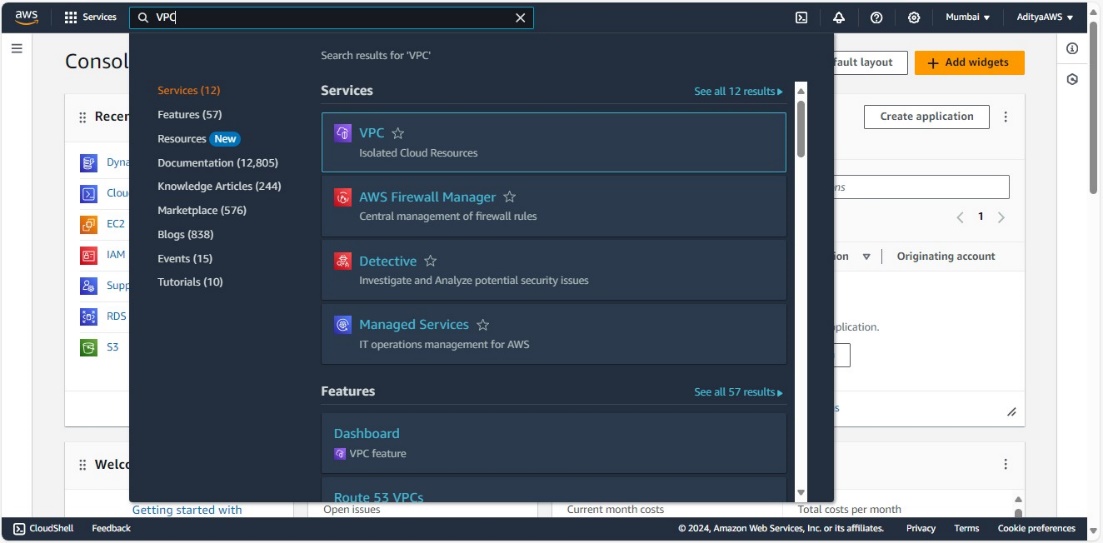
**Task-1. Create a VPC:**

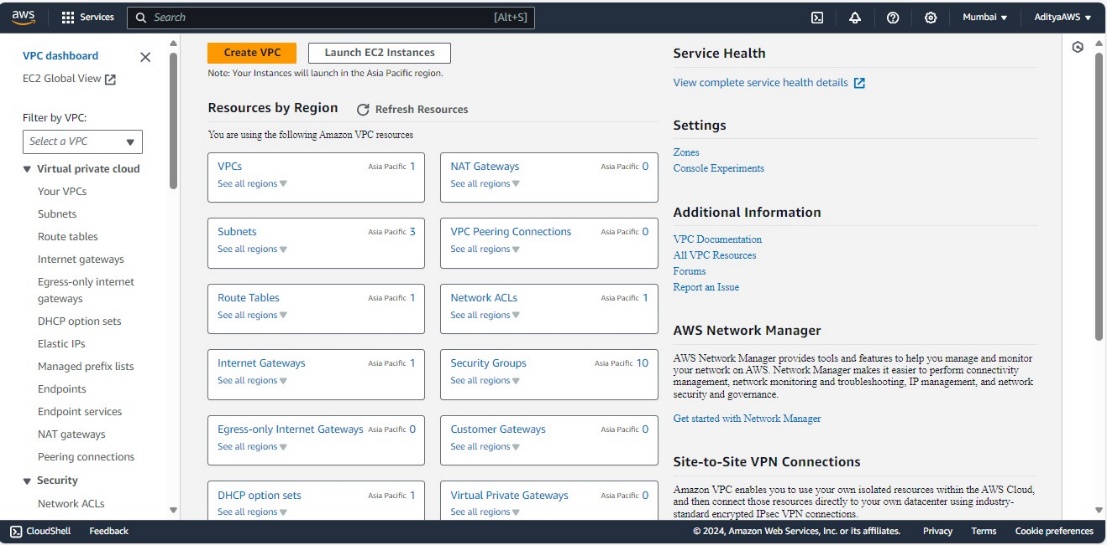
* 1. **Include at least two subnets, each in a different Availability Zone.**
  2. **Internet Gateway (IGW):**
  3. **Do not create NAT gateway but understand how and why it is needed?**

**Steps to create a VPC with two subnets in different Availability Zones and attaching an Internet Gateway (IGW):**

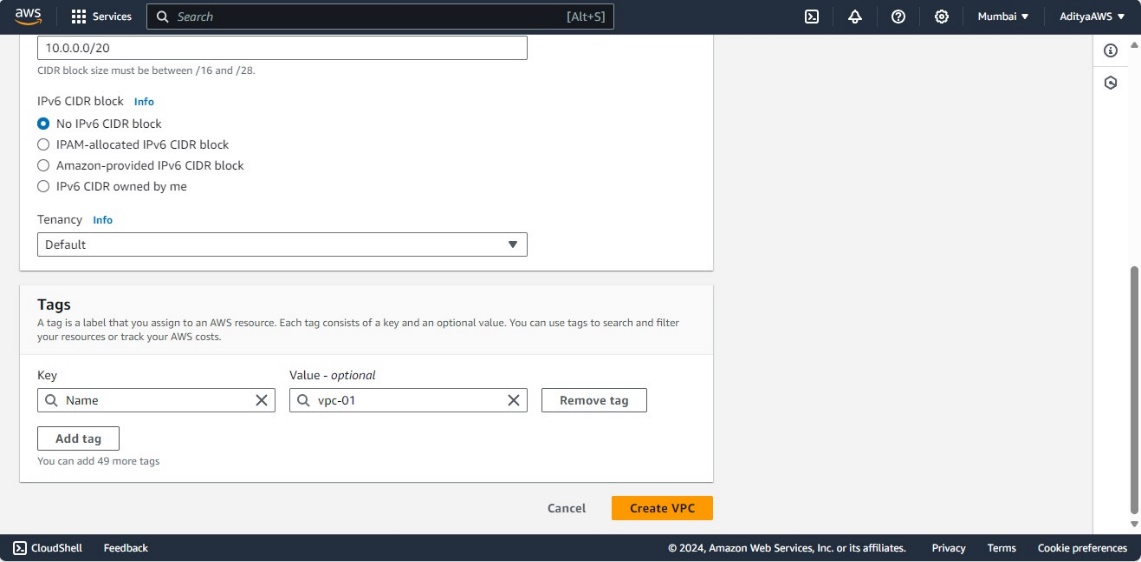
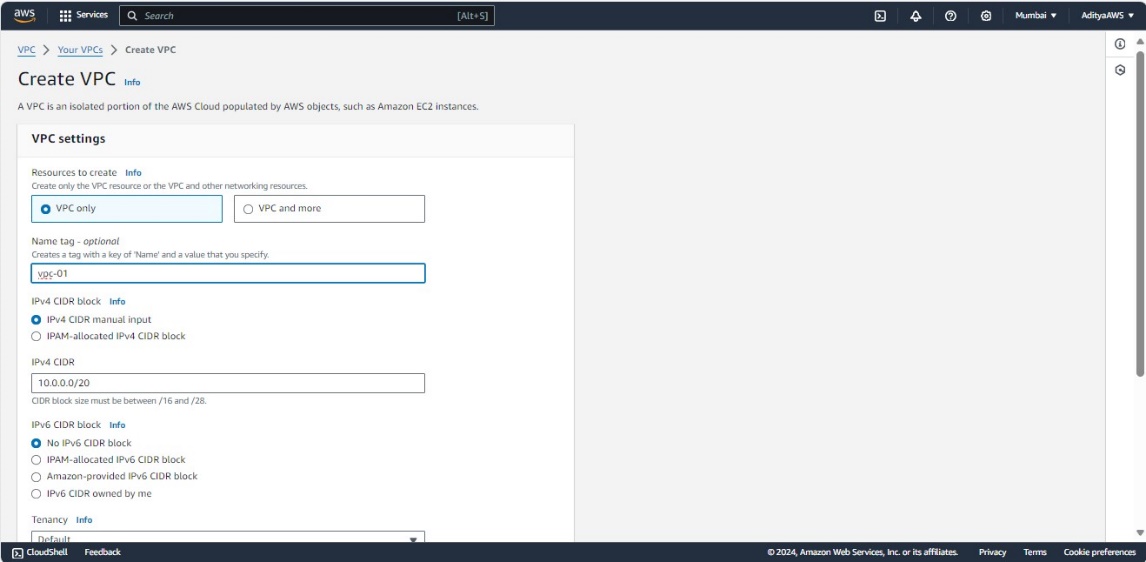
1. Search VPC in Console home and go to VPC.



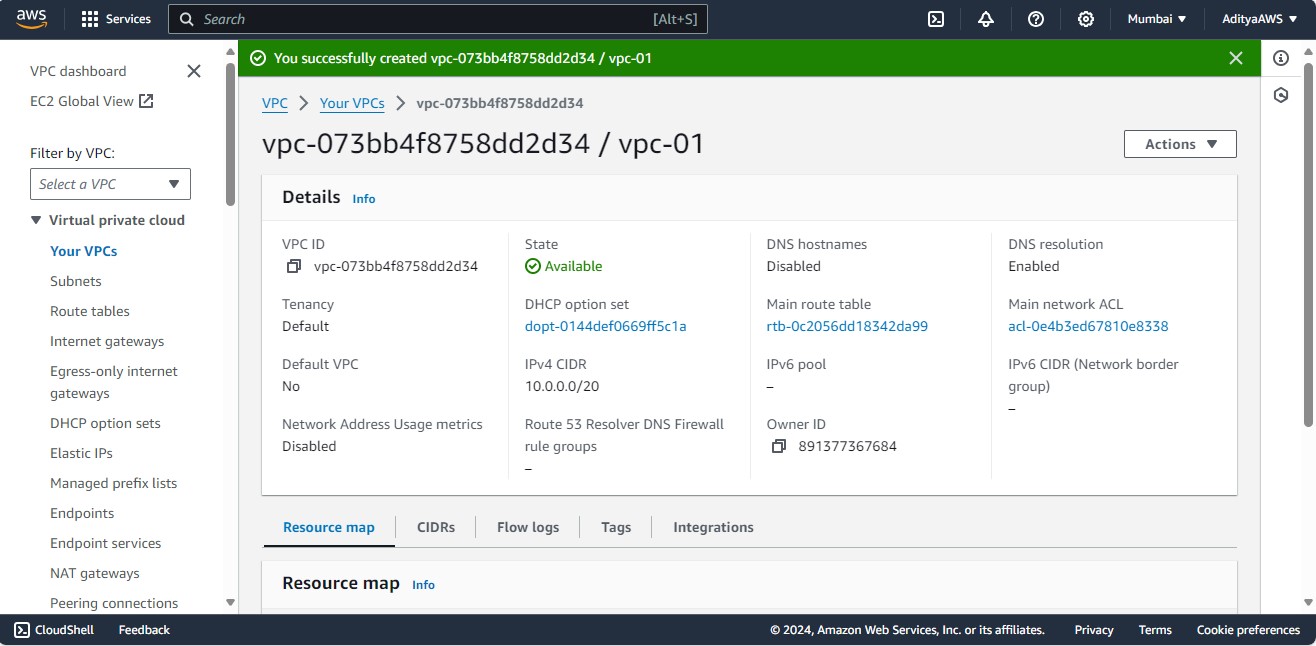
1. Click on “Create VPC” in the VPC dashboard.



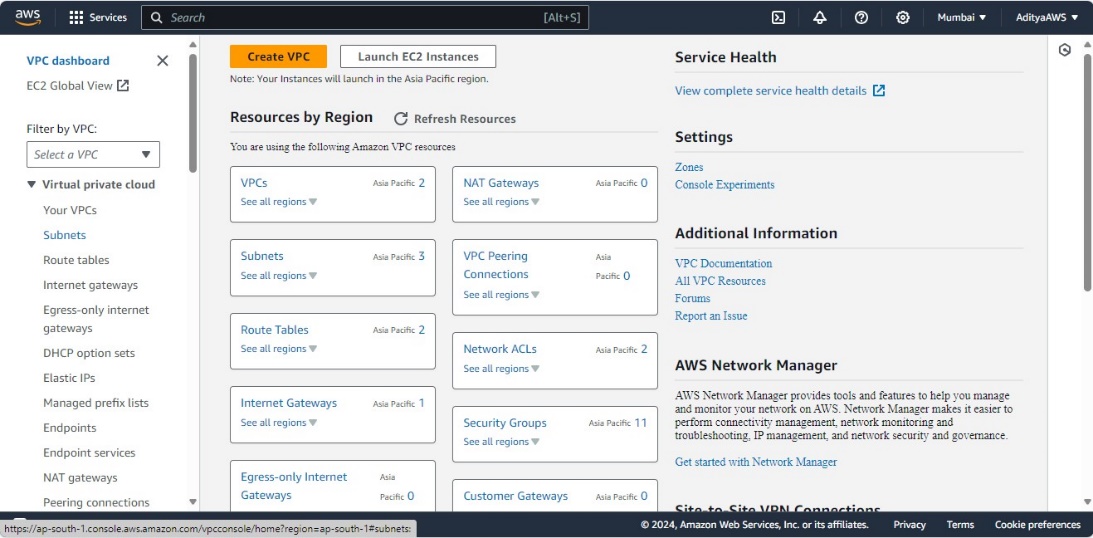
1. Select VPC only, give your VPC a name and set the IPv4 CIDR block, and click “Create VPC”.



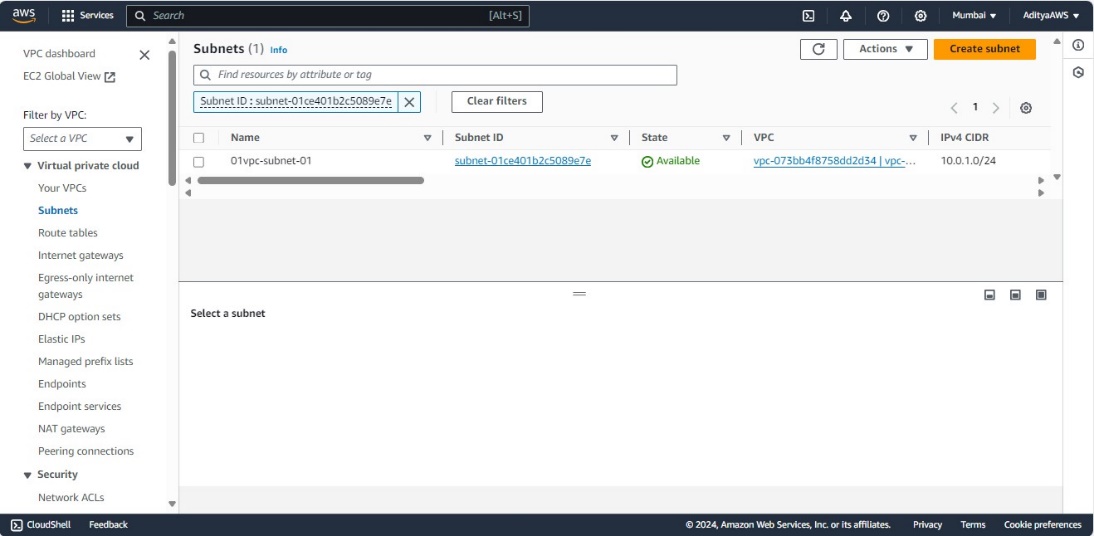
Result:



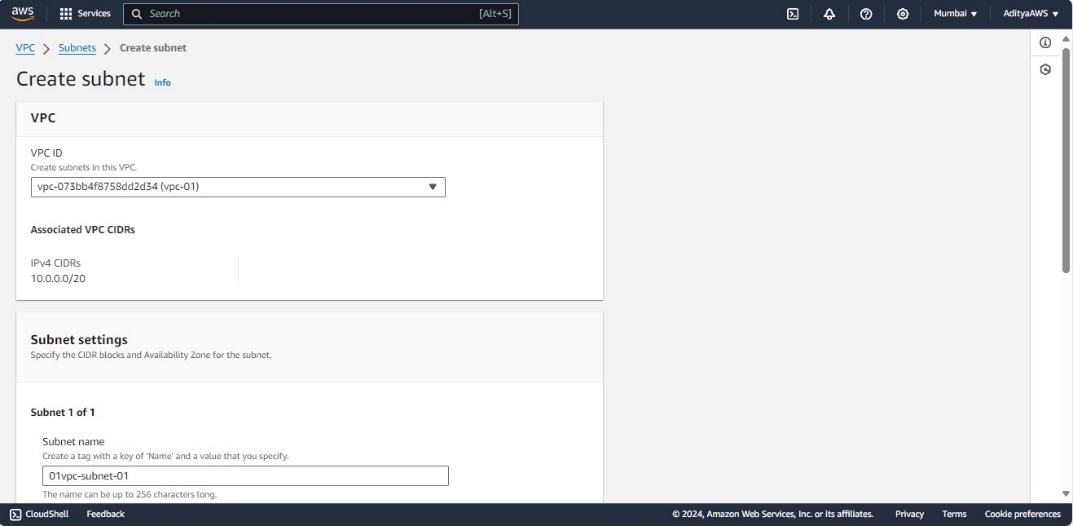
1. Now, click on “Subnets”.

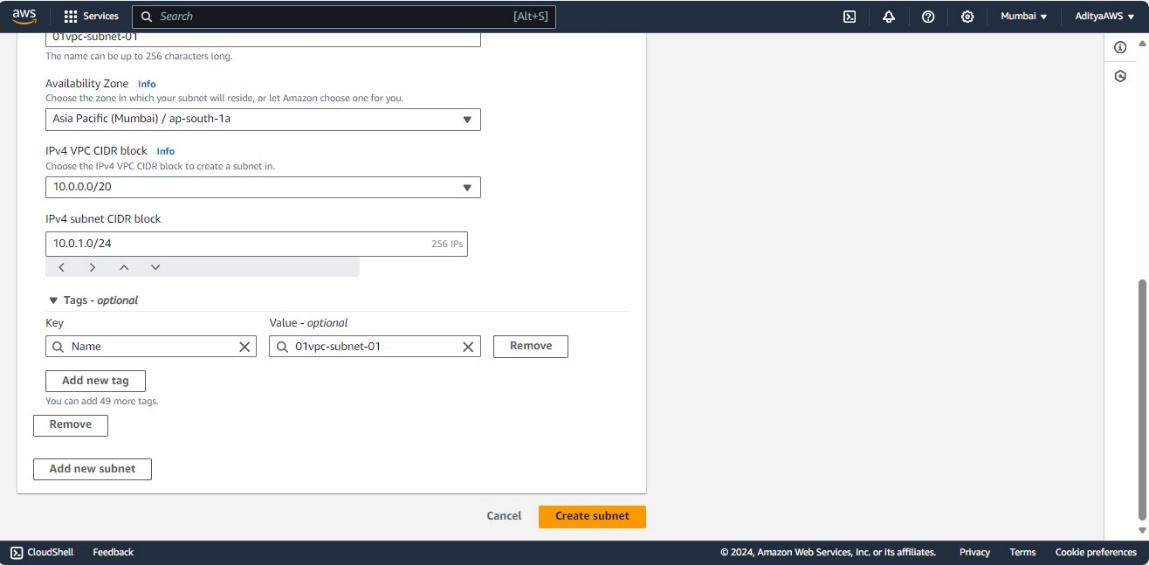


1. Click “Create subnet”.

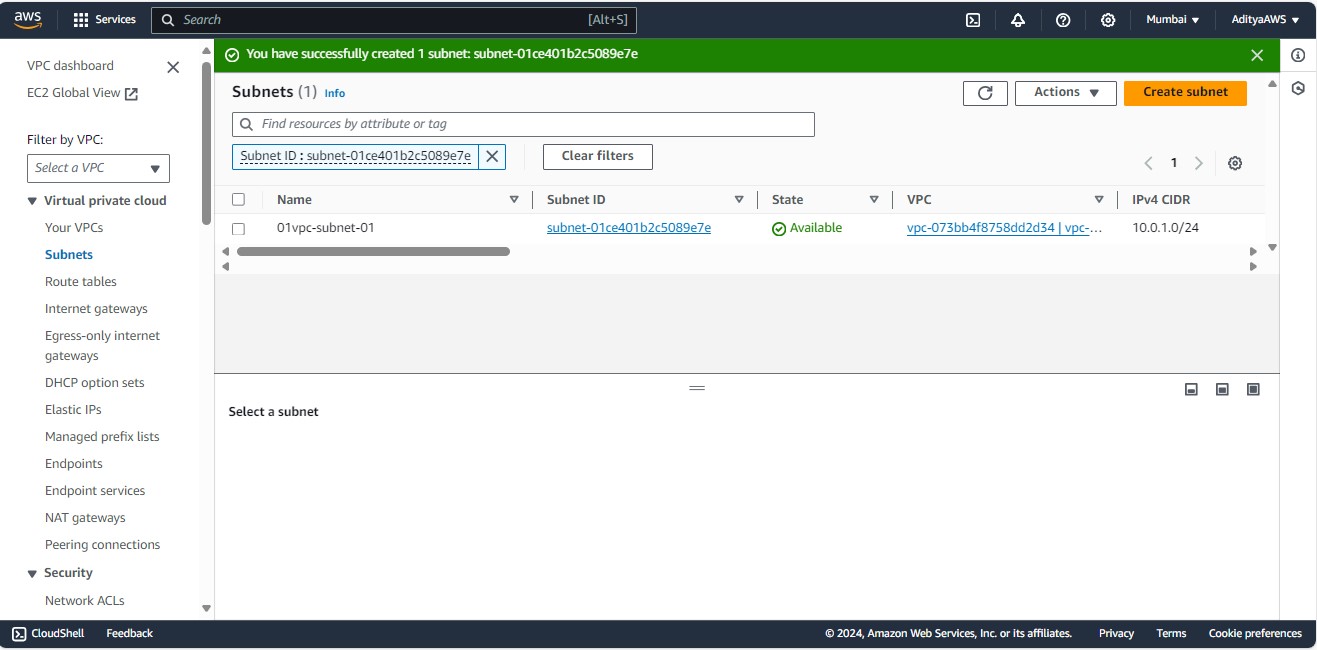


1. Then, choose the VPC that is just created, name the subnet, select an Availability Zone, and set the IPv4 CIDR block. Click “Create subnet”.

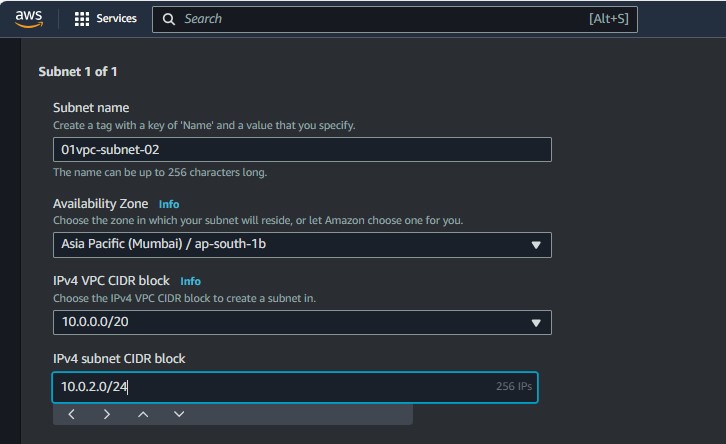




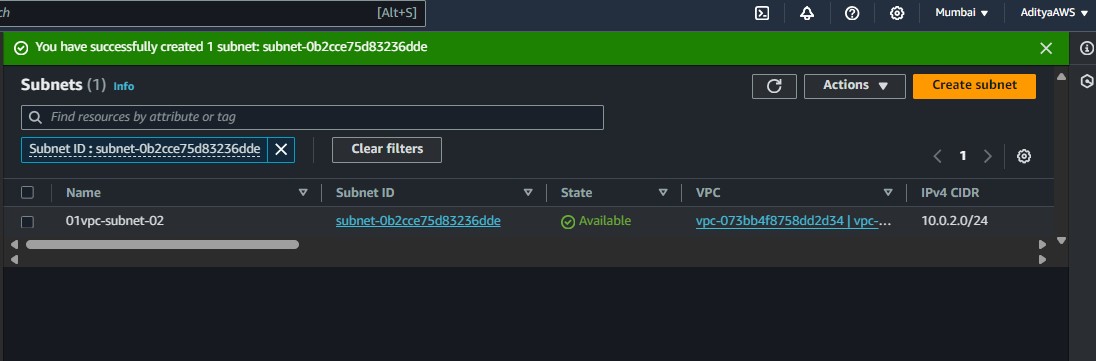
Result:



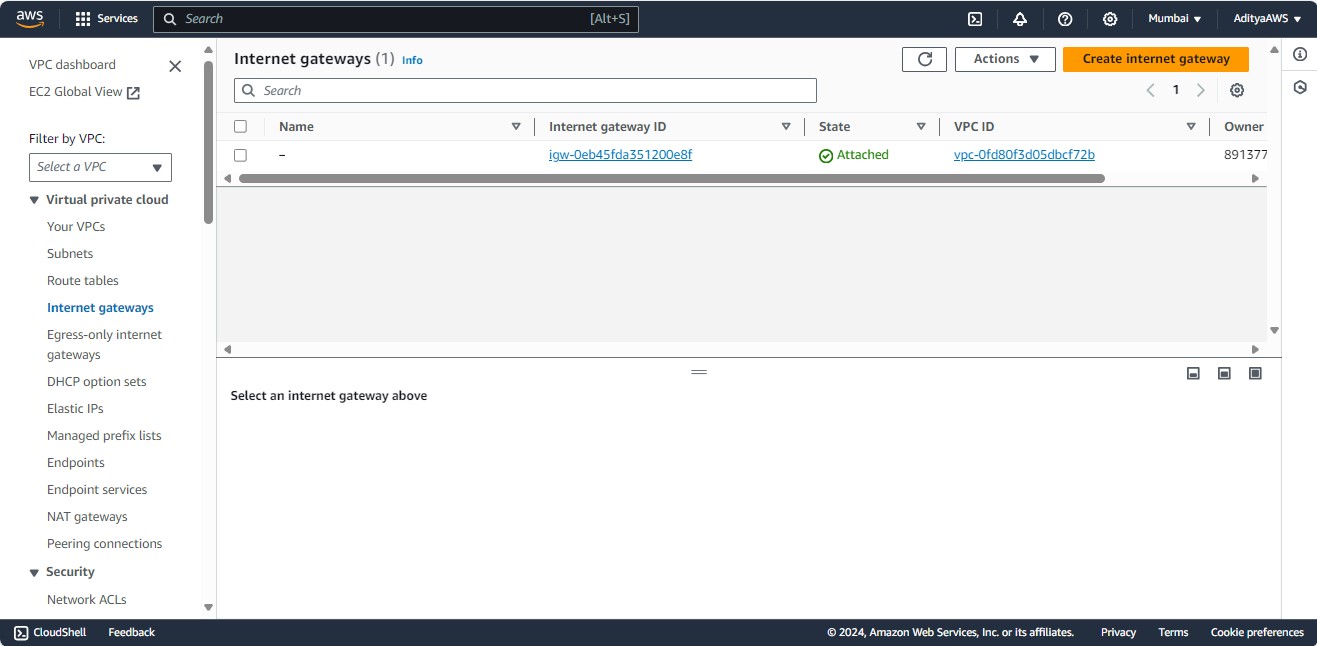
1. Now, repeat the process to create another subnet in a different Availability Zone with a different CIDR block.



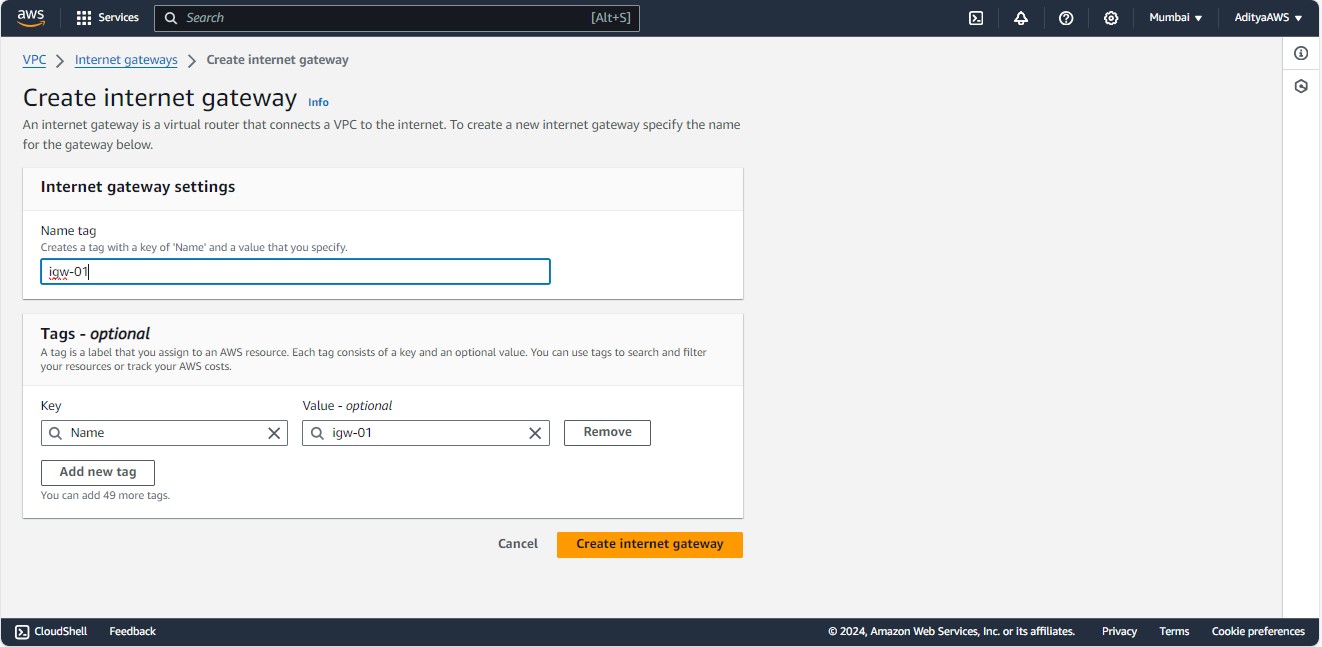
Result:



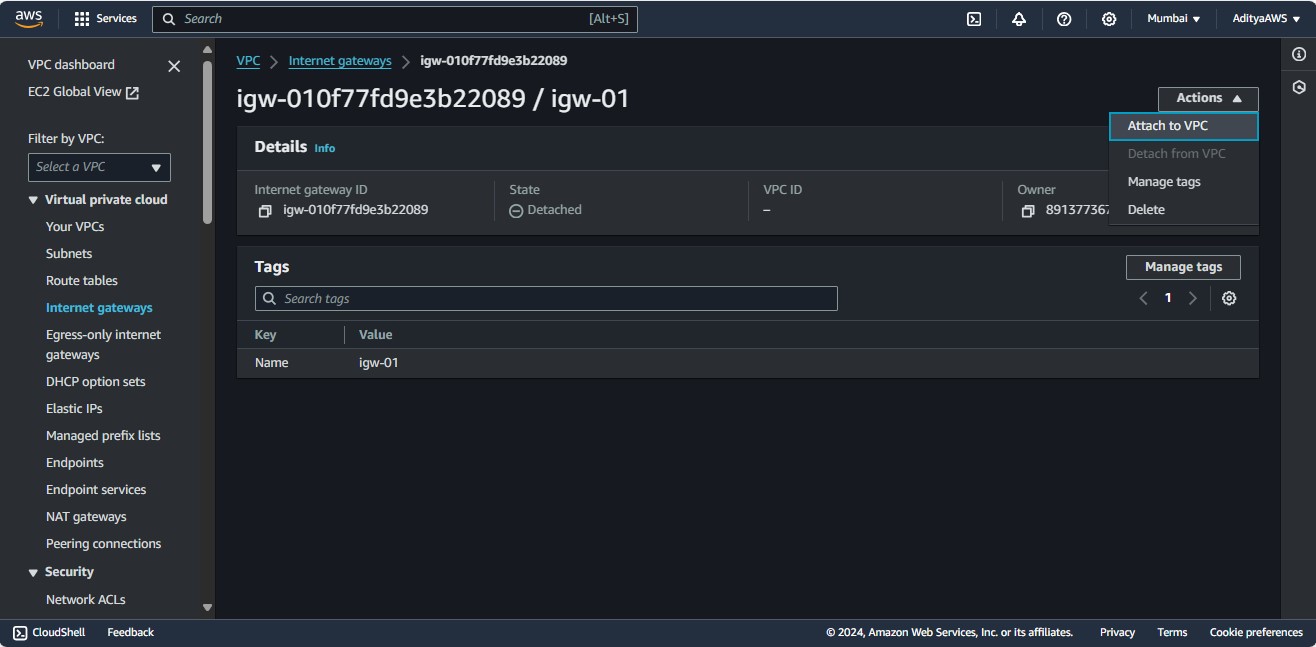
1. Now, to create a Internet Gateway, in the VPC dashboard, click on "Internet Gateways" in the left navigation panel and click on “Create internet gateway”.



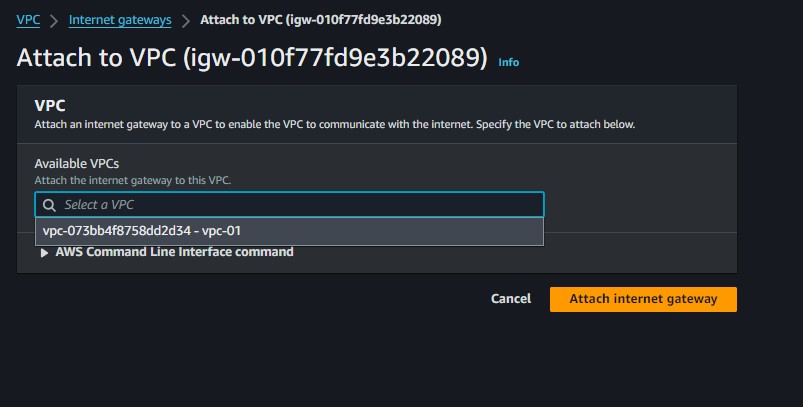
1. Name the internet gateway and click “Create internet gateway”.



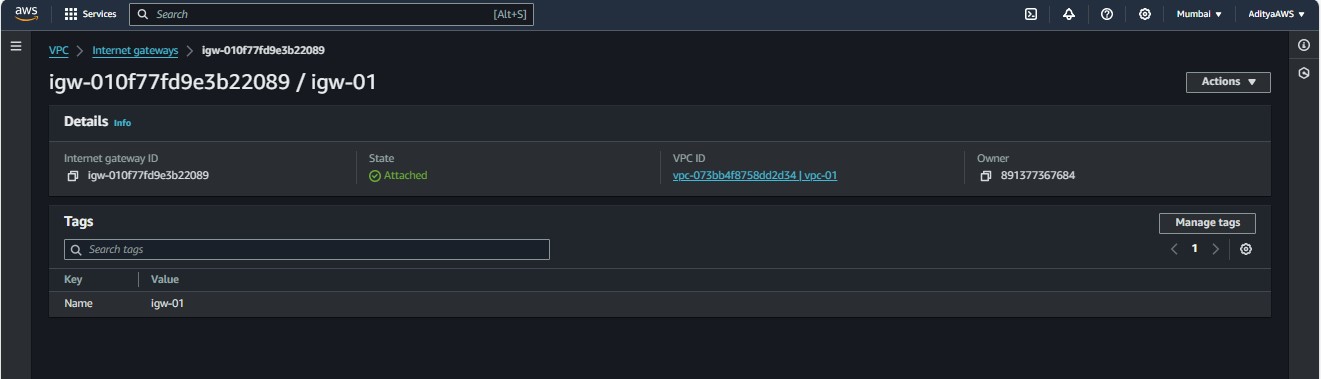
1. Now as the IGW is created successfully, to attach the IGW to the VPC click on “Actions” and click on “Attach to VPC”.



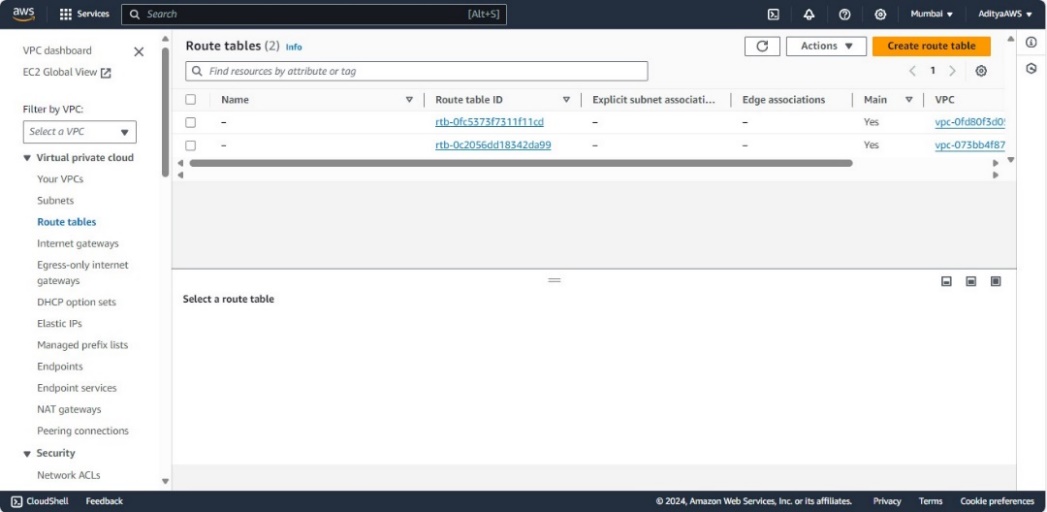
1. Then, select the VPC that we have created and click on “Attach internet gateway”.



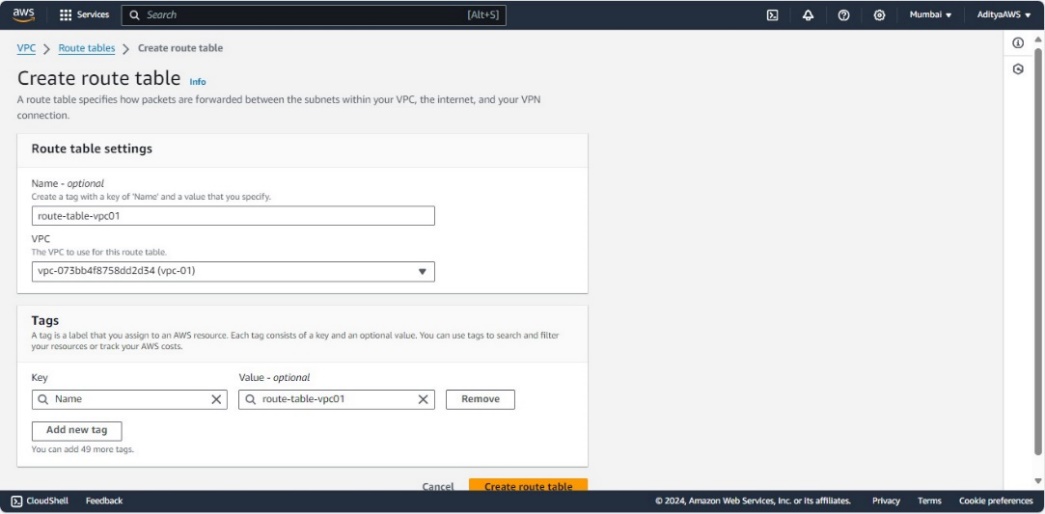
Result:



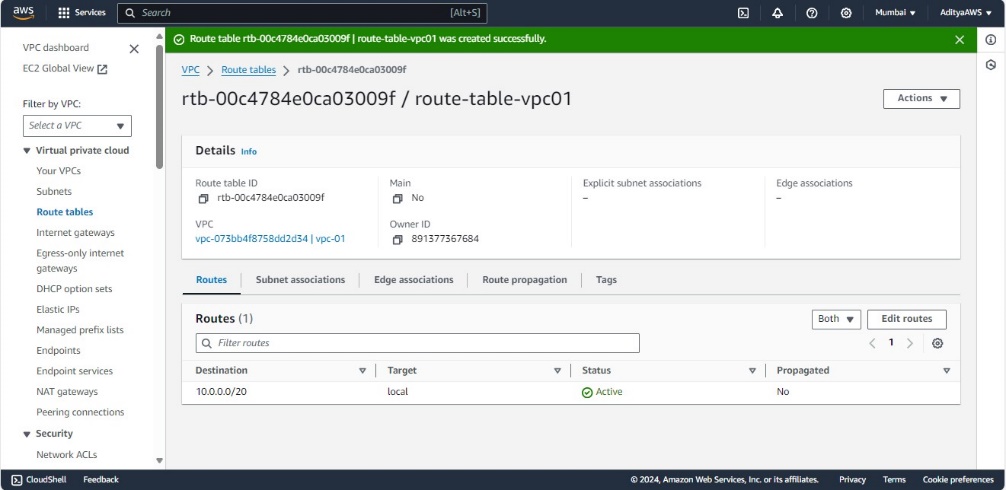
1. Now, there is a default route table but I will create another route table. To create route table click on “Route tables” in the left navigation panel. Click on “Create route table”.



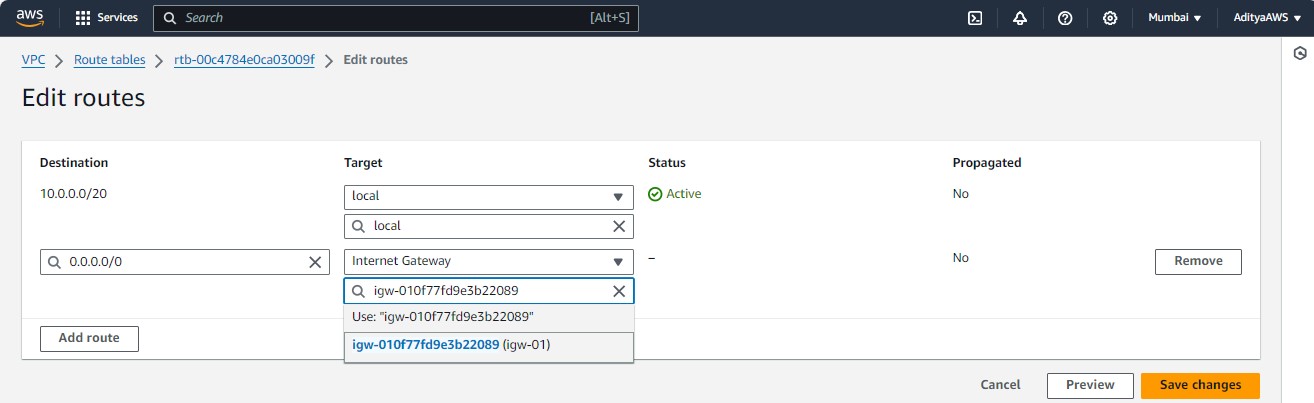
1. Give a name to the route table and choose the VPC (vpc-01). Click on “Create route table”.



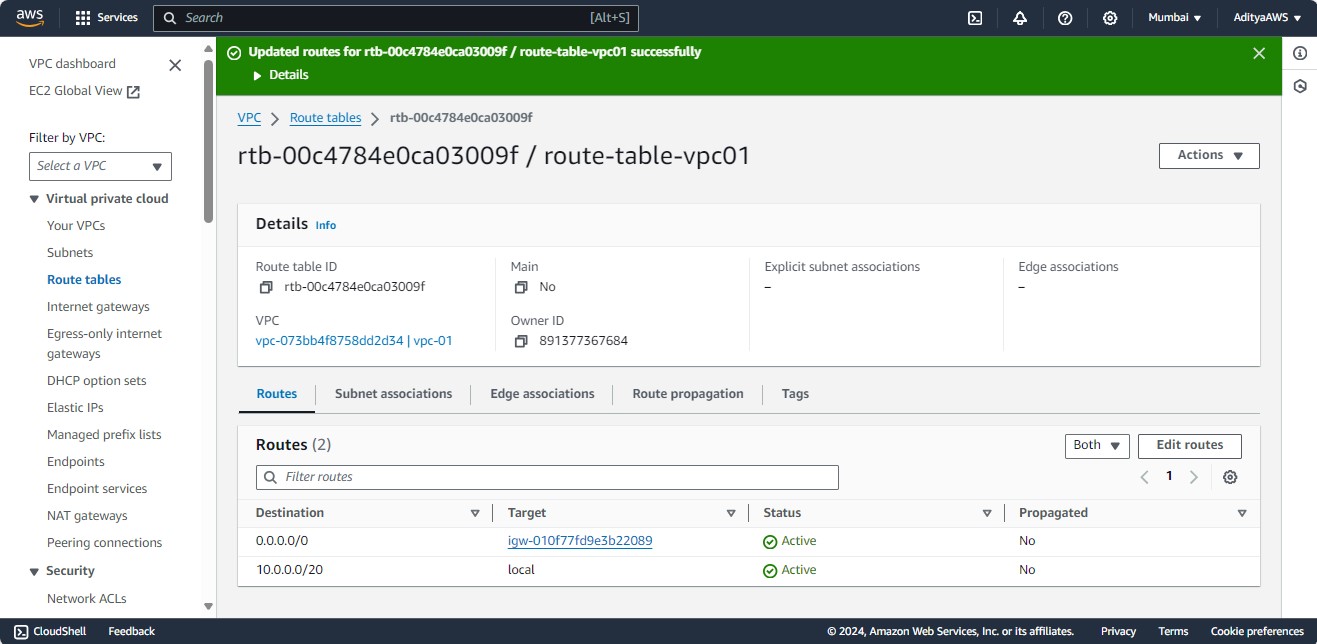
Result:



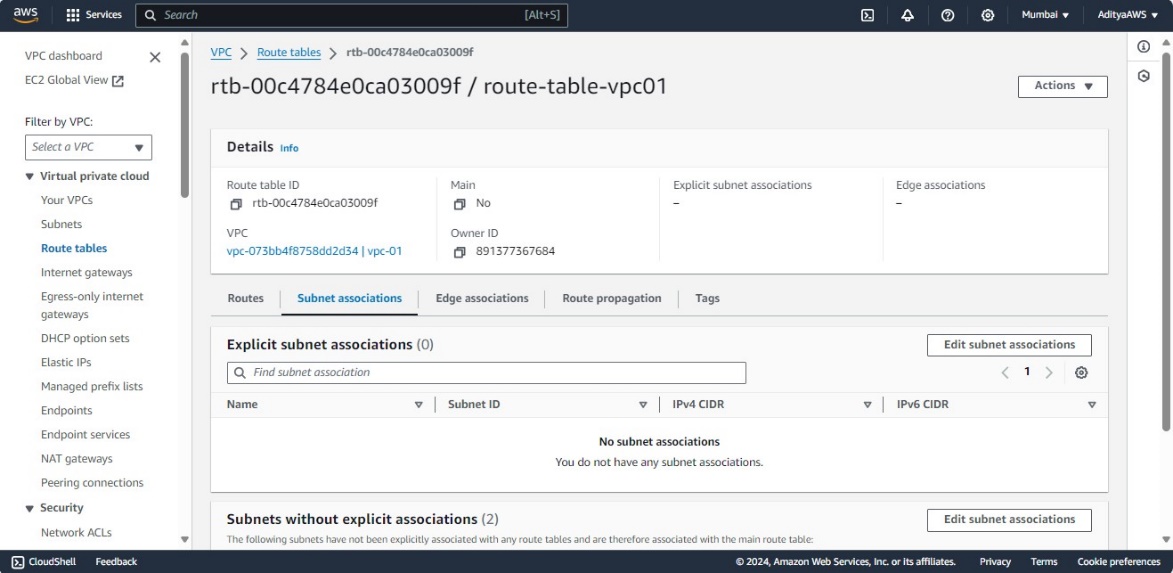
1. Now, in routes tab click on “Edit Routes”, add a route for destination **‘0.0.0.0/0’** and target as igw-01 (that is created and attached to the VPC). Click on “Save changes”.



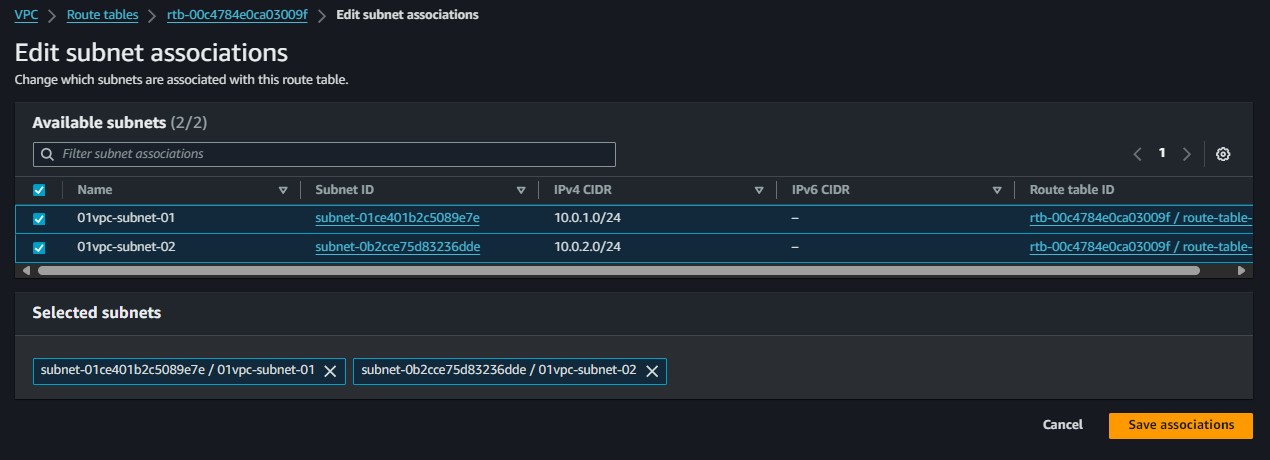
Result:



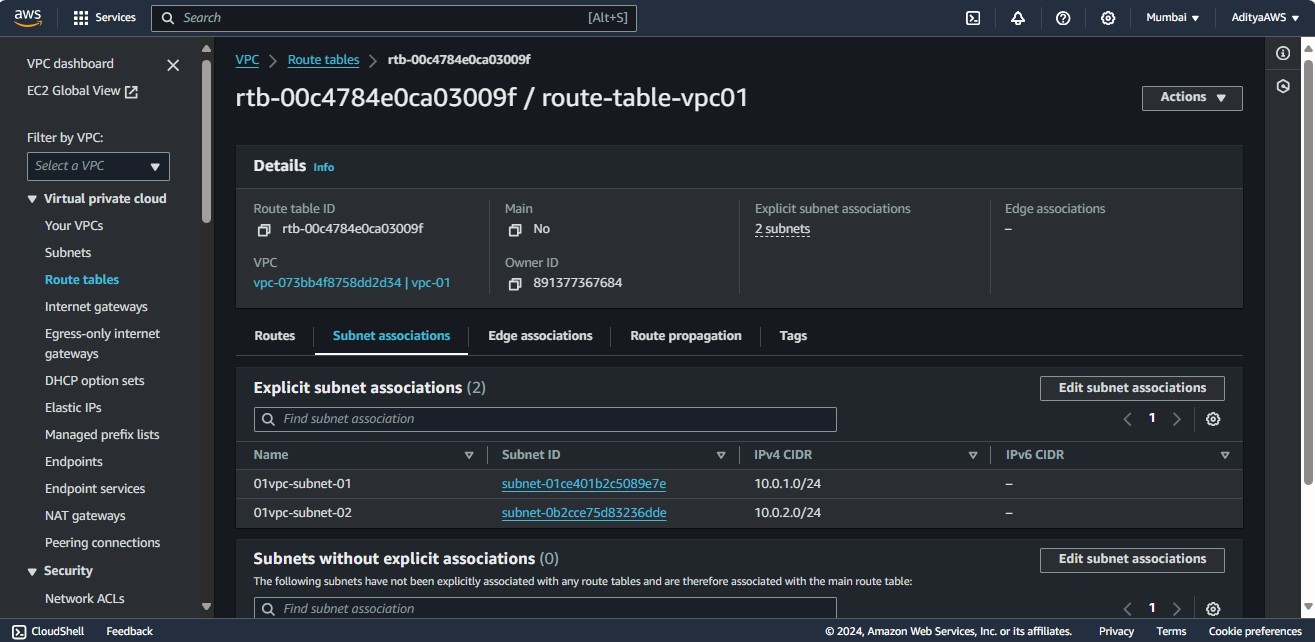
1. To associate the subnets with route table, go to subnet associations tab and click on “Edit subnet associations”.



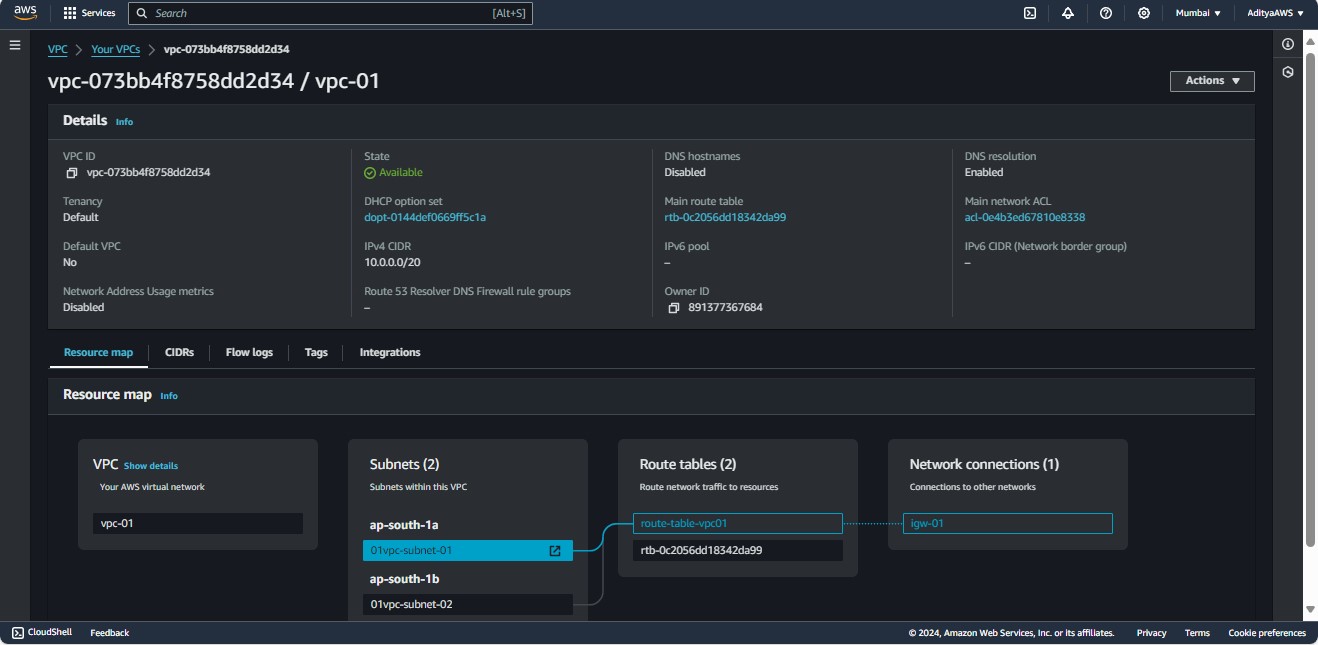
1. Then, select the subnets “01vpc-subnet-01” and “01vpc-subnet-02”. Click on “Save associations”.

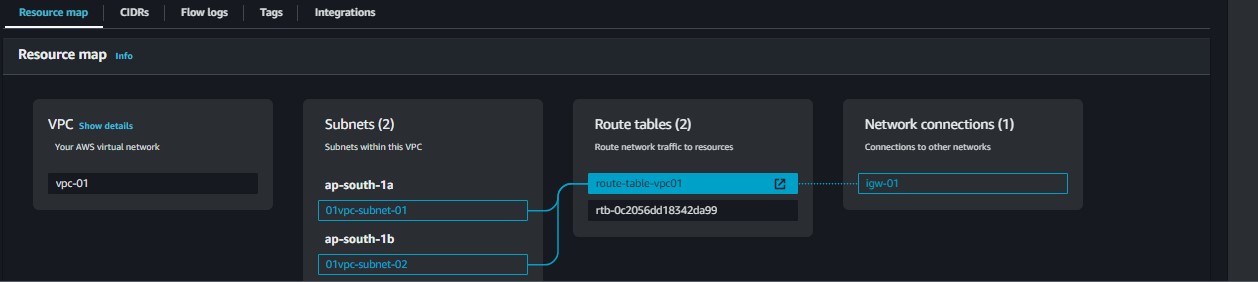


Result:



Now, the VPC is created with two subnets in different availability zones, and the internet gateway is attached to allow communication with the internet from instances in those subnets.





**Network Address Translation (NAT):**

NAT is a method used to map private IP addresses to a public IP address. It allows devices on a private network to communicate with the internet using a single public IP address. NAT is commonly used in scenarios where there is a private network (e.g., within a VPC) that needs to access resources on the internet but does not want to expose individual private IP addresses to the outside world.

**NAT Gateway:**

In AWS, a NAT gateway is a managed service that allows instances in a private subnet to initiate outbound traffic to the internet while preventing inbound traffic from reaching those instances directly. This is useful in situations where you have private instances that need to access the internet for updates, patches, or to download dependencies, but you want to control and secure incoming traffic.

**How and Why NAT Gateway is used:**

Outbound Traffic:

Private Subnets: Instances in private subnets don't have a direct public IP address, and by default, they can't communicate directly with the internet.

NAT Gateway: With a NAT gateway, instances in private subnets can route their outbound traffic through the NAT gateway, which then performs the necessary Network Address Translation to communicate with the internet using a public IP address.

Inbound Traffic:

Private Instances: Since private instances don't have public IP addresses, they are not directly accessible from the internet.

Enhanced Security: NAT gateways add an additional layer of security by not allowing inbound traffic to reach private instances, helping to protect them from unauthorized access.

Scalability and Redundancy:

AWS manages the high availability and scalability of NAT gateways.

If you have multiple subnets across different Availability Zones, each subnet can have its own NAT gateway for redundancy and load distribution.

Logging and Monitoring:

NAT gateways provide logging capabilities, allowing you to monitor outbound traffic from your private instances.

This can be useful for troubleshooting and security analysis.

In summary, a NAT gateway is a secure and scalable solution for allowing instances in private subnets to access the internet for outbound traffic while preventing unsolicited inbound traffic. It is a common component in AWS architectures where there is a need to balance security and functionality for private instances.