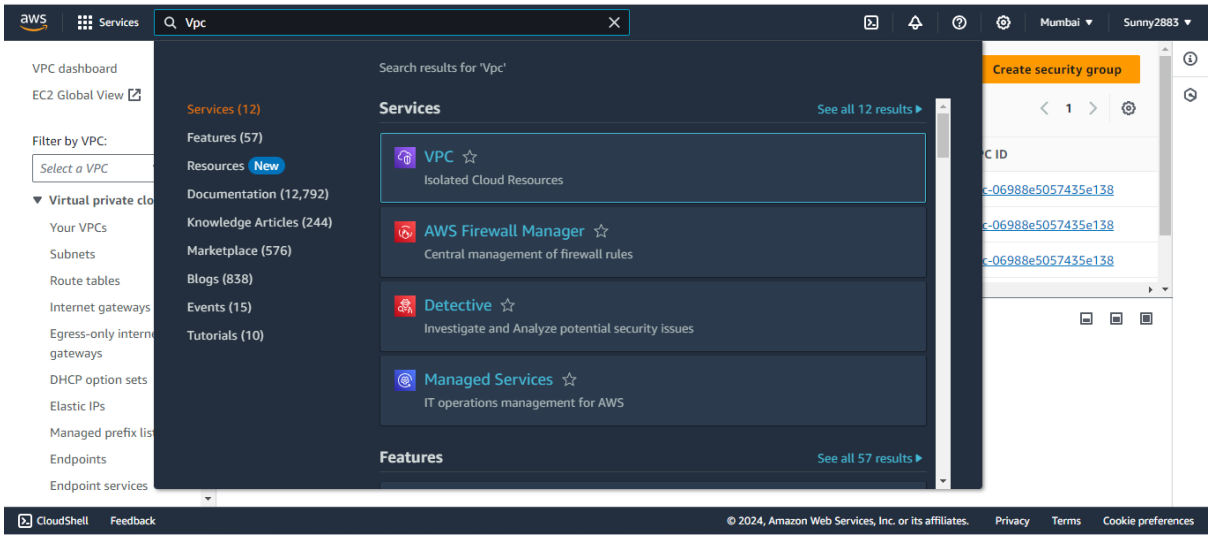
Assignment VPC

Task:1

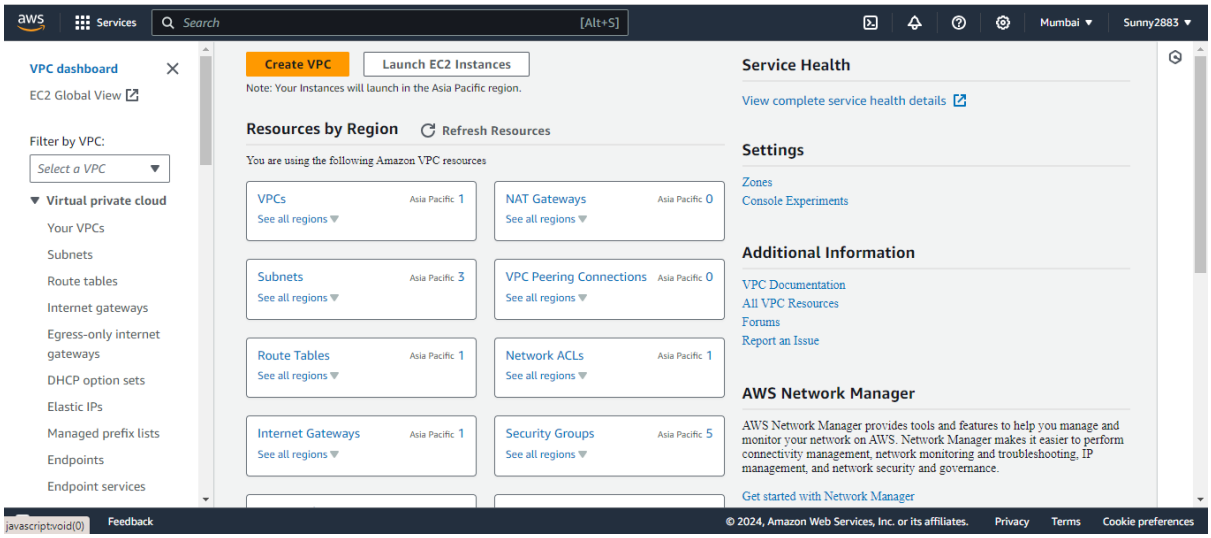
Create a VPC:

Include at least two subnets, each in a different Availability Zone.

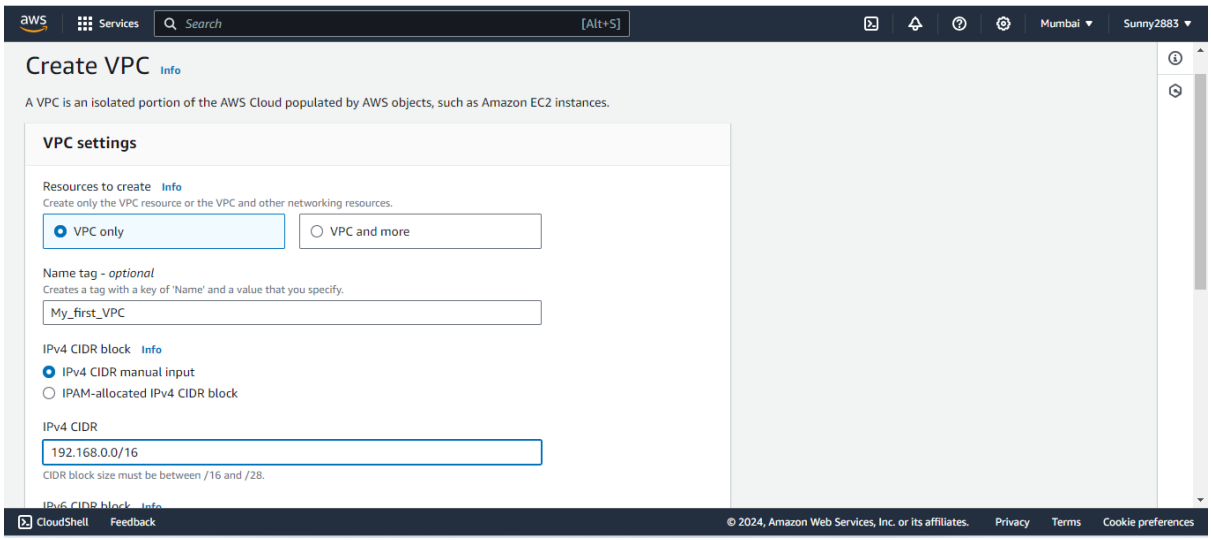
Step1: Go to the "Services" dropdown, search "VPC" .



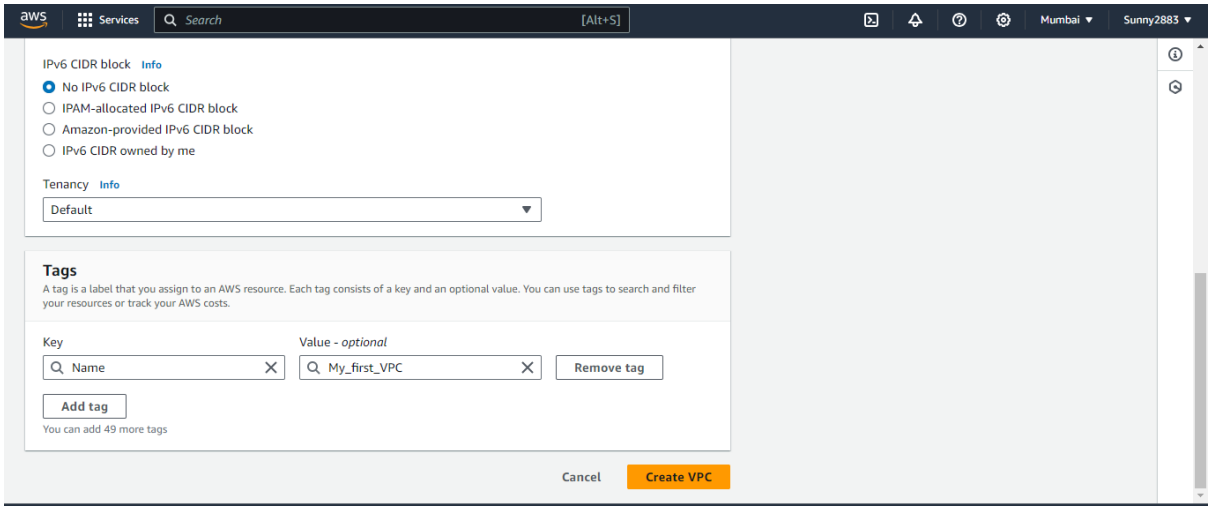
Step2: Click on "Your VPCs" in the left sidebar and Click the "Create VPC" button.



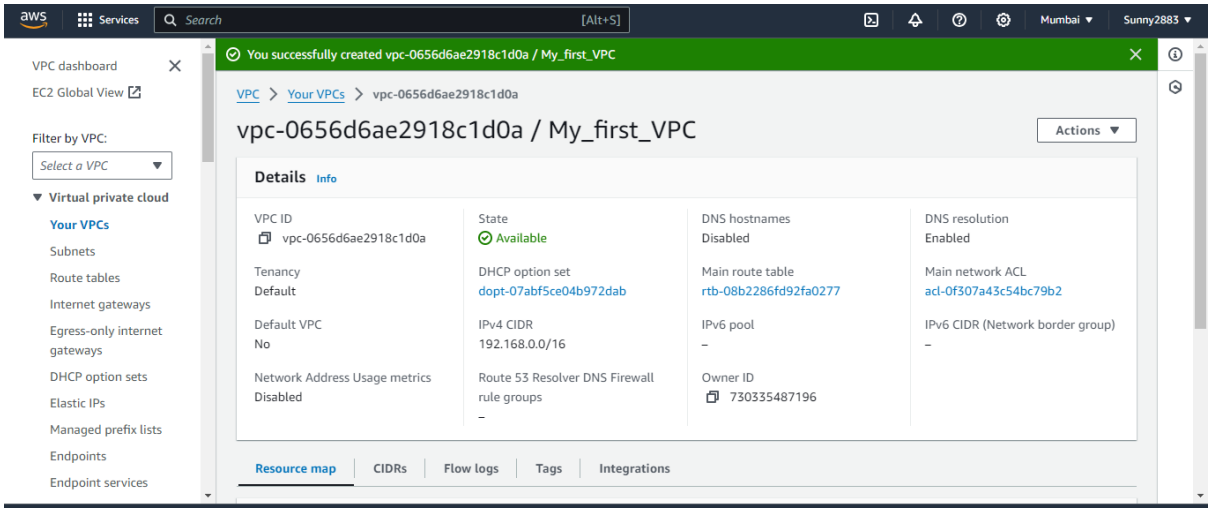
Step3: Enter a name for your VPC and set the IPv4 CIDR block. Ensure that the CIDR block does not overlap with other networks.

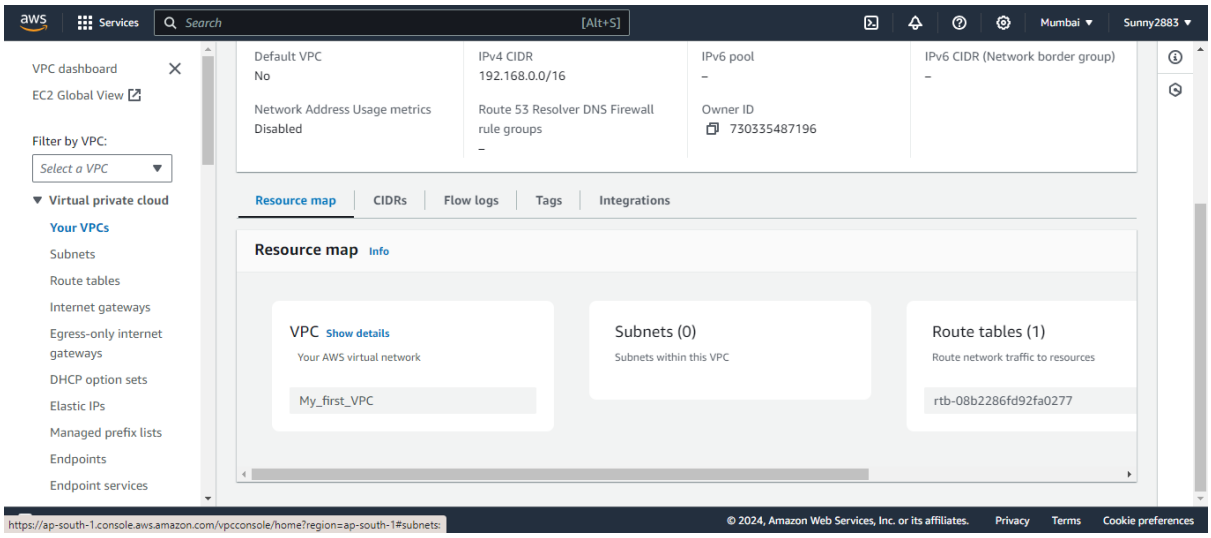


Step4: Review your configurations and click "Create" to create the VPC.

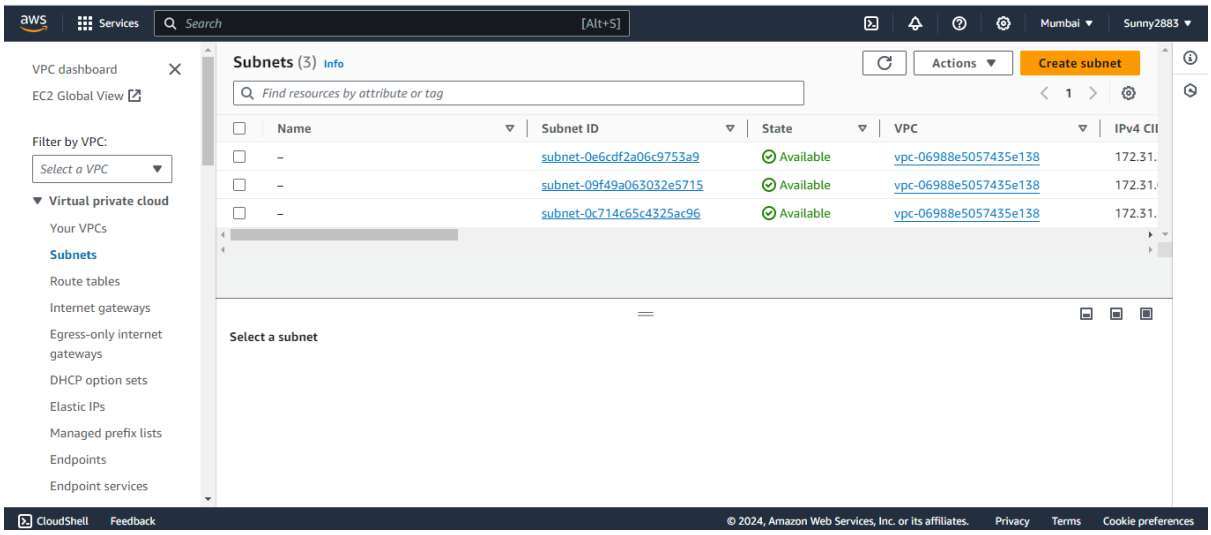


Step5: VPC successfully created.

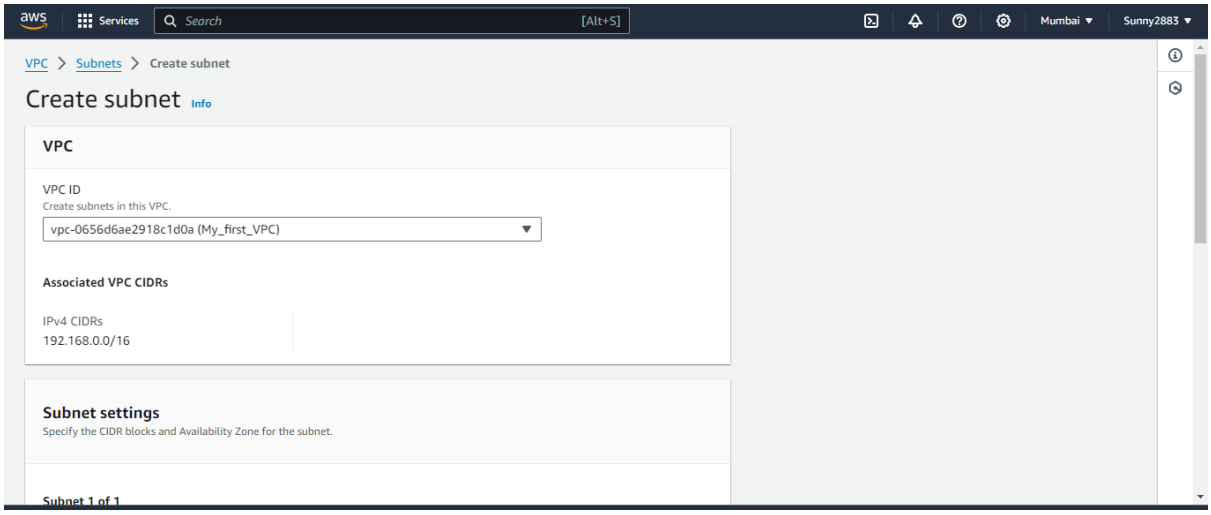




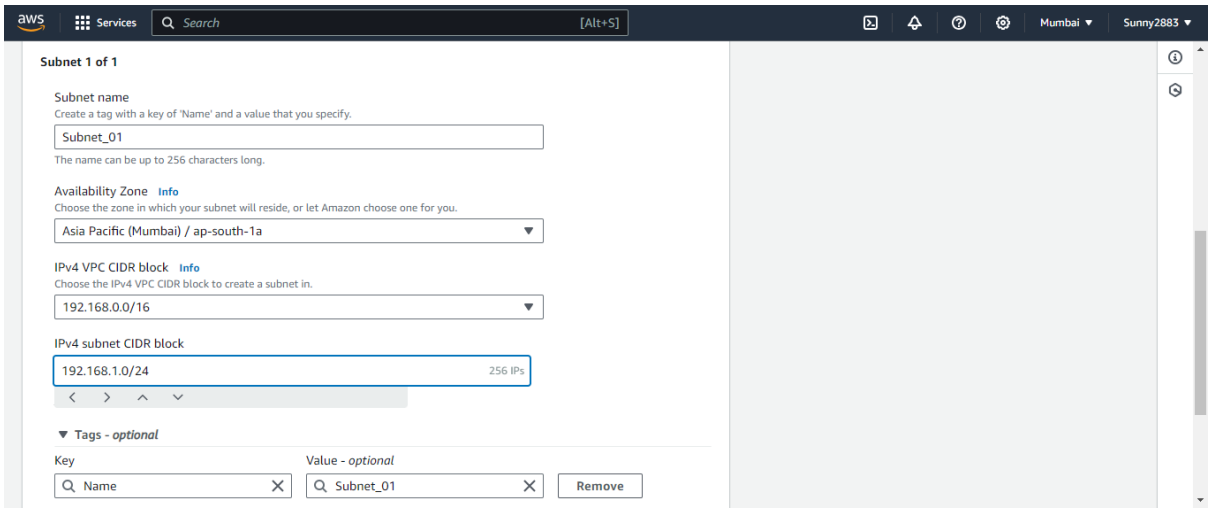
Step6: Go to "Subnets" Section, On the left sidebar, click on "Subnets." Click on the "Create subnet" button.



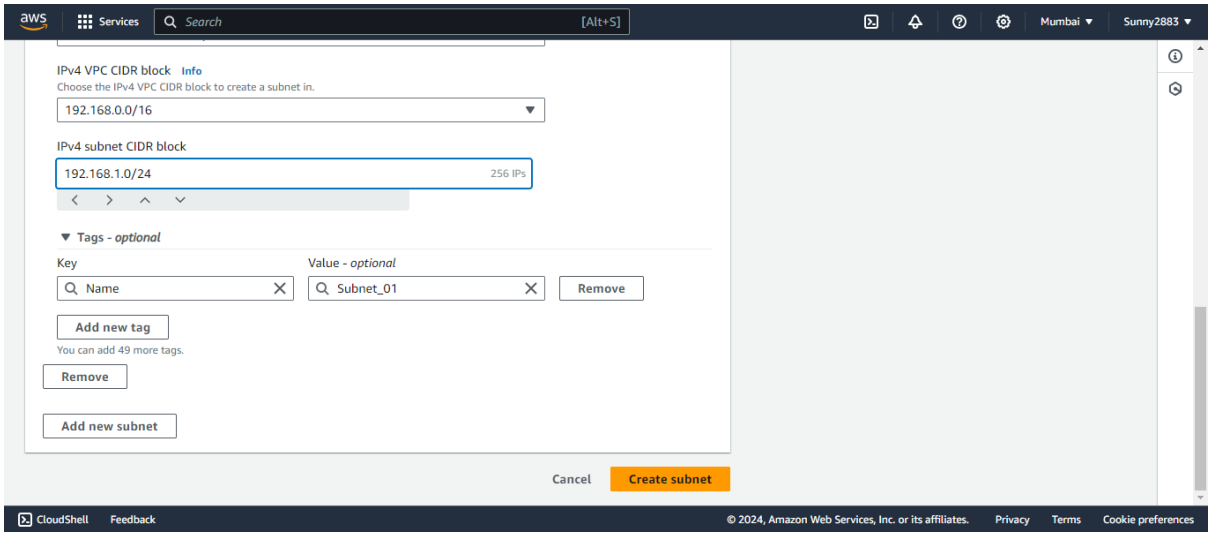
Step7: Choose the VPC in which the subnet will reside.



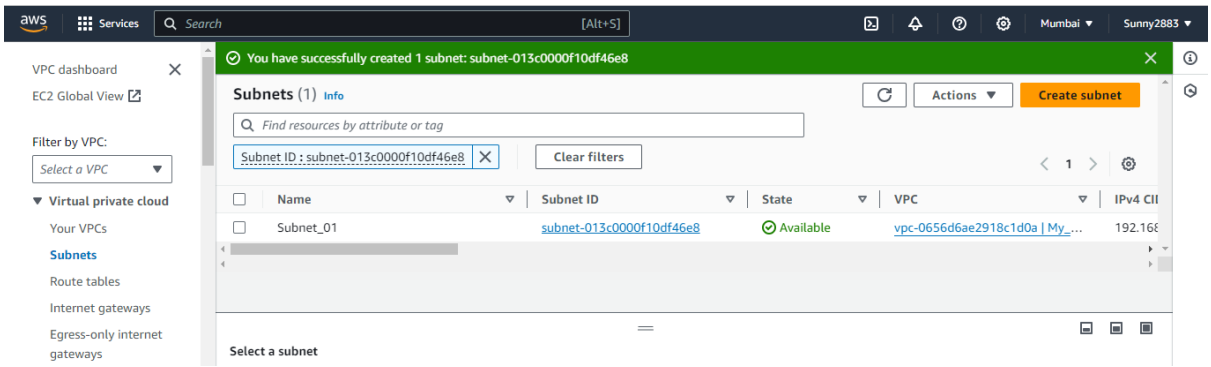
Step8: Provide a name for the subnet. Select the availability zone for the subnet. Specify an IPv4 CIDR block for the subnet. Ensure it is within the CIDR block of the VPC.



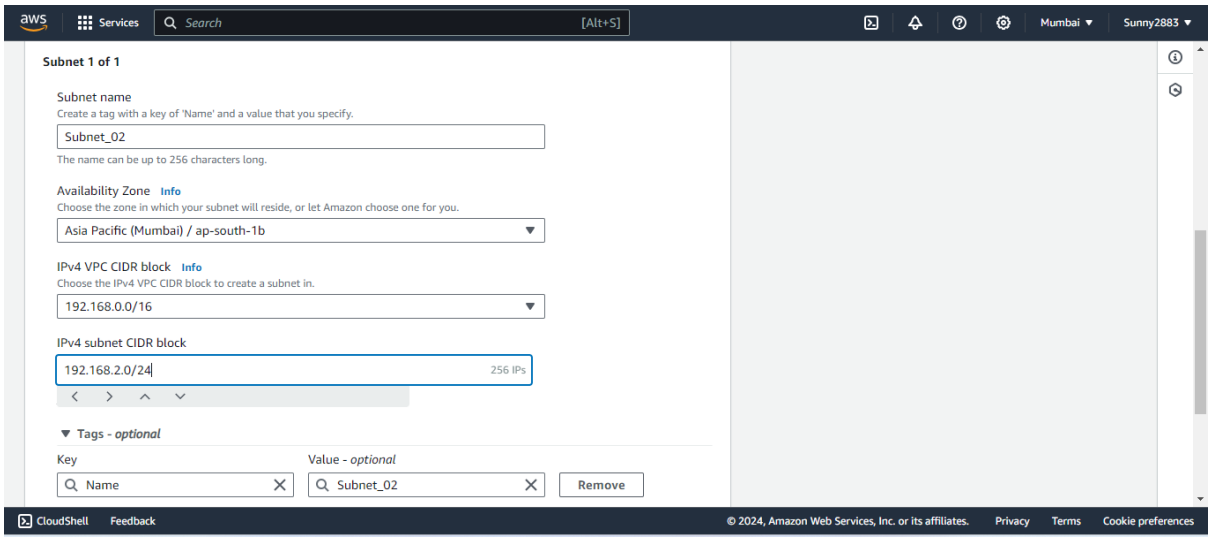
Step9: Review your subnet configuration. Click "Create subnet" to create the first subnet.

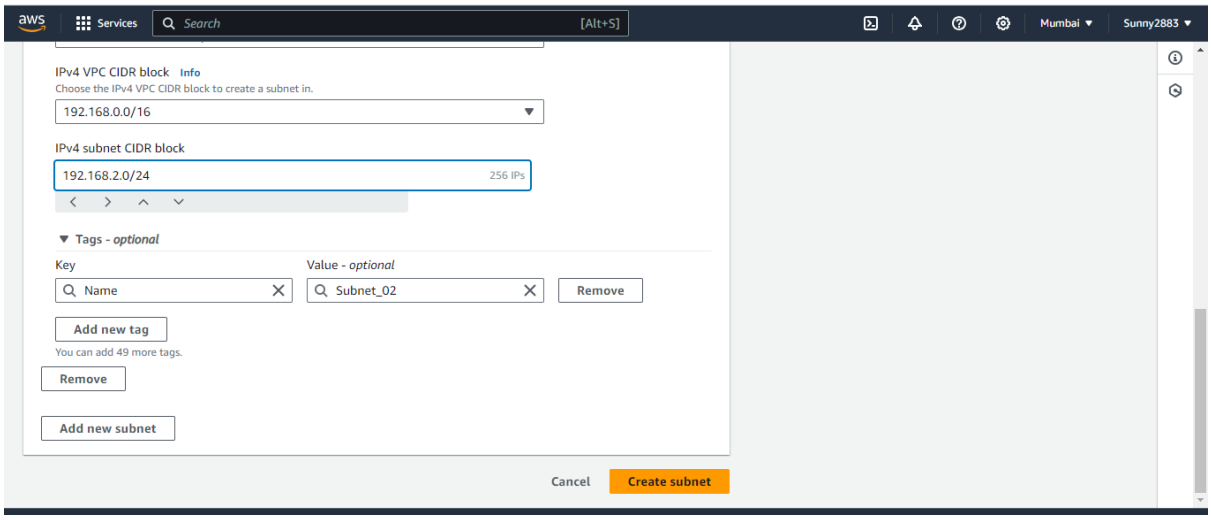


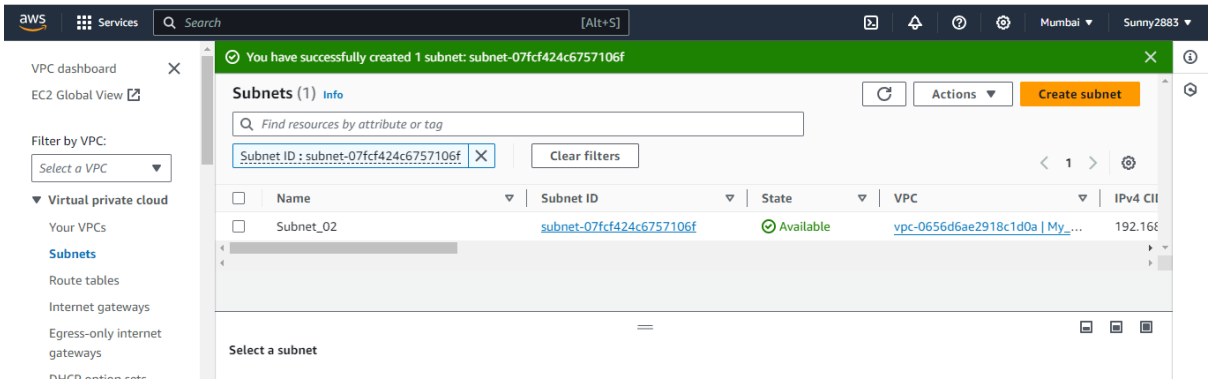
Step10: Review your subnet configuration.



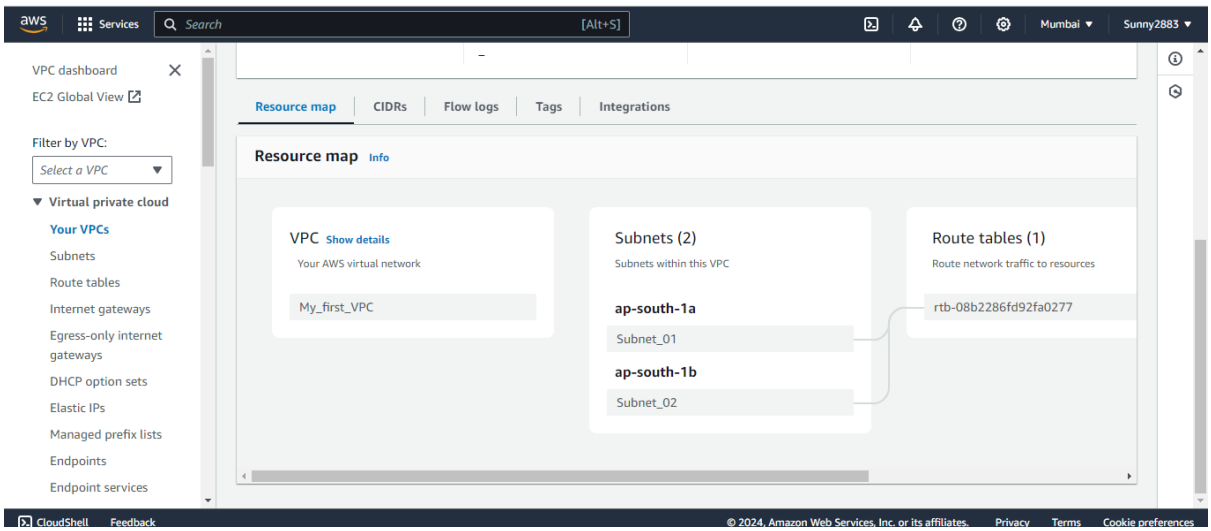
Step11: Repeat the above steps to create additional subnets in different availability zones.





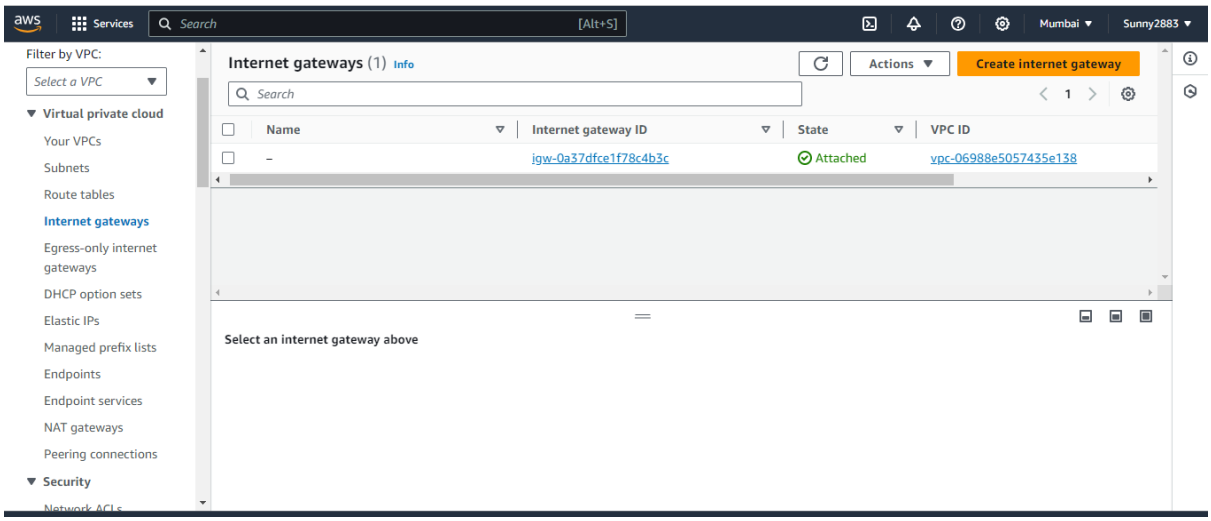


Step12: Resource map of VPC.

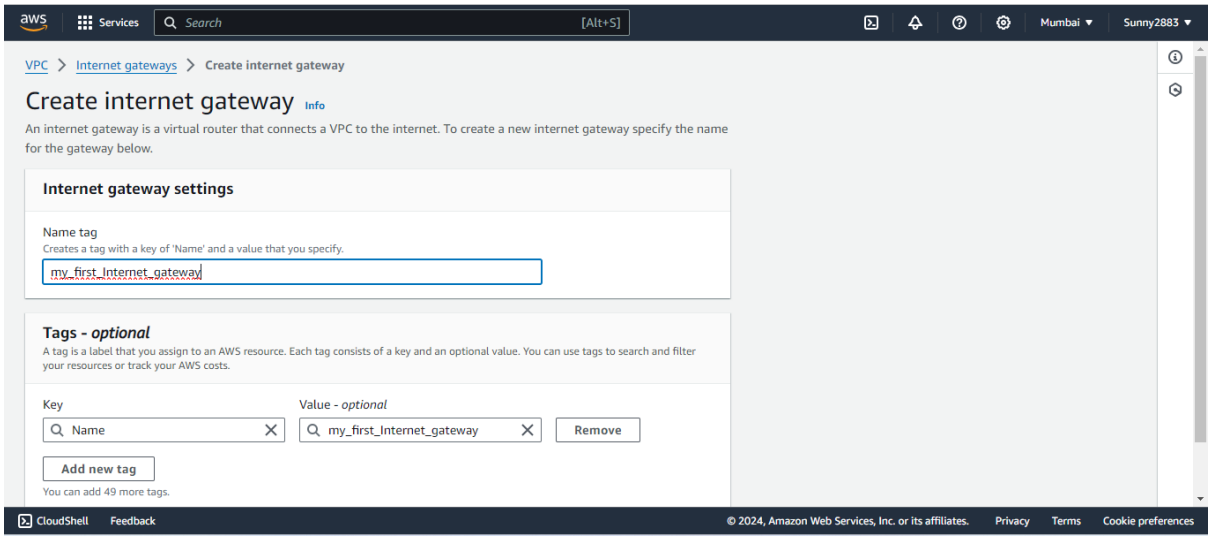


2. Internet Gateway (IGW):

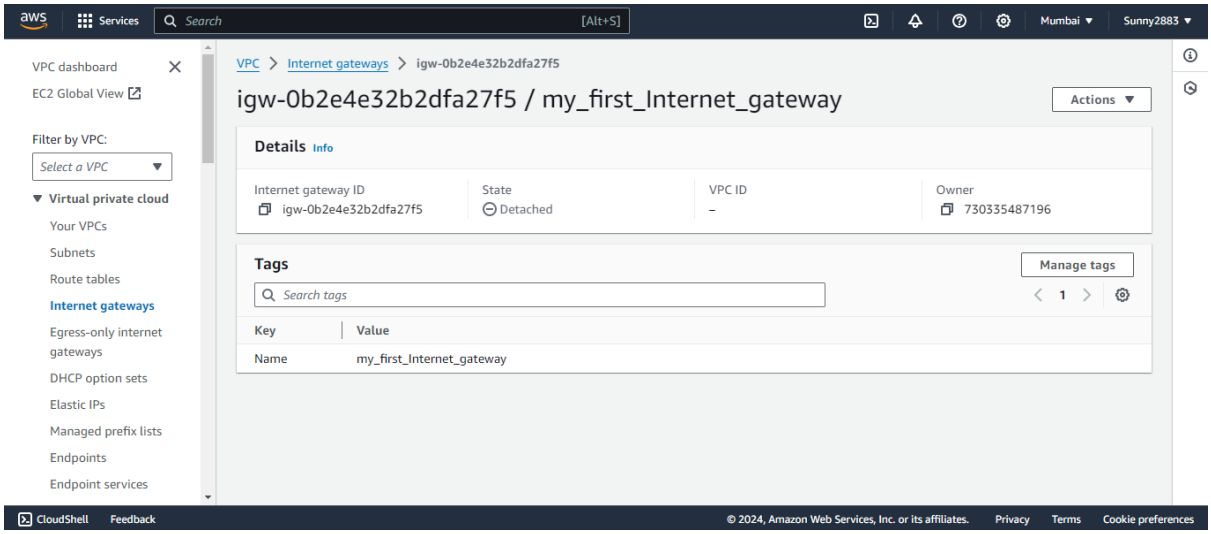
Step1: Go to "Internet Gateways" Section. On the left sidebar, click on "Internet Gateways." Click on the "Create internet gateway" button.



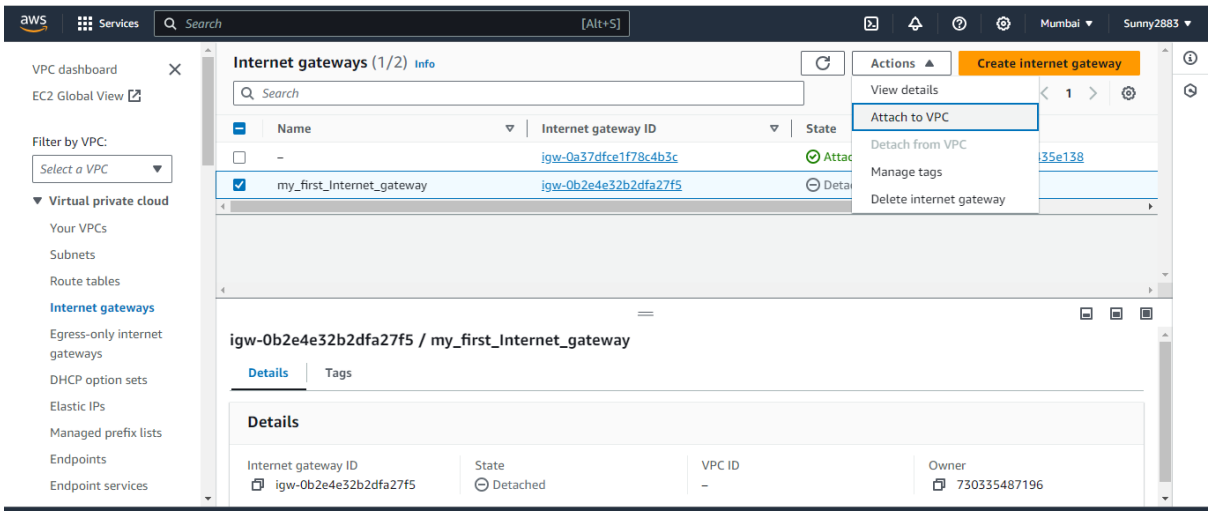
Step2: Provide a name for the internet gateway and create internet gateway.



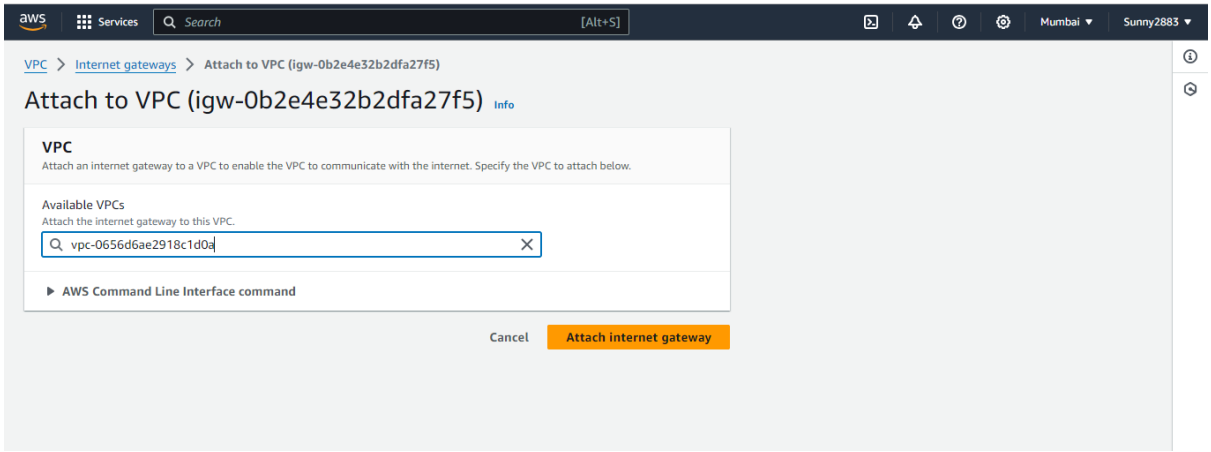
Step3: Configure the details.

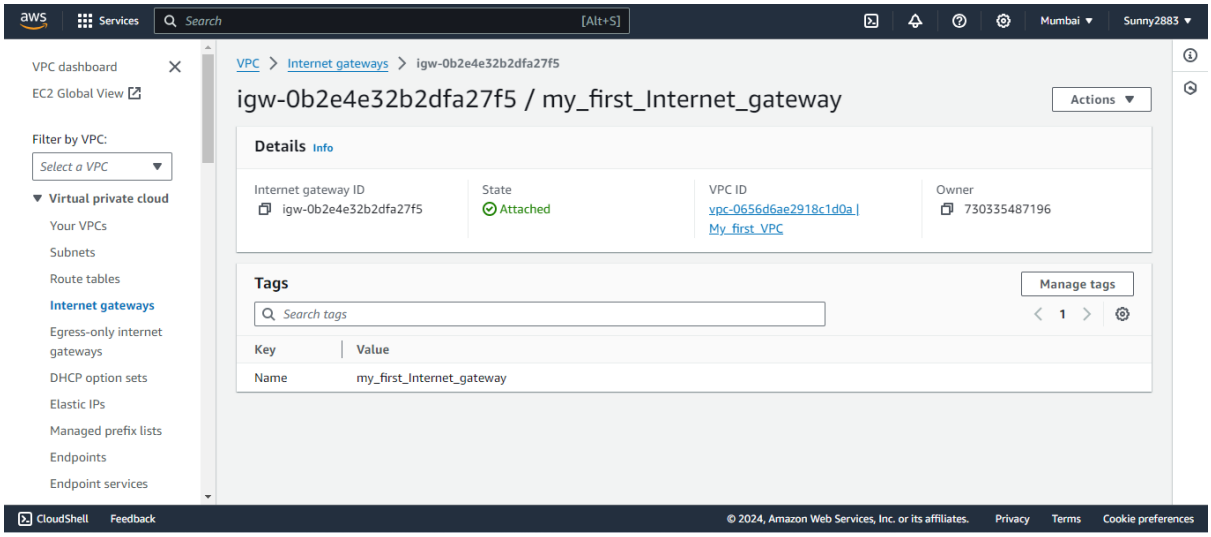


Step4: Select the newly created internet gateway.Click on the "Attach to VPC" button.



Step5: Choose the VPC to which you want to attach the internet gateway. Click attach internet gateway.





3. Do not create NAT gateway but understand how and why it is needed?

How NAT Gateway Works:

Private Subnet Communication:

In a typical VPC setup, you may have public and private subnets.

Instances in the private subnet do not have direct access to the internet.

Outbound Traffic:

When an instance in a private subnet wants to initiate outbound communication (e.g., fetching updates), it sends the traffic to the NAT gateway.

NAT Gateway as an Egress Point:

The NAT gateway acts as an egress point for traffic originating from instances in the private subnet.

Public IP Address:

The NAT gateway has an Elastic IP address associated with it, providing a static public IP for outbound traffic.

Internet Access:

The NAT gateway translates the private instance's private IP to its own public IP when sending traffic to the internet.

Inbound Traffic Filtering:

The NAT gateway only allows responses to the outbound requests initiated by instances in the private subnet. It prevents unsolicited inbound traffic from reaching those instances.

Why NAT Gateway is Needed:

Security:

NAT gateways enhance security by acting as a buffer between instances in private subnets and the internet. They prevent direct incoming connections to private instances, reducing the attack surface.

Outbound Internet Access:

Instances in private subnets can access the internet for software updates, license validations, or other external services without exposing their private IP addresses.

IPv4 Address Conservation:

NAT gateways allow multiple private instances to share a single public IP address, conserving IPv4 addresses.

Elastic IP for Consistency:

The Elastic IP associated with the NAT gateway provides a consistent public IP for outbound traffic, which is useful for scenarios where specific IP whitelisting is required.

Scalability:

NAT gateways are managed services that automatically scale to handle increased traffic. They provide high availability and reliability.