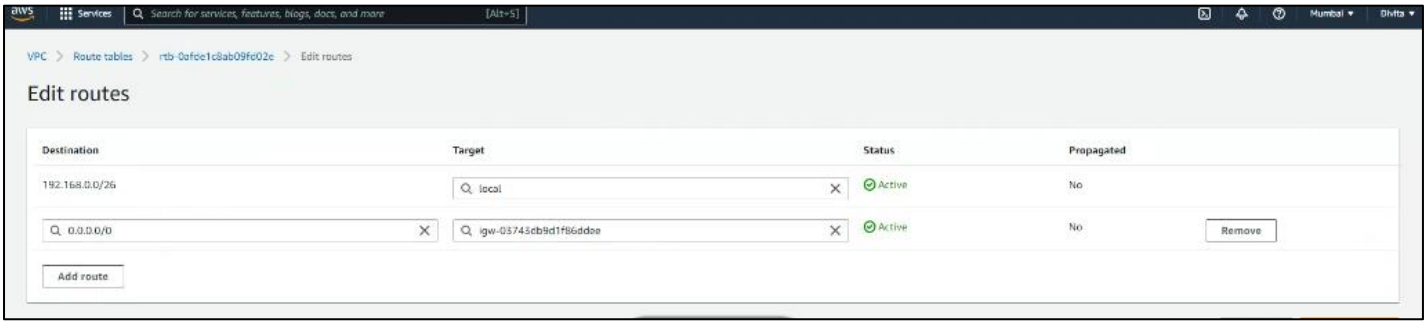
2. Create Internet gateway and attach to VPC (can get this in the left side -> click on “create” on right to create new IG)



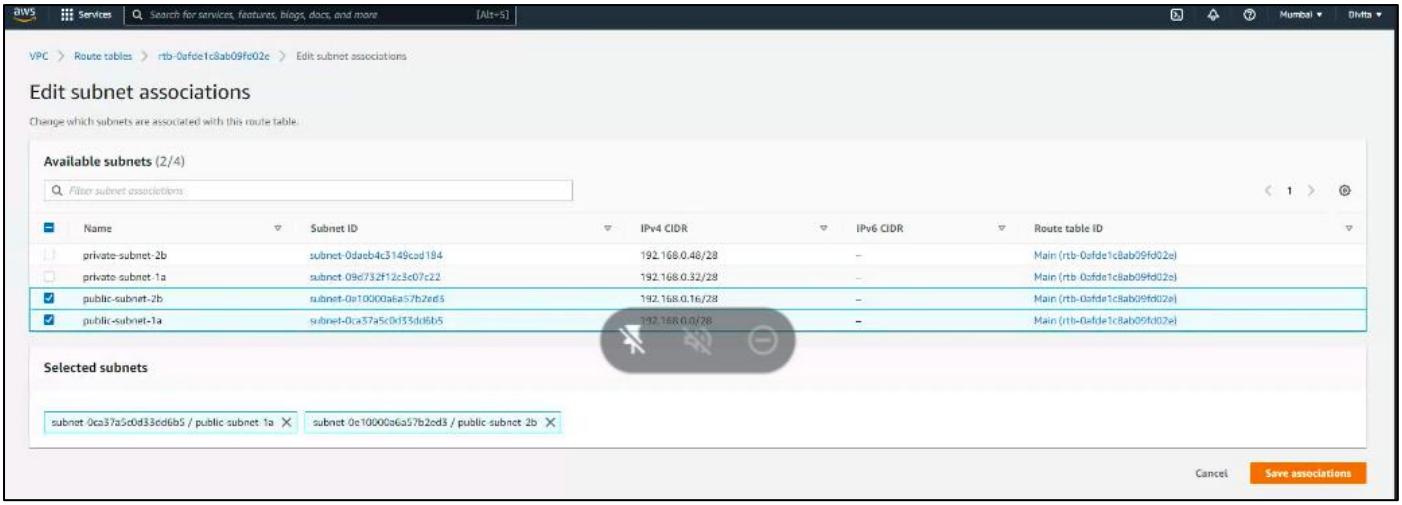
3. Create routing tables (“create new route table” on the right side)



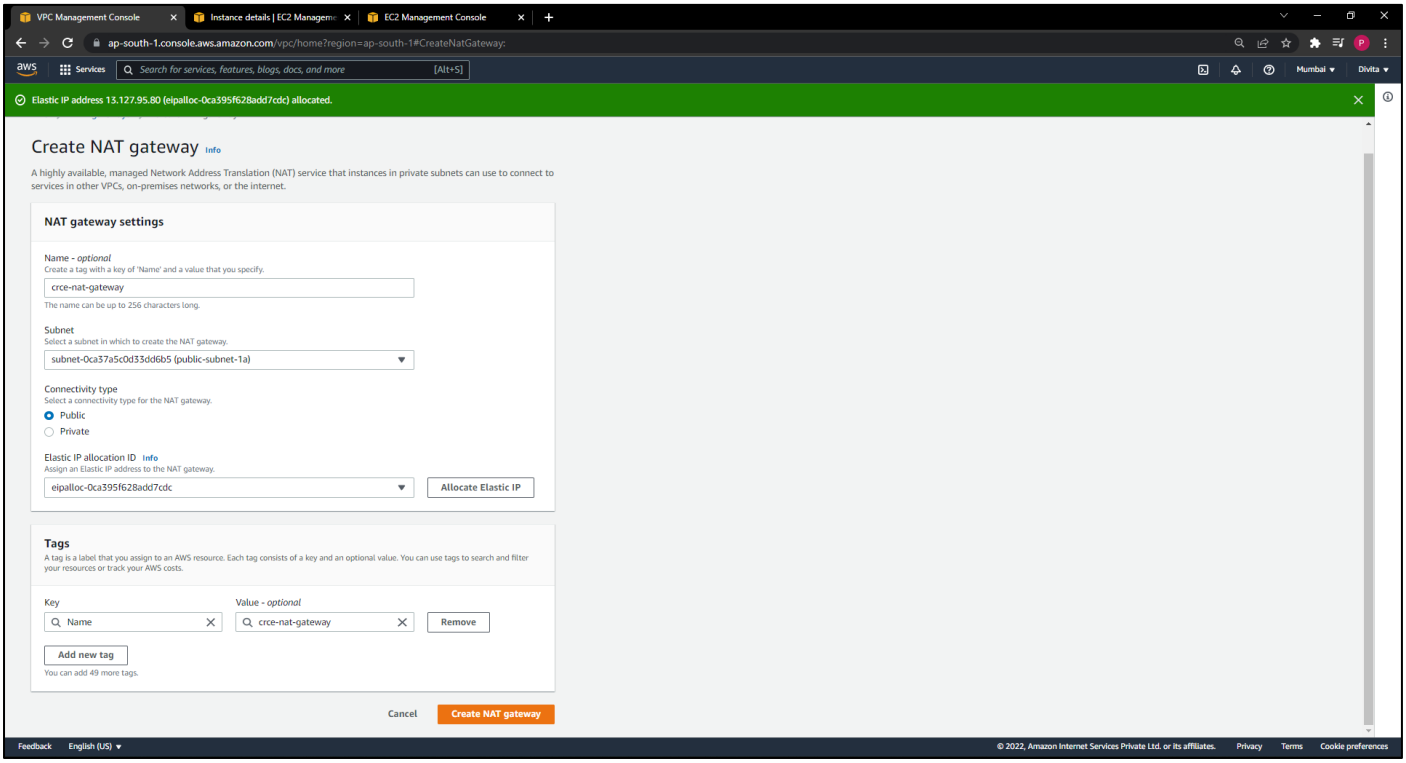
4. Adding Internet Gateway in public routing table (click on the public route table -> scroll down -> edit routes)



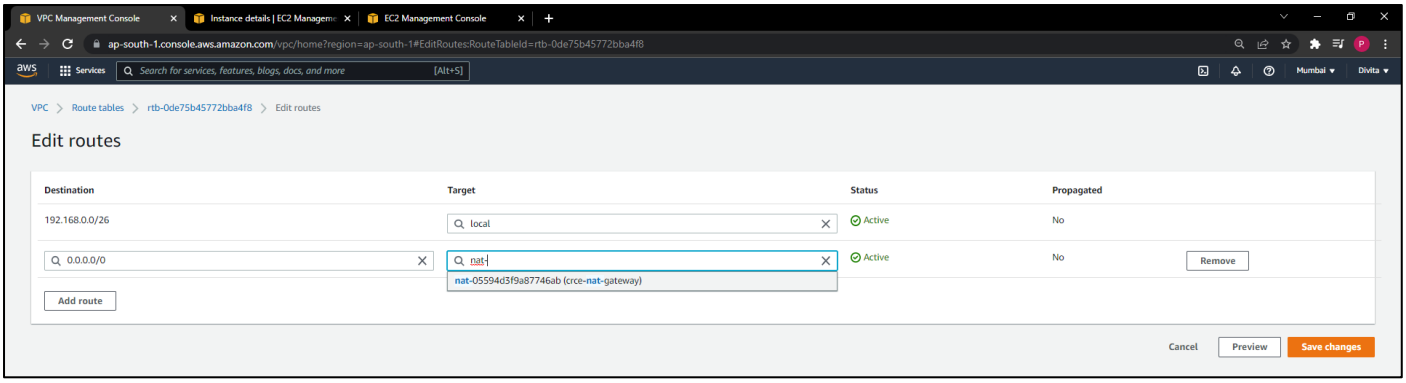
5. Add public subnet to public RT (set this as main)



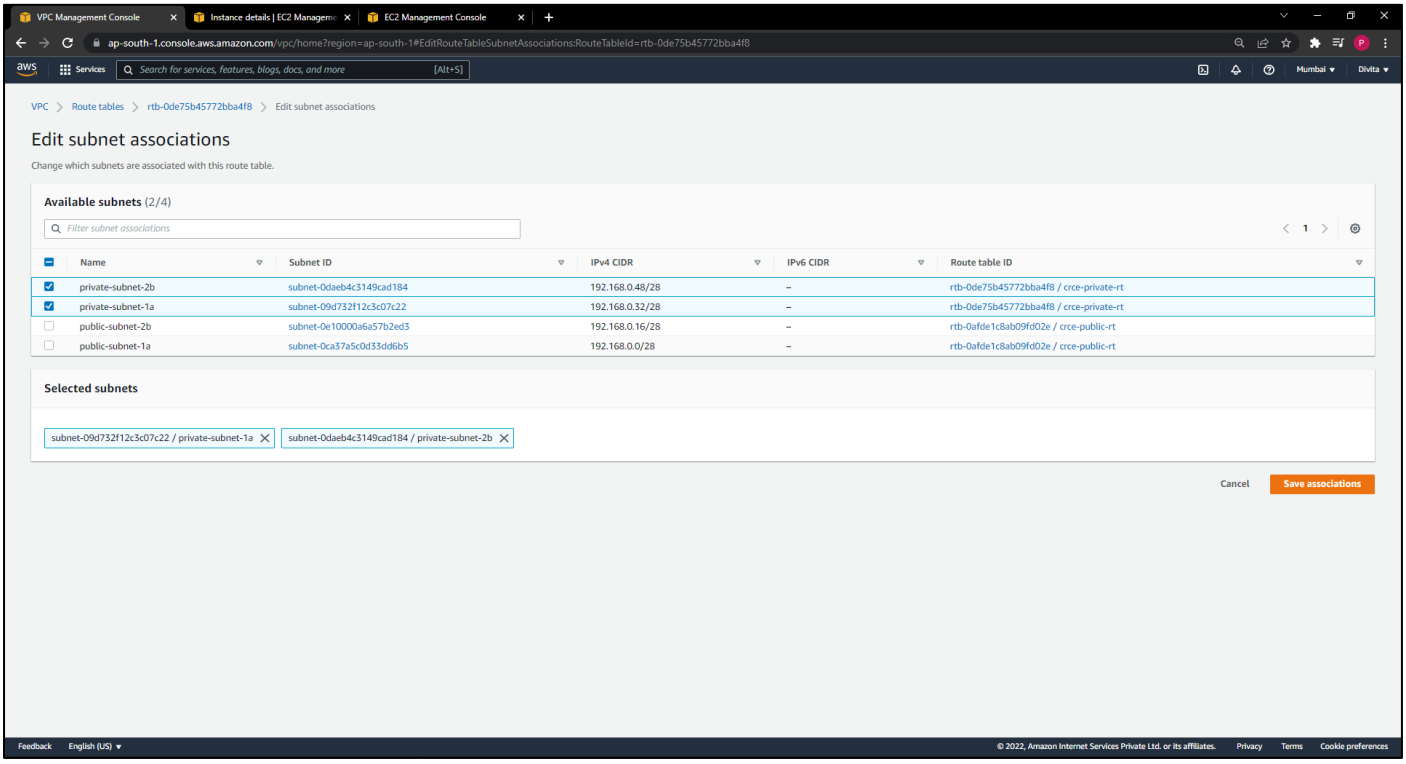
6. Create NAT Gateway in public subnet (can get this in the left side -> click on “create” on right to create new NAT gateway) (ps: remember to select public subnet here)



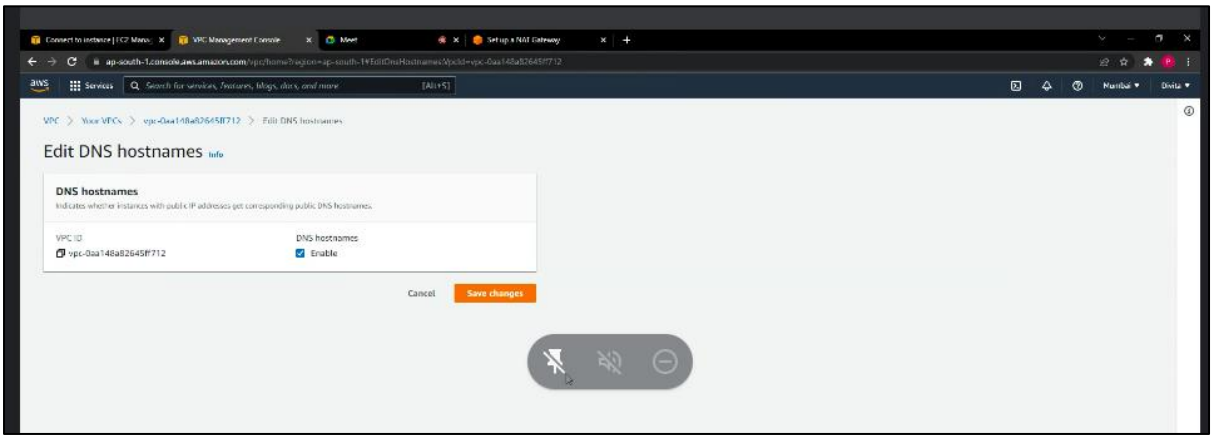
7. Set private routing table for NAT (click on the private route table -> scroll down -> edit routes)



8. Add subnet association (private subnet) in private routing table (select the route table -> actions in the right side -> edit subnet associations)

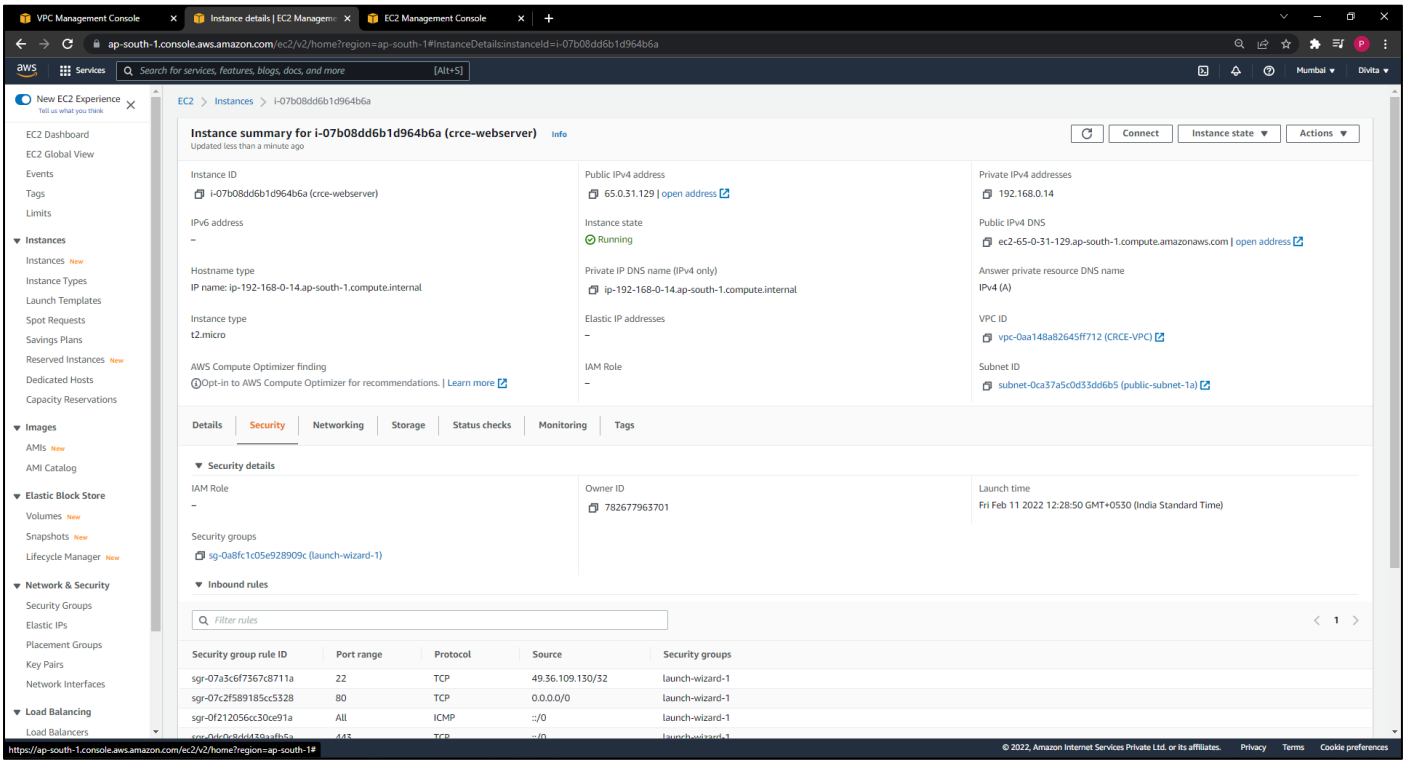


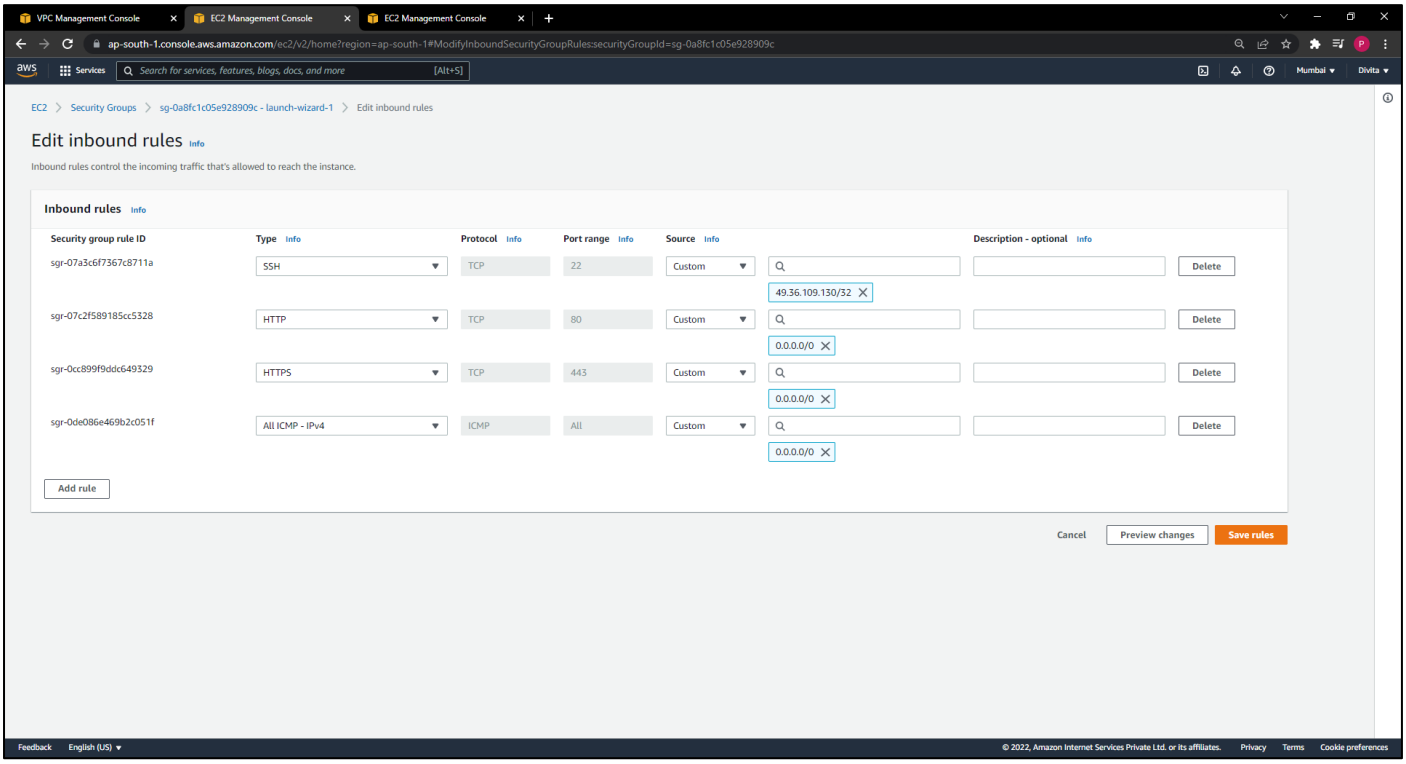
To enable DNS click on Your VPCs -> select your VPC -> Actions on right side -> edit DNS hostnames

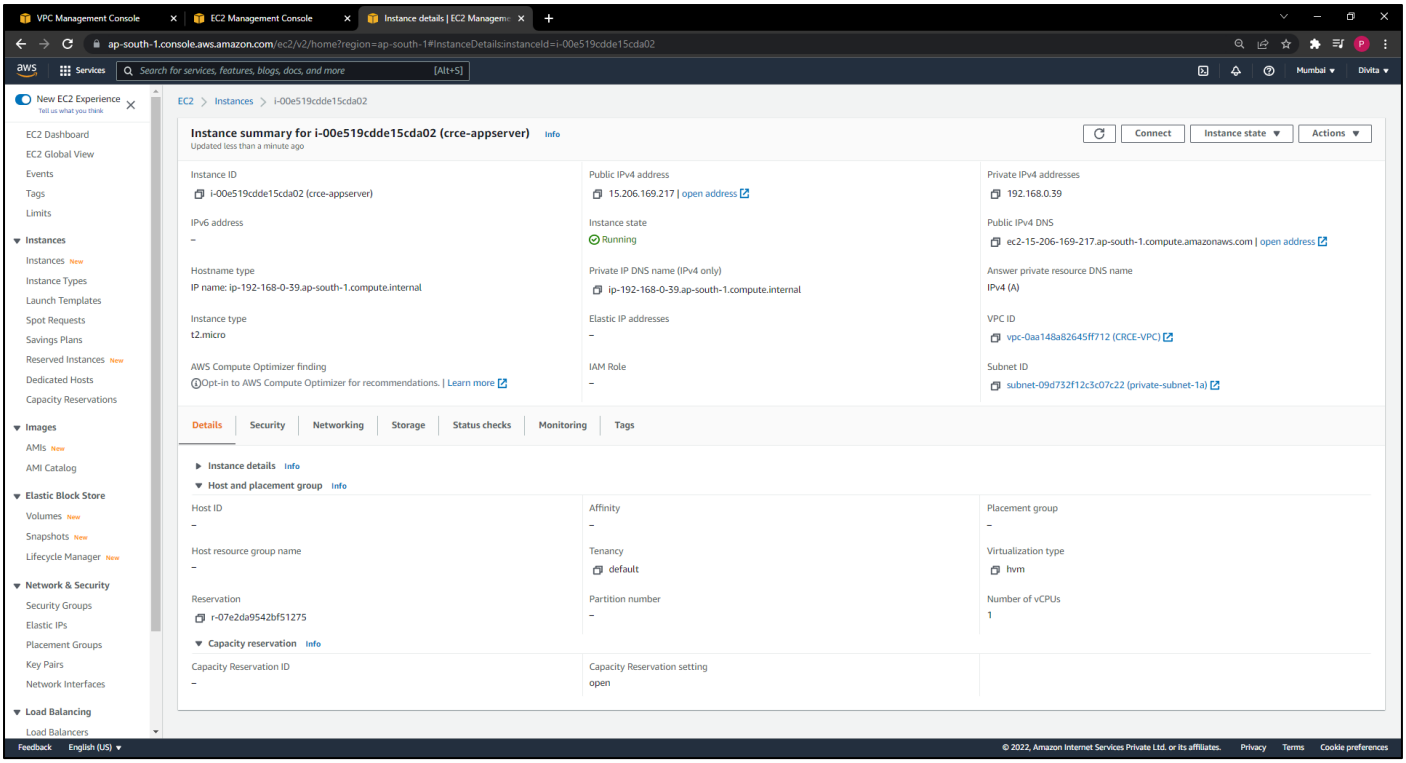


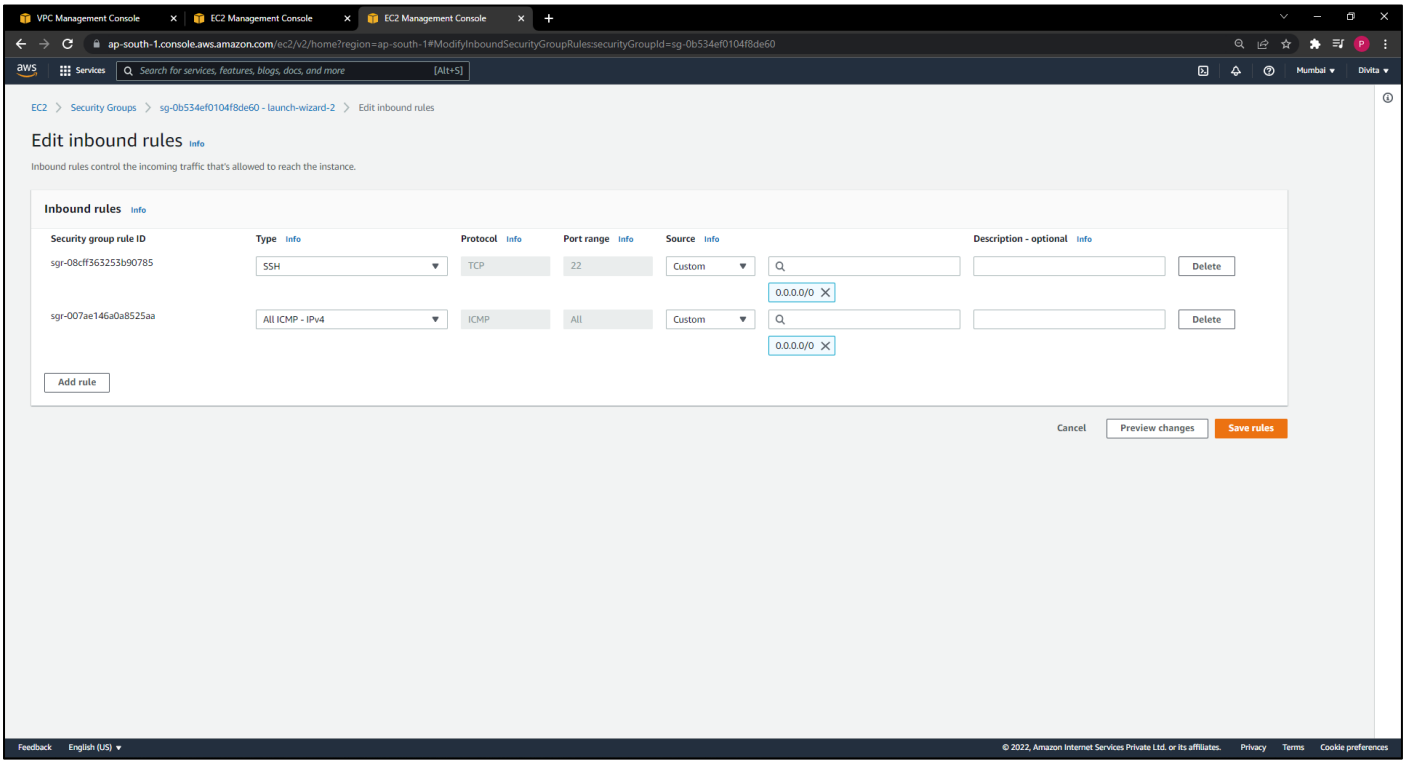
CONNECTION FOR INSTANCES:

- First, create 2 EC2 instances and configure them properly in the respective VPC and public and private subnets as set by you previously (during initial 7 steps)
- For public instance, add security group for rules: SSH, HTTP, HTTPS, ICMP
- For private instance, add SSH and ICMP



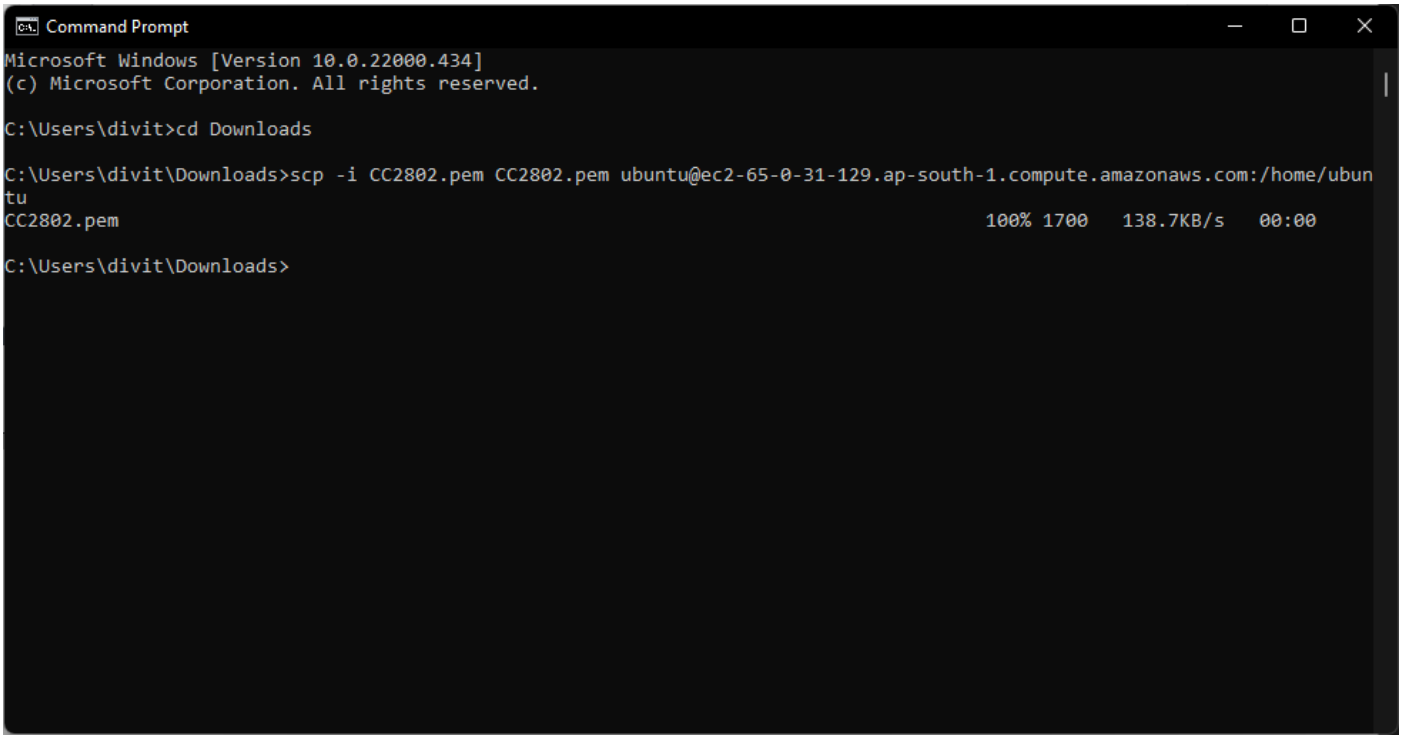




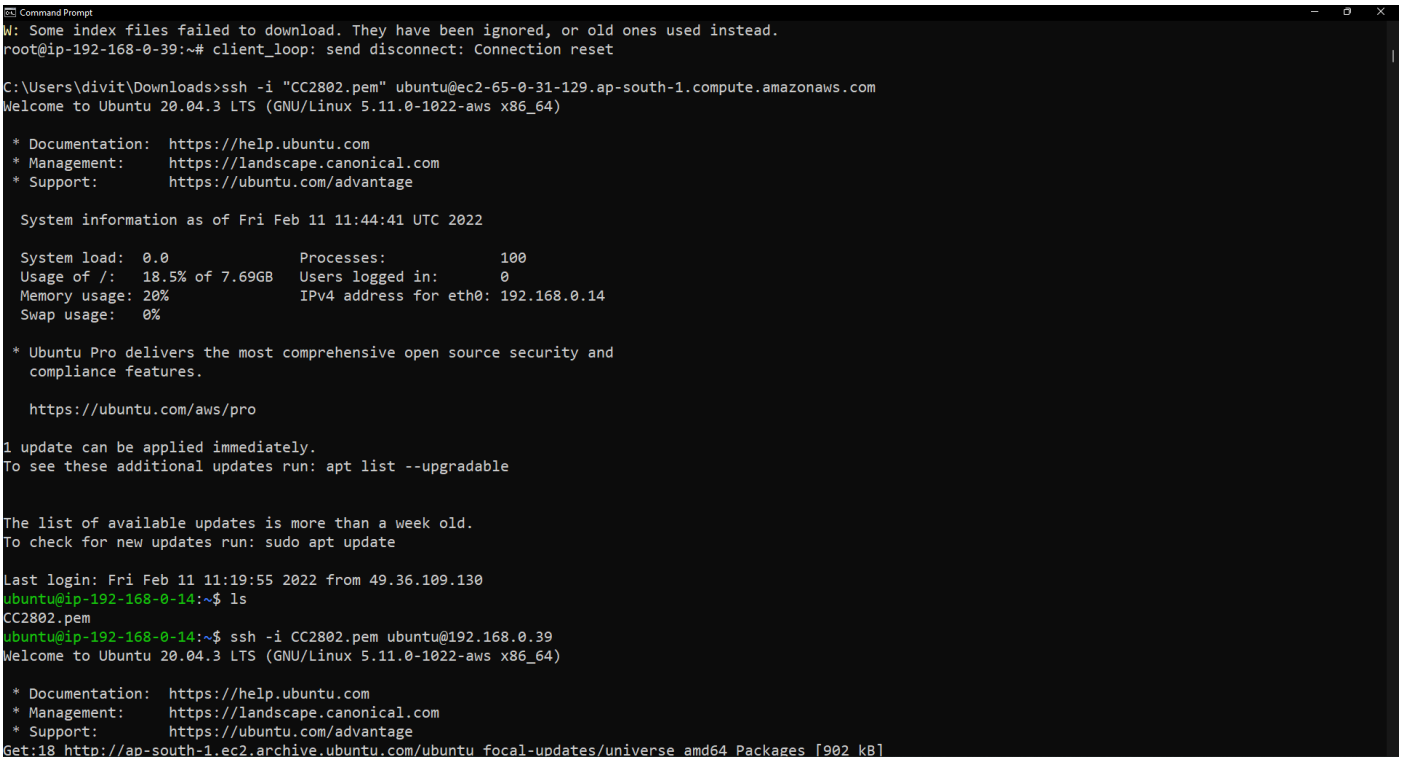


To enable internet on private instance we must do the following:

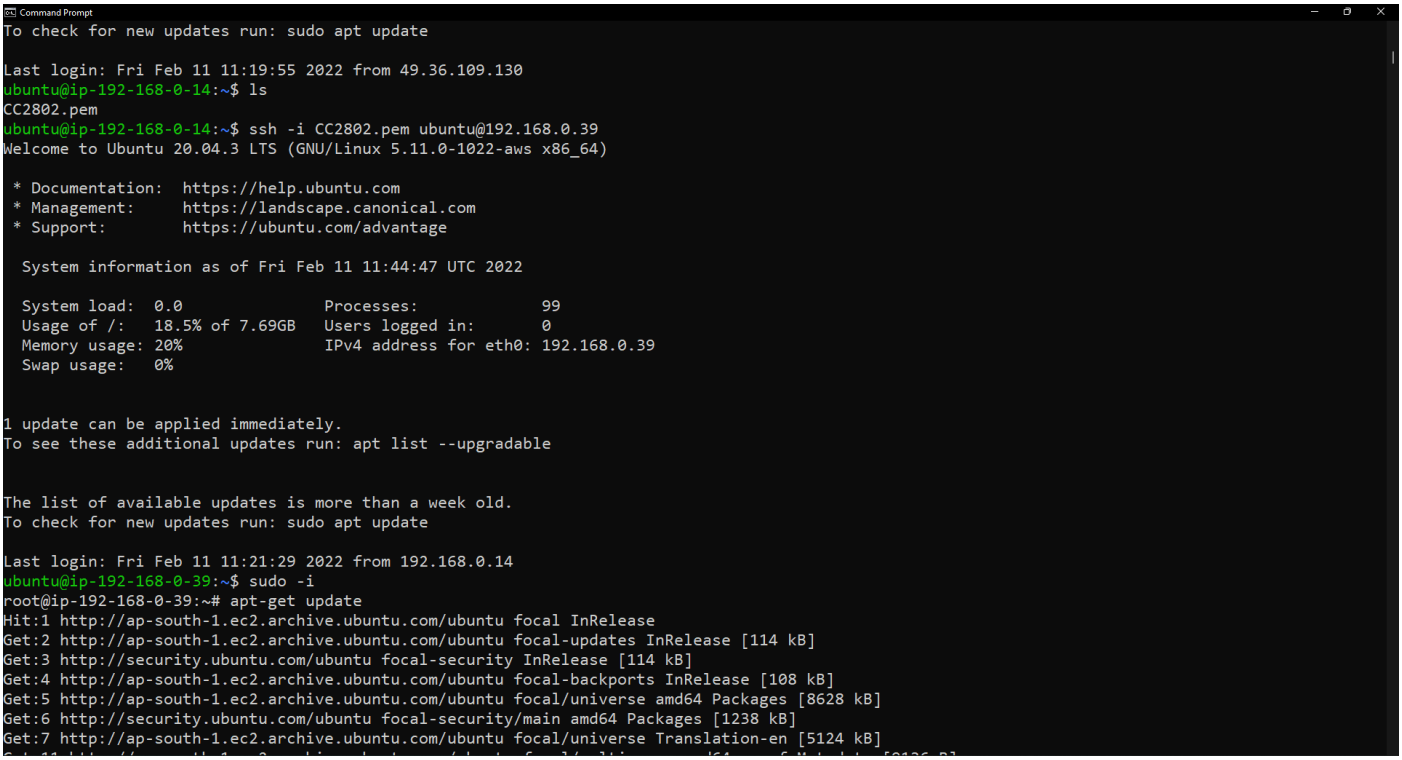
- Go to the folder where the keypair is stored for the instance
- Copy the file from your machine to the public instance
  scp -i keyname.pem keyname.pem ubuntu@public ipv4 dns:/home/ubuntu
  (e.g., scp -i CC2802.pem CC2802.pem ubuntu@ec2-65-0-31-129.ap-south-1.compute.amazonaws.com:/home/ubuntu)
  (Note: if you created instance using linux put ec2-user instead of ubuntu everywhere)



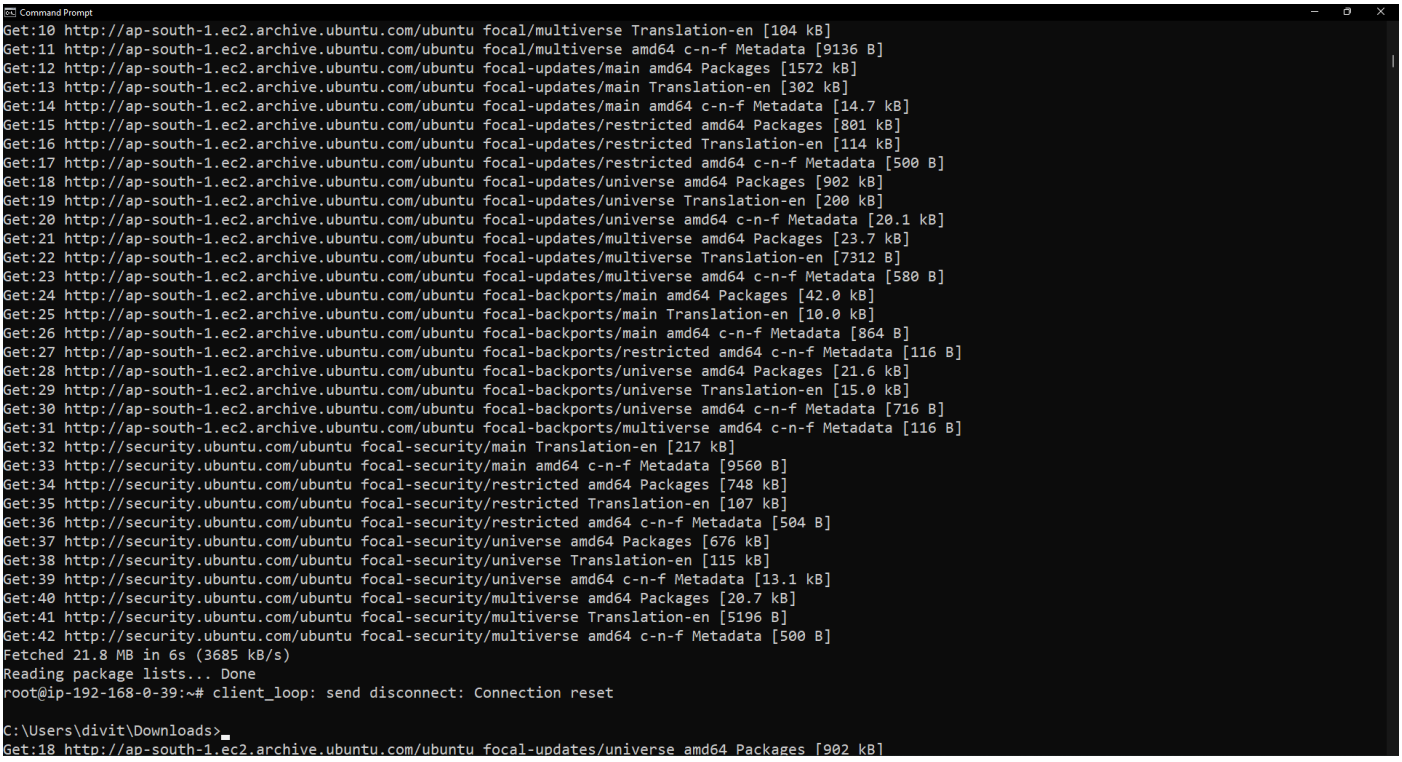
- Now connect your public EC2 instance through SSH or putty



- You can check if the .pem file is copied by ‘ls’ command
- Set the permissions for the file:
  chmod 400 keyname.pem
- To connect private instance, enter the command:
  ssh -i keyname.pem ubuntu@private ip address (private instance)
  (Note: you can see that the ip address is changed from public to private after this)
- To check if connection is correct: sudo -i -> apt-get update



- This will show that the connections are correct and now you can install any dependencies you want from the private instance



Post Lab Questions:

Q.1. What are the components of Amazon VPC?

Ans.1. Elements of Amazon VPC are as follows:

- A Virtual Private Cloud: A logically isolated virtual network in the AWS cloud. You define a VPC's IP address space from ranges you select. VPC IP address ranges are defined using Classless interdomain routing (CIDR) IPv4 and IPv6 blocks. AWS recommends that you specify CIDR blocks from the private address ranges specified in RFC 1918.

RFC 1918 Private IP Range
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Recommended private IPv4 address ranges for AWS VPC CIDR blocks

- Subnet: It is a segment of a VPC's IP address range where you can place groups of isolated resources such as Amazon EC2 services. Each subnet isolates its individual traffic from all other VPC subnet traffic. A subnet can only contain one CIDR block. You can designate different subnets to handle different types of traffic.

  For example, file server instances can be launched into one subnet, web and mobile applications can be launched into a different subnet, printing services into another, and so on.

  - Public Subnet: Where resources are exposed to the internet through Internet Gateway
  - Private Subnet: Where resources are not exposed to the outside world

- Route tables: Route tables contains the rules (routes) that determine how network traffic is directed inside your VPC and subnets. They specify the destination i.e., IP address and target. The target can be Internet gateway, NAT gateway, Virtual private gateway, etc. VPC creates a default route table called the main route table. The main route table is automatically associated with all VPC subnets. Here, you have two options:
  - Update and use the main route table to direct network traffic.
  - Create your own route table to be used for individual subnet traffic.

- Internet Gateway: The Amazon VPC side of a connection to the public Internet.

- NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet. It is used when higher bandwidth, availability with lesser management effort is required. It updates the routing table of the private subnet such that it sends the traffic to the NAT gateway. It supports only UDP, TCP, and ICMP protocols. Each VPC configuration can host one Internet Gateway and provide NAT services using the Internet Gateway, NAT instances, or a NAT gateway.

- Elastic IP addresses (EIPs): EIPs are static public IPv4 addresses that are permanently allocated to your AWS account (EIP is not offered for IPv6). EIPs are used for public Internet access to:
  - An instance

- An AWS elastic network interface (ENI)
- Other services needing a public IP address

You allocate EIPs for long-term permanent network usage.

- Network/subnet security: VPCs use security groups to provide stateful protection for instances. AWS describes security groups as virtual firewalls. VPCs also provide network access control lists (NACLs) to stateless VPC subnets.

- Virtual private gateway: The Amazon VPC side of a VPN (Virtual Private Network) connection for secure transactions. Users can attach it to the VPC from which they want to create the VPN connection.

- Peering Connection: A peering connection establishes a direct connectivity between VPCs and enables you to route traffic via IPv4 or IPv6 private IP addresses between two peered VPCs. Users can create a VPC peering connection between their own VPC and a VPC in another AWS account. This connection helps them to smoothly transfer the data.
- VPC Endpoints: Enables private connectivity to services hosted in AWS, from within your VPC without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies. They allow the VPC to make a connection with other services of AWS without using the internet.

  They are of two types of VPC Endpoints: Interference endpoints, and Gateway endpoints. They are scaled, redundant, and highly available VPC components.

- Egress-only Internet Gateway: A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet and prevent the Internet from initiating any IPv6 connection with your instances. It can be scaled horizontally, is redundant, and highly available. It is used for IPv6 internet traffic only.

Q.2. How do I get started with Amazon VPC?

Ans.2. Your AWS resources are automatically provisioned in a ready-to-use default VPC. To get started using Amazon VPC, you can launch an EC2 instance into your default VPC and default public subnets. Your default VPC is suitable for getting started quickly with Amazon VPC.

You can choose to create additional VPCs by going to the Amazon VPC page in the AWS Management Console and selecting "Start VPC Wizard".
You'll be presented with four basic options for network architectures. After selecting an option, you can modify the size and IP address range of the VPC and its subnets. If you select an option with Hardware VPN Access, you will need to specify the IP address of the VPN hardware on your network. You can modify the VPC to add or remove secondary IP ranges and gateways, or add more subnets to IP ranges.

The four options are:

1. Amazon VPC with a single public subnet only

2. Amazon VPC with public and private subnets

3. Amazon VPC with public and private subnets and AWS Site-to-Site VPN access

4. Amazon VPC with a private subnet only and AWS Site-to-Site VPN access

Q.3. What are the different types of VPC endpoints available on Amazon VPC?

Ans.3. VPC endpoints enable you to privately connect your VPC to services hosted on AWS without requiring an Internet gateway, a NAT device, VPN, AWS Direct Connect connection or firewall proxies. Therefore, you control the specific API endpoints, sites, and services that are reachable from your VPC. Endpoints are horizontally scalable, redundant and highly available virtual devices that allow communication between instances in your VPC and AWS services. You create the type of VPC endpoint that's required by the supported service.

Amazon VPC offers the following different types of endpoints:

- Gateway type endpoints: These endpoints are available only for AWS services including S3 and DynamoDB. These endpoints will add an entry to your route table you selected and route the traffic to the supported services through Amazon's private network. The route table cannot be modified to remove the route entry. It can only be deleted by removing the Endpoint association with the Route table or when the endpoint is deleted. A VPC may have multiple gateway endpoints to different services in a route table or multiple gateway endpoints to the same service in different route tables, but it may not have multiple gateway endpoints to the same service in the same route table. There is no charge for using gateway endpoints.

- Interface type endpoints: An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. It enables you to privately access services by using private IP addresses. It serves as an entry point for traffic destined to a service that is owned by AWS or owned by an AWS customer or partner. These endpoints provide private connectivity to services powered by PrivateLink, being AWS services, your own services or SaaS solutions, and supports connectivity over Direct Connect. AWS charges usage and data processing rates for PrivateLink, so there are additional costs involved with creating and using an interface endpoint.

- Gateway Load Balancer endpoints: A Gateway Load Balancer endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. It serves as an entry point to intercept traffic and route it to a network or security service that you've configured using a Gateway Load Balancer. You specify a Gateway Load Balancer endpoint as a target for a route in a route table. Gateway Load Balancer endpoints are supported only for endpoint services that are configured using a Gateway Load Balancer.

Q.4. What are the connectivity options for Amazon VPC?

Ans.4. Amazon VPC provides multiple network connectivity options for you to use, depending on your current network designs, requirements and security credentials.

These connectivity options include connecting your Amazon VPC to:

- The internet (via an internet gateway)
- Your corporate data centre using an AWS Site-to-Site VPN connection (via the virtual private gateway)
- Both the internet and your corporate data centre (utilizing both an internet gateway and a virtual private gateway)
- Other AWS services (via internet gateway, NAT, virtual private gateway, or VPC endpoints)
- Other Amazon VPCs (via VPC peering connections)

Different connectivity options for Amazon VPC are as follows:

- Network-to-Amazon VPC connectivity options

- AWS Managed VPN – Describes establishing an IPsec VPN connection from your network equipment on a remote network to AWS managed service attached to your Amazon VPC.
- AWS Transit Gateway + VPN – Describe establishing an IPsec VPN connection from your network equipment on a remote network to a regional network hub for Amazon VPCs, using AWS Transit Gateway.
- AWS Direct Connect - Describes establishing a dedicated private, logical connection from your remote network to Amazon VPC, using AWS Direct Connect.
- AWS Direct Connect + AWS Transit Gateway – Describes establishing a dedicated private, logical connect from your remote network to a regional network hub for multiple Amazon VPCs, using AWS Direct Connect and AWS Transit Gateway.
- AWS Direct Connect + VPN – Describes establishing a private, encrypted IPsec VPN connection from your remote network to Amazon VPC, using AWS Direct Connect.
- AWS Direct Connect + AWS Transit Gateway + VPN – Describes establishing a private, encrypted IPsec VPN connection from your remote network to a regional network hub for multiple Amazon VPCs, using AWS Direct Connect and AWS Transit Gateway.
- AWS VPN CloudHub – Describes establishing a hub-and-spoke model for connecting remote branch offices for primary or backup connectivity.
- Software Site-to-Site VPN – Describes establishing a VPN connection from your equipment on a remote network to a user-managed software VPN appliance running inside an Amazon VPC.

- Amazon VPC-to-Amazon VPC connectivity options
  - VPC peering – Describes connecting Amazon VPCs within and across regions using the Amazon VPC peering feature.
  - AWS Transit Gateway – Describes connecting Amazon VPCs within and across regions using AWS Transit Gateway in a hub-and-spoke model.
  - Software Site-to-Site VPN – Describes connecting Amazon VPCs using VPN connections established between user-managed software VPN appliances running inside of each Amazon VPC.
  - Software VPN-to-AWS Managed VPN – Describes connecting Amazon VPCs with a VPN connection established between a user-managed software VPN appliance in one Amazon VPC and AWS managed VPN attached to the other Amazon VPC.
  - AWS Managed VPN – Describes connecting Amazon VPCs with VPN connections between your remote network and each of your Amazon VPCs.
  - AWS PrivateLink – Describes connecting Amazon VPCs with VPC interface endpoints and VPC endpoint services. The private connectivity function negates a requirement for Internet Gateway or VPC peering connection.

- Software remote access-to-Amazon VPC connectivity options
  - AWS Client VPN – Describes connecting software remote access to Amazon VPC and/or internal networks, leveraging AWS Client VPN.
  - Software client VPN – Describes connecting software remote access to Amazon VPC, leveraging user-managed software VPN appliances.

- Transit VPC option
    - Describes establishing a global transit network on AWS using a software VPN in conjunction with an AWS-managed VPN. It's a common strategy for connecting multiple, geographically disperse VPCs and remote networks.