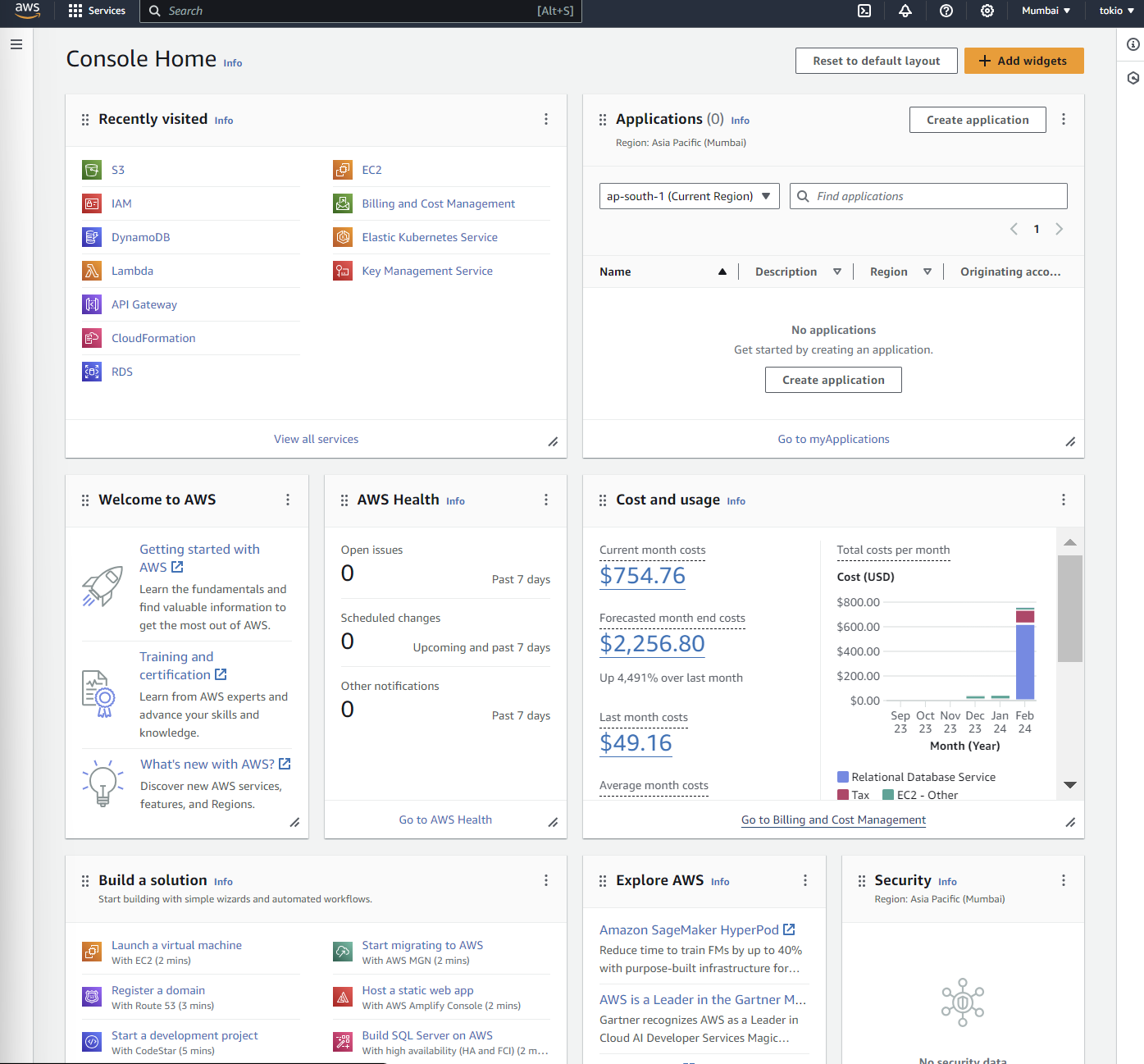
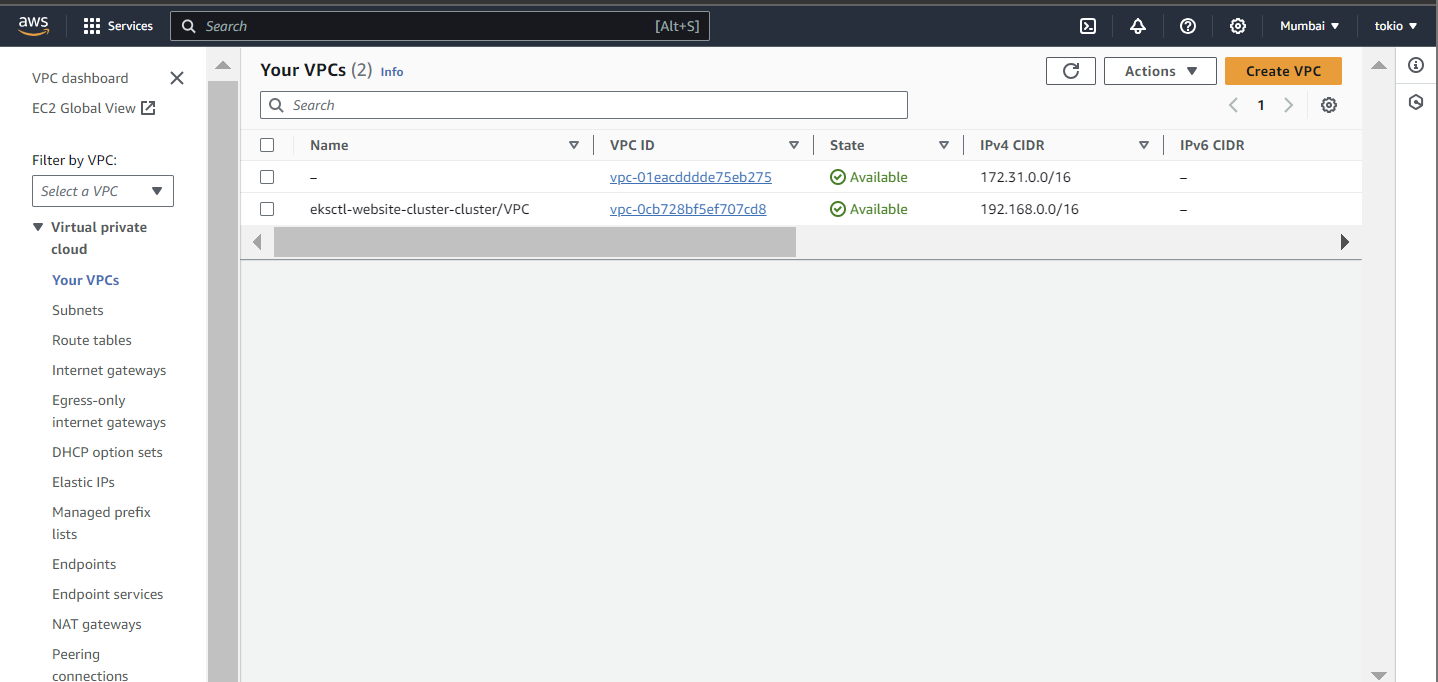
**Experiment-3**

**Problem Statement-** Create a Virtual Private Cloud within AWS infrastructure.

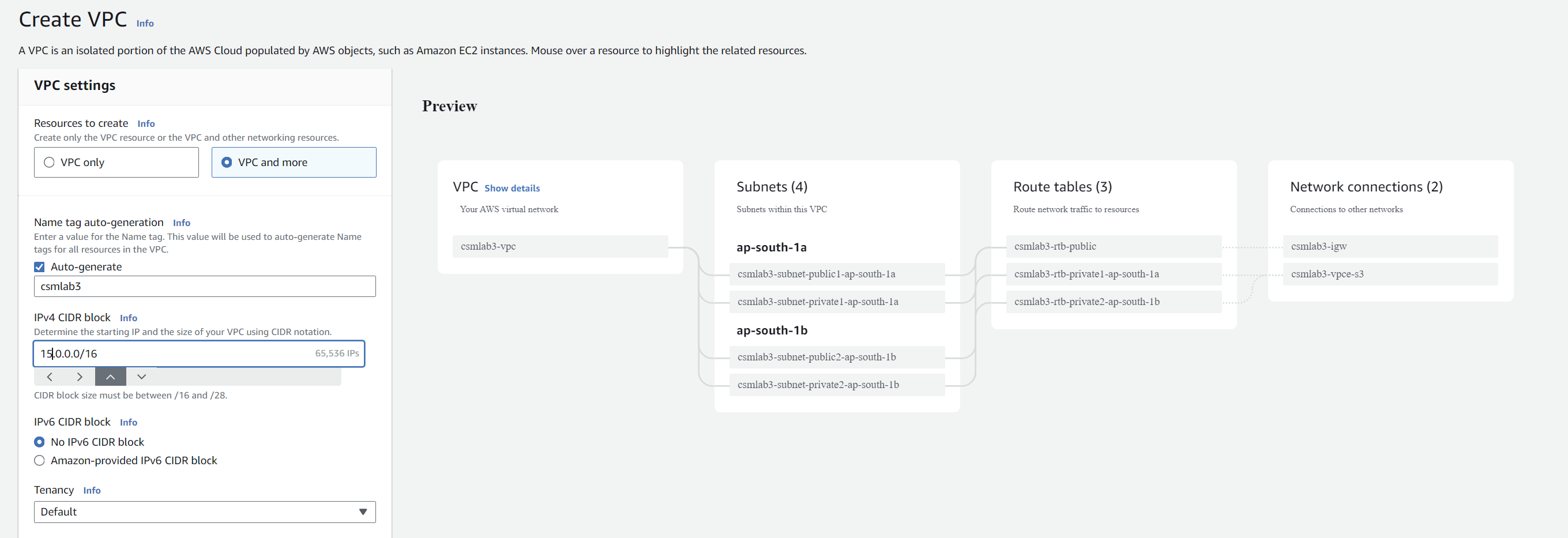
**Step-1:** Go to AWS console and search for “VPC”.

****

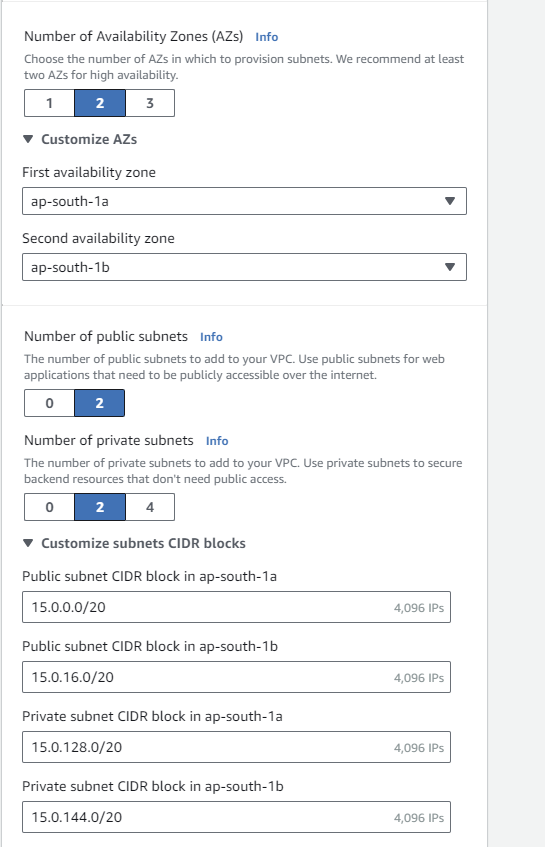
**Step-2:** Now click on “Create VPC” at the top right side.

****

**Step-3:** Now while creating VPC, we have been given two options: either we can configure subnets, availability zones etc by ourselves or we can just create the VPC and rest of the things will be created by default. Here I am customizing everything.

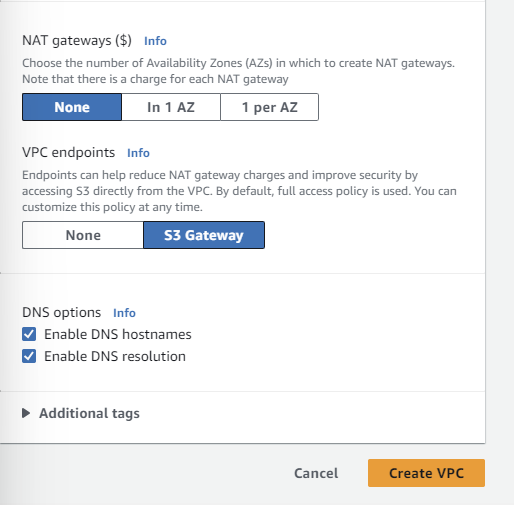
****

**Step-4:** After naming and choosing the CIDR block for IPv4, choose the number of availability zones, private and public subnets that you want.

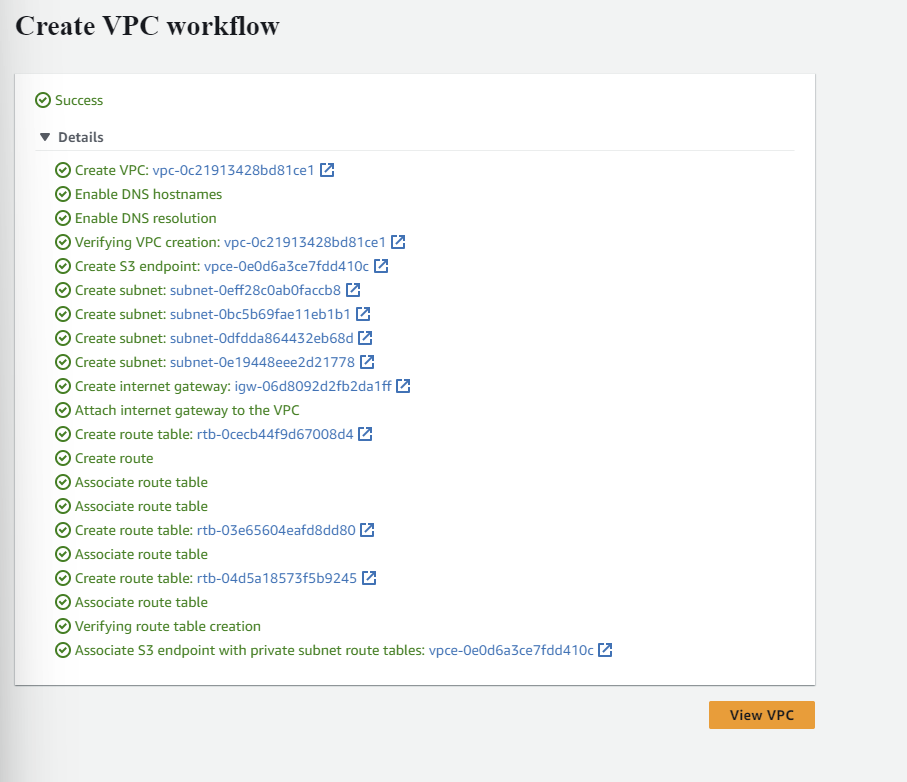
****

**Step-5:** Now chose the availability zone for you NAT gateway and VPC endpoint if you want.

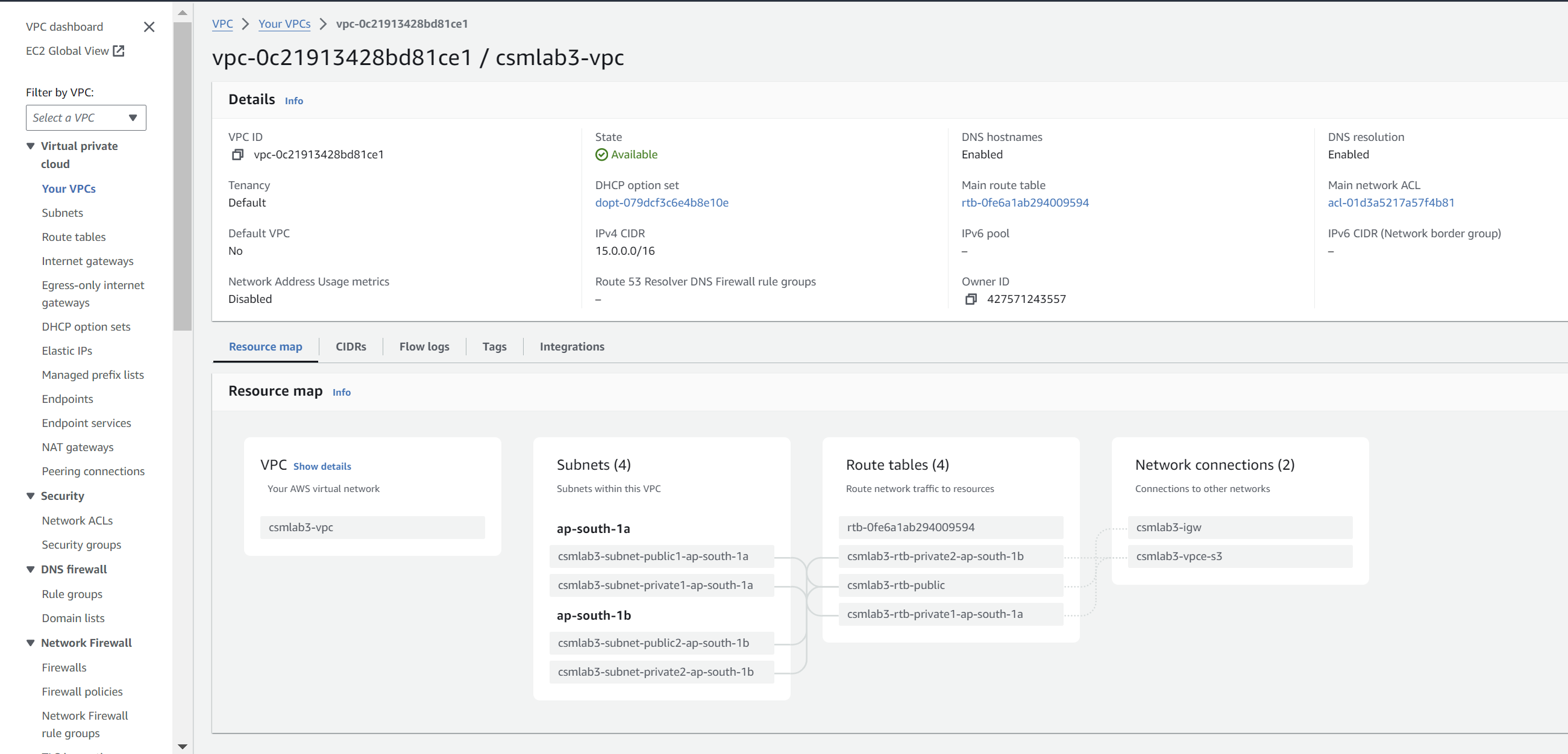
* **NAT Gateways** in AWS allow resources in private subnets to access the public internet for tasks like software updates. By creating a NAT Gateway in a public subnet and configuring routing, resources in private subnets can securely connect to the internet without going through the public internet gateway.
* **VPC Endpoints** provide a private connection between resources in your VPC and AWS services like S3, bypassing the need to access the public internet. This ensures secure and efficient communication with AWS services without exposing traffic to the broader internet.

****

**Step-6:** Then click on “Create VPC”.

****

**Step-7:** The VPC is created. We can click on the View VPC to see it

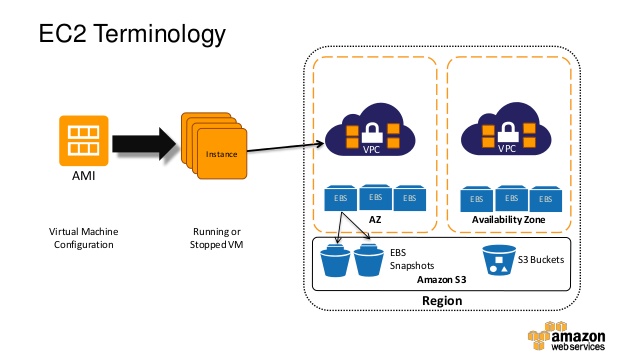
****

**Questions**

**Q1. What is EC2 in AWS? What are the key features of EC2 in AWS?**

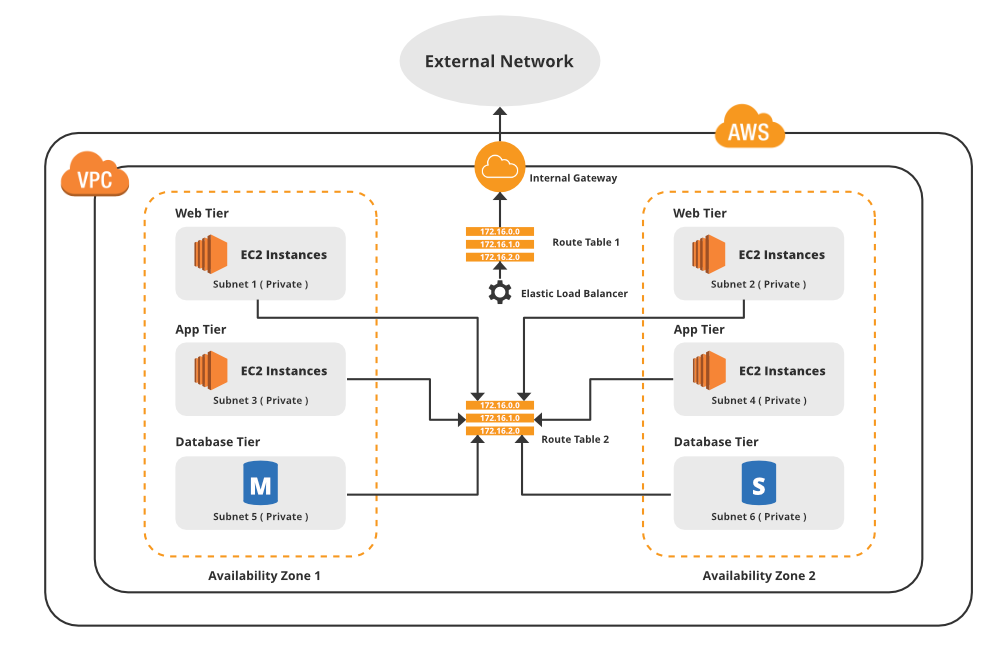
**Ans-** EC2, or Elastic Compute Cloud, is a core web service provided by Amazon Web Services (AWS) that enables users to rent virtual servers and run applications on the cloud. EC2 instances can be easily scaled up or down based on demand, allowing users to dynamically adjust their compute resources. Some key features of EC2 include:

* **Scalability:** EC2 allows users to scale their compute capacity vertically by upgrading to instances with more powerful specifications or horizontally by adding more instances to handle increased workload.
* **Flexibility:** Users have the flexibility to choose from a wide range of instance types with varying combinations of CPU, memory, storage, and networking capabilities to meet the specific requirements of their applications.
* **Cost-Effectiveness:** EC2 offers various pricing options such as On-Demand Instances, Reserved Instances, and Spot Instances, allowing users to optimize costs based on usage patterns and workload characteristics.
* **Integration:** EC2 seamlessly integrates with other AWS services like Elastic Block Store (EBS), Amazon Simple Storage Service (S3), Auto Scaling, and Elastic Load Balancing (ELB), enabling users to build highly scalable and resilient architectures.



**Q2. What does VPC stand for in AWS?**

**Ans-**VPC stands for Virtual Private Cloud. It is a logically isolated section of the AWS cloud where users can launch AWS resources in a virtual network that closely resembles a traditional network environment. VPC allows users to define their own IP address range, create subnets, configure route tables, and control inbound and outbound traffic using security groups and network access control lists (NACLs).



**Q3. Why is EC2 important in AWS?**

**Ans-**EC2 plays a crucial role in AWS as it provides the foundational infrastructure for running various types of applications in the cloud. Its importance stems from several factors:

* **Scalability:** EC2 allows users to scale their compute resources up or down quickly and efficiently to accommodate changing workloads.
* **Flexibility:** Users have the flexibility to choose from a wide selection of instance types and configurations to meet the specific requirements of their applications.
* **Cost-Effectiveness:** EC2 offers flexible pricing options, enabling users to optimize costs based on their usage patterns and budget constraints.
* **Integration:** EC2 seamlessly integrates with other AWS services, allowing users to build complex and scalable architectures that leverage the full power of the AWS ecosystem.

**Q4. What is the primary purpose of creating subnets within a VPC?**

**Ans-**Subnets within a VPC serve several purposes:

* **Resource Segregation:** Subnets allow users to logically segregate resources within the VPC, making it easier to manage and apply security policies.
* **High Availability:** By deploying resources across multiple subnets in different Availability Zones (AZs), users can achieve high availability and fault tolerance for their applications.
* **Traffic Isolation:** Subnets can be used to isolate different types of traffic or applications within the VPC, providing better control over network communication.
* **Routing Control:** Each subnet can have its own route table, allowing users to control the routing of traffic to and from resources within the subnet.

**Q5. Can a VPC span multiple AWS regions?**

**Ans-**No, a VPC is confined to a single AWS region and cannot span multiple regions. However, resources within a VPC can communicate with resources in other regions using inter-region VPC peering or VPN connections.

**Q6. How does the concept of Availability Zone relate to VPCs? Can resources in one availability zone communicate with another resource in another availability zone within the same VPC?**

**Ans-**Availability Zones (AZs) are isolated locations within an AWS region that are engineered to be independent of each other in terms of power, cooling, and network connectivity. When creating a VPC, users can deploy subnets across multiple AZs within the same region for high availability and fault tolerance.

Resources deployed in different AZs within the same VPC can communicate with each other over the internal network using their private IP addresses. AWS ensures low-latency and high-bandwidth connectivity between resources in the same VPC, regardless of their location within the region.

**Q7. How is internet connectivity achieved within a VPC?**

**Ans-**Internet connectivity within a VPC can be achieved by attaching an Internet Gateway (IGW) to the VPC. An IGW serves as a gateway for traffic destined for the internet, allowing instances within the VPC to communicate with resources on the internet and vice versa. Additionally, public-facing instances can be assigned public IP addresses and route table entries to direct internet-bound traffic through the IGW.

**Q8. What is the significance of a route table in a VPC? What is the difference between public, private, and elastic IP addresses?**

**Ans-**A route table in a VPC controls the routing of traffic within the VPC. It determines how traffic is directed between subnets, internet gateways, virtual private gateways, and other network interfaces. Each subnet in a VPC is associated with a route table, which defines the rules for routing traffic to and from the subnet.

Public IP addresses are globally unique addresses assigned to instances that are directly accessible from the internet. Private IP addresses are assigned to instances within a VPC for internal communication and are not routable over the internet. Elastic IP addresses (EIPs) are static IP addresses that can be dynamically allocated to instances and associated with their network interfaces. Unlike public IP addresses, EIPs can be remapped to different instances, making them suitable for scenarios where instances need to be replaced or restarted without changing their public IP address.

**Q9. How can one securely access resources with private IP addresses within a virtual private cloud?**

Securely accessing resources with private IP addresses within a VPC can be achieved through various methods:

* **VPN Connections**: Establishing VPN connections between on-premises networks and the VPC allows secure access to resources over encrypted tunnels.
* **AWS Direct Connect**: Direct Connect provides a dedicated network connection between on-premises data centers and AWS, offering consistent network performance and enhanced security for accessing resources within the VPC.
* **VPC Peering**: VPC peering allows resources in different VPCs to communicate with each other securely over the AWS network backbone.
* **Bastion Hosts or Jump Boxes:** Deploying bastion hosts or jump boxes with public IP addresses in public subnets enables secure access to resources in private subnets via SSH or RDP protocols.
* **PrivateLink:** PrivateLink enables secure and private communication between VPCs and AWS services or third-party services without exposing the resources to the public internet.