Virtual Private Cloud (VPC)

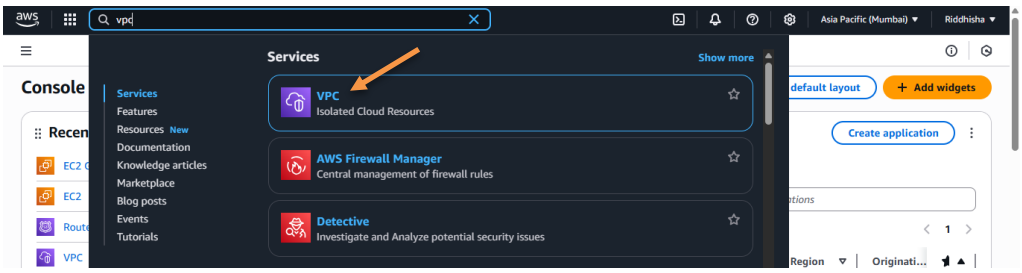
Introduction:

- A Virtual Private Cloud (VPC) is a private, isolated section of the AWS cloud where you can create and manage your own virtual network.
- It allows you to launch AWS resources such as EC2 instances, databases, and load balancers in a secure environment that you control.
- With a VPC, you can customize things like your IP address range, create subnets, set up route tables, and configure network gateways.
- By default, we can create 5 VPCs in a region and in a single VPC, we can create 200 subnets.
- Security is a major benefit of VPC. You can use features like "Security Groups" and "Network ACLs" to control which traffic is allowed in and out of your network. This helps in building safe, scalable, and high-performance applications in the cloud.

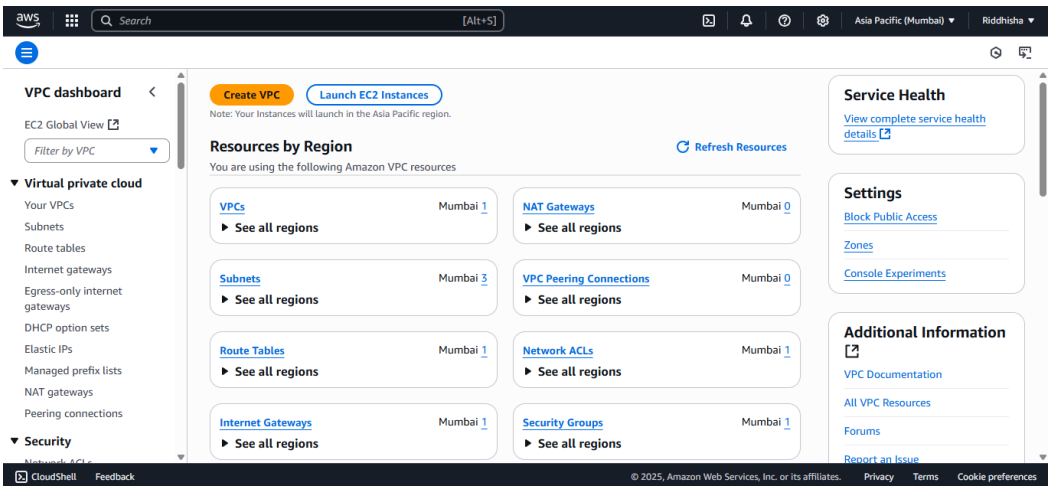
Step by Step Instructions:

Step 1:

- Open “AWS Management Console” on any browser.
- Search “VPC” and open it.



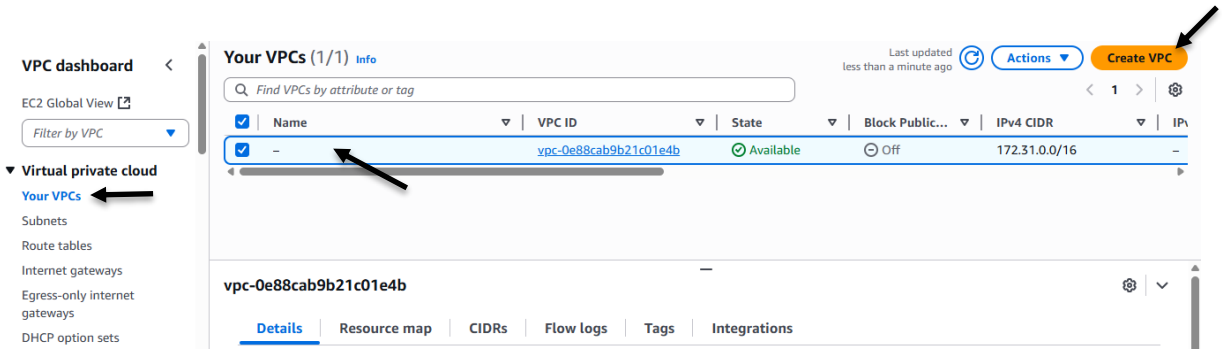
- The VPC Console will open.



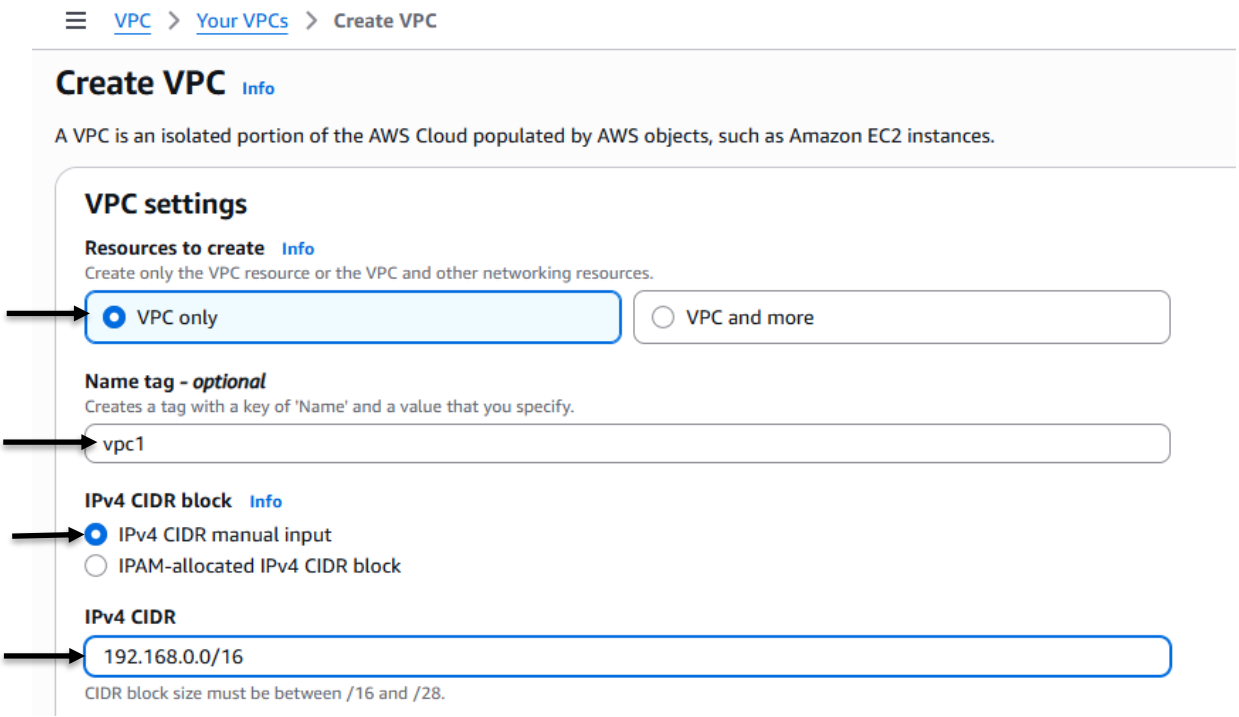
Creating a VPC:

Step 2:

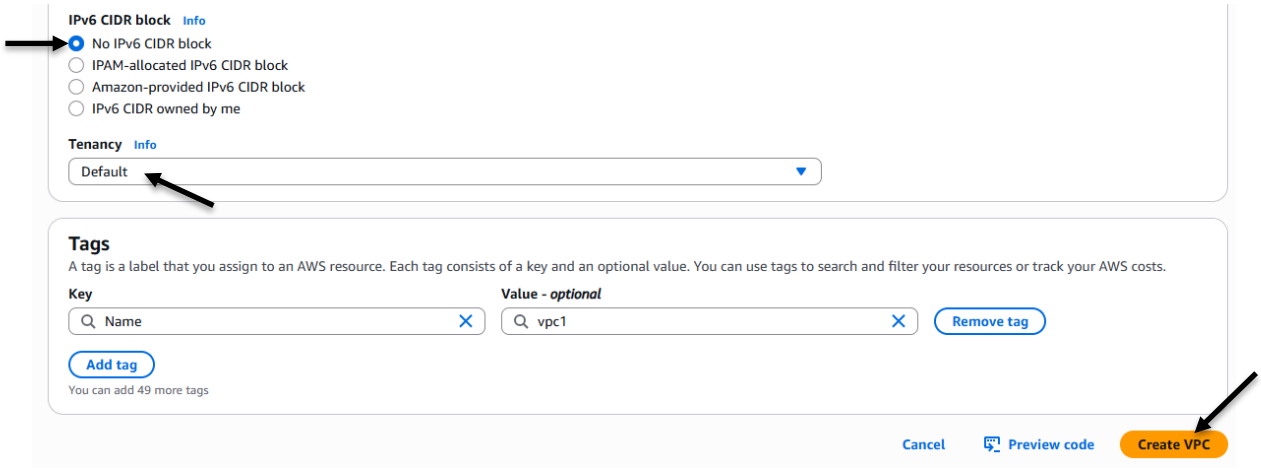
- Go to “Your VPCs”.
- Since we are in Mumbai region, we can see that by default, there is already 1 VPC created.
- Click on “Create VPC”.



- In “Resources to create”, select “VPC only”.
- Give a name to your VPC (e.g. “vpc1”).
- In “IPv4 CIDR block”, select the CIDR manual input option and enter the IPv4 CIDR as “192.168.0.0/16”.

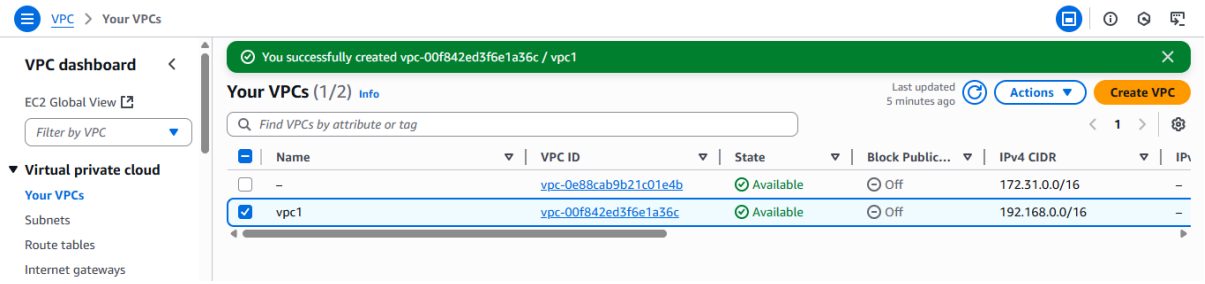


- In “IPv6 CIDR block”, select “No IPv6 CIDR block”.
- Leave the “Tenancy” at “Default”.
- Click on “Create VPC”.



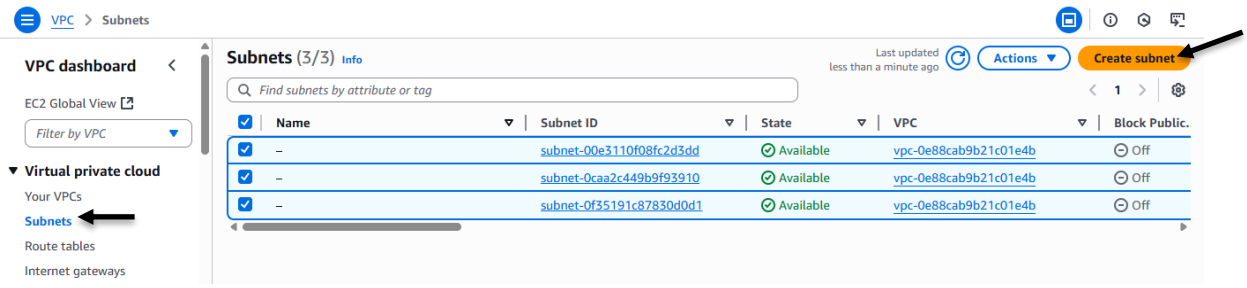
Step 3:

- Your VPC is now created.



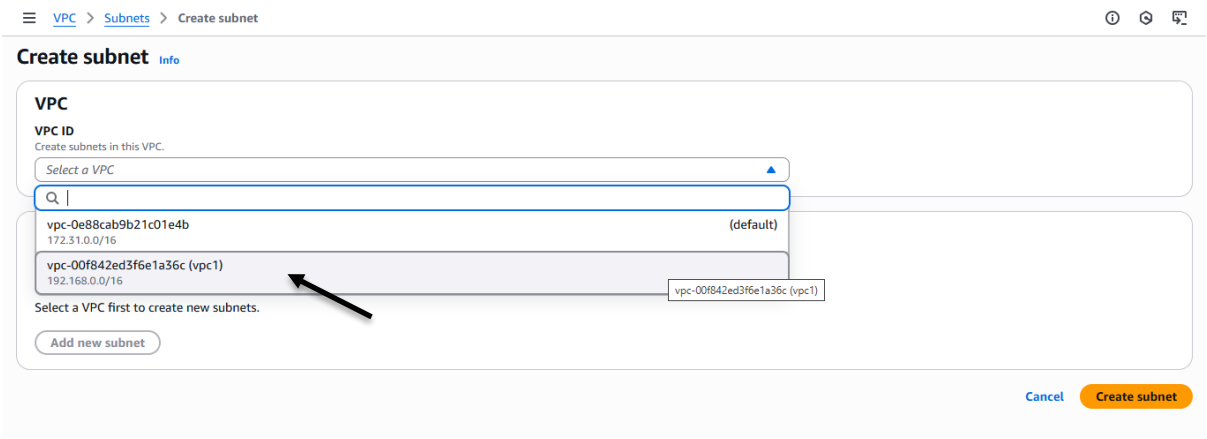
Creating a Subnet:

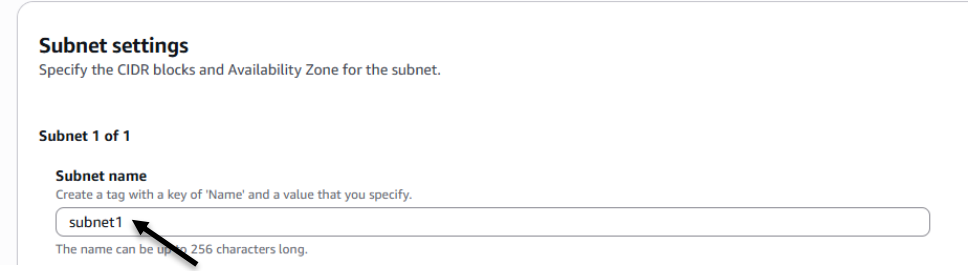
- Now go to “Subnets” under “Virtual private cloud” and there you can see 3 subnets are already created (for Mumbai region only).
- Click on “Create subnet”.



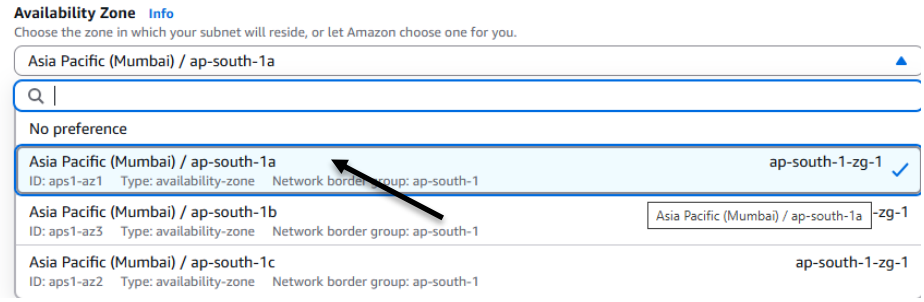
Step 4:

- In “VPC ID”, select the VPC that you just created i.e. “vpc1”.
- Under “Subnet settings”, give a name to your subnet (e.g. “subnet1”).

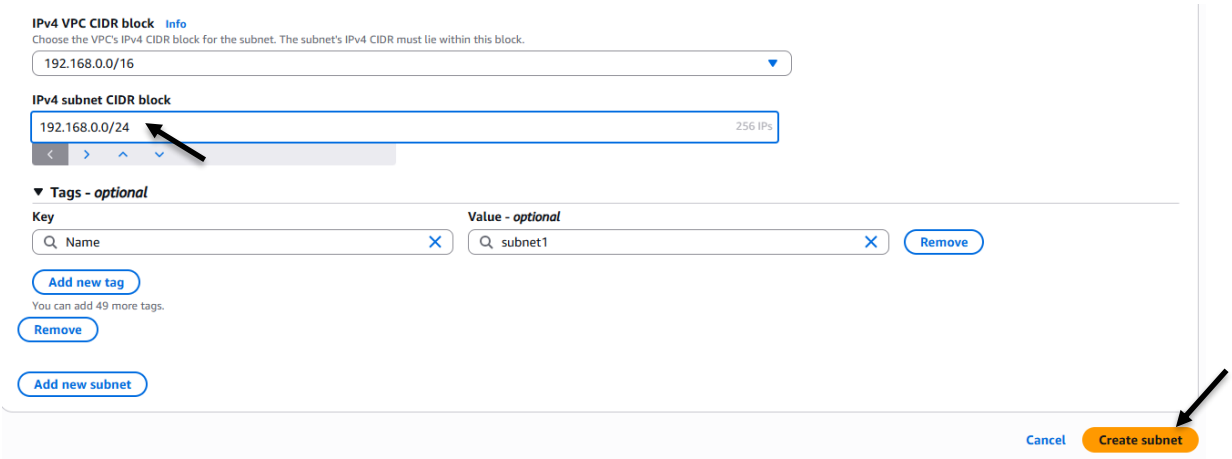




- In “Availability Zone”, select any zone as per your preference.
- I have selected “ap-south-1a”.

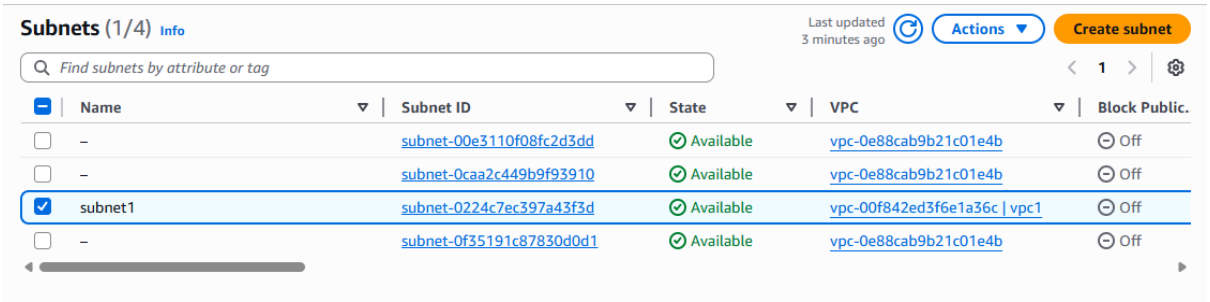


- Leave “IPv4 VPC CIDR block” as it is.
- In “IPv4 subnet CIDR block”, type “192.168.0.0/24”.
- Click on “Create subnet”.



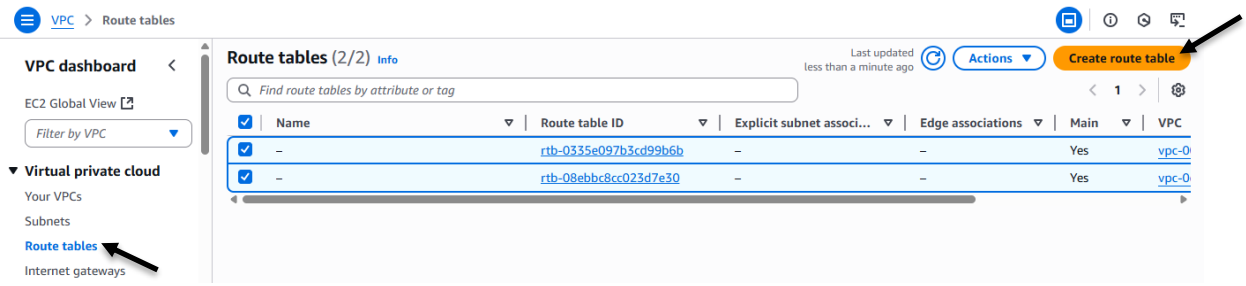
Step 5:

- Your subnet is now created.



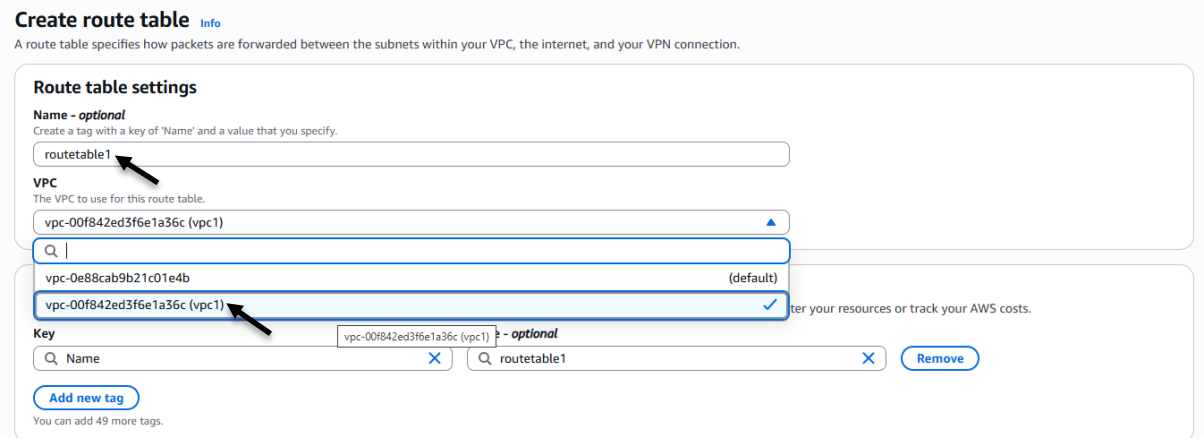
Creating a Route Table:

- Under “Virtual private cloud”, go to “Route tables”.
- There you can see 2 route tables are already created (for Mumbai region only).
- Click on “Create route table”.

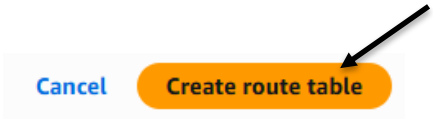


Step 6:

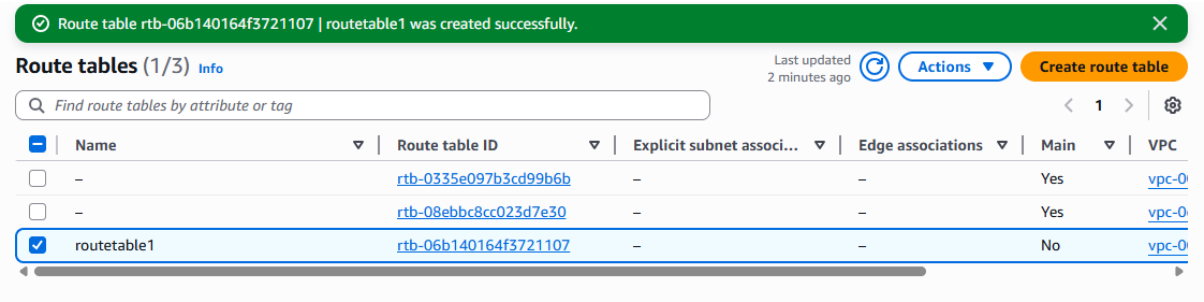
- Give a name to your route table (e.g. “routetable1”).
- In “VPC”, select the VPC that you have created i.e. “vpc1”.



- Click on “Create route table”.



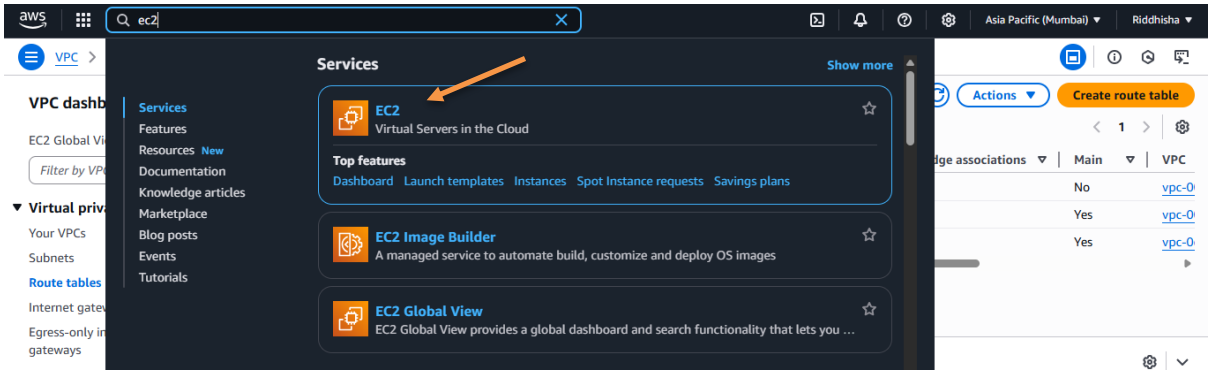
- Your route table is created.



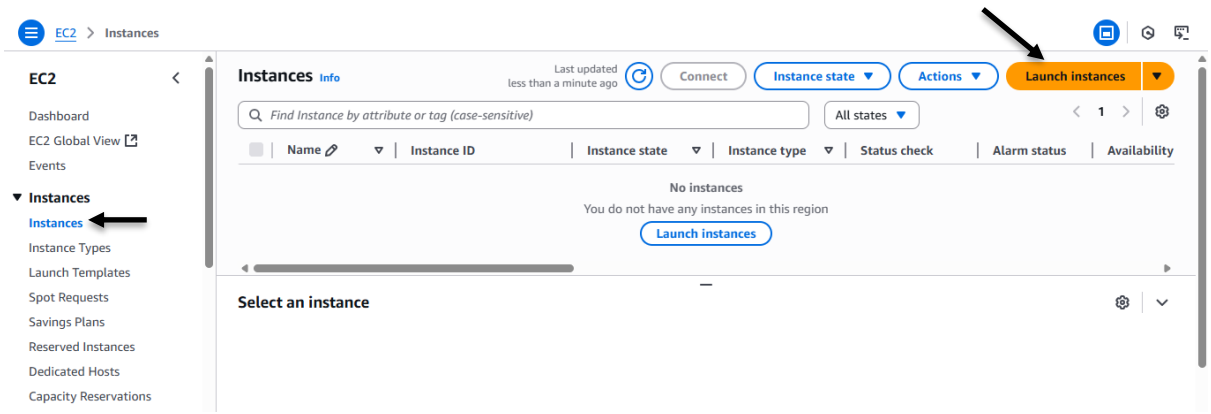
Now Launch an Instance:

Step 7:

- Now duplicate the tab.
- Search and open “EC2”.

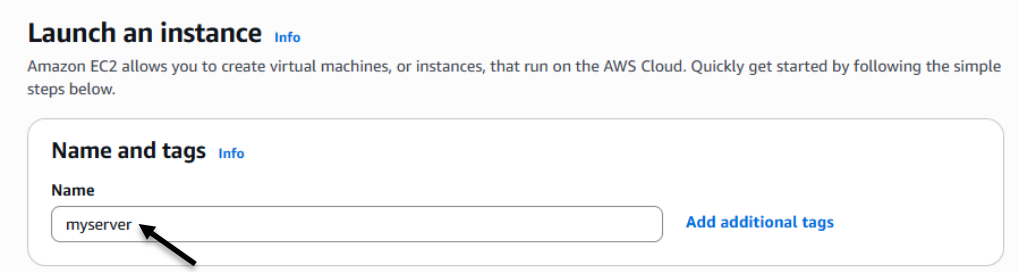


- Under “Instances”, click on “Launch instances”.

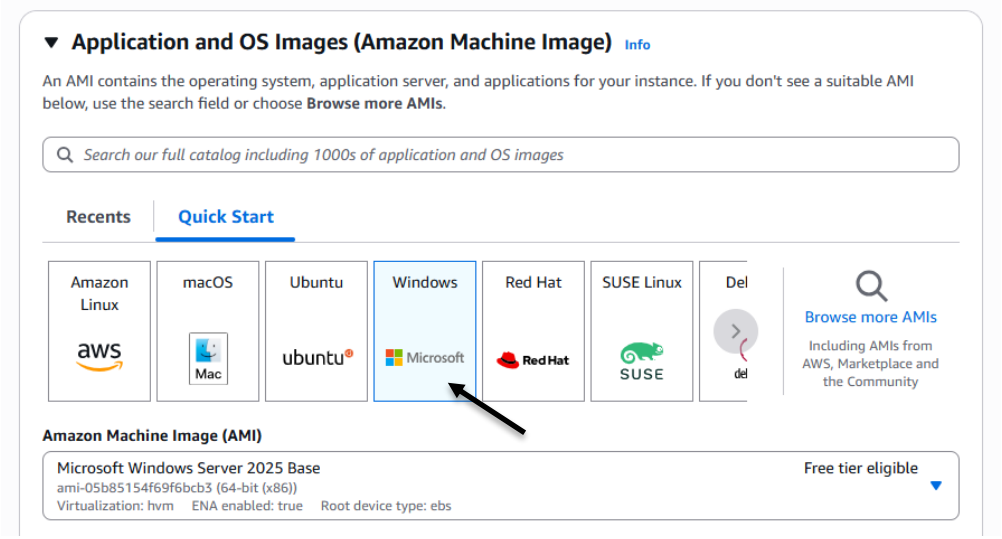


Step 8:

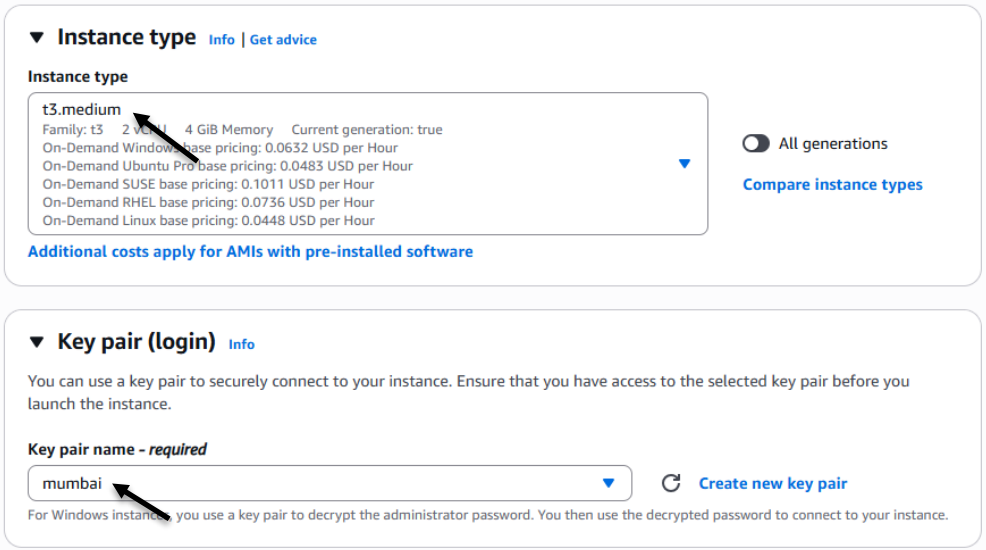
- Give a name to your server.



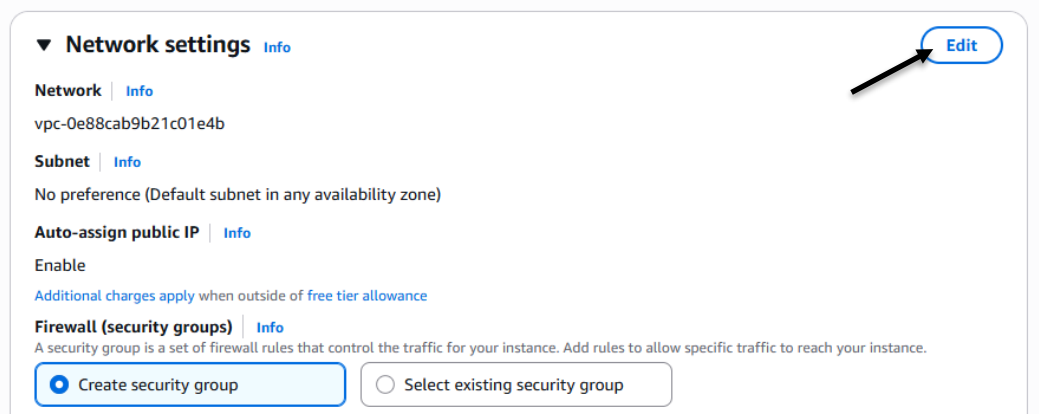
- Select “Windows” under “Application and OS Images (AMI)”.



- Select any instance type as per your preference (e.g. “t3.medium”).
- Select any key pair of Mumbai region (e.g. “mumbai”).

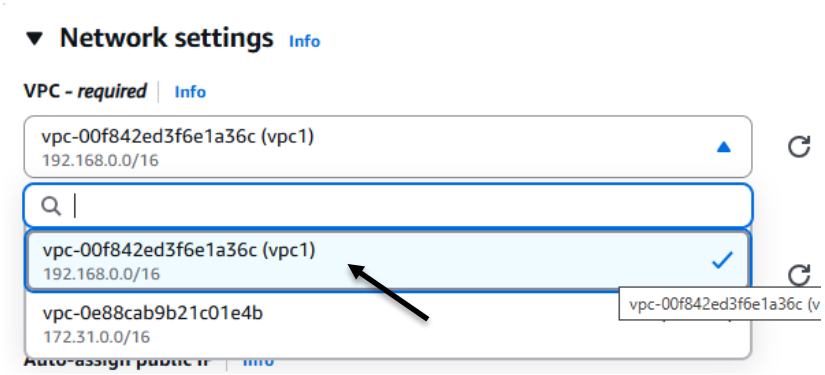


- In “Network settings”, click on “Edit” button.

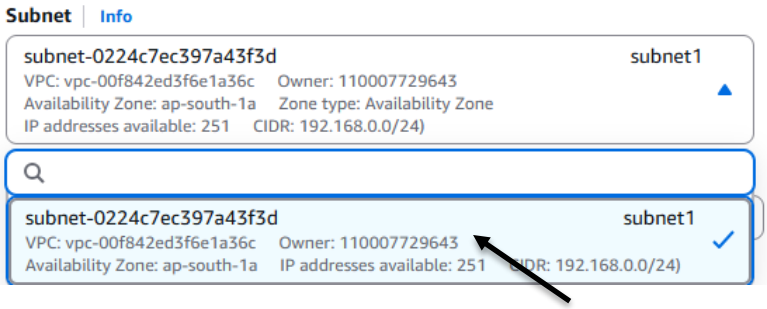


Step 9:

- In “VPC - required”, select “vpc1” that you have created.



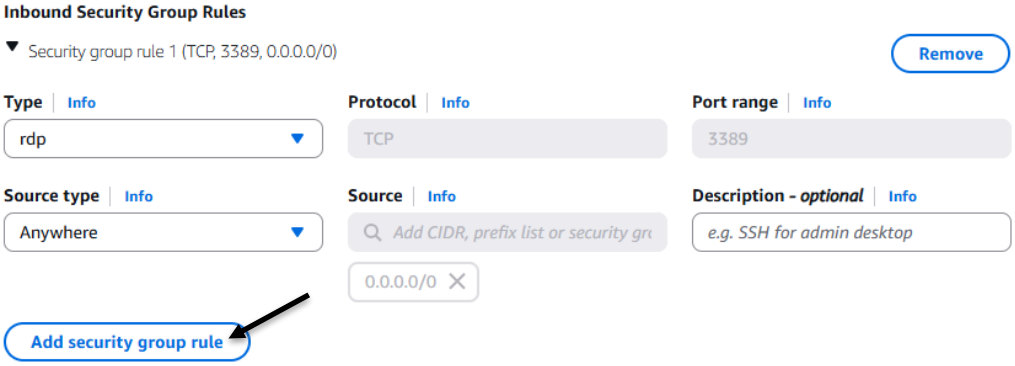
- In “Subnet”, select “subnet1” that you have created.



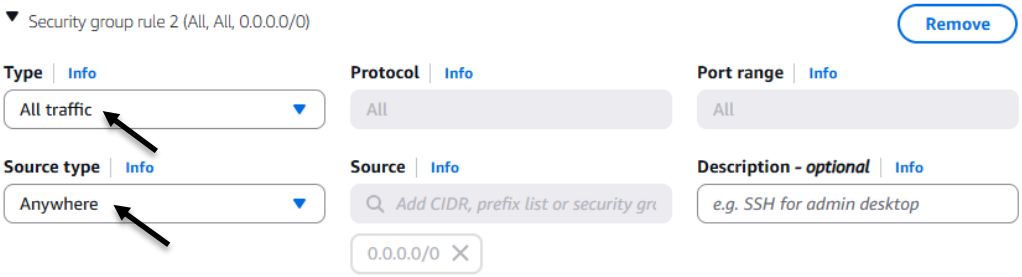
- Select “Enable” option in “Auto-assign public IP”.

- Give a name to the security group (e.g. “SG1”).

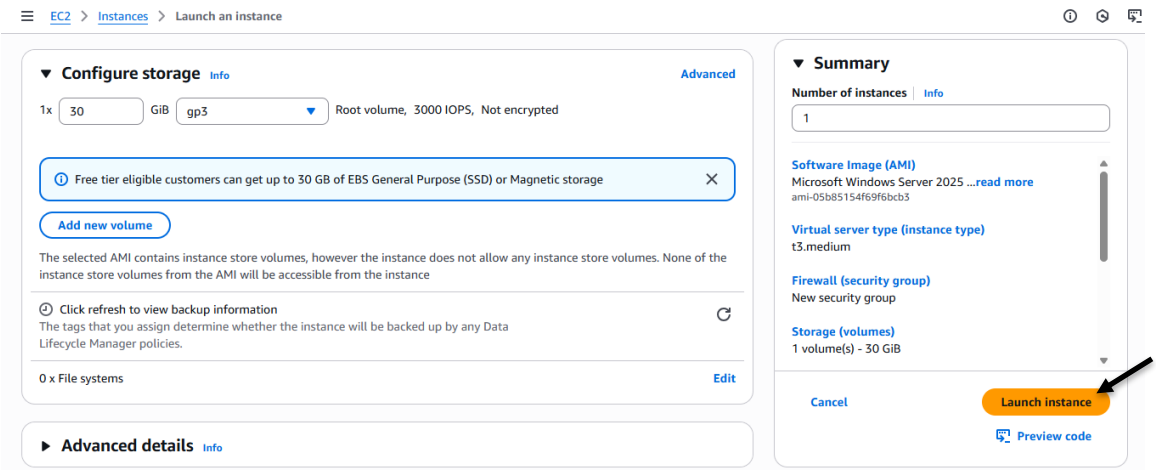
- Under “Inbound Security Group Rules”, leave the first rule as it is i.e. “RDP – Anywhere”.
- Click on “Add security group rule”.



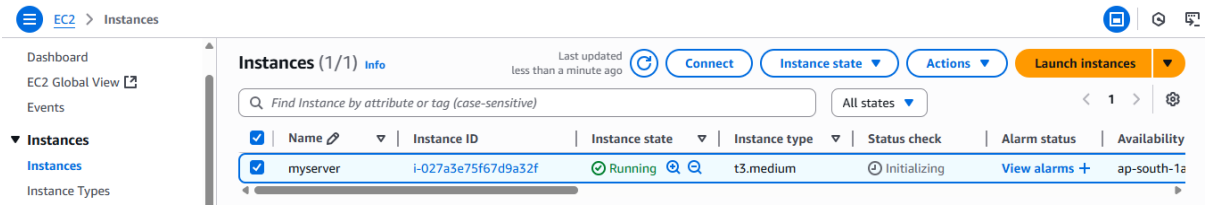
- Add second rule as “All traffic - Anywhere”.



- Leave the other settings as it is and click on “Launch instance”.

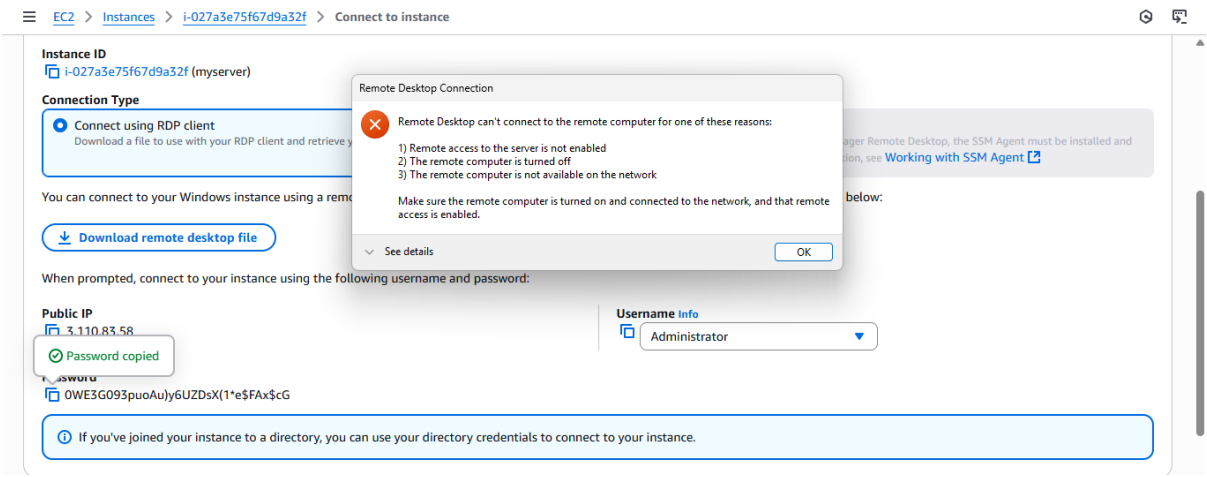


- Your instance is launched and is running.



Step 10:

- Now if you try to connect your instance, it will not be connected.
- To connect an instance, we need to create an internet gateway.



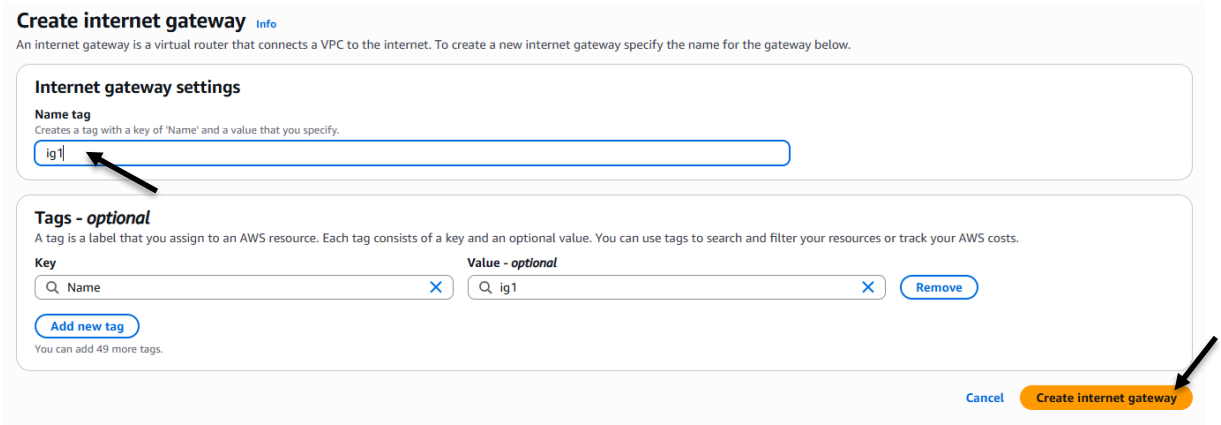
Creating an Internet Gateway:

Step 11:

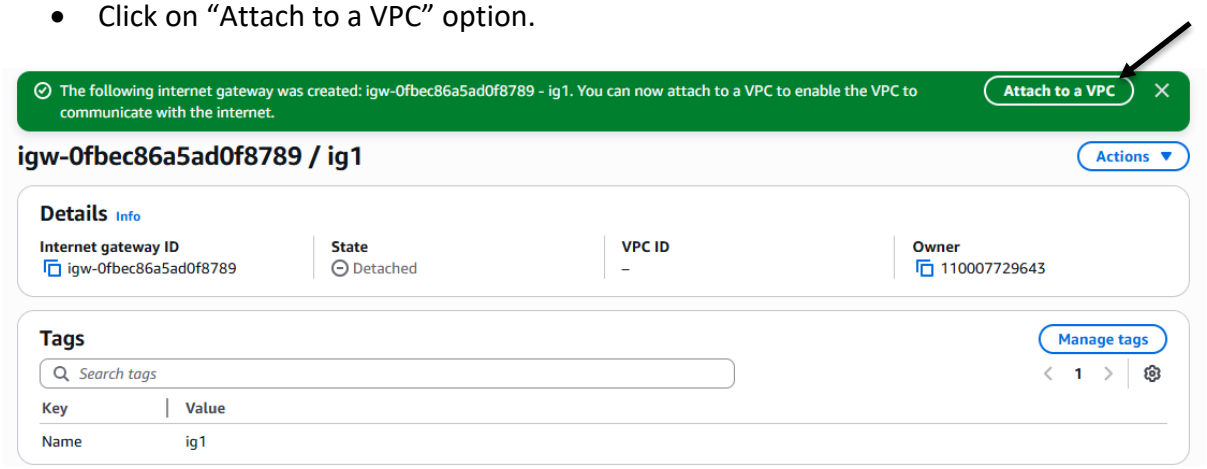
- Go back to “VPC” tab and click on “Internet gateways”.
- There you can see that 1 internet gateway is already created (for Mumbai region only).
- Click on “Create internet gateway”.

Step 12:

- In “Internet gateway settings”, name your internet gateway (e.g. “ig1”).
- Click on “Create internet gateway”.

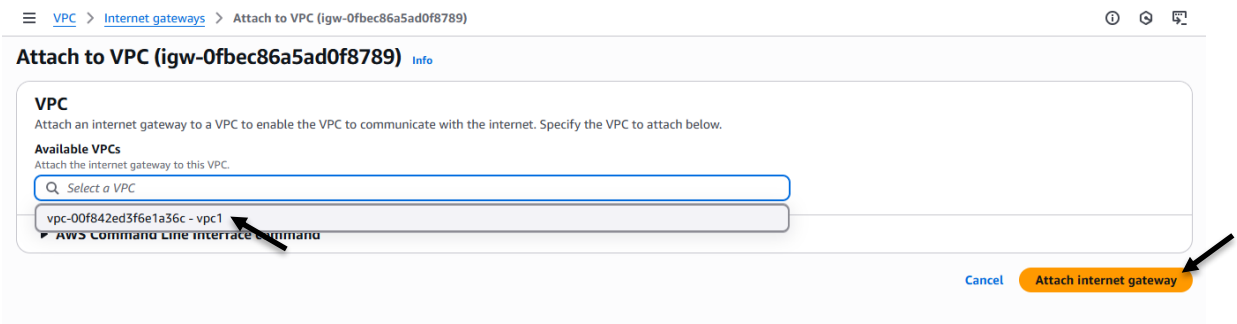


- Your internet gateway is now created.
- Click on “Attach to a VPC” option.

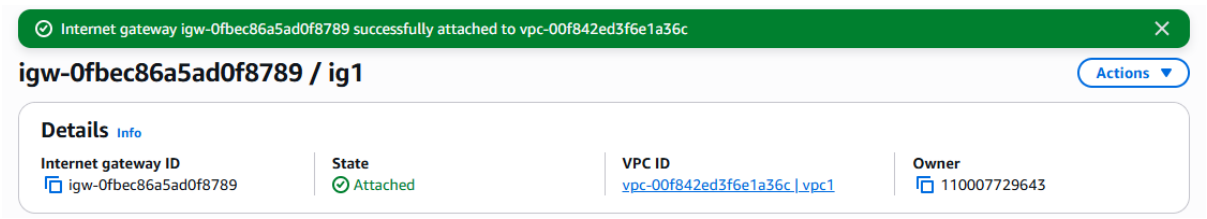


Step 13:

- Under “Available VPCs”, select your VPC i.e. “vpc1”.
- Click on “Attach internet gateway”.

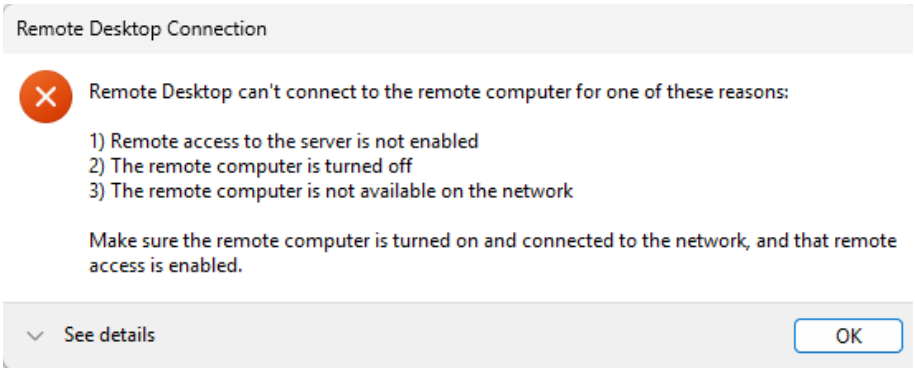


- The internet gateway “ig1” is successfully attached to your VPC “vpc1”.



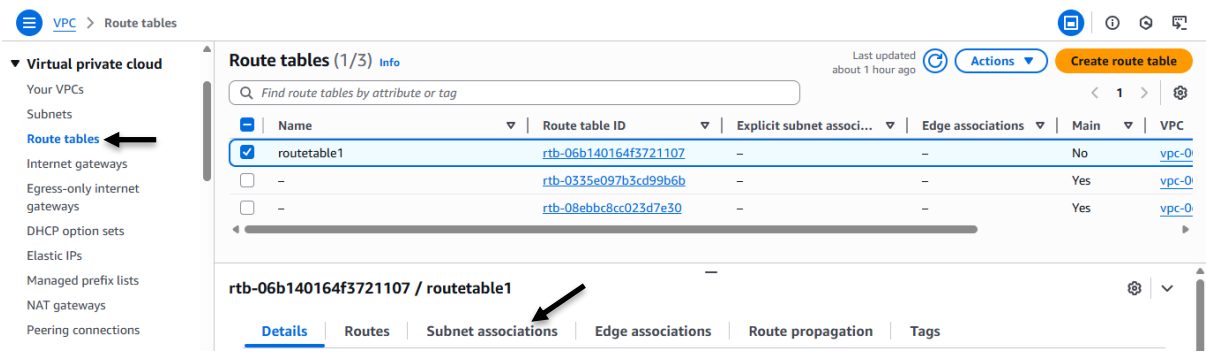
Step 14:

- Go to “EC2” tab and once again, try to connect your instance.
- It still won’t get connected because we have not added rules to the route table yet.



Adding Rules to the Route Table:

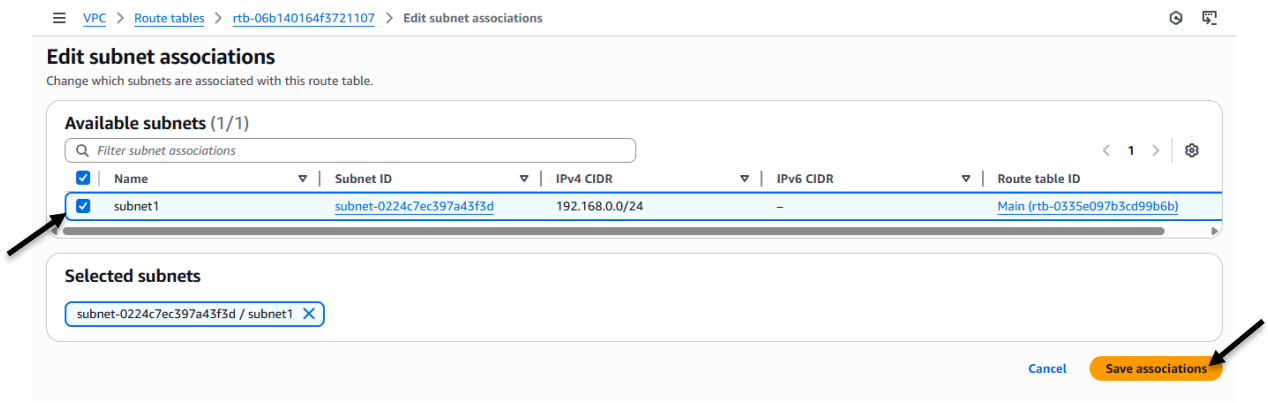
- Again, go back to the “VPC” tab.
- Under “Route tables”, select the route table that you have created.
- From the options below, click on “Subnet associations”.



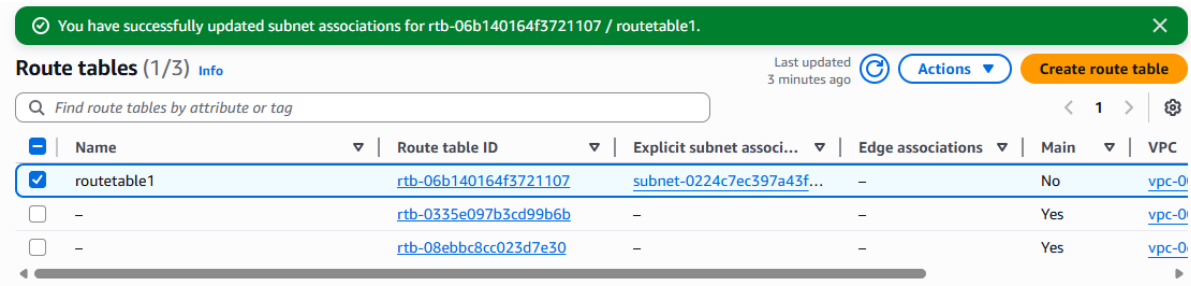
Step 15:

- Now click on “Edit subnet associations” button.

- Under “Available subnets”, select the subnet that you have created i.e. “subnet1”.
- Now click on “Save associations”.

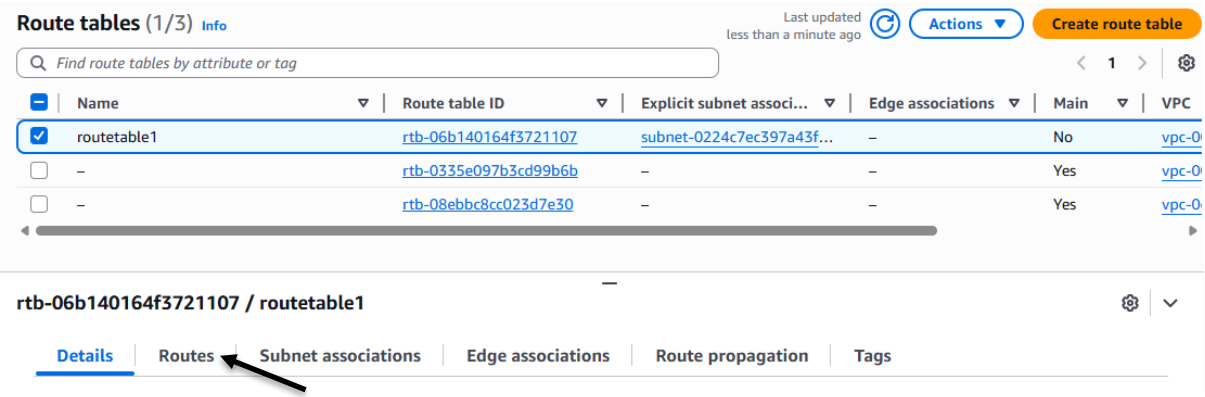


- Subnet association is successfully updated.

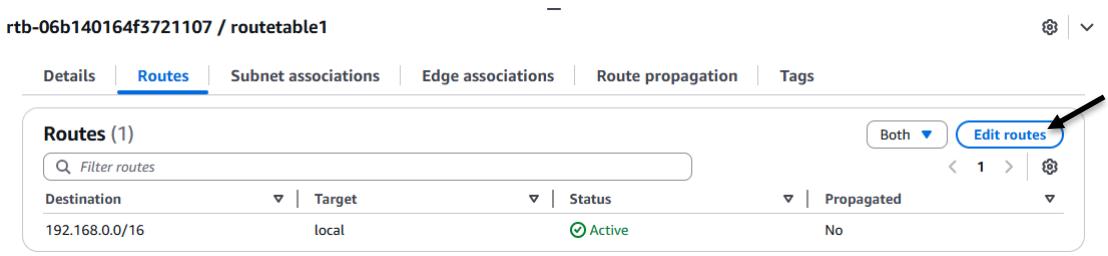


Step 16:

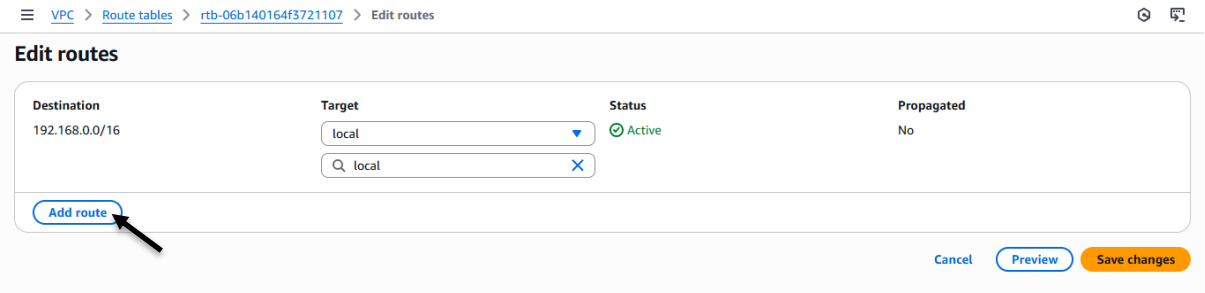
- Again, select the route table that you have created.
- From the options below, click on “Routes”.



- You can see that one route is already added.
- Now click on “Edit routes”.

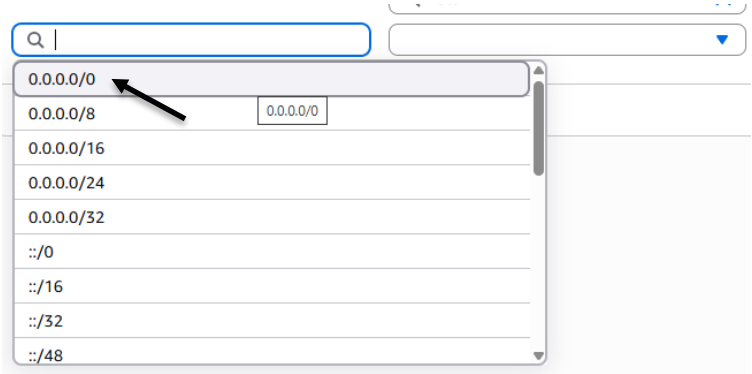


- Click on “Add route” button.

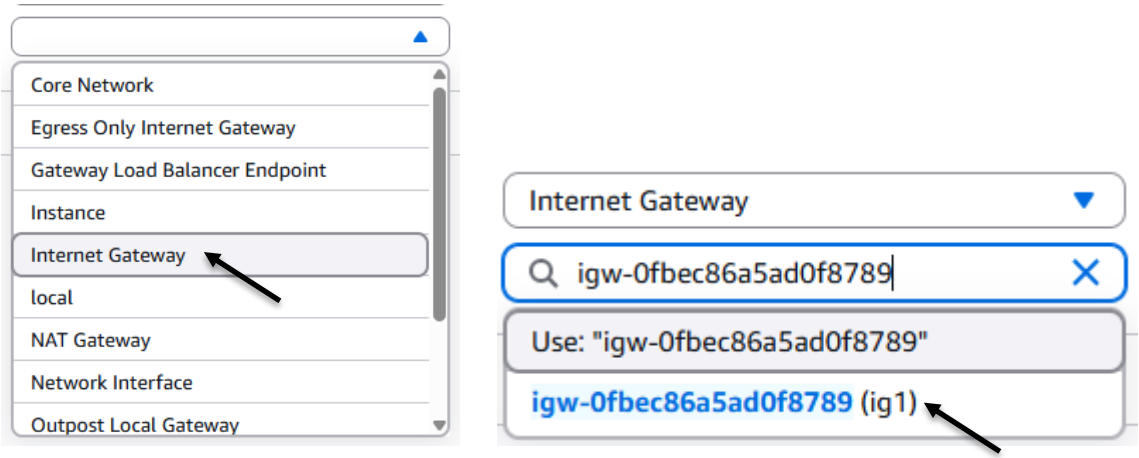


Step 17:

- Add route “0.0.0.0/0” in destination from the options.

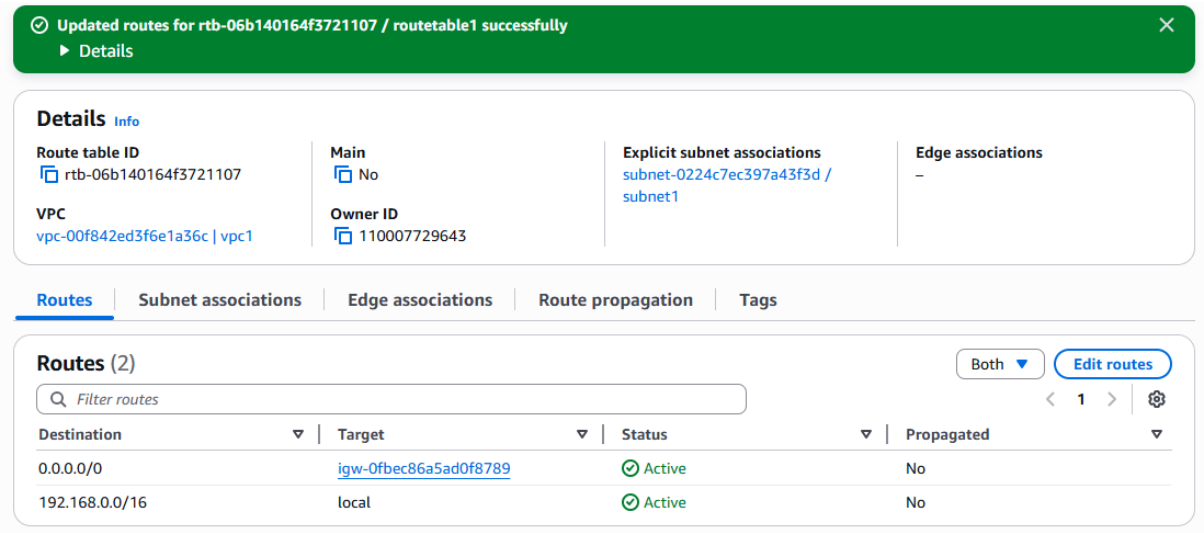


- In “Target”, add “Internet Gateway”.
- Select the internet gateway that you have created.



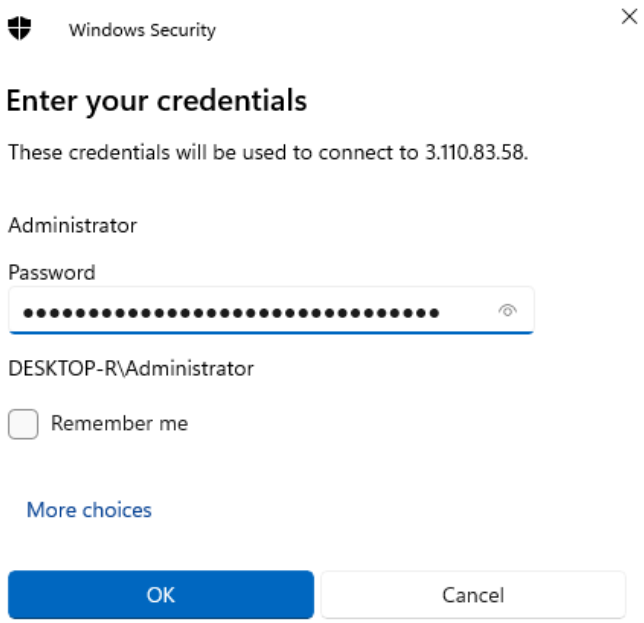
- Click on “Save changes”.

- The routes are now updated for the route table.

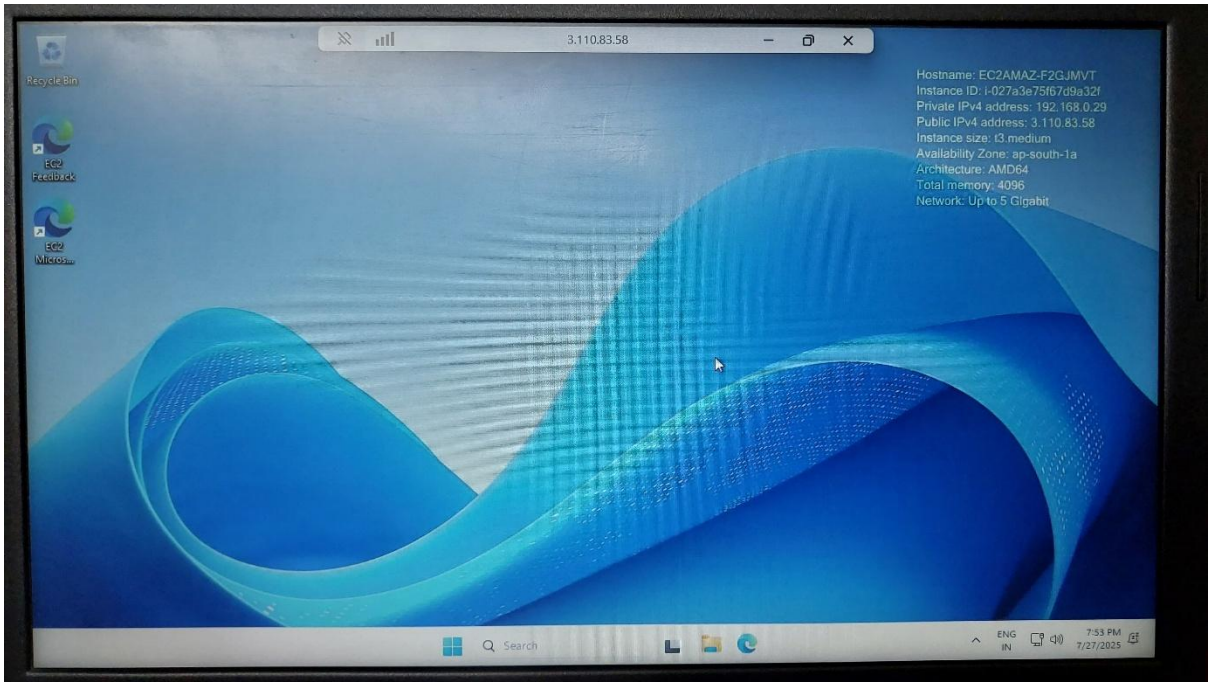


Step 18:

- Go back to “EC2” tab and try to connect your instance again.
- Generate the password as usual, decrypt it and paste there.



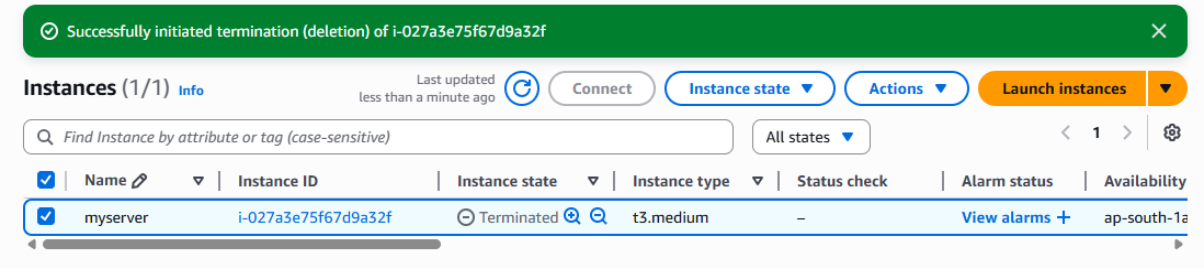
- Click on “OK”.
- Your instance is now connected.
- This shows that if we are creating our own VPC, subnet and route table, then it is necessary to attach them to an internet gateway.
- Only then the server will get connected.



Now terminate your instance:

Step 19:

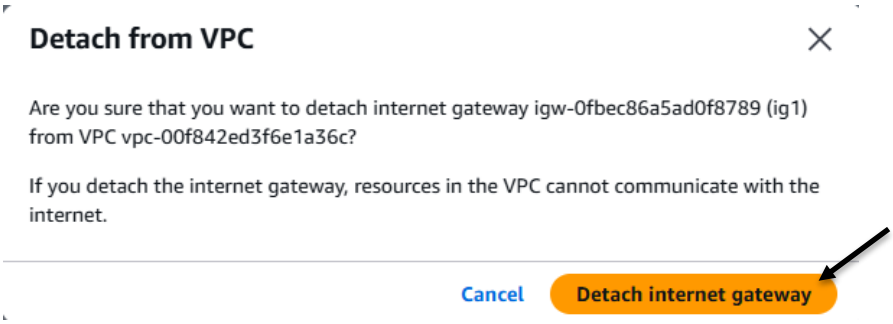
- On the “EC2” tab, go to “Instances” and terminate your instance.



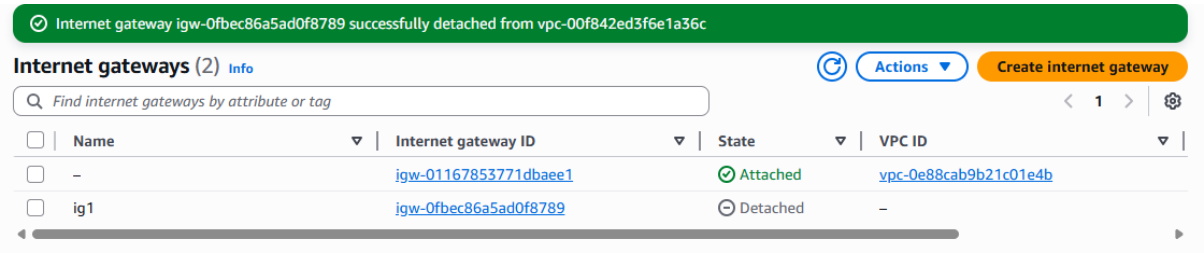
Deleting Internet Gateway:

- Go back to “VPC” tab and under “Internet gateways”, select the internet gateway that you have created.
- Click on “Actions” and then click on “Detach from VPC”.

- Click on “Detach internet gateway”.

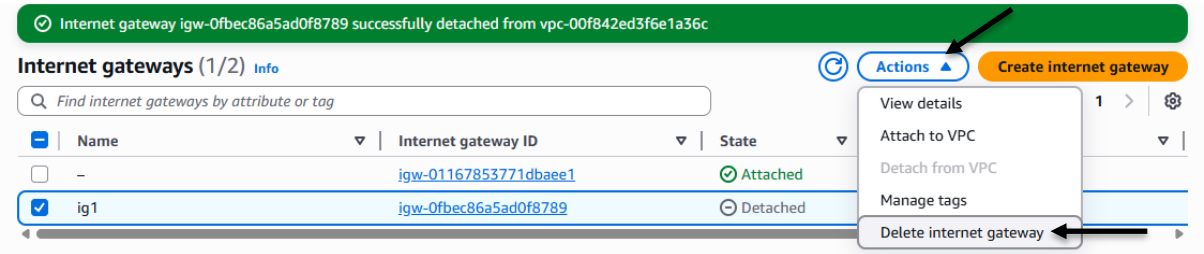


- Your internet gateway is successfully detached.

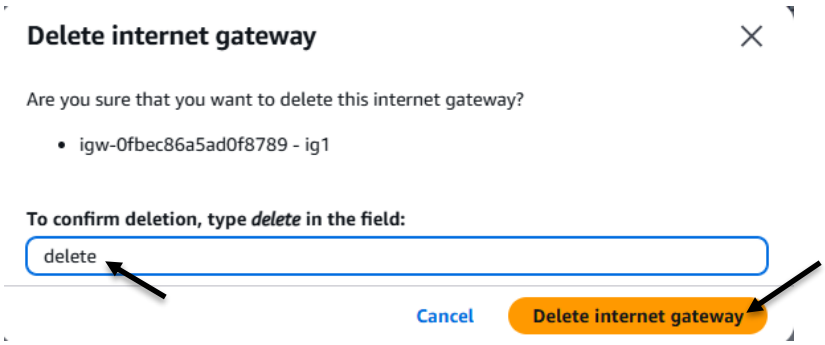


Step 20:

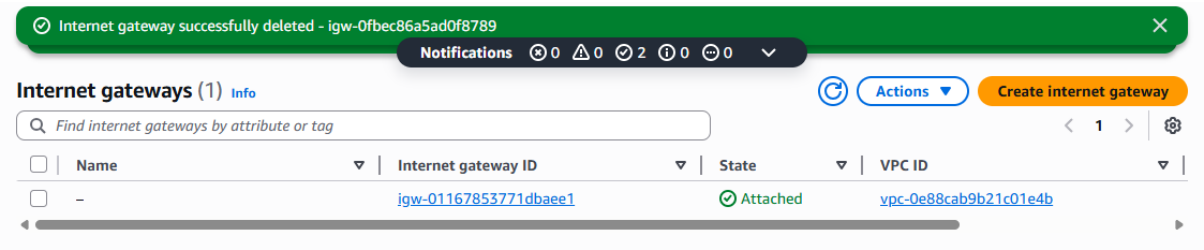
- Now select your internet gateway again and go to “Actions”.
- Click on “Delete internet gateway”.



- Type “delete” and click on “Delete internet gateway”.



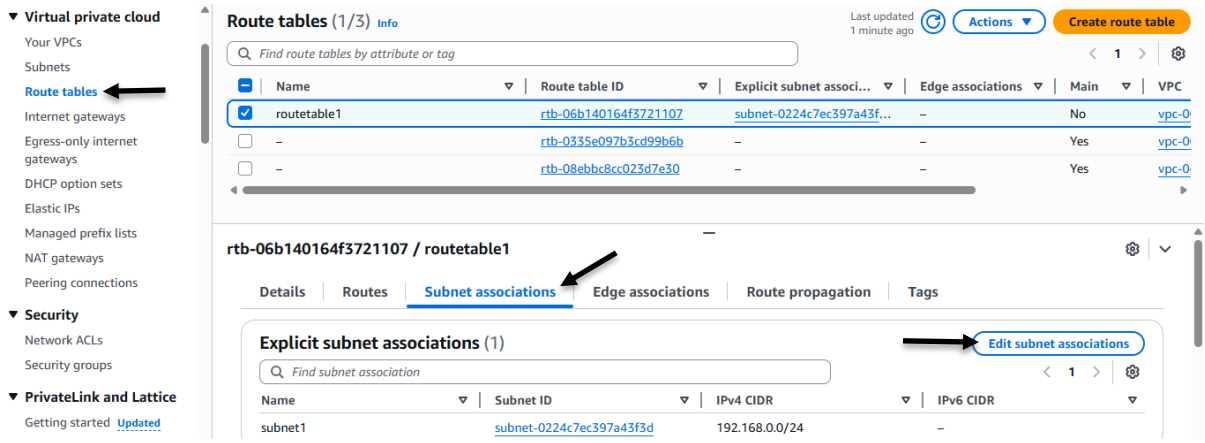
- Your internet gateway is successfully deleted.



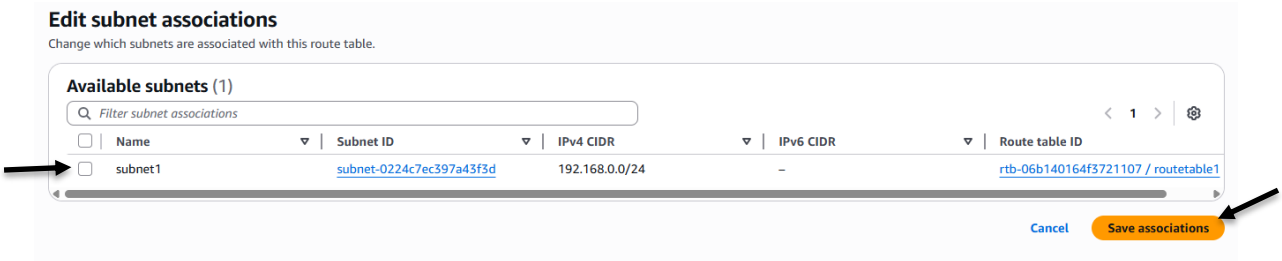
Deleting Route Table:

Step 21:

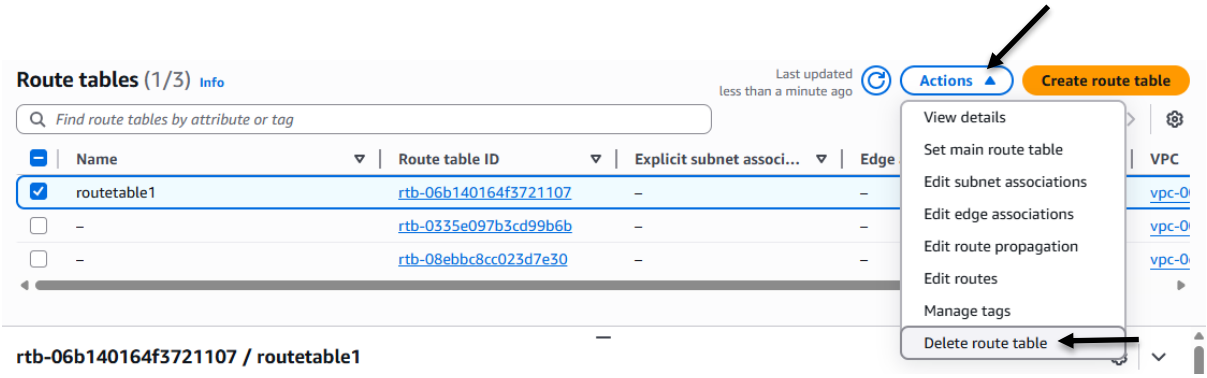
- Now go to “Route tables” under “Virtual private cloud” and select the route table that you have created.
- Go to “Subnet associations” and then click on “Edit subnet associations”.



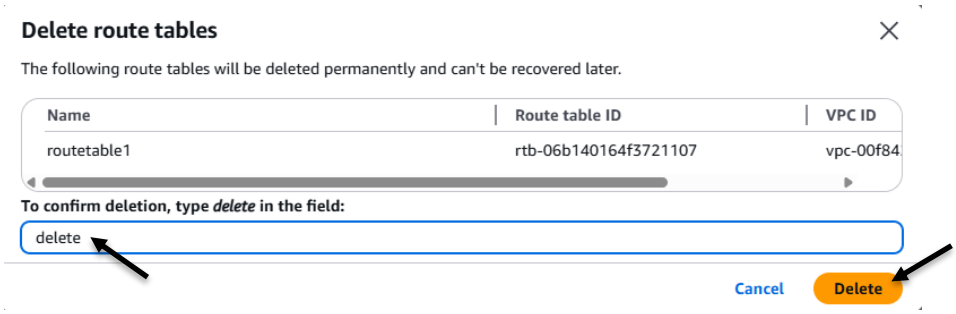
- Remove “subnet1” from “Available subnets”.
- Click on “Save associations”.



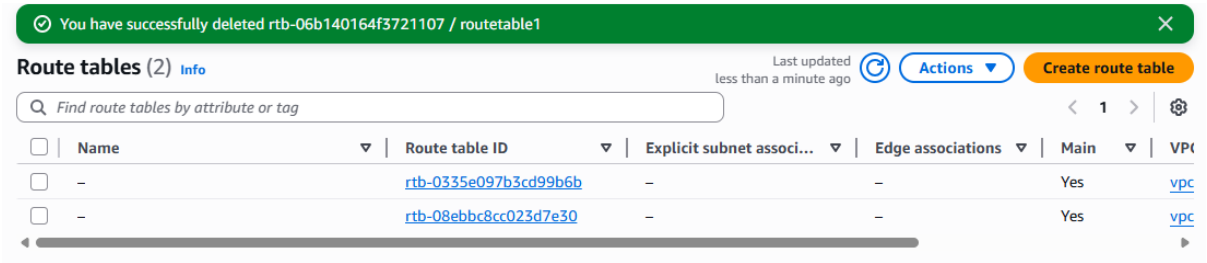
- Now select the route table and go to “Actions”.
- Click on “Delete route table”.



- Type “delete” and click on “Delete” button.



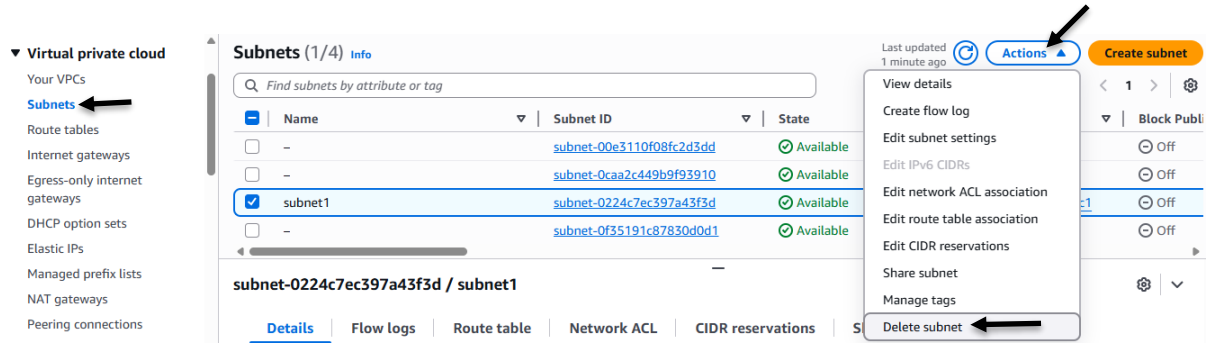
- Your route table is successfully deleted.



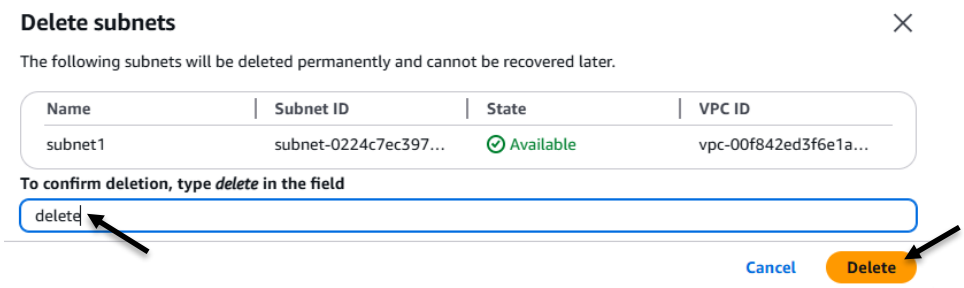
Deleting Subnet:

Step 22:

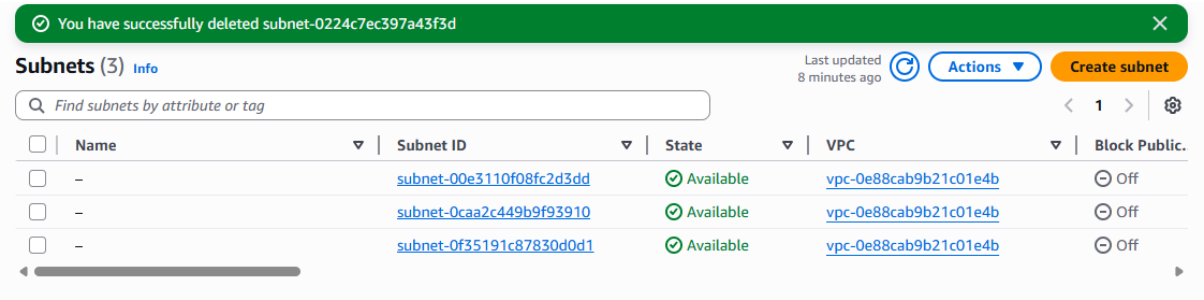
- Go to “Subnets” under “Virtual private cloud” and select the subnet that you have created.
- Click on “Actions” and then click on “Delete subnet”.



- Type “delete” and click on “Delete” button.



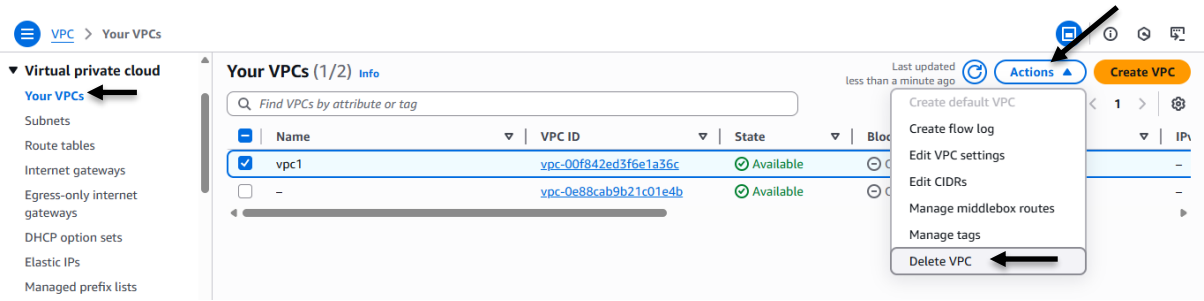
- Your subnet is successfully deleted.



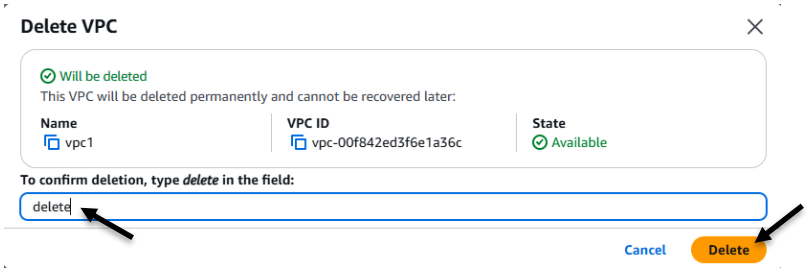
Deleting VPC:

Step 23:

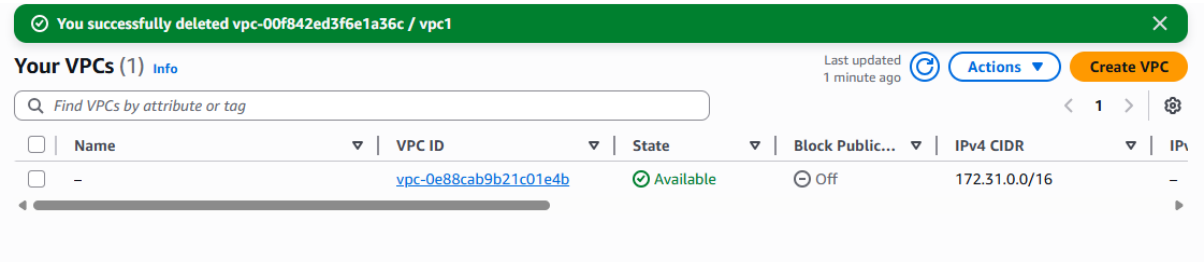
- Go to “Your VPCs” under “Virtual private cloud” and select the VPC that you have created.
- Click on “Actions” and then click on “Delete VPC”.



- Type “delete” and click on “Delete” button.



- Your VPC is also deleted successfully.



Some Important Terms:

“Subnet”

- A “Subnet” is a smaller part of a VPC that divides the network into sections.
- It helps organize and isolate resources within the VPC.
- You can have public and private subnets based on internet access.

“CIDR” (Classless Inter-Domain Routing)

- “CIDR” defines the IP address range for your VPC and subnets.
- It uses a format like “192.168.0.0/16” to show how many IPs are available.
- It helps in managing IP allocation and network size.

“Internet Gateway”

- An “Internet Gateway” allows communication between resources in a VPC and the internet.
- It is attached to the VPC and linked with public subnets.
- Without it, instances cannot send or receive data from the internet.

“Route Table”

- A “Route Table” contains rules (routes) that decide where network traffic goes.
- Each subnet in a VPC must be linked to a route table.
- It helps control traffic flow between subnets and to the internet.

“Security Groups”

- “Security Groups” act like virtual firewalls for your instances.
- They control incoming and outgoing traffic based on rules you define.
- They are stateful, meaning allowed return traffic is automatically permitted.
