

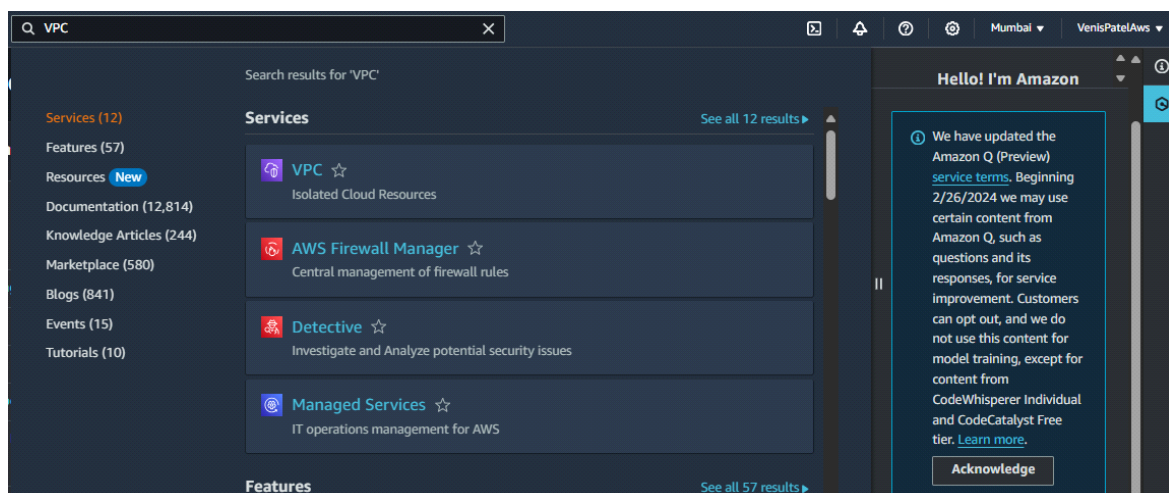
# Assignment VPC

## Task1 : Create a VPC:

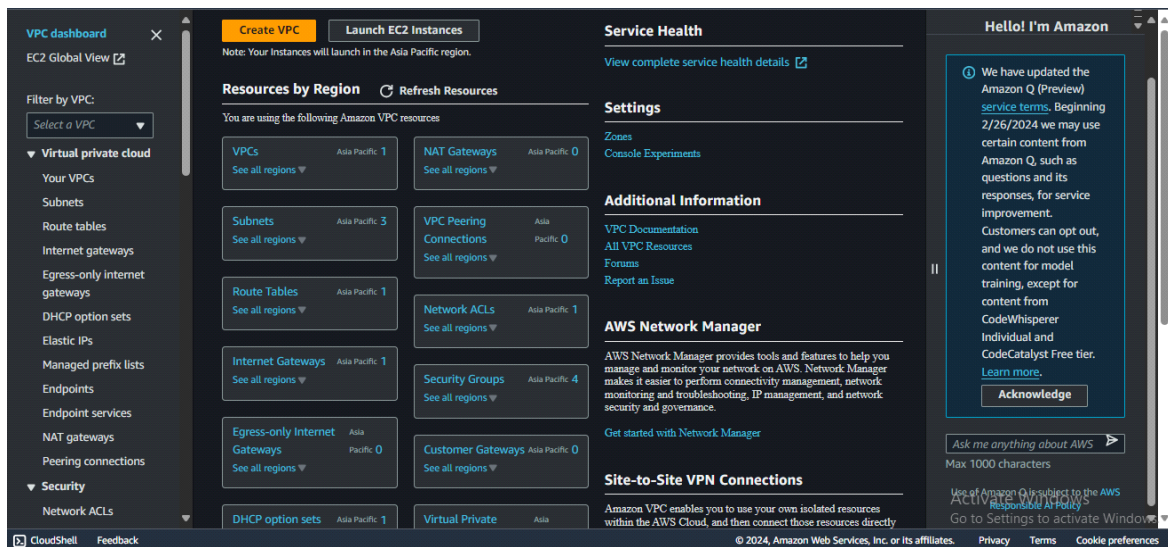
1. Include at least two subnets, each in a different Availability Zone.
2. Internet Gateway (IGW):
3. Do not create NAT gateway but understand how and why it is needed?

### ➤ STEPS:

1. Go to AWS console and search for "VPC" and select VPC isolated cloud services.



## 2. Now select on "Create VPC"



## 3. Give name to VPC as "VenisAwsVPC" and scroll down.



4. Select Number of Availability zones as 2 and select two different AZ's as "ap-south-1-a" and "ap-south-1-b" and keep everything as unchanged and select on create VPC .

**Tenancy** [Info](#)  

Default

**Number of Availability Zones (AZs)** [Info](#)  
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.  

123

**Customize AZs**  
First availability zone  

ap-south-1a

  
Second availability zone  

ap-south-1b

**Number of public subnets** [Info](#)  
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.  

02

**Number of private subnets** [Info](#)  
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.  

024

**Customize subnets CIDR blocks**

**NAT gateways (\$)** [Info](#)  
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway  

NoneIn 1 AZ1 per AZ

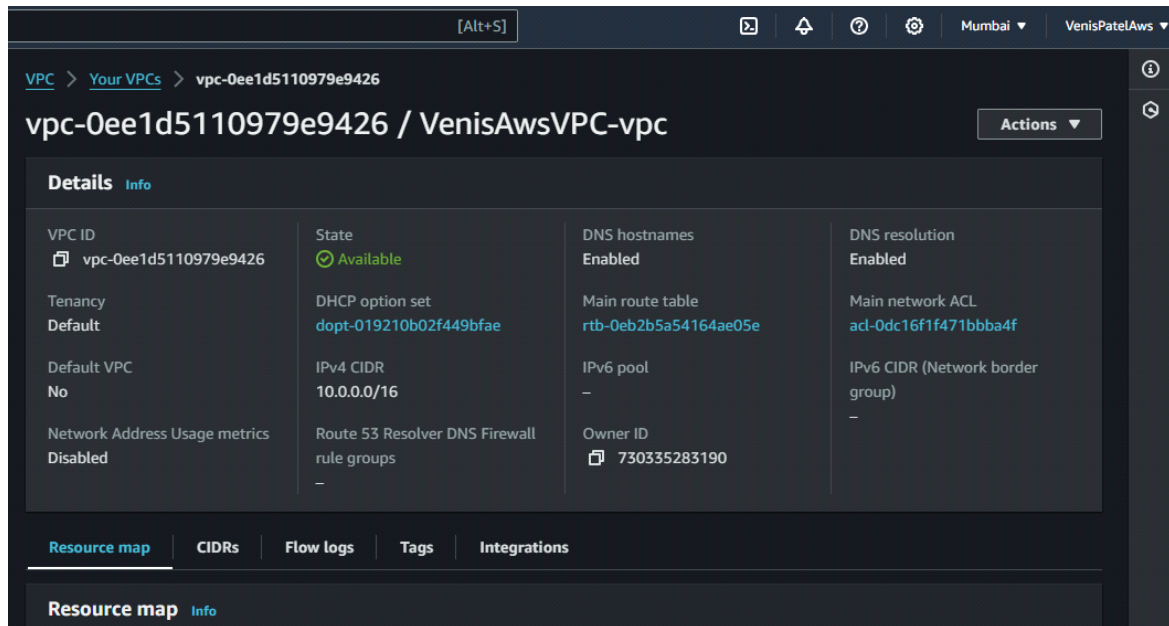
**VPC endpoints** [Info](#)  
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.  

NoneS3 Gateway

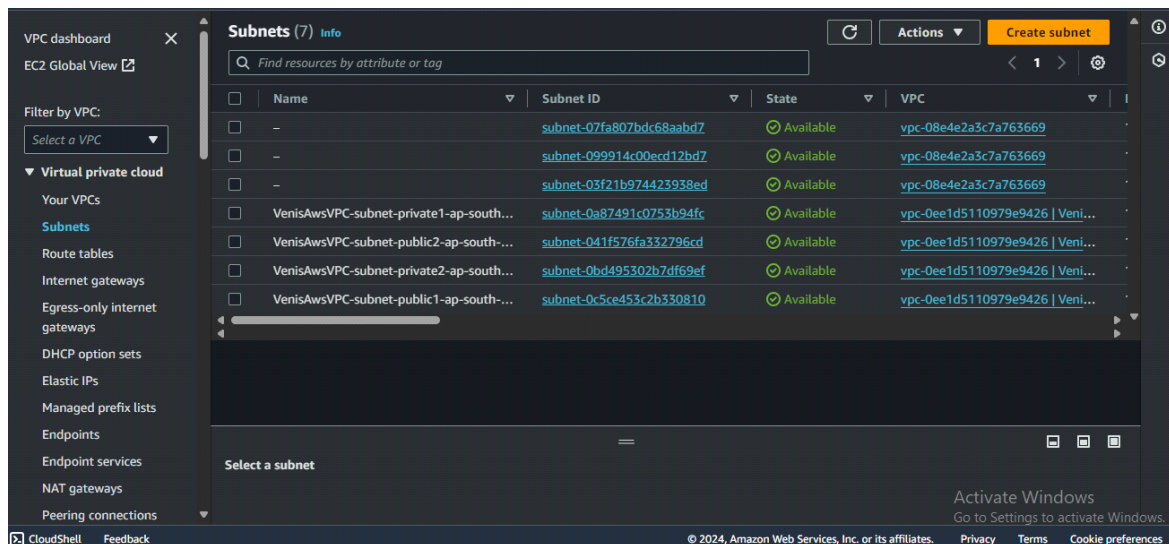
**DNS options** [Info](#)  
☒ Enable DNS hostnames  
☒ Enable DNS resolution

**Additional tags**

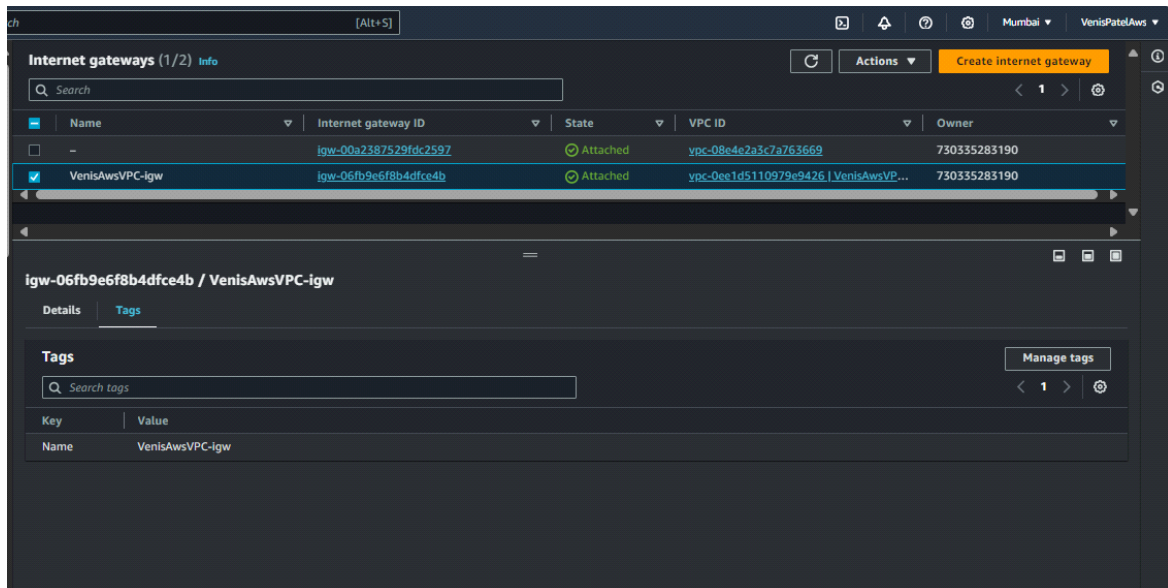
5. Now here we can see that VPC has been created .



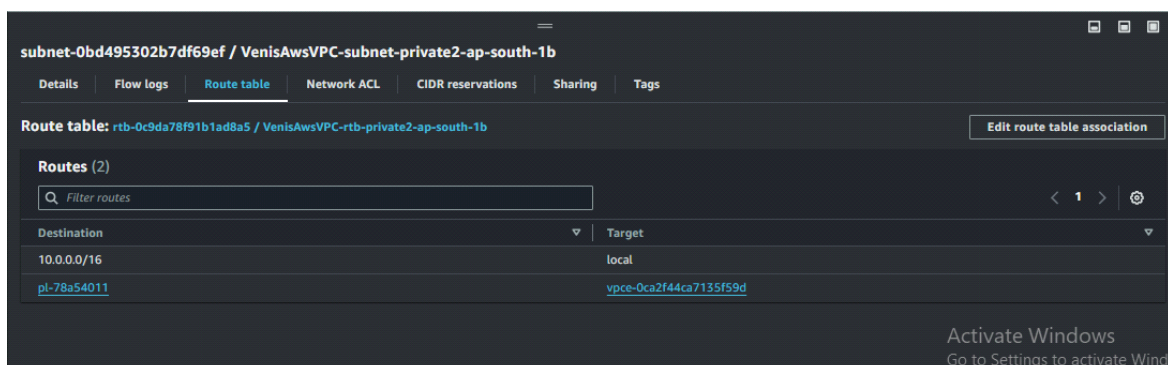
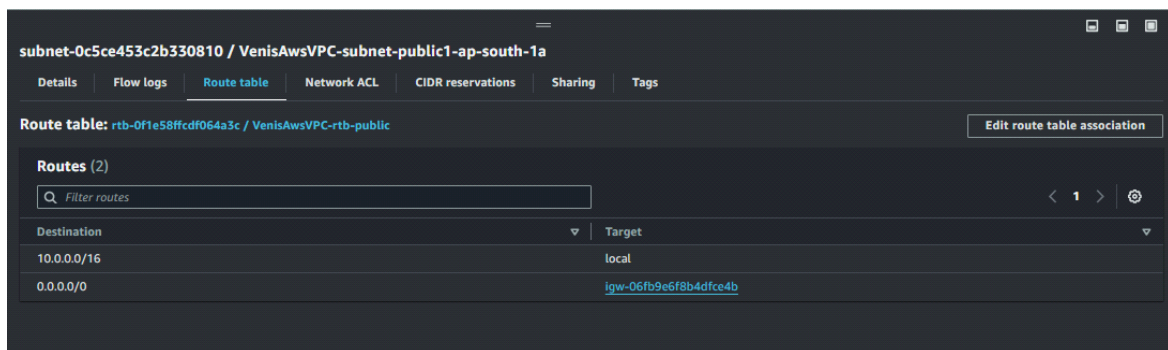
6. Here we can see that subnets have also been created in two different availability zones .



7. Now go to Internet gateway and attach it to VPC .



8. Now for route table here we can see that for public subnet's route table is allowing traffic from everywhere so it would be accessible from anywhere through internet whereas for private subnet's route table , we are not allowing traffic from everywhere so we will not be able to access in future .





9. Now we have to create two instances , one which will be connecting to public subnet and one which will be connecting to priavate subnet , So first of lets create for public .

➤ Give name to the instance and select required Quick start .

Name  
VenisPatelVpcPublicInstance [Add additional tags](#)

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE L

Browse more AMIs  
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-06b72b3b2a773be2b (64-bit (x86)) / ami-05e9973de0eba6123 (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description  
Amazon Linux 2 Kernel 5.10 AMI 2.0.20240131.0 x86\_64 HVM gp2

10. Now go in Advanced networking setting and select VPC which we created and select subnet public1 from south-1a Availability zone, Assign Auto-assign public Ip as "enable" and select on create new security group and give name to that.

▼ **Network settings** [Info](#)

VPC - required [Info](#)

vpc-0ee1d5110979e9426 (VenisAwsVPC-vpc)  
10.0.0.0/16

Subnet [Info](#)

subnet-0c5ce453c2b330810 VenisAwsVPC-subnet-public1-ap-south-1a  
VPC: vpc-0ee1d5110979e9426 Owner: 730335283190  
Availability Zone: ap-south-1a IP addresses available: 4091 CIDR: 10.0.0.0/20

Create new subnet

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required

VpcPublicInstanceSecurityGroup

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-:/()#,@[]+=&:!\$\*

Description - required [Info](#)

launch-wizard-3 created 2024-02-12T05:46:14.109Z

Inbound Security Group Rules

Security group rule 1 (All, All, 0.0.0.0/0) [Remove](#)

Type [Info](#) Protocol [Info](#) Port range [Info](#)

11. Now in inbound security rules , Select all traffic and source as Anywhere to get accessible from internet .

Security group name - *required*

VpcPublicInstanceSecurityGroup

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=&:!\$\*

Description - *required* | [Info](#)

launch-wizard-3 created 2024-02-12T05:46:14.109Z

Inbound Security Group Rules

▼ Security group rule 1 (All, All, 0.0.0.0/0) Remove

Type   <a href="#">Info</a>	Protocol   <a href="#">Info</a>	Port range   <a href="#">Info</a>
All traffic ▼	All	All
Source type   <a href="#">Info</a>	Source   <a href="#">Info</a>	Description - <i>optional</i>   <a href="#">Info</a>
Anywhere ▼	<input type="text" value="Add CIDR, prefix list or security group"/> 0.0.0.0/0 ✕	<input type="text" value="e.g. SSH for admin desktop"/>

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

12. Now here we can see that our instance has been created , Now select that instance and click on connect .

Instances (1/5) | [Info](#)

Any state

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	VenisAwsVPCP...	i-02744a17277d25023	Running	t2.micro	Initializing	<a href="#">View alarms +</a>	ap-south-1a	ec2-43-205-206-129.ap...
<input type="checkbox"/>	VenisPatelAws...	i-0ac8e9b67b89e484b	Stopped	t2.micro	-	<a href="#">View alarms +</a>	ap-south-1a	-
<input type="checkbox"/>	AwsInstance	i-0f079c7b827f9d1fc	Stopped	t2.micro	-	<a href="#">View alarms +</a>	ap-south-1a	-

Instance: i-02744a17277d25023 (VenisAwsVPCPublic)

Details | Status and alarms [New](#) | Monitoring | Security | Networking | Storage | Tags

▼ Instance summary | [Info](#)

Instance ID i-02744a17277d25023 (VenisAwsVPCPublic)	Public IPv4 address 43.205.206.129 <a href="#">Open address</a>	Private IPv4 addresses 10.0.5.95
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-43-205-206-129.ap-south-1.compute.amazonaws.com <a href="#">Open address</a>
Hostname type IP name: ip-10-0-5-95.ap-south-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-0-5-95.ap-south-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations <a href="#">Learn more</a>
Auto-assigned IP address 43.205.206.129 [Public IP]	VPC ID vpc-0ee1d5110979e9426 (VenisAwsVPC-vpc) <a href="#">Open address</a>	

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





15. Now go to Network settings and select VPC that we created and select subnet as private-2 which is from different Availability zone as "south-1b" and disable Auto-assign public Ip . Now create new security group , which will not allow all the traffic to access out instance .

The screenshot shows the AWS Network settings console. The 'VPC' dropdown is set to 'vpc-0ee1d5110979e9426 (VenisAwsVPC-vpc)'. The 'Subnet' dropdown is set to 'subnet-0bd495302b7df69ef VenisAwsVPC-subnet-private2-ap-south-1b'. The 'Auto-assign public IP' is set to 'Disable'. Under 'Firewall (security groups)', the 'Create security group' button is selected. The 'Security group name' is 'launch-wizard-4'. The 'Description' is 'launch-wizard-4 created 2024-02-12T06:07:18.598Z'. Under 'Inbound Security Group Rules', a rule is shown for 'ssh' on 'TCP' port '22' from 'My IP' (110.226.124.147/32).

**Network settings** Info

VPC - required Info  
vpc-0ee1d5110979e9426 (VenisAwsVPC-vpc)  
10.0.0.0/16

Subnet Info  
subnet-0bd495302b7df69ef VenisAwsVPC-subnet-private2-ap-south-1b  
VPC: vpc-0ee1d5110979e9426 Owner: 730335283190  
Availability Zone: ap-south-1b IP addresses available: 4090 CIDR: 10.0.144.0/20  
Create new subnet

Auto-assign public IP Info  
Disable

Firewall (security groups) Info  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.  
Create security group Select existing security group

Security group name - required  
launch-wizard-4  
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./[]+=&:~!\$\*

Description - required Info  
launch-wizard-4 created 2024-02-12T06:07:18.598Z

Inbound Security Group Rules  
Security group rule 1 (TCP, 22, 110.226.124.147/32) Remove

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Name Info	Description - optional Info
My IP	Add CIDR, prefix list or security group 110.226.124.147/32	e.g. SSH for admin desktop

16. Now select on created instance and click on connect , Here we can see that we are not able to connect to our instance because it has been created in private subnet.

