

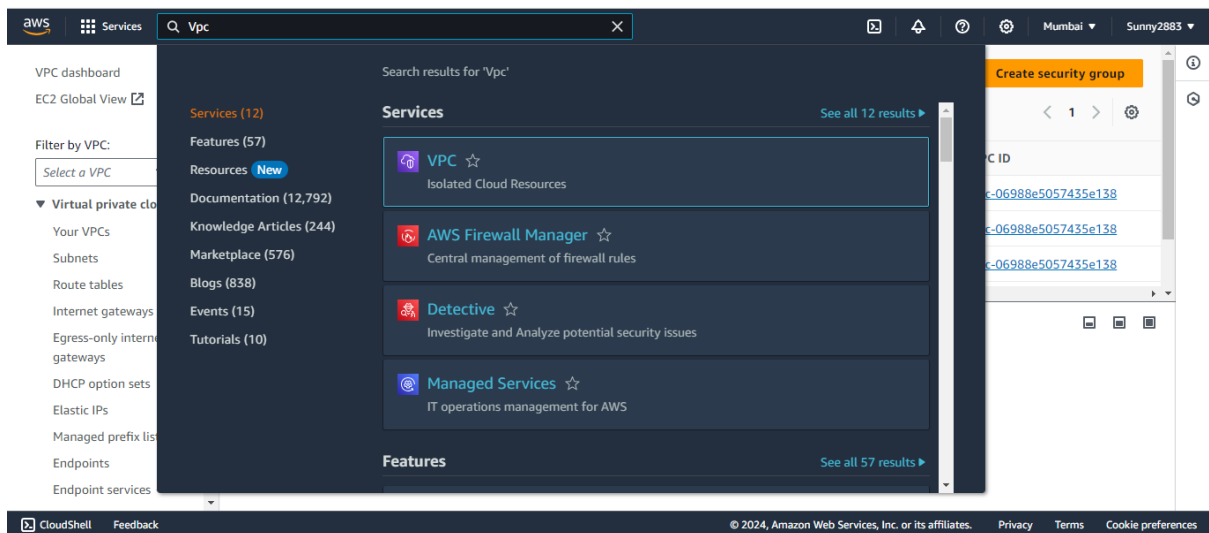
Assignment VPC

Task:1

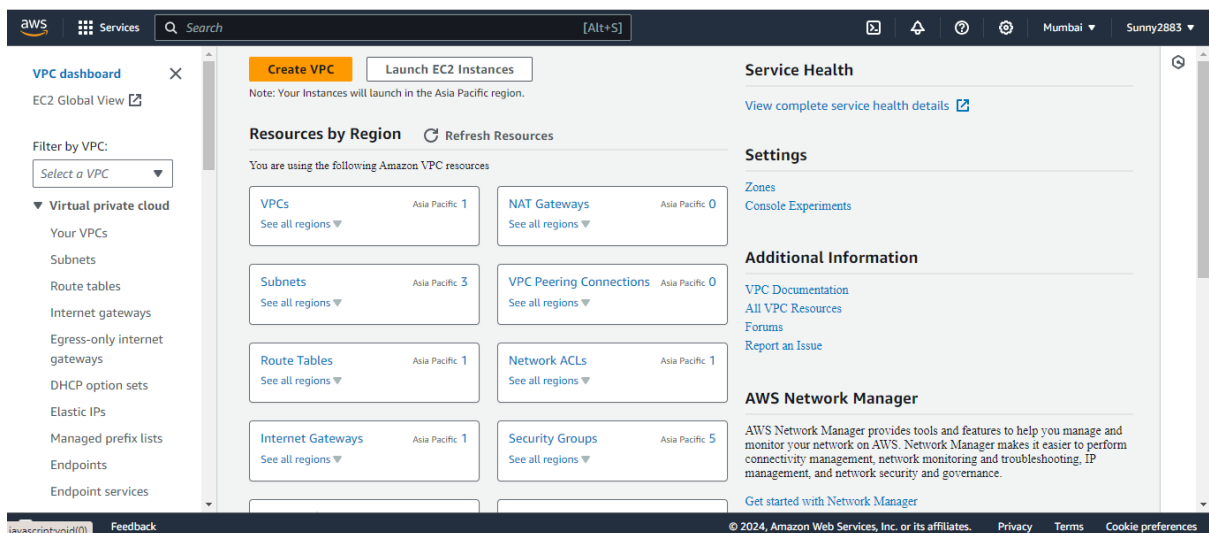
Create a VPC:

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

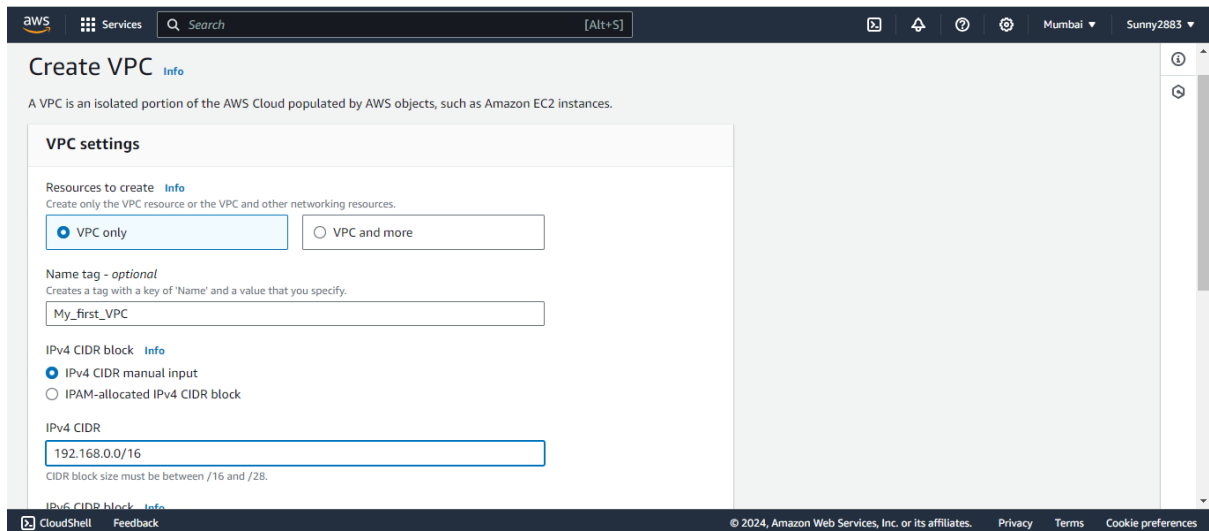
Step1: Go to the "Services" dropdown, search "VPC" .



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.



Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - optional [Info](#)
Creates a tag with a key of 'Name' and a value that you specify.

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

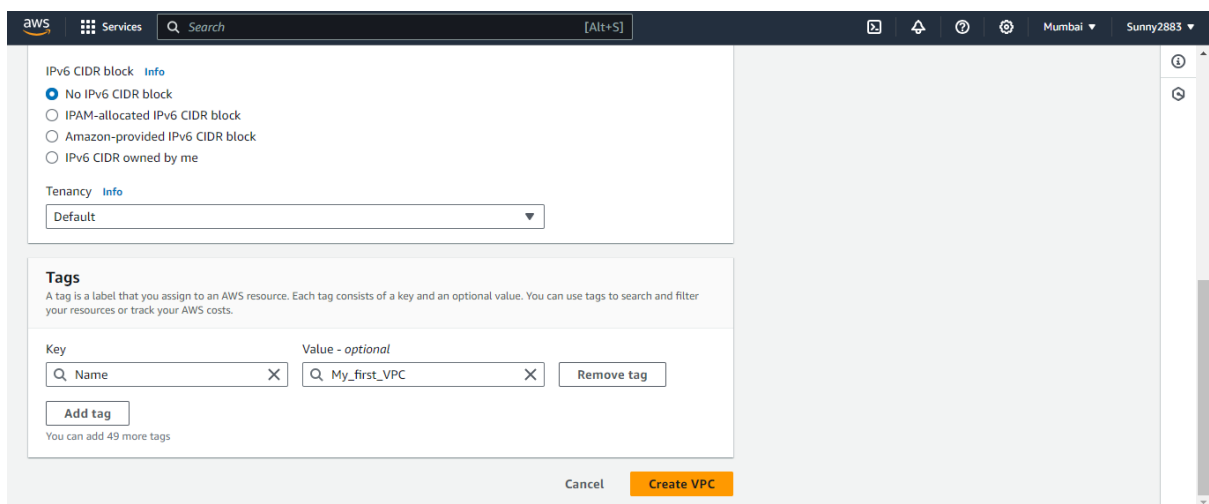
IPv4 CIDR

CIDR block size must be between /16 and /28.

[IPv6 CIDR block](#) [Info](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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



IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

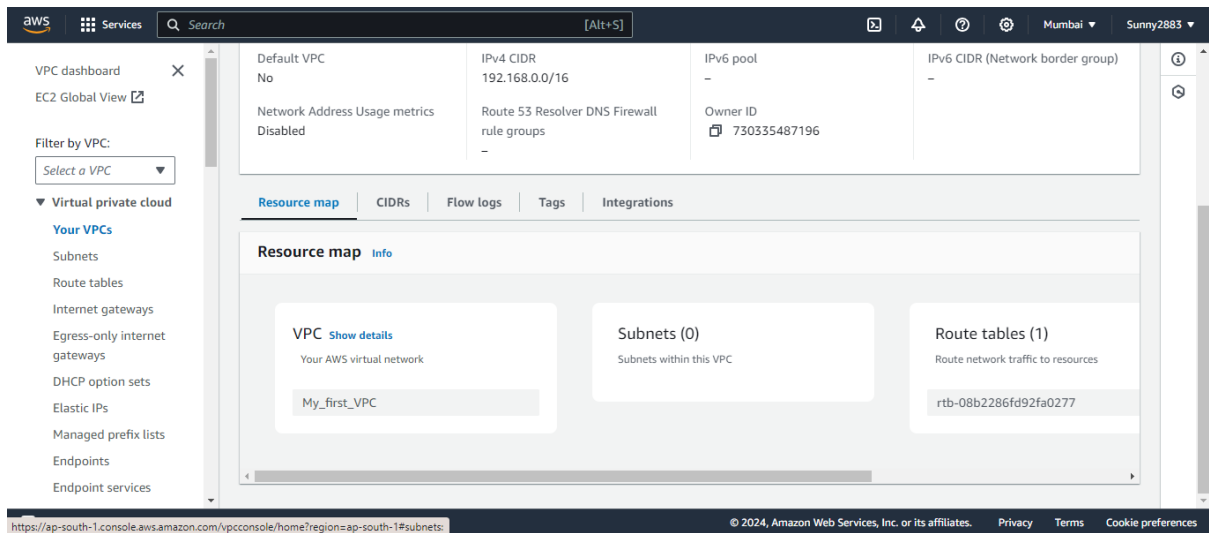
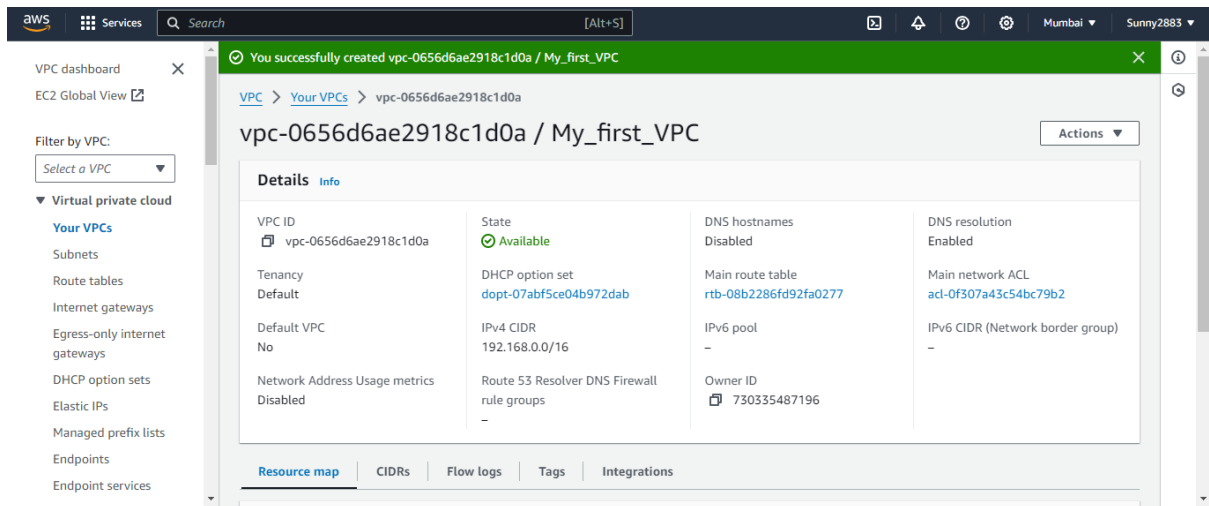
Tenancy [Info](#)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

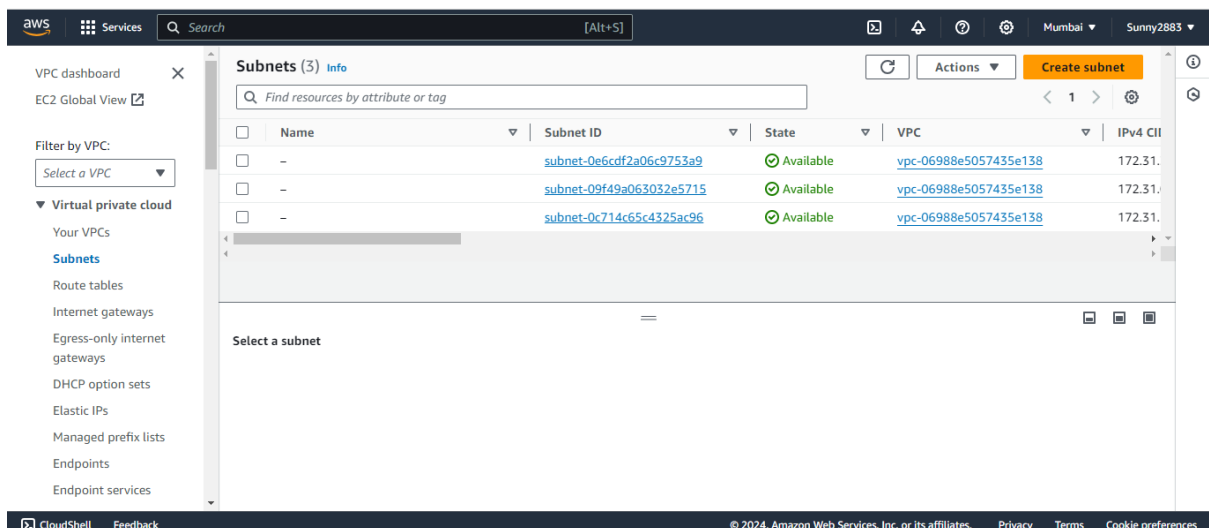
Key **Value - optional**

You can add 49 more tags

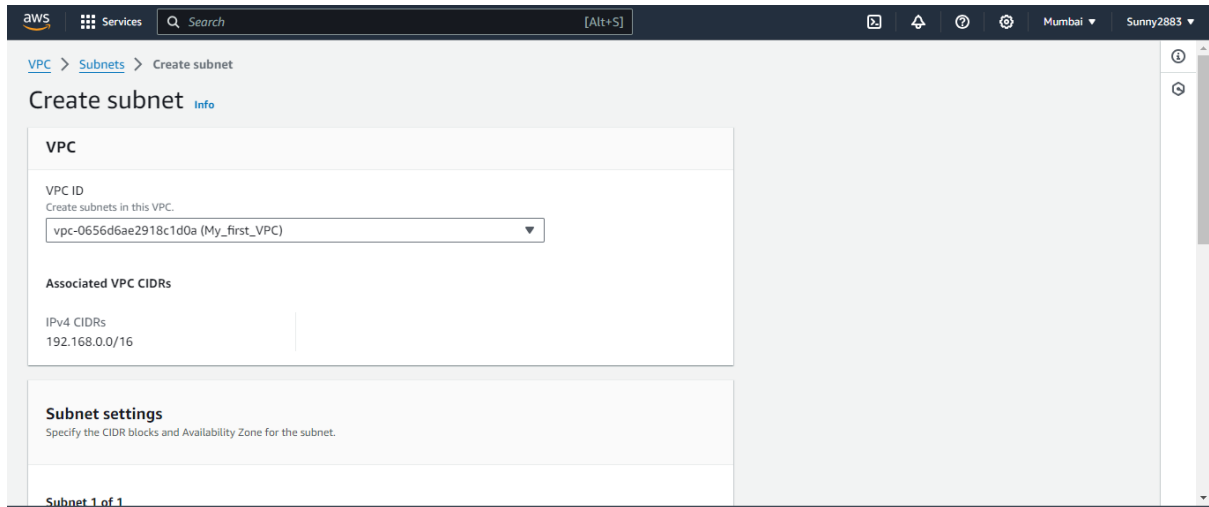
Step5: VPC successfully created.



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

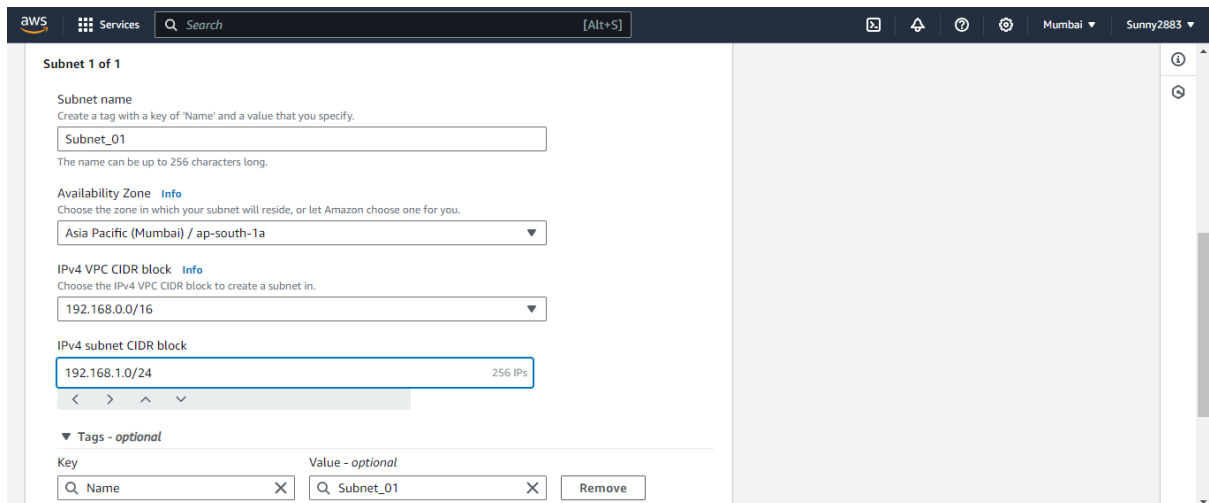


Step7: Choose the VPC in which the subnet will reside.



The screenshot shows the AWS Management Console 'Create subnet' page. The breadcrumb navigation is 'VPC > Subnets > Create subnet'. The page title is 'Create subnet' with an 'Info' link. Under the 'VPC' section, the 'VPC ID' is set to 'vpc-0656d6ae2918c1d0a (My_first_VPC)'. Below it, 'Associated VPC CIDRs' shows 'IPv4 CIDRs' as '192.168.0.0/16'. The 'Subnet settings' section is partially visible, with the instruction 'Specify the CIDR blocks and Availability Zone for the subnet.'

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.



The screenshot shows the 'Subnet 1 of 1' configuration page. The 'Subnet name' is 'Subnet_01'. The 'Availability Zone' is 'Asia Pacific (Mumbai) / ap-south-1a'. The 'IPv4 VPC CIDR block' is '192.168.0.0/16'. The 'IPv4 subnet CIDR block' is '192.168.1.0/24' with a '256 IPs' indicator. The 'Tags' section shows a key 'Name' with value 'Subnet_01'.

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

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.1.0/24 256 IPs

▼ Tags - optional

Key	Value - optional	
Q Name	Q Subnet_01	Remove

Add new tag
You can add 49 more tags.

Remove

Add new subnet

Cancel Create subnet

Step10: Review your subnet configuration.

Subnets (1) [Info](#)

Find resources by attribute or tag

Subnet ID : subnet-013c0000f10df46e8 Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	Subnet_01	subnet-013c0000f10df46e8	Available	vpc-0656d6ae2918c1d0a My...	192.168.1.0/24

Select a subnet

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

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Subnet_02
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1b

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.2.0/24 256 IPs

▼ Tags - optional

Key	Value - optional	
Q Name	Q Subnet_02	Remove

aws Services Search [Alt+S] Mumbai Sunny2883

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.2.0/24 256 IPs

Tags - optional
Key Value - optional
Name Subnet_02 Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet

Cancel Create subnet

aws Services Search [Alt+S] Mumbai Sunny2883

You have successfully created 1 subnet: subnet-07fcf424c6757106f

VPC dashboard EC2 Global View

Filter by VPC: Select a VPC

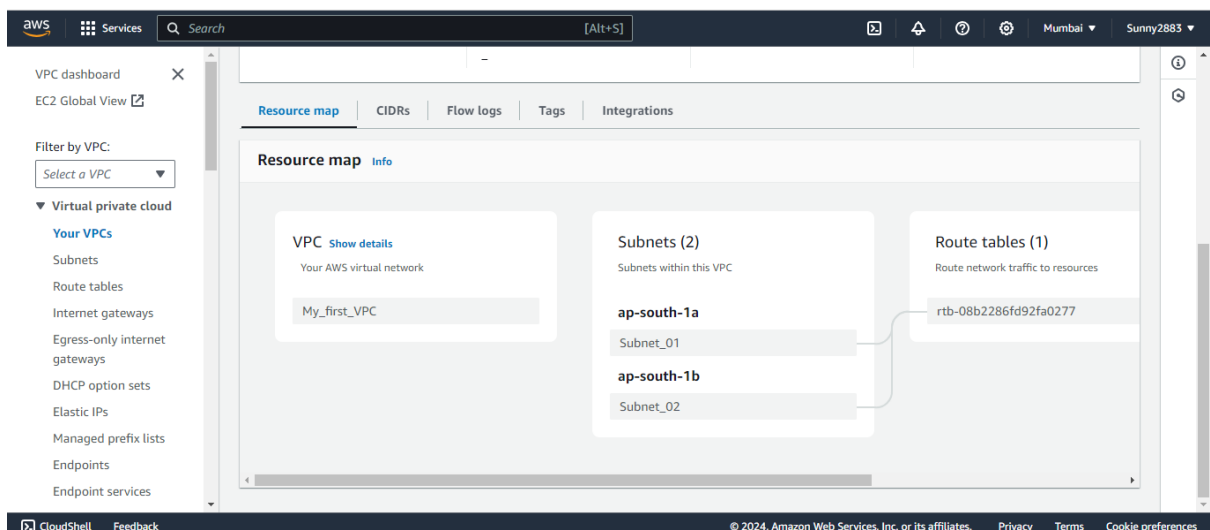
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
NAT option sets

Subnets (1) Info
Find resources by attribute or tag
Subnet ID : subnet-07fcf424c6757106f Clear filters

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	Subnet_02	subnet-07fcf424c6757106f	Available	vpc-0656d6ae2918c1d0a My_...	192.168.2.0/24

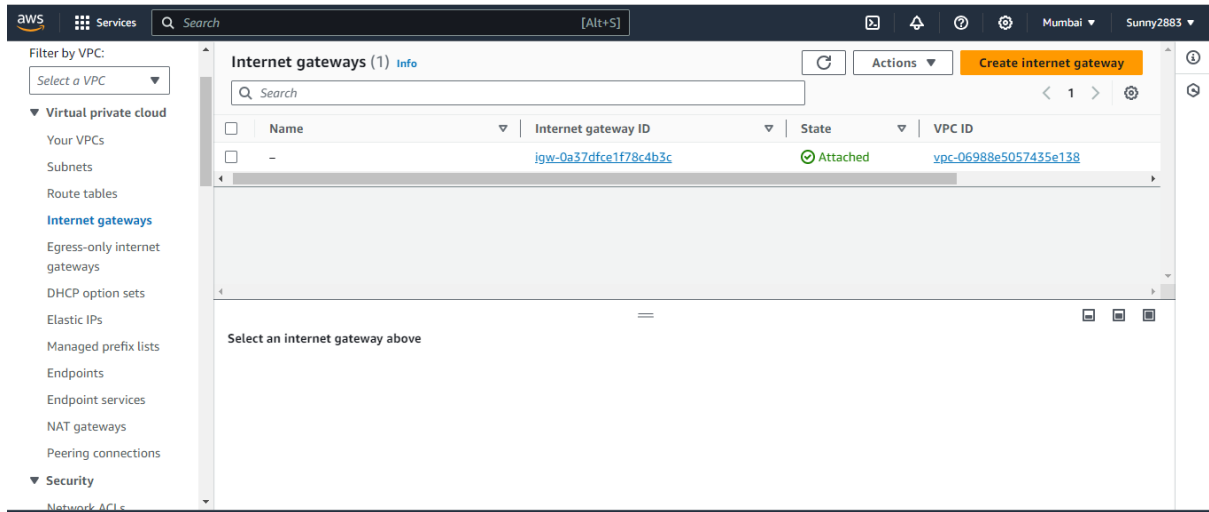
Select a subnet

Step12: Resource map of VPC.

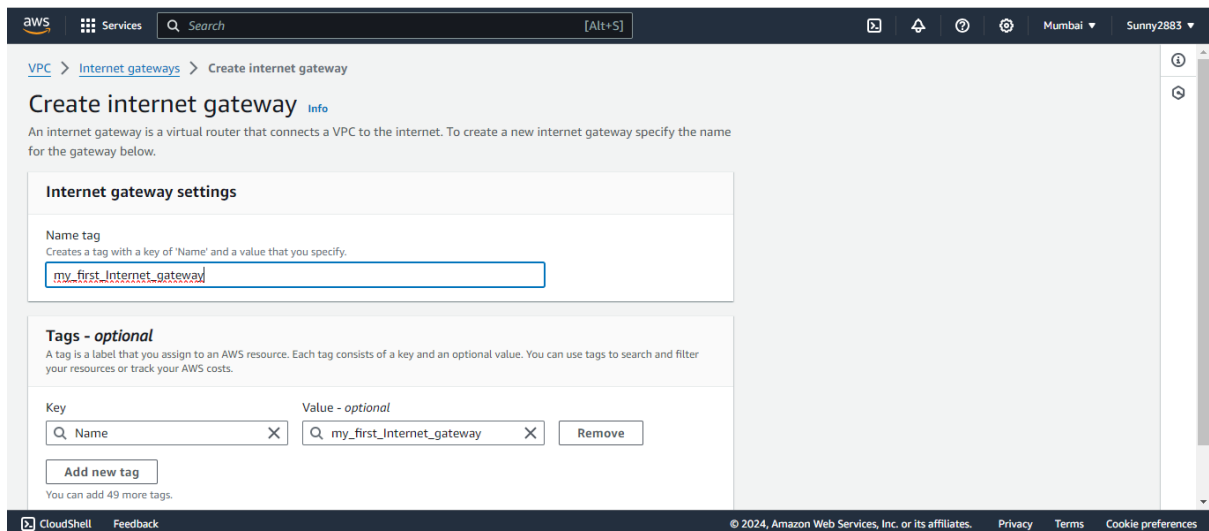


2. Internet Gateway (IGW):

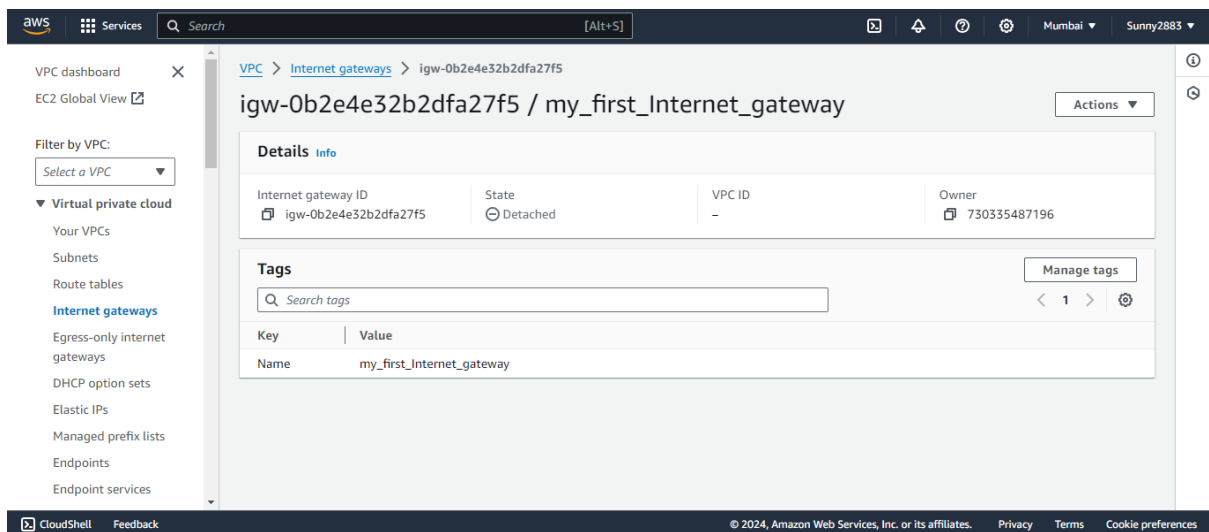
Step1: Go to "Internet Gateways" Section. On the left sidebar, click on "Internet Gateways." Click on the "Create internet gateway" button.



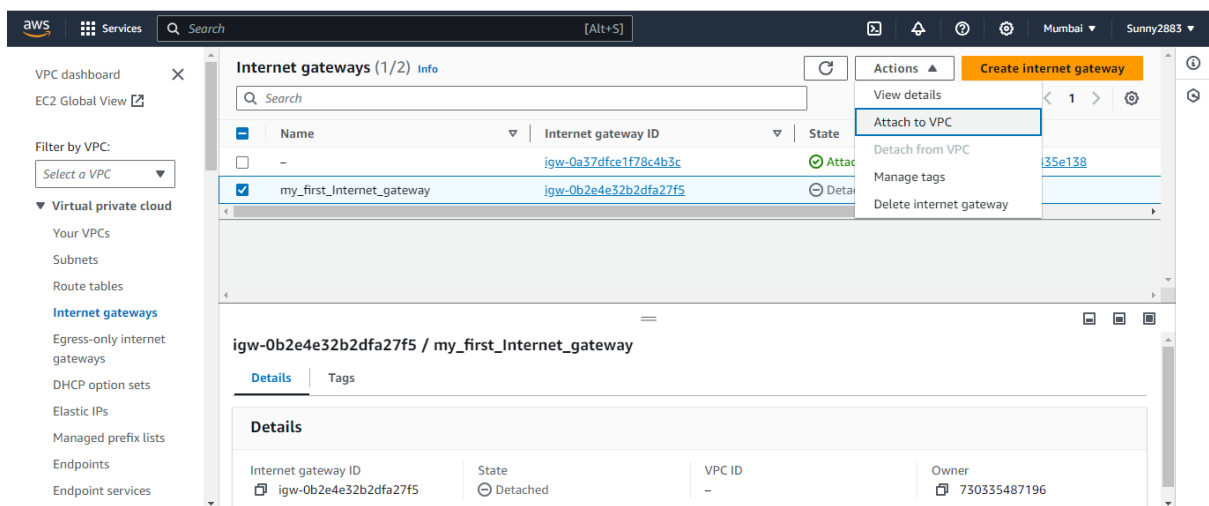
Step2: Provide a name for the internet gateway and create internet gateway.



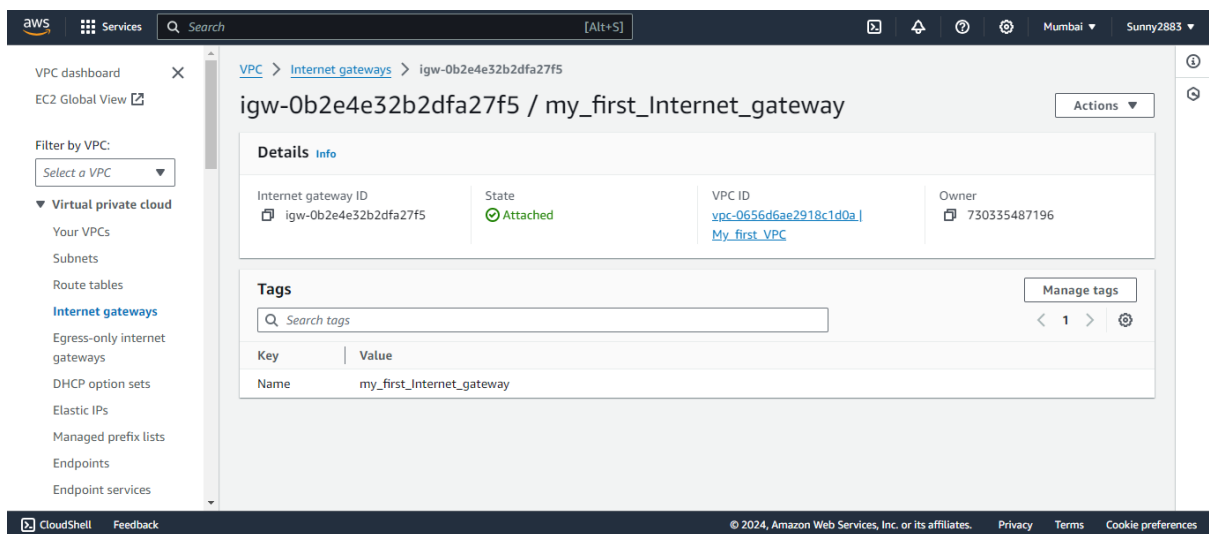
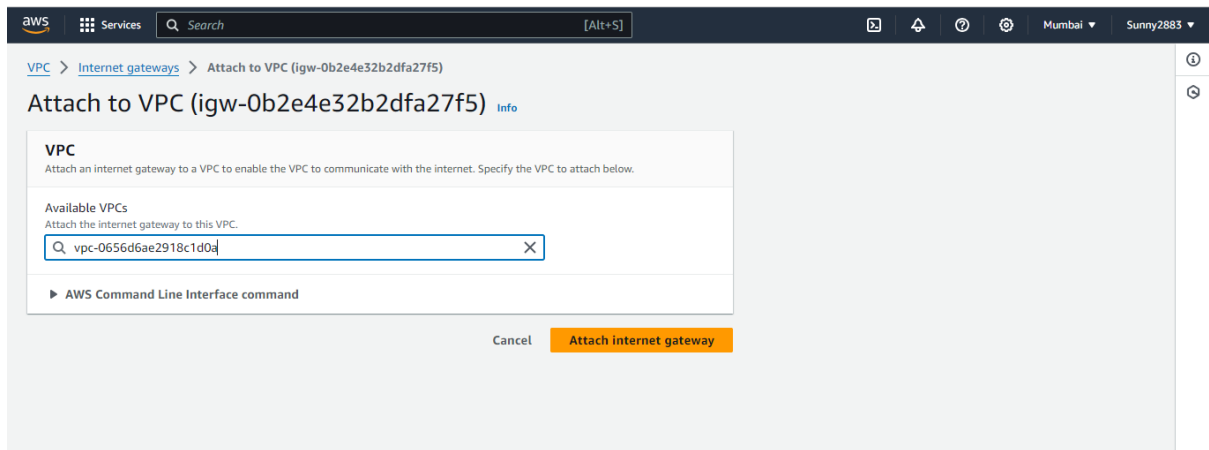
Step3: Configure the details.



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.