AWS VPC (Virtual Private Cloud)

Amazon Virtual Private Cloud (Amazon VPC) is a service provided by Amazon Web Services (AWS)

AWS VPC provides a way to create a private, isolated network environment within the AWS Cloud, giving you control over your virtual networking environment and allowing you to build scalable, highly available applications.

It forms the foundation for deploying and connecting various AWS resources in a secure and controlled manner.

WHY VPC?

- Isolation and Customization
- Networking Components
- Security
- Connectivity
- Elastic Load Balancing (ELB)
- Hybrid Cloud Connectivity
- Scalability and High Availability
- Integration with Other AWS Services

Isolation and Customization

Isolation: With VPC, you can create isolated sections of the AWS Cloud, known as VPCs, where you can launch resources in a virtual network.

Customization: You have complete control over your VPC, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Networking Components

Subnets: You can divide your VPC into multiple subnets, each associated with a specific availability zone. Subnets allow you to group resources and apply different network policies.

Route Tables: Each subnet in a VPC must be associated with a route table, which controls the traffic routing between subnets.

Internet Gateway: Provides a connection between your VPC and the internet, allowing resources in your VPC to communicate with the internet.

NAT Gateway/NAT Instance: Allows private subnets to initiate outbound traffic to the internet while preventing inbound traffic from reaching those resources directly.

Security

Security Groups: Act as a virtual firewall for your instances to control inbound and outbound traffic at the instance level.

Network Access Control Lists (NACLs): Operate at the subnet level and act as a firewall for controlling traffic in and out of one or more subnets.

Connectivity

VPC Peering: Allows you to connect one VPC with another via a direct network route.

VPN Connections: You can establish secure connections between your onpremises data centers and your VPC using Virtual Private Network (VPN) connections.

Elastic Load Balancing (ELB)

Application Load Balancer (ALB) and Network Load Balancer (NLB): Can be deployed within a VPC to distribute incoming traffic across multiple instances.

Hybrid Cloud Connectivity

AWS Direct Connect: Establishes dedicated network connections from your on-premises data centers to AWS.

AWS VPN: Allows you to connect your on-premises network to your VPC over the internet.

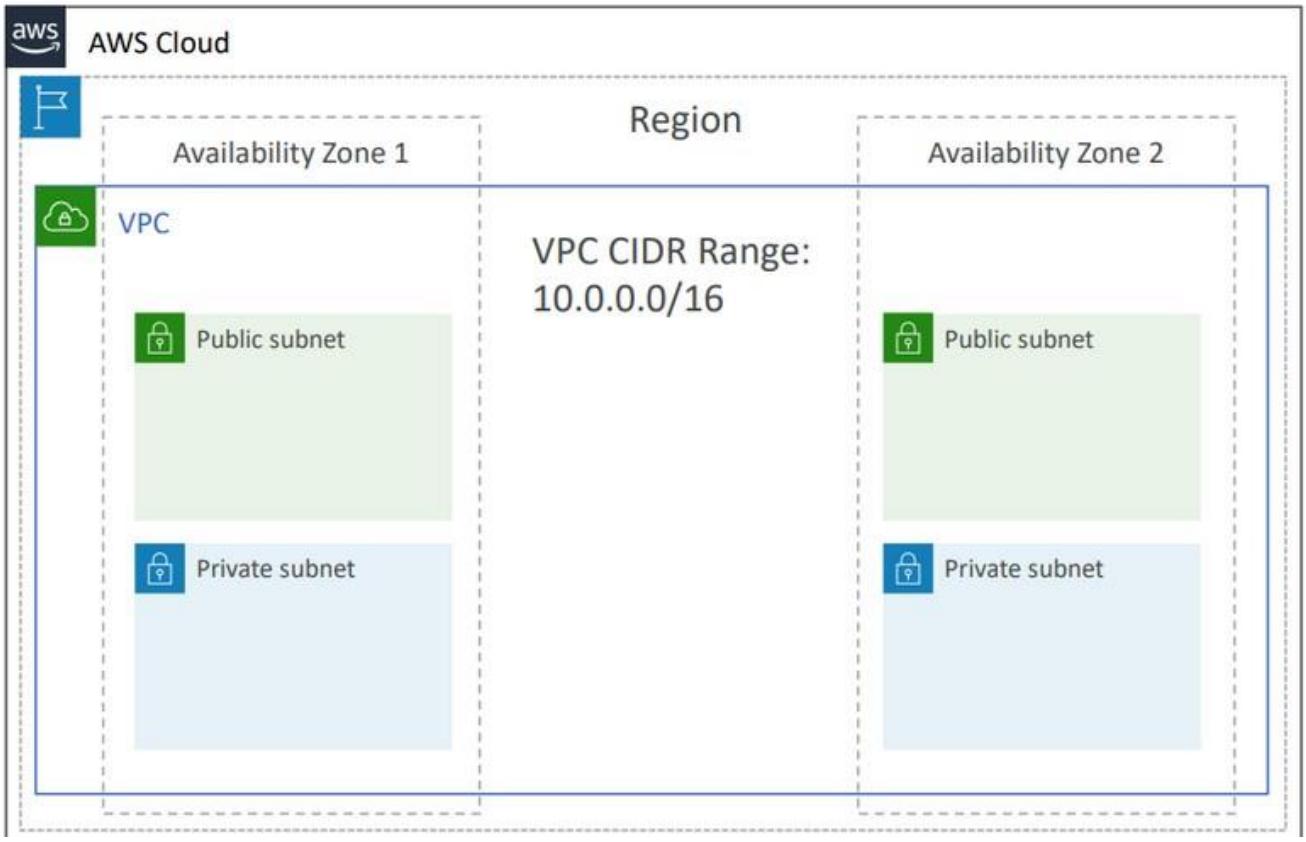
Scalability and High Availability

Auto Scaling: Allows you to automatically scale your Amazon EC2 instances based on conditions you define.

Multi-AZ Deployments: Resources can be deployed across multiple availability zones for improved fault tolerance.

Integration with Other AWS Services

VPC integrates with various AWS services, such as Amazon S3, Amazon RDS, AWS Lambda, etc., allowing you to build complex and scalable architectures.



Block Diagram of VPC

IP Address

An IP address, or Internet Protocol address, is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.

It serves two main purposes: host or network interface identification and location addressing.

IPv4 vs. IPv6

IPv4 (Internet Protocol version 4):
This is the most widely used IP version. It consists of four sets of numbers separated by dots, for example, 192.168.0.1.

IPv6 (Internet Protocol version 6):

This newer version was introduced to address the exhaustion of IPv4 addresses. IPv6 uses a longer address format, composed of eight groups of four hexadecimal digits, separated by colons, like 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Public vs. Private IP Addresses

Public IP Address:
This is the address assigned to a device by the Internet Service Provider (ISP) and is visible on the Internet.

Private IP Address:
These are used within a private network and are not directly accessible from the Internet. Common private IP address ranges include 192.168.x.x, 172.16.x.x to 172.31.x.x, and 10.x.x.x.

Static vs. Dynamic IP Addresses

Static IP Address:
A fixed IP address that doesn't change. It's manually configured and is often used for servers and network devices that need a consistent address.

Dynamic IP Address:
An IP address that is automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server. This is more common for devices in home networks.

DHCP (Dynamic Host Configuration Protocol)

DHCP is a network protocol used to automatically assign IP addresses and other network configuration information to devices on a network.

Subnetting

Subnetting is the practice of dividing a network into sub-networks to improve performance and security.

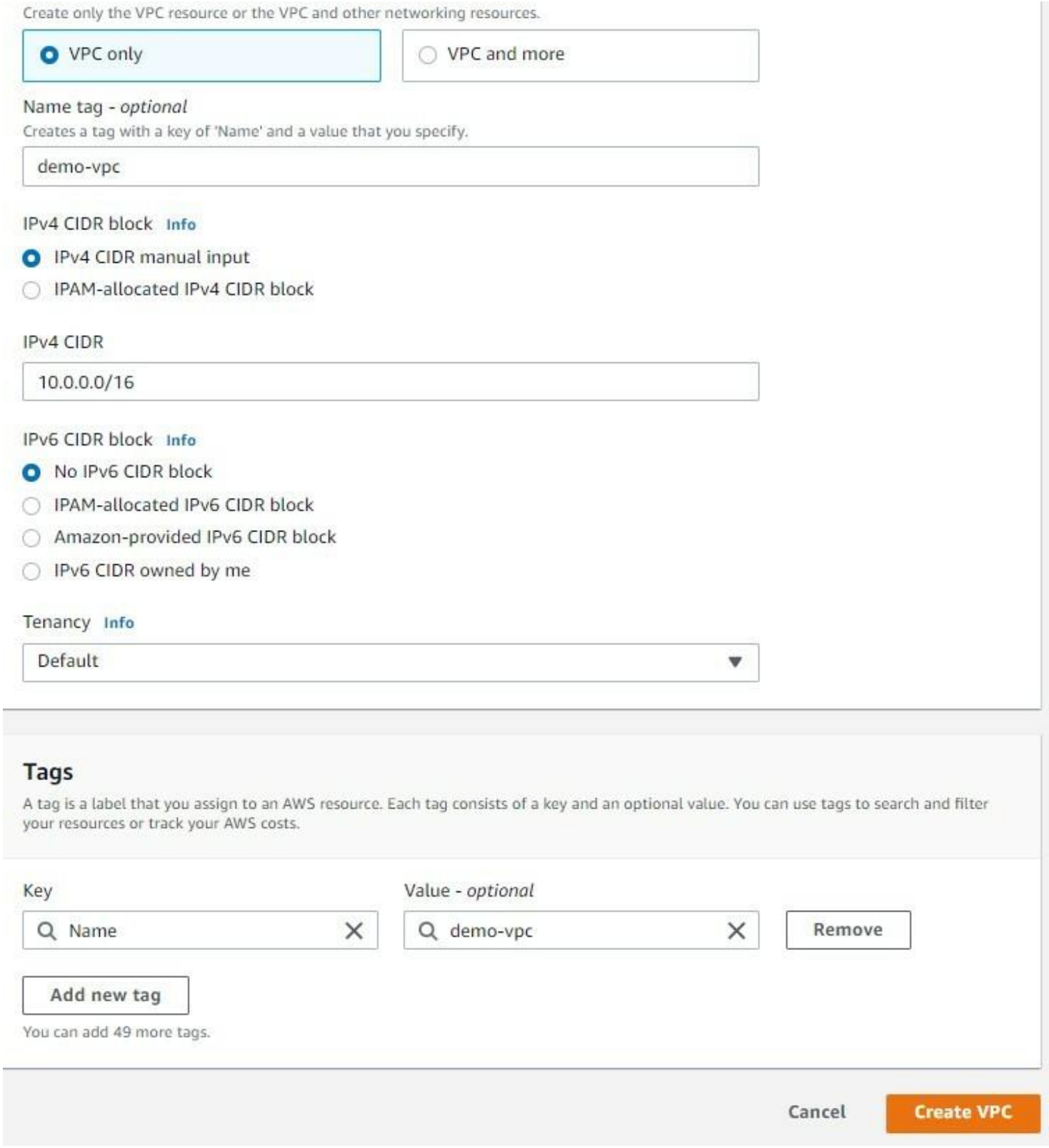
Overview

- VPC – Virtual Private Cloud
- Subnets – Tied to an AZ, network partition of the VPC
- Internet Gateway – at the VPC level, provide Internet Access
- NAT Gateway / Instances – give internet access to private subnets
- NACL – Stateless, subnet rules for inbound and outbound
- Security Groups – Stateful, operate at the EC2 instance level or ENI • VPC Peering – Connect two VPC with non overlapping IP ranges, nontransitive
- Elastic IP –fixed public IPv4, ongoing cost if not in-use
- VPC Endpoints – Provide private access to AWS Services within VPC
- PrivateLink – Privately connect to a service in a 3rd party VPC
- VPC Flow Logs – network traffic logs
- Site to Site VPN – VPN over public internet between on-premises DC and AWS
- Client VPN – OpenVPN connection from your computer into your VPC
- Direct Connect – direct private connection to AWS
- Transit Gateway – Connect thousands of VPC and on-premises networks together

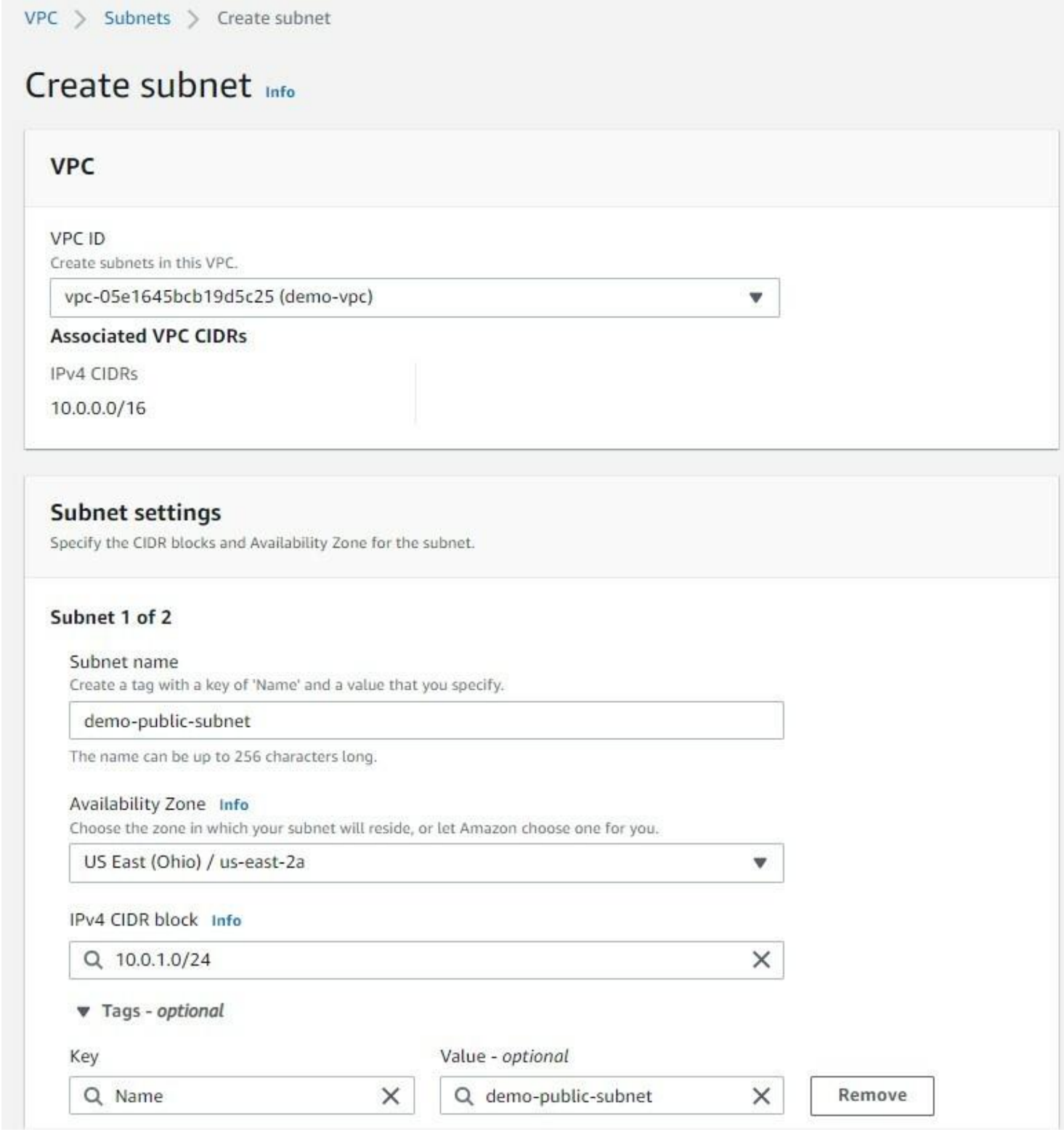
Process of Creating VPC in AWS

Step:1 In AWS Management Console search and go VPC services after that click creates vpc button.

Step:2 Give the name for VPC and add IPv4 CIDR.

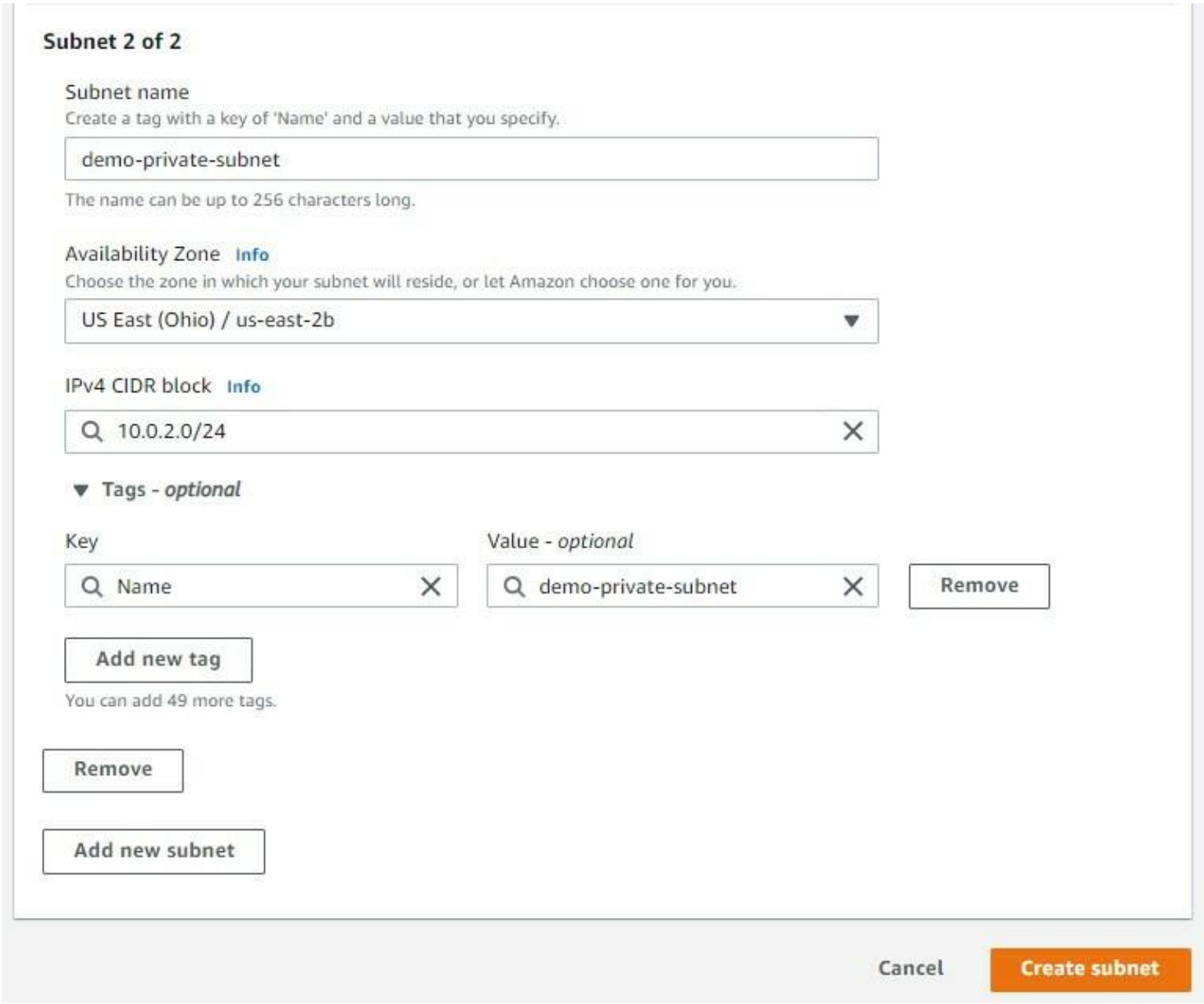


Step:3 Create Two Subnets. Firstly create a public subnet. You can use the 10.0.1.0/24 CIDR range for the public subnet. Select the availability zone and give the name for the subnet.



Step:4 Now the same interface, click add new subnet button for private subnet creation.

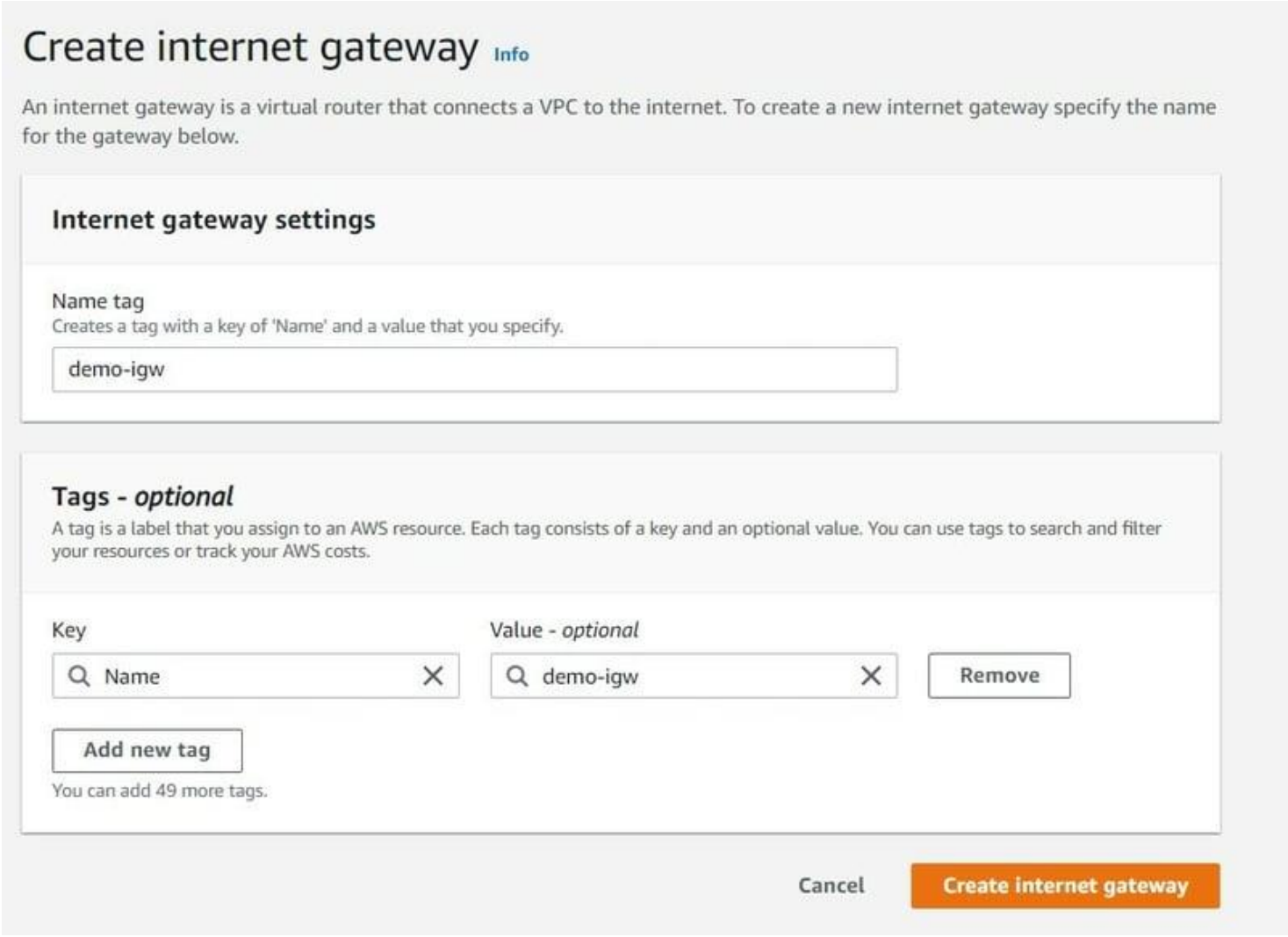
Add IPv4 CIDR as 10.0.2.0/24. After that give the subnet name and select the availability zone. finally, click create subnet button.



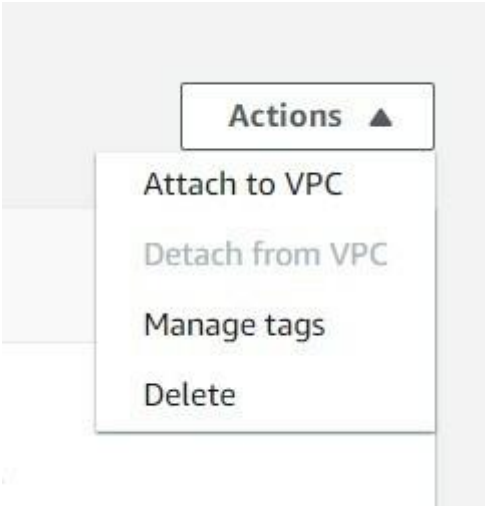
Step: 5 Now create an internet gateway for public subnet internet access. In VPC Console select Internet Gateway and create internet gateway. Give the name of Internet Gateway and hit create button.

You should connect internet gateway only to the public subnet

One internet gateway will get connected only to one subnet.

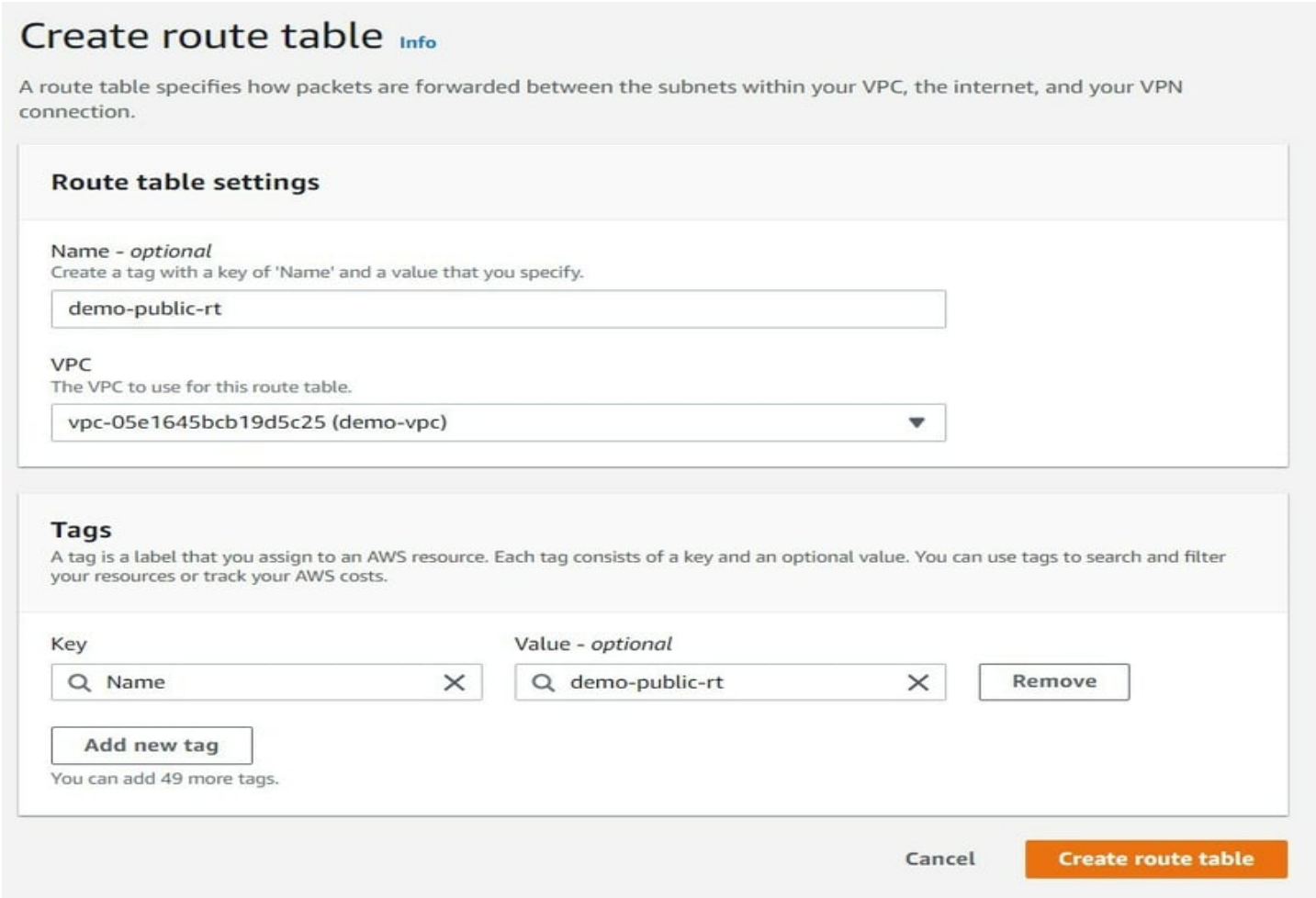


Step:6 Next, we want to attach this internet gateway for VPC. You can select the internet gateway and click Attach to VPC.

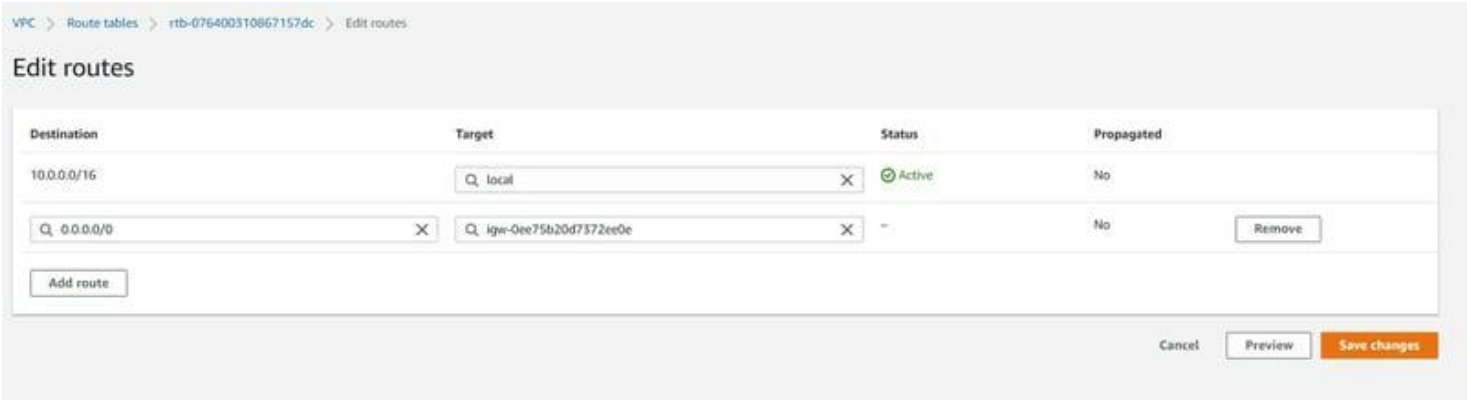


Next, select the previously created VPC and click attach internet gateway button.

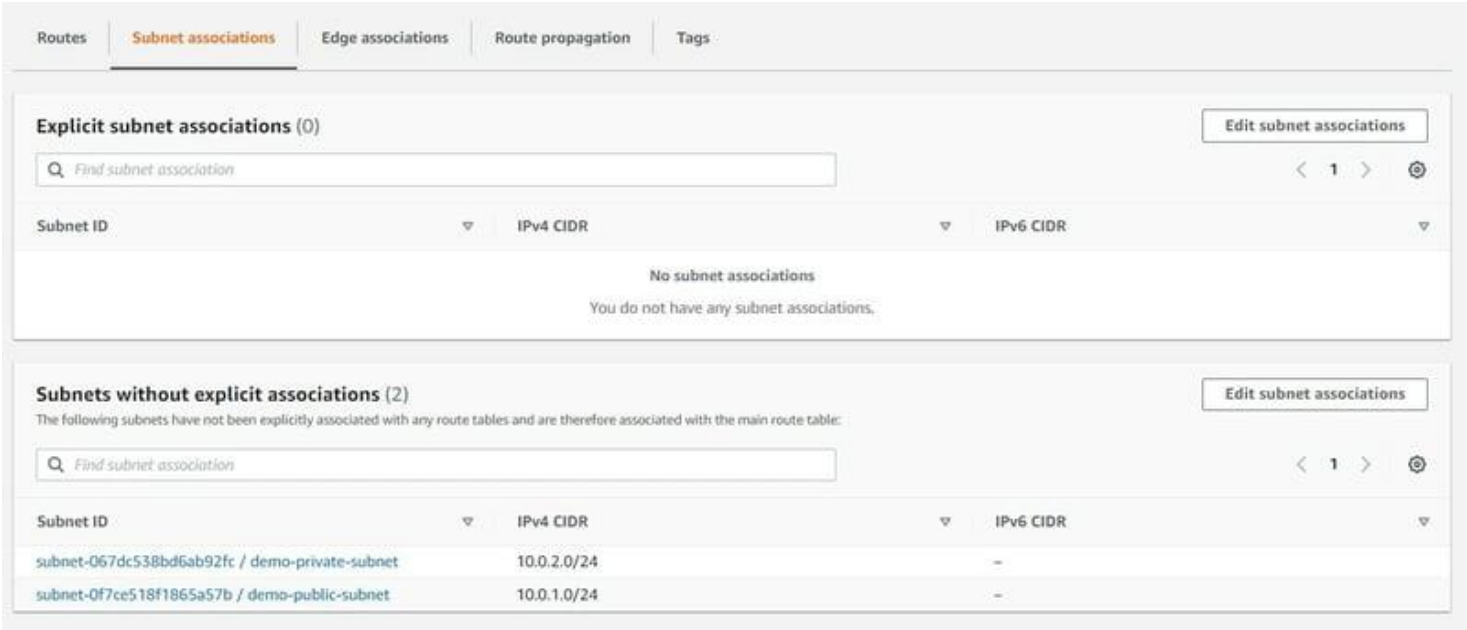
Step:7 Next, Go to the route table and create a route table for the public subnet. give the name for the route table and select the previously created VPC. The next click creates the route table button.



Step:7 Click the public subnet route table click the Route tab and add route 0.0.0.0/0 and select the previously created Internet Gateway. next hit the save changes button.



Step: 8 In the public subnet route table click the subnet association section and click “edit subnet associations" section.



Next, select a subnet and click the save association button.

Step: 9 Now click on Routes and click on add route

Select internet gateway that you created and